SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Henri Korpinen

Turvatoimintojen määrittely ja todentaminen mallipohjaisen systeemisuunnittelun avulla

Opinnäytetyö
Kevät 2021
SeAMK tekniikka
Insinööri (ylempi AMK), Automaatiotekniikka

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan koulutusyksikkö

Tutkinto-ohjelma: Insinööri (ylempi AMK), Automaatiotekniikka

Tekijä: Henri Korpinen

Työn nimi: Turvatoimintojen määrittely ja todentaminen mallipohjaisen systeemisuunnittelun avulla

Ohjaaja: Niko Ristimäki

Vuosi:2021 Sivumäärä:69 Liitteiden lukumäärä:3

Opinnäytetyön toimeksiantajana oli Prima Power Oy, joka yrityksenä on maailmanmarkkinoilla yksi isoimpia levytyökoneita ja -järjestelmiä tuottava yritys. Yritys valmistaa työkoneita neljässä eri maassa ja palvelee asiakkaita kansainvälisesti yli 70 maassa.

Työn tavoitteena oli löytää mallintamisen avulla yksinkertaisempi ja tehokkaampi esitystapa riskianalyysiin perustuville turvatoiminnoille. Tämän esitystavan tulisi vastata erityisesti suunnittelijoiden ja koneen testaajien tarpeisiin järjestelmän elinkaaren eri vaiheissa. Tutkimuksessa selvitettiin mallipohjaisen systeemisuunnittelun soveltuvuutta koneturvallisuuden kehittämiseksi. Toimintakuvauksen mallissa olisi esitettävä turvapiirien vaikutus eri laitteiden rajapintojen välillä.

Tutkimuksen tarkoitus oli olla kartoittava ja tutkimusstrategiana oli kvalitatiivinen tapaustutkimus. Tutkimusmenetelminä käytettiin nykyisen suunnittelumallin analysointia, tutkimuskyselyä ja haastatteluja. Tutkimuskysely järjestettiin Finn-Power Oy:n sähkösuunnitteluosastolle. Haastateltavana oli sähkösuunnitteluosaston pääsuunnittelijoita ja ohjaussuunnitteluosaston pääsuunnittelijoita. Tutkimusmenetelmien arvioinnin pohjalta valittiin mallinnustyökalu.

Tutkimuksessa selvisi, että turvatoimintojen suunnitteluprosessin aikana ilmenee tiedon hukkaa ja myös suunnittelun jälkeiset muutokset uudelle turvatoiminnolle ovat yleisiä. Ratkaisuksi pyrittiin mallintamaan kaaviomallinnustyökalun avulla turvatoimintojen vaatimuskaavio ja aktiviteettikaavio. Tämän jälkeen eri toiminnot sijoitetaan koneen tuotantolinjan layoutin pohjalle. Layoutin toiminnot ovat interaktiivisia malleja, joiden avulla voisi simuloida eri laitteiden vaikutukset keskenään. Kyselyn perusteella kaaviomallinnustyökalu olisi luontevinta olla integroituna Jira-tehtävienhallintaohjelmistoon.

Tutkimuksen tuloksena mallinnettiin SysML-profiilin elementeillä CombiGeniuksen turvatoimintoja. Laajan varastojärjestelmän layoutin pohjalle toteutettiin interaktiivinen esitystapa eri konevyöhykkeiden vaikutuksesta toisiinsa. Tutkimuksen myötä mallipohjainen systeemisuunnittelu tuli tutummaksi työn tekijälle ja myös käsitteenä suunnitteluosastojen pääsuunnittelijoille.

Asiasanat: turvatoiminto, turvavyöhyke, määrittely, todentaminen, mallipohjainen systeemisuunnittelu, SysML

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Master’s Degree in Automation Technology

Author:Henri Korpinen

Title of thesis: Definition and verification of safety functions by using model-based system engineering

Supervisor: Niko Ristimäki

Year:2021 Number of pages:69 Number of appendices:3

The thesis was commissioned by Prima Power Oy, which is one of the largest companies producing sheet metal working machines and systems on the world market.

The aim of the work was to find a simpler and more efficient way of presenting safety functions based on risk analysis through modeling. This modeling should specifically meet the requirements of designers and machine testers at different stages of the system life cycle.

The purpose of the study was to be a survey and the research strategy was a qualitative case study. The research methods used were an analysis of the current design model, a research questionnaire and interviews. The modeling tool was chosen based on the evaluation of the research methods.

The solution was to use a modeling tool to model a diagram for the requirements and an activity diagram of safety functions. The various functions would then be assigned at the machine's production line layout drawing.

As a result of the study, the safety functions of CombiGenius were modeled with elements of the SysML profile. Also, an interactive presentation of the effect of different safety zones on each other was implemented.

Keywords: safety function, definition, verification, model-based system engineering, SysML

SISÄLTÖ

Kuva-, kuvio- ja taulukkoluettelo

Käytetyt termit ja lyhenteet

Suoritustaso	Turvaluokituksen taso (Performance level, PL), jonka avulla määritellään ohjausjärjestelmän osien kykyä suorittaa turvallisuuden takaava toiminto.
Turvatoiminto	Koneen toiminto, jonka vikaantuminen tai puuttuminen aiheuttaa välittömän tapaturmaan johtavan riskin kasvamisen.
Turvakomponentti	Itsenäinen komponentti, joka toimii turvatoiminnon toteuttamiseksi, jonka vikaantuminen vaarantaa turvallisuuden ja joka ei ole välttämätön koneen toimimisen kannalta.
Turvavyöhyke	Turvakomponentin turvatoiminnon pysäyttämä ohjauksen alue, joka pysäytyksen jälkeen vaaraton.
Pysäytysluokka	Pysäytystoiminnot jaetaan kolmeen luokkaan: 0,1 ja 2. Luokka 0 on välitön tehon poisto, luokka 1 valvottu pysähtyminen ja sen jälkeen tehon poisto ja luokka 2 valvottu pysähtyminen, jossa teho säilyy.
Passiivinen suojaus	Suojaus, joka suojaa vaaravyöhykettä jatkuvasti.
Aktiivinen suojaus	Suojaus, joka tulee toimintaan jonkin vian tai diagnostiikan havainnon seurauksena.
PSBB-linjasto	Lyhenne sanoista punch,shearing, buffering ja bending. Koostuu yleensä Prima Powerin koneista SG/SB, PSR ja EBe.
SG/SB	Shear Genius/Shear Brilliance, kulmaleikkurikone.
PSR	Picking&Stacking Robot, poiminta/pinonta robotti.
EBe	Bending machine, sähköservolla toimiva taivutusautomaatti.
Night-Train FMS	Ohutlevykomponenttien tuotantojärjestelmä.
IOW/MOW-asema	Input/Output wagon ja Manual output wagon. Liittyvät Night-Train järjestelmään materiaalien lastaamiseen ja valmiiden kappaleiden purkamiseen varastosta.

CG	CombiGenius, kombikone, joka työstää ohutlevyä servoiskulla ja laserilla.
LU	Loading unloading robot, ohutlevyn lastaus robotti 2D-laser-koneelle, joka myös purkaa jäljelle jääneen levyn rangan.
LST	Loading stacking robot, ohutlevyn lastaus ja pinontarobotti.
Lean-menetelmä	Toimintastrategia, joka pyrkii arvon maksimointiin parantamalla jatkuvasti prosessien tehokkuutta.
MBSE	Model based system engineering, mallipohjaisen systeemisuunnittelun menetelmät.
INCOSE	International Councel on Systems Engineering, kansainvälinen järjestelmätekniikan neuvosto.
OMG	Object Management Group, tietokoneteollisuuden standardikonsortio.
UML	Unified Modeling Language, OMG:n vuonna 1997 standardoima graafinen mallinnuskieli.
SysML	Systems Modeling Language, määritelty UML:n laajennuksena. Kieleen on lisätty järjestelmäsuunnittelun tarvitsemat osat ja siitä on poistettu ohjelmistospesifiset osat.
AutomationML	Automation Markup Language, XML-pohjainen formaatti automaatioon liittyvän datan siirtoon ja tallennukseen.
HTML5	Uusin versio HTML-merkintäkielestä (Hypertext markup Language).
URL-osoite	Verkkosivuston tai tiedoston sijainti internetissä.
OPC UA-rajapinta	Open Platform Communications Unified Architecture, avoimen standardin tiedonsiirtoprotokolla.

1 Johdanto

1.1 Työn tausta

Prima-Power Oy:n sähkösuunnitteluosasto suunnittelee eri laitteiden suojaukset yhdessä mekaniikkasuunnittelun kanssa ja pysäytystoiminnot yhdessä ohjaussuunnittelun kanssa eri konemalleille riskianalyysin perusteella. Riskianalyysi laaditaan standardin 13849-01 perusteella ja turvapiireistä tehdään komponenttimallit, joista saadaan laskettua suoritustaso.

Sähkösuunnitteluosasto koostuu kuudesta sähkösuunnittelijasta, kahdesta pääsuunnittelijasta ja sähkösuunnittelun esimiehestä. Sähkösuunnittelijat ja pääsuunnittelijat on jaettu kahteen ryhmään, joista toisen ryhmän päävastuualueeseen kuuluvat perustyöstökoneet sekä linjastokoneet, ja toisen ryhmän päävastuualueena ovat materiaalinhallintalaitteet ja varastojärjestelmät. Ajoittain on käytössä alihankintasuunnittelun kautta kaksi sähkösuunnittelijaa, jotka ovat vastuussa etenkin retrofit-suunnittelusta. Seinäjoen toimipisteen sähkösuunnitteluosaston lisäksi italialaisen emoyhtiön Prima industrien sähkösuunnittelijat vastaavat 2D-laser-koneista ja taivutusautomaateista. Asiakastoimitukset ovat nykyisin siirtymässä yhä enemmän järjestelmätoimituksiin, eikä yksittäisiä ”stand alone”-koneita myydä enää yhtä isoja määriä kuin ennen. Tämä tarkoittaa, että myydyt järjestelmäkokonaisuudet pitävät sisällään useamman suunnittelutiimien koneita, ja suunnittelu vaatii yhtä enemmän yhteistyötä tiimien välillä. Tästä johtuen turvapiirien toiminnasta ja turvapiiriin liittyvien eri laitteiden rajapinnoista olisi hyvä olla jonkinlainen kartta tai malli, josta selviää nopeasti pysäytystoimintojen vaikutus eri laitteisiin. Lisäksi yksinkertaistettu selkeä esitystapa palvelisi myös ohjaussuunnittelua, käyttöönottotestaajia, huoltoa ja loppuasiakasta järjestelmän elinkaaren eri vaiheissa.

1.2 Työn tavoite

Työn tavoitteena on löytää mallintamisen avulla yksinkertaisempi ja tehokkaampi esitystapa riskianalyysiin perustuville turvatoiminnoille. Tämän esitystavan tulisi vastata erityisesti suunnittelijoiden ja koneen testaajien tarpeisiin. Mallista täytyisi nähdä helposti, kuinka turvavyöhykkeet toimivat ja millaisista turvaluokitelluista komponenteista järjestelmä koostuu. Toimintakuvauksessa esitettävä turvapiirien vaikutus eri koneiden välillä, myös kolmannen osapuolen laitteen turvapiirien välillä, täytyisi myös mallintaa. Samalla kun turvapysäytystoimintojen kuvauksia selkeytetään myös itse turvatoiminnoissa voitaisiin pyrkiä

yksinkertaisempaan toteutukseen. Tämä helpottaisi tulevaisuudessa laajempien turvaohjainten käyttöön siirtymistä. Työn tavoitteena olisi vastata nyt ja mahdollisesti laajemmin tulevaisuudessa lopputyön myötä seuraaviin kysymyksiin:

- Mikä olisi paras tapa mallintaa turvatoimintoja?
- Millä tavalla nyt on mallinnettu turvatoiminnallisuutta? Voisiko nykyistä mallia kehittää palvelemaan useampaa sidosryhmää?
- Kuinka mallinnusta ylläpidetään järjestelmän elinkaaren ajan?
- Voisiko mallia hyödyntää uuden työntekijän/harjoittelijan perehdyttämisessä?

1.3 Työn rakenne

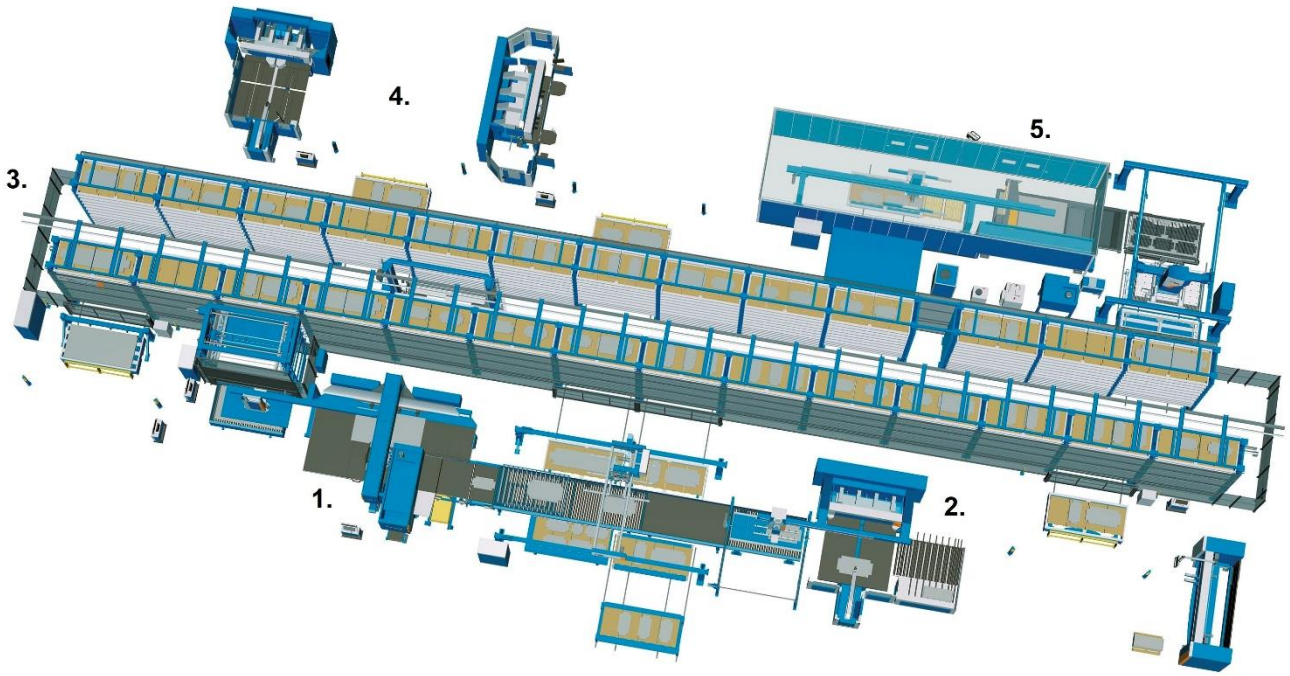
Opinnäytetyön ensimmäisessä luvussa eli johdannossa käydään läpi työn taustaa, tavoitetta, rakennetta sekä kohdeyrityksen esittely pääpiirteissään. Toinen luku koostuu olennaisten turvateknisten ratkaisujen esittelystä ja turvastandardien läpikäymistä liittyen järjestelmän suojauksen suunnitteluun. Kolmannessa luvussa käsitellään teoreettista taustaa liittyen mallipohjaiseen systeemisuunnitteluun. Neljännessä luvussa tulee esiin tutkimismenetelmä sekä vertaillaan eri mallinnussovelluksia. Viidennessä luvussa on turvatoiminnon mallintamista esimerkin keinoin ja kuudennessa osassa ovat johtopäätökset ja pohdinta tutkimustyöhön liittyen.

1.4 Yritysesittely

Milanon pörssissä noteerattu Prima Industrie Group jaetaan Prima Poweriin ja Prima Electroon. Prima Power on työstökonedivisioona, kun taas Prima Electro valmistaa teollisuuselektroniikkaa ja laserlähteitä. Finn-Power on osa Prima Poweria ja sijaitsee Seinäjoella. (Prima Power, [viitattu 23.3.2021].)

Prima Power valmistaa useita erilaisia levytyökoneita ja -järjestelmiä, joita myydään ympäri maailman laajasti yli 70 maassa. Prima Power on vuosien saatossa tuottanut maailmalle yli 10000 levytyökonetta ja -järjestelmää. Seinäjoella levytyökeskusten valmistuksesta ja suunnittelusta toteutetaan lävistävät ja leikkaavat työstökoneet sekä niihin liittyvät

materiaalinhallintalaitteet. Prima Powerin tuotannosta vastaavat yksiköt ovat Suomessa, Yhdysvalloissa, Kiinassa ja Italiassa, jossa sijaitsee myös yrityksen pääkonttori. (Prima Power, [viitattu 23.3.2021])



Kuva 1. Prima-Powerin NT-FMS -järjestelmä (Prima Power mediabank, [viitattu 23.3.2021])

Kuvassa 1 on esimerkkinä esitettynä NightTrain-varastojärjestelmä, johon on liittynyt neljä erilaista tuotantosolua Prima-Powerin eri yksiköistä. Kokonaisuus koostuu seuraavista osista:

1. PSBB-linjasto, johon materiaali tulee NightTrain-varastolta FLD-lastausliitynnän kautta. Materiaali työstetään SG-kulmaleikkurityöstökoneella, josta valmiit kappaleet pinotaan PSR-robotilla kasettivaunulle, joka vie kappaleet takaisin varastoon. PSR-robotti voi myös nostella osan kappaleista eteenpäin Ebe-taivutusautomaatille. Kaikki edellä mainitut laitteet, paitsi Ebe, valmistetaan Suomessa ja testataan Seinäjoella.

2. Ebe-taivutusautomaatti. Taivuteltavat kappaleet voivat tulla SG-koneelta tai manuaalisesti ohisyöttölastauksella. Valmiit kappaleet puretaan purkupöydälle. Ebe-taivutusautomaatti valmistetaan ja testataan Italiassa, Cologna Venetassa.

3. Night-Train FMS -varasto. Kasettihyllyjen välissä kiskolla kulkee nosturi, joka kuljettaa joko materiaalikasetteja tai valmiiden kappaleiden kasetteja. Varastoon voidaan lastata materiaalia ja purkaa levyjä materiaalivaunuilla IOW- ja MOW-asemien kautta. Näiden laitteiden valmistus tapahtuu Suomessa.

4. Bce-taivutusautomaatteja, joihin materiaali tuodaan manuaalisesti taivutettavaksi. Materiaalia voidaan saada varastolta materiaalivaunulla IOW-aseman kautta. Valmistus on Italiassa, Cologna Venetassa.

5. 2-D-laser-kone platino/LaserGenius, johon lastataan materiaali LU-lastaus/ranganpurkurobotilla työstettäväksi. Valmiit kappaleet pinotaan LST-pinonta/lastausrobotti kasettivaunulle. 2D-laser-työstökone valmistetaan Torinon Collegnossa, Italiassa. Kuitusuoja, LST ja LU valmistetaan Suomessa. Laitteet yhdistetään yleensä vasta loppuasiakkaalla, missä laitteet testataan.

2 Järjestelmän suojauksen suunnittelu

2.1 Koneiden turvallisuutta koskevat säädökset

Koneen turvallisuuden lähtökohtana on vaarojen tunnistaminen ja niistä aiheutuvien riskien arviointi ja pienentäminen jo koneen suunnitteluvaiheessa. Suunnittelun alkuvaiheessa tehdään alustava riskien arviointi, jota päivitetään suunnittelun edetessä. Väärinkäyttöä tapahtuu koneiden yhteydessä toisaalta unohtamisen ja erehtymisen seurauksena ja toisaalta tarkoituksellisesti, kun turvatoimintoja poistetaan koneesta tai toimitaan muutoin ohjeiden vastaisesti. (Siirilä &Tytykoski 2016, 42.) Turvajärjestelmät rakentuvat turvakomponenteista. Turvakomponentti ei ole välttämätön koneen toiminnan kannalta. Turvakomponentin puuttuminen tai vikaantuminen kuitenkin huonontaa koneen turvallisuutta. Jotta komponenttia pidettäisiin turvakomponenttina, se on oltava erikseen hankitavissa, eikä koneen rakentajan omaan koneeseen rakentama. (Siirilä & Tytykoski 2016, 38.) Konetta suunniteltaessa ei riitä sen varmistaminen, että kone on turvallinen sitä normaalisti käytettäessä. Turvallisuutta on tarkasteltava koneen elinkaaren kaikissa vaiheissa valmistamisesta päättyen koneen hävittämiseen. Suunnittelija on vähintään osavastuussa lähes kaikkien koneen elinkaaren vaiheiden turvallisuudesta. Usein suunnittelussa keskitytään normaalin tuotantokäytön suunnittelemiseen, vaikka koneen elinkaaren kaikkiin vaiheisiin liittyvän riskien hallinnan olisi oltava olennainen osa suunnitteluprosessia. Suunnittelijan on huolehdittava siitä, että suunnitelman mukainen tuote täyttää työturvallisuuslakien ja konelakien vaatimukset, jotka Suomessa ovat voimassa valtioneuvoston asetuksena koneiden turvallisuudesta. (Siirilä & Tytykoski 2016, 108.)

Säädösten mukaan jokaisella koneella on oltava yksi valmistaja, joka vastaa koneen täyttävän sitä koskevien säädösten vaatimukset. Suuren järjestelmän suunnitteluun osallistuu useita henkilöitä ja mahdollisesti useita yrityksiäkin. Konekokonaisuutta pidetään kuitenkin yhtenä koneena, joten sillä on oltava yksi koko järjestelmästä vastaava valmistaja. Kokonaisvastuun ottavasta yrityksestä on sovittava jo suunnitteluvaiheessa. Vastuullisella yrityksellä on oltava sellainen osaaminen ja tieto koneesta, että se voi oikeasti arvioida kokonaisuuden vaatimustenmukaisuutta ja turvallisuutta. Riskien arviointi ja hallinta ovat olennainen osa koneen suunnittelua ja valmistusta. Koneen tekniset ratkaisut ovat periaatteessa vapaasti valittavissa, kunhan lopputuloksena koneen riskit ovat riittävän pienet. (Siirilä & Tytykoski 2016, 108-110.)

Suunnittelijan roolia ja vastuuta on pyritty selkeyttämään VTT:n USVA-hankkeessa. Hankkeessa käsiteltiin prosessilaitoksen turvallisuuden varmistamista, mutta samat periaatteet sopivat myös suuren automaattisen konejärjestelmän suunnitteluun. Koko suunnitteluorganisaation vastuunjaon on oltava selkeä. Erityisesti laajan kokonaisuuden suunnitteluprojektin aikana prosessin pitää edetä siten, että eri suunnitteluryhmien välisellä tiedonvaihdolla ja vuorovaikutteisella suunnittelulla päädytään turvallisuuden kannalta mahdollisimman hyvään lopputulokseen. Automaatiojärjestelmien kehittämisohjelmat ovat laajoja kokonaisuuksia, joihin osallistuu ihmisiä, joiden peruskoulutus, kokemustausta, asenteet, valmiudet, toimintaperiaatteet ja jopa kieli eroavat toisistaan. Tällöin ihmisten välinen kommunikaatio asettaa erityisiä haasteita kaiken muun lisäksi turvajärjestelmän suunnitteluun. (Malmén, Nissilä, Wallin & Virolainen 2012, 73.)

Tietoa suunnittelutyöstä välitetään erilaisten piirustusten, kaavioiden, materiaali- ja laiteluettelojen ja määrittelyjen avulla. Mitä selkeämpiä ja yksikäsitteisempiä nämä dokumentit ovat, sitä todennäköisemmin suunnittelutieto välittyy tarkoitetussa muodossa. Kaikkea tietoa ei kuitenkaan voida siirtää pelkkinä kaavioina. Tarvitaan myös sanallisia kuvauksia kohteen toiminnasta. Kirjoitettuun tekstiin ja sanallisiin selityksiin liittyy aina väärinymmärtämisen ja tulkinnan mahdollisuuksia, erityisesti kun pyritään tiiviiseen ja niukkasanaiseen esitystapaan. (Malmén, Nissilä, Wallin & Virolainen 2012, 73-74.)

2.2 Tekninen turvallisuus

Konetta käyttöönotettaessa ei käytännössä kovin perusteellista tarkastusta ole mahdollista tehdä. Usein jo pinnallinenkin tarkastelu voi paljastaa merkittäviä turvallisuuspuutteita. Olennaisia asioita selvitettäväksi ovat ainakin seuraavat:

- Onko mahdollista päästä koneen vaaravyöhykkeelle minkään turvalaitteen havaitsematta?
- Onko mahdollista yltää kädellä koneen vaarakohtiin koneen käydessä?
- Onko koneessa tarpeelliset suojukset, turvalaitteet ja käyttötavat?
- Onko turvatoimintojen standardin 13849-01 mukainen suoritustaso riittävä?

- Onko suuressa konejärjestelmässä turvallinen pääsy kaikkiin käyttö-, säätö-, huolto- ja tarkastuskohteisiin?

- Onko koneen melutaso riittävän alhainen ja säteilyn aiheuttamien terveyshaittojen syntymisen estämisestä huolehdittu? (Siirilä &Tytykoski 2016, 137.)

Uuden koneen suunnitteleminen tai laajan automaattisen konejärjestelmän arvioiminen ovat niin vaativia tehtäviä, että kunnollisen tuloksen aikaansaamiseksi riskiarviointi on tehtävä ryhmässä. Automaattisissa konejärjestelmissä on muista koneista poikkeavia turvallisuuteen vaikuttavia ominaisuuksia, esimerkiksi:

- Järjestelmän tilaa ja toimintoja voi olla vaikea hahmottaa, esim. pysähtyneenä oleva robotti voi liikkua seuraavaksi mihin suuntaan tahansa.

- Järjestelmän tila ei selviä konejärjestelmää katsomalla. Pysähtyneenä oleva järjestelmä voi olla useassa eri tilassa, kuten:

    - energiansyötöstä erotettuna

    - pysäytettynä, mutta energian syöttöön kytkettynä

    - käsikäytöllä ohjauskäskyä odottamassa

    - ohjelman tunnistaman häiriön pysäyttämänä tai odottamassa seuraavan työvaiheen päättymistä, jotta kappale voi siirtyä seuraavaan koneyksikköön

    - ohjelmassa olevan virheen pysäyttämänä

- Järjestelmät ovat monimutkaisia ja niissä voi olla ohjelmavirheistä, anturivioista, sähkömagneettisista ilmiöistä tai muista syistä olevia häiriöitä, joiden syitä voi olla hankala löytää

- Automaattisissa järjestelmissä ei ihmistä tarvita tuotannon aikana. Käyttäjiä kuitenkin tarvitaan vastaan tulevissa tilanteissa, kuten kunnossapito, vian haku, häiriön

selvittäminen, materiaalin lisäys ja puhdistus. Näissä tilanteissa ollaan vaaravyöhykkeellä tai lähellä vaarakohtia. (Siirilä&Tytykoski 2016, 311.)

Konejärjestelmän toiminta-alue erotetaan kokonaan ympäristöstä. Odottamaton käynnistyminen estetään mahdollisimman luotettavasti vaaravyöhykkeellä oltaessa. Vaaravyöhykkeelle saa päästä vain vaikuttamalla turvalaitteeseen. Silloin ohjausjärjestelmä siirtää konejärjestelmän turvalliseen tilaan turvalaitteelta tulevan tiedon perusteella. Kuittauksilla ja näkyvyydellä vaaravyöhykkeille pyritään varmistamaan suojausta sulkiessa ja konetta käynnistäessä, että kukaan ei ole vaaravyöhykkeellä. Ohjausjärjestelmän turvatoimintojen suoritustason on oltava riittävä, että turvallisuus on varmistettu vikatilanteessakin. (Siirilä&Tytykoski 2016, 311.)

Energiasyötön keskeytyminen samanaikaisesti turvalaitteille ja toimilaitteille on aiheutettava koneen pysähtyminen ja siten turvallinen tila. Ohjausjärjestelmä on suunniteltava siten, että pysähtyminen on mahdollisimman hallittu ja turvallinen tällaisissakin tilanteissa. Energian syötön palaaminen katkoksen jälkeen ei saa aiheuttaa koneen käynnistymistä. Jos kone on pysähtynyt energian syötön katkeamisen takia, sen seurauksena ainakin monimutkaiset järjestelmät voivat joutua epämääräiseen tilaan. Siitä toipuminen turvallisesti vaatii useita kuittauksia ja ajoja käsiohjauksella. Ohjausjärjestelmä ei saa sähköjen palaamisen jälkeen itse kuittaantua ja eikä tehdä muutakaan toimintoa, mikä myöhemmin voisi johtaa vaaratilanteeseen. Kun jännite tai paine alittaa tai ylittää etukäteen asetetun sallitun vaihtelurajan, turvalaitteiden on annettava pysäytyskäsky ja seurauksena on oltava hallittu pysähtyminen. (Siirilä &Tytykoski 2016, 316.)

2.3 Konejärjestelmien vyöhykkeet

Vaikka suurtakin saman ohjauksen alla toimivaa konejärjestelmää pidetään koneasetuksessa yhtenä koneena, järjestelmän turvatoimintoja jaetaan kuitenkin usein pienempiin osiin, joita nimitetään vyöhykkeiksi. Vyöhykkeisiin jakaminen voi koskea energiansyötöistä erottamista, turvalaitteiden aikaan saamia pysäytyksiä tai hätäpysäytystä. (Siirilä &Tytykoski 2016, 583.) Prima-Powerin järjestelmissä kuitenkin hätäseispysäytystä ei koskaan jaeta vyöhykkeisiin, vaan hätäseipainike pysäyttää aina koko järjestelmän.

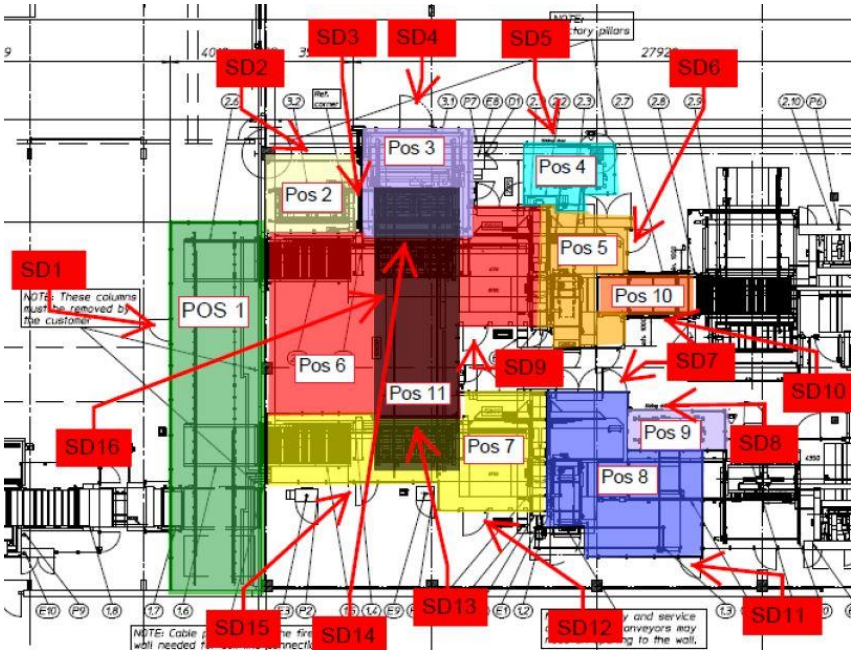
Vyöhykkeisiin jakamista koskevat perusvaatimukset ovat seuraavat:

- Eri vyöhykkeet on osoitettava selvästi ja on oltava ilmiselvää, mitkä koneen osat kuuluvat mihinkin vyöhykkeeseen

- Vastaavasti on oltava ilmiselvää, mitkä ohjauslaitteet tai turvalaitteet kuuluvat mihinkin vyöhykkeeseen

- Vyöhykkeiden rajapinnat on suunniteltava siten, ettei mikään toisella vyöhykkeellä tapahtuva toiminto aiheuta vaaroja toiselle vyöhykkeelle, joka on pysäytettynä ihmisen ollessa vyöhykkeellä. (Siirilä & Tytykoski 2016, 584.)

Suurissa konejärjestelmissä on yleensä selvää, että turvalaite saa aikaan kohdalla olevan konejärjestelmän osan pysähtymisen ja pysähtyneenä pysymisen. Useimmiten ei ole ollenkaan selvää, miten laajalle alueelle pysäytyskäsky ulottuu ja missä tilassa mahdollisesti muut konejärjestelmän osat ovat. Vaatimusten mukaan pitäisi olla kuitenkin ilmiselvää turvalaitteen pysäyttämän vyöhykkeen laajuus. Pysäytystoiminnon laajuus on selkeintä, kun pääsee vain alueelle, jossa turvalaite on saanut aikaan luotettavan pysäytystilan. Jos vierekkäisiin vyöhykkeisiin kulkeminen on mahdollista suojauksen sisällä, liikkumista valvotaan vyöhykkeiden rajoilla olevilla turvalaitteilla. (Siirilä &Tytykoski 2016, 587.)



Kuva 2. Turvavyöhykkeisiin jakaminen (Prima Power 2019)

2.3.1 Konejärjestelmien pysäyttäminen

Perussääntönä on koko konejärjestelmän pysäyttäminen, jos niiden toiminnan jatkuminen voi aiheuttaa vaaraa, kun yksi osa pysäytetään. Poikkeuksellisesti kuitenkin sellaiset koneyhdistelmän osat saavat jäädä käyntiin, jos niiden toiminnan jatkuminen ei aiheuta vaaraa. Turvallisuusvyöhykkeiden ansiosta tuotanto linjan muissa osissa voi jatkua ainakin jonkin aikaa, kun yhdessä osassa ollaan poistamassa häiriötä tai lisäämässä materiaalia. Riskien hallitseminenkin on hankalaa, jos konelinja on yksi suuri kokonaisuus. (Siirilä 2009, 424.) Suuressa linjassa ei esimerkiksi mistään kohdasta voi katsomalla varmistaa, että vaaravyöhykkeelle ei ole jäänyt ketään, kun turvatoiminnon kuittauksen jälkeen konetta käynnistetään. Käsikäyttöisen kuittauspaikan on sijaittava vaaravyöhykkeen ulkopuolella ja sen on oltava turvallisessa paikassa, josta on oltava hyvä näkyvyys kuitattavalle alueelle. (SFS-EN ISO 13849-1 2015, 38.) Turvallisuusvyöhykkeisiin jakaminen on otettu huomioon myös koneturvallisuuden perusstandardissa SFS-EN 12100-2 (2010, 64.), jonka mukaan turvalaitteiden, hätäpysäyttimien, syötönerotuskytkimien ja sulkuventtiilien merkinnöillä on tehtävä selväksi mille alueelle mikäkin turvalaite tai hallintaelin vaikuttaa. Täytyy olla ilmiselvää, missä menevät vyöhykkeiden rajat ja mihin vyöhykkeeseen mikäkin hallintaelin vaikuttaa. (SFS-EN ISO 12100 2010, 64.) Sen lisäksi, että konejärjestelmä on erotettavissa energiansyötöstä, suurissa konelinjoissa on lisäksi oltava mahdollisuus sopivien osakokonaisuuksien erottamiseen (SFS-EN ISO 14118 2018, 10).

2.3.2 Odottamaton käynnistyminen vaaravyöhykkeellä

Tapaturmaan johtaneen tilanteen alussa automaattinen kone on usein pysähtyneenä luokan 2 pysäytykseen eli kyseessä on normaali tuotantopysäytys, jossa energiansyöttö jää päälle. Kun kone ei liiku, se on vaarattoman tuntuinen. Kun vaaravyöhykkeelle on mentävä häiriön, puhdistuksen tai muun syyn vuoksi, odottamattoman käynnistymisen syynä voi olla automaattisen ajon esteenä olevan häiriön poistaminen tai ohjelman aikaan saama käynnistyminen, kun lopussa ollutta tuotetta on lisätty, anturi tunnistaessa jälleen tai toinen työntekijä käynnistää koneen tarkoituksellisesti vaaravyöhykkeellä olevasta henkilöstä tietämättä. Tapaturma on mahdollinen, kun vaaravyöhykettä ei ole suojattu kokonaan. Vaarakohtaan on päässyt turvalaitteeseen vaikuttamatta esimerkiksi kaiteen yli tai välistä, kuljetinta pitkin tai vastaavalla tavalla. Pääsy vaaravyöhykkeelle saa olla vain turvalaitteeseen vaikuttamalla, jolloin koneen tila muuttuu energiansyötön seurauksena niin, että odottamaton

käynnistyminen esimerkiksi valoverhoon tai muuhun anturiin vaikuttamisen seurauksena on estetty. Tarkoituksellinen, vahingossa syntyvä tai viasta aiheutuva käynnistyskäsky ei käynnistä konetta ennen kuin pääsyä valvova turvalaite on taas toiminnassa ja alueelta ulos tuleminen on kuitattu. Kun riskit ovat suuret tai kun vaaravyöhykkeelle ei ole riittävää näkyvyyttä, turvalaitteen, esimerkiksi laserskanneri tai tuntomatto, on havaittava vaaravyöhykkeellä oleva henkilö jatkuvasti. (Siirilä 2009, 36.)

Erikoistilanteissa, kuten koneella opettamalla tehtävä ohjelmointi, vian haku tai säätäminen, ollaan vaaravyöhykkeellä koneen käydessä tai ollessa käynnistymisvalmiina. Riskien saaminen riittävän pieniksi vaatii koneen ja ohjausjärjestelmän suunnittelijoilta huolellista paneutumista näiden tilanteiden turvallisuusongelmiin. Jos vaaravyöhykkeellä on oltava koneen ollessa käynnissä, turvallisuus on varmistettava näiden toimintojen aikana pakkokäytön tai hitaiden liikkeiden avulla. (Siirilä 2009, 36.)

Järjestelmä on toteutettava niin, että manuaalinen ohjaus/käynnistäminen on mahdollista vain yhdestä ohjauslaitteesta kerrallaan. Erityisesti konelinjoissa toisiaan seuraavien koneiden käyttäminen ja pysäyttäminen oikeassa järjestyksessä on välttämätöntä ruuhkien, törmäysten ja muiden ongelmien välttämiseksi. Riskit kasvavat aina, kun ongelmia syntyy ja vaaravyöhykkeille joudutaan menemään ongelmien selvittämiseksi. (A 12.6.2008/400)

Kuittausta tarvitaan vähentämään vikaantumisesta aiheutuvan odottamattoman käynnistymisen todennäköisyyttä. Kuittaus on tarpeen erityisesti silloin, kun vaaravyöhyke on laaja ja turvalaitetta käytetään vain vaaravyöhykkeelle menon havaitsemiseen. (Siirilä 2009, 390.) Jos läsnäolon havaitsevan turvalaitteen käyttämistä ei pidetä mahdollisena, vaaraa aiheuttavan odottamattoman käynnistymisen mahdollisuutta voidaan vähentää käyttämällä kahta kuittauspainiketta. Alueelta poistuessa painetaan ensin vaaravyöhykkeellä olevaa kuittausta, jonka jälkeen turvalaite suljetaan ja vaaravyöhykkeen ulkopuolella olevaa kuittausta on painettava lyhyehkön ajan kuluessa. Tällöin on jo varsin epätodennäköistä, että vaaravyöhykkeelle jää joku henkilö vahingossa havaitsematta. (Siirilä 2009, 391.)

2.4 Turvatoiminnot

Turvatoiminto on standardin SFS-EN ISO 12100 (2010) mukaan koneen toiminto, jonka vikaantuminen voi aiheuttaa välittömän riskin (riskien) kasvamisen (SFS-EN ISO 12100 2010,

22). Turvallisuuteen liittyvän ohjausjärjestelmän tehtävänä on toteuttaa riskien hallitsemiseksi tiettyjä turvatoimintoja silloin, kun järjestelmä toteaa toiminnon tarpeelliseksi anturitietojen, ohjelmakäskyn, havaitun vian tai muun syyn vuoksi (Siirilä 2009, 59). Ohjausjärjestelmän avulla aikaan saatavaa koneen turvallisuutta on tarkasteltava kokonaisuutena, joka alkaa antureista ja päättyy turvatoiminnon suorittaviin koneen toimilaitteisiin ja jarruihin. Kun turvalaitteilla ja ohjausjärjestelmällä toteutettua riskien vähentämistä tarkastellaan, on otettava huomioon koko toimintaketjun luotettavuus. Vaikka anturit ja johdotukset olisivat kahdennettuja ja niitä valvotaan turvareleillä, turvallisuus voidaan menettää kiinni hitsautuneen kontaktorin, auki juuttuneen venttiilin tai toimimattoman jarrun vuoksi. Kokonaisuudessa ei saa olla heikkoja lenkkejä, joiden vikaantuminen voisi aiheuttaa turvatoiminnon menettämisen. Koko toimintaketjun suunnilleen saman tasoinen luotettavuus voidaan saada aikaan kahdentamalla ja valvomalla kriittisimpiä tai vikaantumisille altteimpia komponentteja. (Siirilä 2009, 61.)

Turvatoiminnon viimeisenä vaiheena on yleensä liikkeiden pysäyttäminen tai koneen saattaminen muuten turvalliseen tilaan (esim. laserleikkuupään sulkimen sulkeminen). Pysäytyskäskyn jälkeen sähkömoottoria hidastetaan hallitusti tai jarrutetaan nopean pysähtymisen aikaansaamiseksi. Kun liike on pysähtynyt, kontaktori tai muu kytkin avautuu, jolloin moottori on erotettu energiansyötöstä. Paineilmalla käytettävissä järjestelmissä venttiilin sulkeutuminen vastaa kontaktorin koskettimien avautumista. (Siirilä 2009, 95.)

Ohjausjärjestelmän muutokset vaikuttavat usein hyvin olennaisesti koneen turvallisuusominaisuuksiin, vaikka koneen muut ominaisuudet pysyvät lähes ennallaan. Ohjausjärjestelmän muutosten yhteydessä on otettava huomioon ainakin seuraavia asioita:

- Koneen pysähtymiseen kuluva aika tai muut vasteajat saattavat pidentyä tai lyhentyä

- Käyttöjen muuttaminen säädettäviksi tai ohjauksen muuttaminen releistä ohjelmoitavaan logiikkaan muuttaa todennäköisesti pysäytysluokkia. Jos pysäytysluokkaa 2 käytetään henkilön vaaravyöhykkeellä käynnin aikana, pysähtyneenä pysymistä on valvottava

- Odottamattomaan käynnistymiseen johtavat syyt ja käynnistymisen todennäköisyys muuttuu

- Vikaantumistavat ja vikojen aiheuttamat vaaratilanteet muuttuvat. Alkuperäisen suunnittelun lähtökohdat otettava huomioon komponentin vaihdon yhteydessä. (Siirilä 2009, 65.)

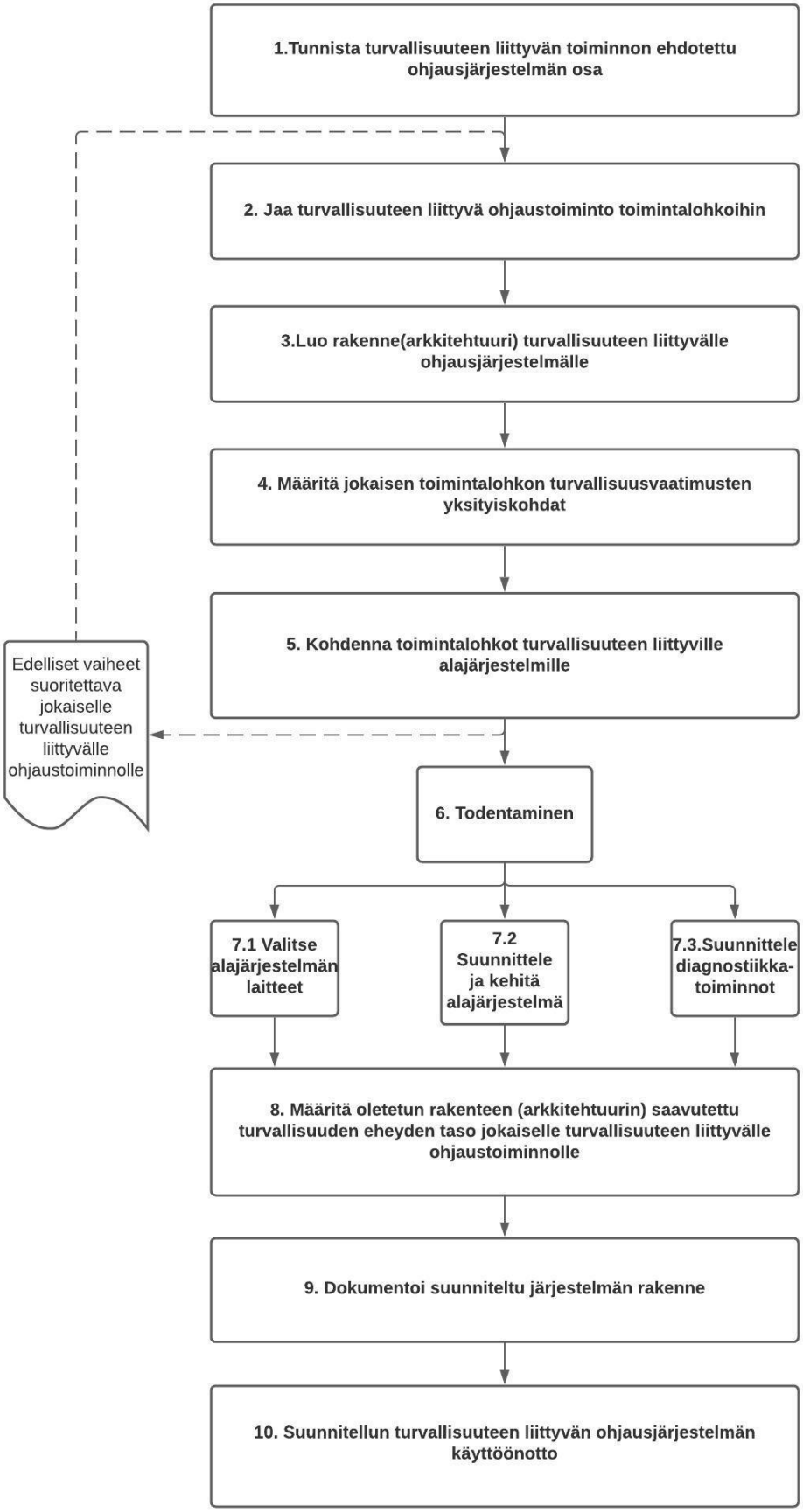
Olennaista kokonaisuuden suunnittelussa on myös vähentää käyttäjän houkutusta käyttää konetta muuten kuin tarkoitetulla tavalla. Turvatoiminnon tarkoituksellisen mitätöinnin mahdollisuus on otettava huomioon ainakin seuraavissa tapauksissa:

- Suojaustoimenpide hidastaa tuotantoa tai häiritsee käyttäjän muita toimintoja
- Suojaustoimenpidettä on vaikea käyttää
- Osallisena ovat muut henkilöt kuin itse käyttäjä
- Käyttäjä ei tunnista suojaustoimenpidettä tai sitä ei pidetä tarkoitukseen sopivana. (SFS-EN ISO 12100 2010, 48.)

Yksi keskeinen ohjausjärjestelmää koskeva vaatimus on, että koneen turvallisuus on varmistettu ohjausjärjestelmän tai energiansyötön vikaantuessakin. Vähänkään monimutkaisemmassa koneessa on siten oltava jonkinlainen vikaantumisen valvonta. (SFS-EN ISO 12100 2010, 66.)

Kuviossa 1 on turvallisuuteen liittyvä kaavio ohjausjärjestelmän suunnittelun vaiheista.

Koneet ja niiden ohjausjärjestelmät on suunniteltava niin, että ne ovat riittävän turvallisia ilman hätäpysäytystäkin. Standardin SFS-EN ISO 12100-2 kohdan 6.3.5.2 mukaan hätäpysäytys ei ole varsinaisesti turvatoiminto, vaan täydentävä suojaustoimenpide. Koska hätäpysäytys on kaiken varalta oleva lisäsuojaustoimenpide, muita turvallisuusratkaisuja ei ole lupa jättää pois. Hätäpysäytys on tarkoitettu pienentämään suojausten ja turvalaitteiden suunnittelun jälkeen koneeseen jääviä jäännösriskejä. Hätäpysäytystä voidaan tarvita vikatilanteissa tai kun huolellisesta suunnittelusta huolimatta tapahtuu jotain yllättävää ja vaarallista. (SFS-EN ISO 12100 2010, 90.)



Kuvio 1. Turvallisuuteen liittyvän ohjausjärjestelmän suunnittelu (SFS-EN ISO 62061 2005, 60).

2.5 Suunnitteluvirheiden ja muiden systemaattisten vikojen välttäminen

Systemaattiset virheet ovat tyypillisiä monimutkaisissa järjestelmissä. Järjestelmän turvallisuusvaatimukset on määriteltävä niin yksityiskohtaisesti, että niiden toteuttaminen, todentaminen ja kelpuutus voidaan tehdä oikein ja yksiselitteisesti. Turvallisuusmäärittelyyn sisältäviin asioihin on otettu kantaa mm. standardissa SFS-EN 62061, näitä asioita ovat:

- Koneelle tehdyn riskien arvioinnin tulokset mukaan lukien kaikki turvatoiminnot, joiden on määritelty olevan tarpeellisia riskien vähentämisprosessissa.

- Ohjelmoitavan logiikan tai muun ohjelmoitavan ohjausjärjestelmän kaikkien niiden toimintojen kuvaus, jolla voi olla vaikutusta turvallisuuteen. Kuvaukseen kuuluvat myös:

    - rakennevaatimukset

    - kuvaus koneen siitä toiminnasta, jonka turvallisuuteen liittyvän ohjaustoiminnon on tarkoitus saada aikaan tai estää

    - tapa, jolla tietty tila saavutetaan ja pidetään yllä

    - tieto siitä, onko tavoitteena jatkuva vai tietyssä tilanteessa toteutettava turvatoiminto.

- Kaikki ulkoiset liitännät sekä ihmisen ja koneen rajapinnat. Samoin on käsiteltävä järjestelmän sisällä olevien alajärjestelmien väliset rajapinnat.

- Kaikki huomioon otetut vikaantumistavat ja niiden esiintymisen todennäköisyys ja esiintymistaajuus sekä tavat, joilla vikojen aiheuttamat vaikutukset on otettu huomioon. Myös muut turvatoiminnon suoritustason laskennan arviot.

- huomioon otettavat ympäristöolosuhteet sekä sähkömagneettisen immuniteetin rajat ja muut ympäristöolosuhteita koskevat rajat. (SFS-EN ISO 62061 2005, 46-48.)

Toisin kuin satunnaisilla komponenttivioilla, systemaattinen vioilla on syynsä, jotka voidaan poistaa vain muuttamalla esimerkiksi suunnittelua, valmistusprosessia, toimintatapoja tai

dokumentaatiota. Systemaattiset viat syntyvät tuotteen elinkaaren jossain vaiheessa esimerkiksi määrittelyssä, suunnittelun aikana tai ohjausjärjestelmän turvallisuuteen liittyvän osan muutosten aikana. Monikanavarakenteiden toteuttaminen ja komponenttivikojen todennäköisyyden analyysi ovat tärkeitä tekijöitä turvallisuustekniikan suunnittelussa. Turvallisuusperiaatteita on lueteltu standardin 13849-01 liitteessä C. (DGUV 2017.)

2.5.1 Erilaisia ohjauspiirejä ja niiden vikamuotoja

Konejärjestelmissä on niiden monimutkaisuudesta riippuen hyvin erilaisia ohjausjärjestelmiä ja ohjauspiirejä, jonka myötä vikaantumistavat vaihtelevat. Kiinteästi langoitetut sähkömekaaniset piirit koostuvat usein releistä, jotka ovat yhteydessä toisiinsa johtimien tai painettujen piirien välityksellä. Vikamuodot ovat usein tiedossa ja viat tunnistettavissa, esim. katkos, koskettimen hitsaus jne. Yhteisviat eivät ole kovinkaan todennäköisiä. Sähkömekaanisissa piireissä fysikaalisten tekijöiden aiheuttamia joitain vaarallisia vikoja voidaan jättää huomioon ottamatta, koska vikaantuminen tapahtuu aina turvalliseen suuntaan eli aiheuttaa pysähtymiskäskyn. Tällä perinteisellä tekniikalla on mahdollista tehdä hyvin luotettavia ohjausjärjestelmiä. (STSARCES - Standards for Safety Related Complex Electronic Systems 2014.)

Ohjauspiirinä yksinkertaiset elektroniset piirit tehdään enimmäkseen diodeista ja kytkiminä käytettävistä transistoreista. Niiden tyypilliset vikamuodot ovat samoja kuin sähkömekaanisilla piireillä. Lisäksi ne ovat herkkiä sähkömagneettisille häiriöille ja komponentit voivat vikaantua yhtä aikaa samasta syystä. Lisäksi yhdenkin komponentin vikaantuminen voi johtaa muidenkin vikaantumiseen. Ohjelmoitavissa piireissä on mikrosuorittimen ja pysyvän muistin lisäksi muutettavissa olevaa muistia, joka sallii käyttäjän tekevän ohjelmallisesti muutoksia ohjauspiirin käskyihin. Edellä esitettävien vikamuotojen lisäksi on siksi otettava huomioon ohjelmistoon tulevat virheet ja tarkoittamattomat muutokset. Sen vuoksi käyttäjän ohjelmoitavissa olevia ohjausjärjestelmiä ei tulisi käyttää turvallisuustarkoituksiin. Ilman uudelleenohjelmointi mahdollisuutta olevat ohjelmoidut piirit koostuvat muistista, jota voidaan vain lukea. Tietojen käsittely koostuu peräkkäisistä käskyistä, jolloin mikä tahansa vika voi muuttaa mikroprosessorilta tulevien käskyjen järjestystä. Tästä voi olla seurauksena järjestelmän virheellinen toiminta. Vikojen aiheuttamien vaarojen torjumiseksi käytetään kahdentamista sekä järjestelmän automaattista kunnon valvontaa ennen toiminnon

aloittamista ja toiminnan aikana. (STSARCES - Standards for Safety Related Complex Electronic Systems 2014.)

Järjestelmän ja ohjelmiston suuruus ja monimutkaisuus aiheuttavat sen, että aina on varauduttava mahdollisiin ohjelmiston virheisiin. Lisäksi järjestelmässä voi olla systemaattisia virheitä, kun kaikkia mahdollisuuksia ei ole osattu etukäteen ottaa huomioon. (STSARCES - Standards for Safety Related Complex Electronic Systems 2014.)

2.5.2 Systemaattisten vikojen tai virheiden muotoja

Vaikeimmin ennen järjestelmän käyttöönottoa havaittavissa olevat virheet syntyvät toiminnallisten vaatimusten ja ominaisuuksien määrittelyssä. Vaatimus voi olla väärä tai virheellinen. Vaatimus voi olla oikein määritelty, mutta vaatimus voi olla tarpeeton tai ylimääräinen. Vaatimus voi olla looginen, mutta se ei sovi järjestelmän asettamiin rajoitteisiin. Vaatimus voi lisäksi olla vaillinainen variaatioiden, attribuuttien tai muiden ominaisuuksien määrittelemättömyyden vuoksi. Vaatimuksen täytyy olla myös todennettavissa. Pelkkä testauksen suunnittelu ei riitä, vaan testaus pitää olla myös mahdollista toteuttaa annetuilla resursseilla. (Siirilä 2009, 196.)

Yksi syy suunnitteluvirheiden, ohjelmavirheiden ja muiden systemaattisten vikojen tai virheiden esiintymiseen on kova kiire. Järjestelmällinen riskien arviointi, suunnitelmiin tehtävien muutosten vaikutusten arviointi ja muut turvallisuuden kannalta tarpeelliset tehtävät jäävät helposti jalkoihin, kun toimitusten määräajat uhkaavat lähestyä. Määräajat ovat monesti epärealistisen tiukkoja, koska hinnan lisäksi toimituksista kilpaillaan myös toimitusajoilla. (Siirilä 2009, 196-197.)

Laadukkaasta suunnittelusta huolimatta virheitä voi päästä valmiiseen järjestelmään asti, joten niihin on varauduttava. Määrittelyissä on otettava huomioon prosessin häiriöt, prosessituotteiden vioittuminen, ihmisten virheet sekä itse automaatiojärjestelmän viat. (Siirilä 2009,198.) Ohjausjärjestelmän suunnittelussa on pyrittävä yksinkertaisuuteen ja hallittavuuteen. Järjestelmän rakenteen on minimoitava yksittäisen ohjelmavirheen vaikutuksen leviäminen ja mahdollistettava järjestelmälle asetettujen vaatimusten todentaminen. (Siirilä 2009, 201.)

2.6 Määrittely ja dokumentointi

Suunnittelutyön dokumentointi keskittyy siihen mitä on suunniteltu. Toimivuuden ja turvallisuuden varmistamiseksi tulisi välittää tieto myös siitä, miksi on suunniteltu näin. Suunnittelutyön dokumentoinnissa ja tiedon siirtämisessä toisille suunnitteluosapuolille ja myös tuleville käyttäjille tulisi tarvittavassa laajuudessa välittää perusteet tehdyille ratkaisuille sekä ratkaisuja koskevat rajoitukset ja mahdolliset heikkoudet. Näiden tietojen puuttuminen voi aiheuttaa häiriöitä ja myös onnettomuusmahdollisuuksia esimerkiksi kohteeseen liittyvien muutostöiden yhteydessä tai käytettäessä suunnittelua jonkin vastaavan kohteen suunnittelun pohjana. (Malmén, Nissilä, Wallin& Virolainen 2012, 74.)

Huolellinen dokumentointi suunnittelun, kehittämisen sekä muutosten tekemisen kaikissa vaiheissa on välttämätön ohjausjärjestelmän laadukkaalle toteutukselle. Standardin SFS-EN 62061 mukaan turvallisuuteen liittyvän ohjausjärjestelmän rakenne ja sen diagnostiikkatoiminnot on dokumentoitava. Dokumentoinnin on oltava tarkka ja tiivis kokonaisuus, jota tarvitsevien henkilöiden on helposti ymmärrettävä. Dokumentoinnin on sovittava tarkoitukseensa, sen on oltava sidosryhmien saatavissa ja ylläpidettävissä. Ohjausjärjestelmien turvallisuusvaatimusten mukaisuus pyritään varmistamaan todentamisella (verification) ja kelpuutuksella (validation). (SFS-EN ISO 62061 2005, 50.)

3 Mallipohjainen systeemisuunnittelu

3.1 Lean-ajattelu integroidussa tuotekehityksessä

Globaalin kilpailun kiristyessä, tuotteiden elinkaaren lyhentyessä ja tuotteiden monimutkaistuessa yrityksillä on kasvava paine siirtyä peräkkäisissä vaiheissa etenevästä tuotekehityksestä rinnakkaiseen kehittämiseen. Toimivalla rinnakkaissuunnittelulla pyritään luomaan vakautta ja toistettavuutta, näin suunnittelu kyetään viemään läpi virheettömämmin ja lyhyemmässä ajassa. Tuotekehityksen varhainen vaihe nähdään usein prosessissa vaiheena, jolloin tehdään suuria päätöksiä ja periaatelinjauksia myös turvallisuuteen, mikä sitten vaikuttaa merkittävästi lopputuotteeseen ja sen kustannuksiin. Tästä syystä on tärkeää, että laajan ja monipuolisen ryhmän osaamista hyödynnetään alusta alkaen. (Huhtala & Pulkkinen 2009,178.) Monissa tutkimuksissa on päädytty siihen, että kaikkein tehokkain tapa koordinoida ihmisten työn aikaansaannoksia on kasvotusten käyty keskustelu. Tiedon hajonnasta usein johtuu, että tuotekehittäjät käyttävät suuren osan ajastaan tiedon etsimiseen. (Huhtala & Pulkkinen 2009, 188-189.)

Lean-suunnitteluprosessilla pyritään eliminoimaan hukkaa, keskittymään arvon tuottamiseen ja parantamaan vaiheaikaa. Oleellista on, että virheet pyritään saamaan mahdollisimman läpinäkyviksi. Suunnittelija saattaa aloittaa yhdellä mallilla, havaita sen olevan puutteellinen, oppia mallin avulla ongelmasta lisää ja sitten muuttaa sitä. Erityisesti uusia tuotteita suunniteltaessa tuotekehittäjä oppii paljon suunnittelun edetessä siitä, mikä tulee ja mikä ei tule toimimaan. (Huhtala & Pulkkinen 2009,192.)

Kompleksisia järjestelmiä pitääkin ajatella enemmän kehittyvinä, kuin valmiiksi suunniteltuina systeemeinä. On määriteltävä tavoitteet ja käytettävä hyväksi todettuja elementtejä ja ohjattava koko systeemiä kohti haluttua lopputulosta. Tätä voidaan soveltaa myös itse järjestelmän suunnittelun prosesseihin. Ajan myötä kehittyneiden prosessien selvittäminen voi olla parempi lähtökohta kuin määritellä suoraan lopulliset uudet prosessit. Muita suositeltavia periaatteita ovat:

- Tunnista paikalliset toimenpiteet, joilla voi olla laajat seuraukset. Valmistaudu muutoksiin.

- Säilytä useita ratkaisuvaihtoehtoja. Luo tarkoituksella monimuotoisuutta systeemiin.
- Tunnista eri muutosnopeudella kehittyvät osiot.
- Luovu täydellisestä optimoinnista.
- Koordinoi ja yhdistä ihmisiä ja ryhmiä. (Sheard & Mostashari 2008, 9-17.)

3.2 Suunnitteluprosessin päävaiheet

Suunnitteluprosessi alkaa määrittelystä. Kehitysprojektille asetetaan yleiset tavoitteet ja vaatimukset. Vaatimuksien määrittelemiseen osallistuvat projektin sidosryhmät, kuten tuotepäälliköt, käyttäjät sekä suunnittelijat. Asiakkaat ja omistajat laativat yleensä korkeamman tason vaatimuksia, jotka täytyy jaotella alemman tason vaatimuksiksi. Korkeamman tason vaatimukset eivät lähtökohtaisesti ole hyödynnettävissä sellaisenaan epätarkkuuden vuoksi. Vaatimukset siis kehittyvät suunnitteluprosessin aikana ja niiden täyttymistä tarkastellaan V-mallin mukaisesti läpi projektin. (Liu 2015, 43.) V-mallista kerrotaan lisää seuraavassa luvussa.

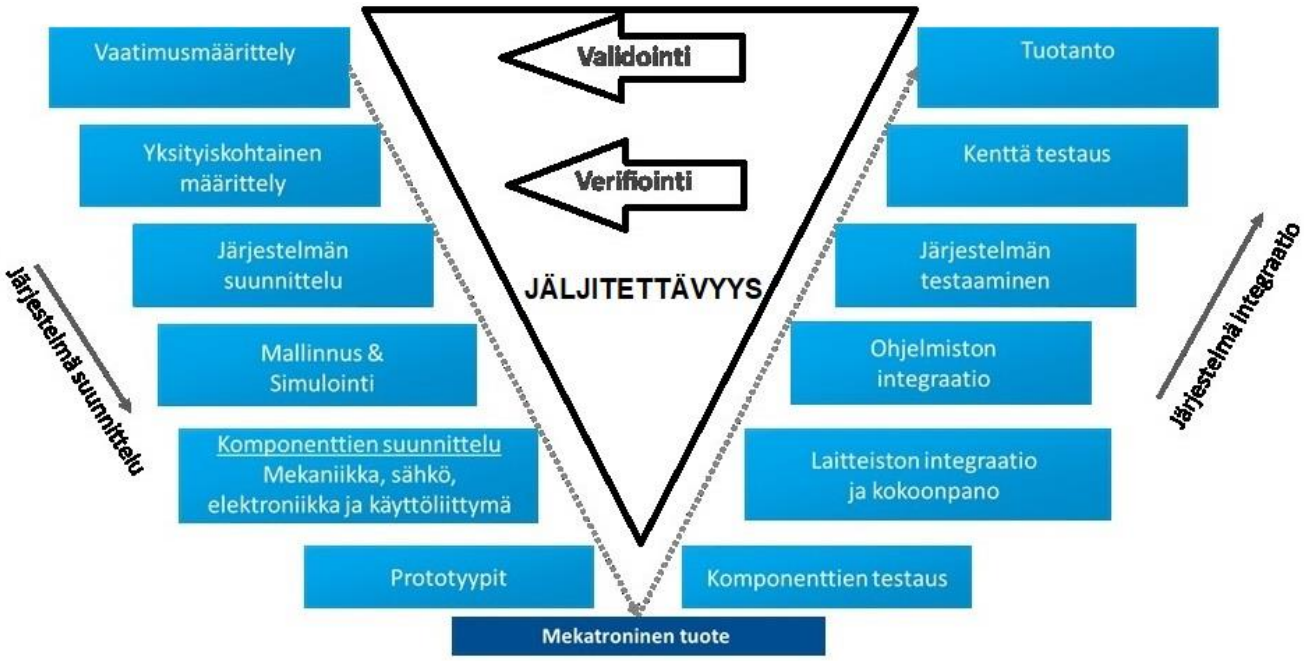
Konseptia tarkennetaan järjestelmä- ja komponenttitasoisessa kuvauksessa. Tekniset ratkaisut eivät ole olennaisia tässä vaiheessa, koska konseptoinnissa ei ole tarkoitus sitoutua liikaa tiettyyn toteuttamistapaan tai luoda ratkaisua jonkun tarkoin määritellyn komponentin ympärille. Konseptoinnin pyrkimyksenä ei ole siis löytää sovellukselle valmista ratkaisua vaan luoda pohja myöhempää kehitystyötä ja tarkentavaa suunnittelua varten. Konseptien avulla saadaan luotua ensimmäinen kokonaiskäsitys suunnitteilla olevasta järjestelmän osasta ja sen toiminnasta. Tämän perusteella voidaan tehdä karkeita arvioita lopputuloksesta. Konsepti voi olla sanallinen kuvaus järjestelmän toiminnallisuuden toteuttamisesta. (Liu 2015, 50-51.)

Tarkentavassa suunnitteluvaiheessa on syytä hyödyntää malleja ja simulaatioita, joiden avulla voidaan tutkia järjestelmän toiminnallisuuksia sekä ohjelmistojen ja komponenttien välistä integraatiota. Malleja voidaan rakentaa yhdistämällä prosessin aikana syntyneitä dokumentaatioita, tällöin lopputuloksena on joustava ja tehokas suunnittelutyökalu. Simulointituloksien luotettavuuteen vaikuttaa mallin yksityiskohtaisuus ja tarkkuus verrattuna aitoon systeemiin. (Liu 2015, 62.)

3.3 V-malli tuotekehityksen tueksi

V-malli on suoraviivainen tuotekehityksen menetelmä, joka on kehitetty alun perin ohjelmistokehityksen tarpeisiin. V-mallin tuotekehityksen prosessi rakentuu V-kirjaimen muotoon (Kuvio 2) alkaen aina vaatimustenmäärittelystä valmiin laitteen tuotantoon saattamiseen. Vasen puoli kuvaa systeemin vaiheiden määrittelyä ja eri järjestelmien suunnittelua. Oikea puoli kuvaa järjestelmien, laitteiston, komponenttien ja ohjelmistojen testausta sekä näiden integrointia yhdeksi kokonaiseksi mekatroniseksi laitteeksi. V-mallin puutteena on sen muokattavuus kesken kehitysprosessin. Esimerkiksi järjestelmätestauksen aikana havaitun vian vuoksi voidaan joutua palaamaan järjestelmäsuunnittelun vaiheeseen ja korjaamaan havaittu bugi tai kytkentävirhe sähköpiirustuksessa.

V-mallia on haasteellista soveltaa pitkän aikavälin projekteihin, jotka sisältävät useita muutoksia kesken tuotekehitysprosessin. Muutosten vuoksi suunniteltu aikataulu ja budjetti voivat ylittyä projektin aikana. V-mallin etuna on sen lineaarisen tuotekehitysprosessin selkeät vaiheet, jotka helpottavat pitämään tiukan aikataulun ja projektin tavoitteen ryhmän jäsenten mielessä. V-malli soveltuu hyvin projekteihin, joiden kesto ja laajuus on tarkoin määritelty. (Powell-Morse 2016)



Kuvio 2. V-mallin tuotekehitysprosessi (Graessler, Hentze & Bruckmann 2018, 2-6.)

3.4 Mallipohjaisen systeemisuunnittelun lähestymistapa

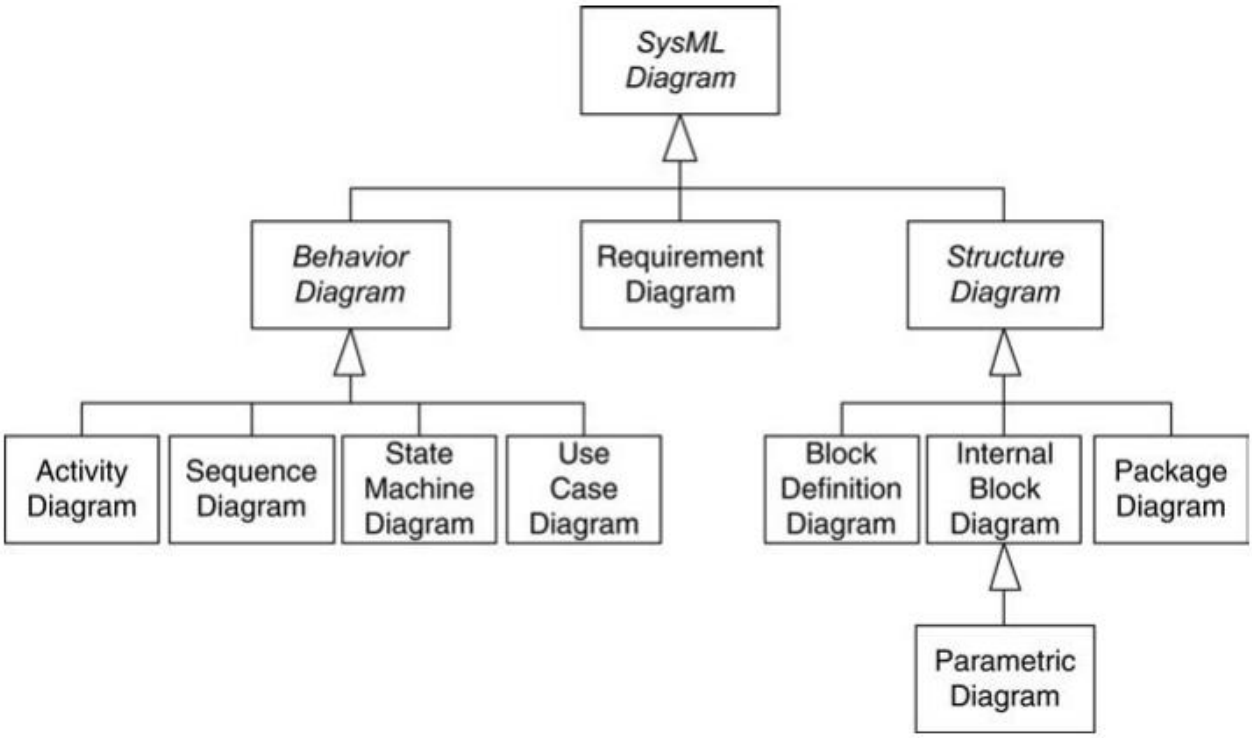
Malli kuvaa tai simuloi kohteena olevaa järjestelmää. Järjestelmän mallinnuksessa on kiinnitettävä huomiota siihen, mitkä ominaisuudet ovat keskeisiä mallissa, ja mitä tarkoitusta varten ne palvelevat. Malli voi olla vaikka vain järjestelmän tietyn ominaisuuden mittaaminen, mutta mallia voidaan hyödyntää myös mm. todentamiseen, kommunikointiin, koulutukseen ja ohjeistamiseen. Fyysinen prototyyppi pitää yleensä sisällään lähes kaikki samat ominaisuudet kuin lopputuotekin, kun taas malliin on yleensä määritelty vain tietyt tarkastelun kohteena olevat ominaisuudet, kuten käyttäytyminen ja rakenne. Mallit helpottavat erityisesti abstraktien järjestelmien esimerkiksi täysin uusien järjestelmien ja konseptien tutkimista. (VTT 2013, 57.)

Mallipohjaista suunnittelua on käytetty kauan useilla insinöörialoilla esimerkiksi mekaniikka- ja sähkösuunnittelussa. Mallipohjainen systeemisuunnittelu eli MBSE (model based systems engineering) on suunnittelumenetelmä, jossa suunniteltavasta systeemistä muodostetaan kuvaileva malli. Jotkut rajaavat MBSE-menetelmän lähinnä kuvailevien mallien käyttöön järjestelmän vaatimusten ja konseptien kuvaamiseen. Toiset näkevät sen hyvinkin laajasti kaikenlaisten mallien hyödyntämisenä järjestelmän elinkaaren aikana mukaan lukien erilaiset virtuaaliympäristöjen ja lisätyn todellisuuden sovellukset. Olennaista mallipohjaisuudessa on sen kytkeminen osaksi systeemisuunnittelun prosesseja. Voidaan ajatella, että systeemisuunnittelu on ylätason prosessi, jonka sisällön hallintaa MBSE tukee. [INCOSE 2014] INCOSE-yhdistyksen (International Council on Systems Engineering) mukaan MBSE-menetelmää on sovellettava järjestelmän koko elinkaaren ajan ja aikaisessa vaiheessa monimutkaisen järjestelmän käyttäytymisen ymmärtämisen tueksi. [INCOSE 2014]

Mallipohjaiseen systeemisuunnitteluun sisältyy kolme peruspilaria: mallinnusmenetelmä, mallinnuskieli ja mallinnustyökalu (Delligatti 2013,4). Systeemin malli saadaan aikaan noudattamalla perinteisiä systeemisuunnittelun prosesseja ja käyttämällä mallipohjaisen systeemisuunnittelun menetelmiä. Malli luodaan aikaisessa vaiheessa suunnitteluprosessia ja se kehittyy projektin edetessä. Mallin muodostamisessa voidaan käyttää esimerkiksi graafisia UML- tai SysML-mallinnuskieliä. (Weilkiens 2007,11.)

SysML-kieltä voidaan käyttää apuna, kun määritellään järjestelmän arkkitehtuuria sekä komponentteja. UML-kieli keskittyy enemmän ohjelmiston toiminnalliseen suunnittelemiseen.

Molemmat edellä mainituista kielistä kuuluvat GPML (general-purpose modeling language) -kieliin ja niitä käytetään kuvaamaan järjestelmän arkkitehtuuria sekä sanomanvaihtoa. UML-kielille on olemassa oma CCITT-standardi (CCITT Z.120). (Liu 2015, 51–52.)



Kuvio 3. SysML-kaaviot (Delligatti 2013,15)

SysML-profiili koostuu seuraavista kaavioista:

- Systeemin rakennetta kuvaavat kaaviot
    - Block definition diagram, lohkokaavio. Kuvaa järjestelmän/komponenttien hierarkiaa ja luokittelua. Mahdollistaa järjestelmän ominaisuuksien ja käyttäytymisen muuntamisen malleiksi
    - Internal block diagram, sisäinen lohkokaavio. Kuvaa järjestelmän sisäistä rakennetta, komponenttien, rajapintojen ja porttien avulla

- Parametric diagram, parametrinen kaavio. Esittää järjestelmän ominaisuuksien rajoituksia. Parametrisen kaavion avulla voidaan esittää monimutkaisia suhteita, joita voidaan hyödyntää vaatimuksien todentamisessa ja validoinnissa

- Package diagram, pakettikaavio. Mallit sisällytetään paketteihin, pakettikaavio on organisoimista varten. Pakettikaaviossa kuvataan pakettien riippuvuutta toisiinsa. (Delligatti 2013,15-16.)

- Systeemin käyttäytymistä kuvaavat kaaviot

  - Use case diagram, käyttötapauskaavio. Korkean tason kuvaus järjestelmän toiminnasta. Kuvaa järjestelmän systeemien ja myös käyttäjän välisiä vuorovaikutuksia

  - Sequence diagram, sekvenssikaavio. Järjestelmän osien välistä sanomanvaihtoa kuvaava kaavio. Sekvenssikaavioiden avulla mallinnetaan erilaisia skenaarioita järjestelmän toiminnoista. Sekvenssikaaviota käytetään tarkkaan kuvailuun käyttäytymisestä kehitysvaiheessa. Sopii hyvin testivaiheen määrittelyyn.

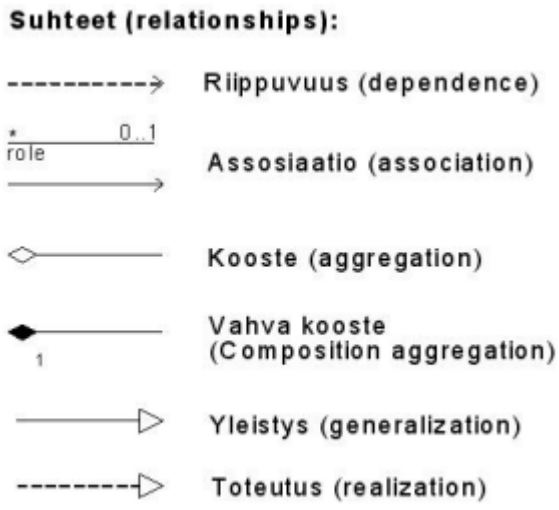
  - State machine diagram, tilakonekaavio. Kuvastaa järjestelmän tilanvaihtoon liittyviä tapahtumia ja toimenpiteitä eri tapahtumien aikana. Kuten sekvenssikaavio, tilakonekaavio kuvaa tarkkaa lohkon käyttäytymistä.

  - Activity diagram, aktiviteettikaavio. Datan- ja ohjauspyyntöjen kulkua kuvaava kaavio. Käytetään yleisesti kuvaamaan järjestelmän sisäistä käyttäytymistä ja toimenpiteitä (Delligatti 2013,15-16)

- Systeemin vaatimusta kuvaava kaavio

  - Requirements diagram, vaatimuskaavio. Vaatimuksien hierarkiaa ja syntymistä kuvaava kaavio. Yhdistää ja varmentaa vaatimuksia mallin elementteihin. (Delligatti 2013,15-16)

Mallien lohkojen välisillä yhteyksillä on eri merkitykset. Lohkojen väliset suhteet ovat assosiaatioita (association), riippuvuuksia (dependency), yleistyksiä (generalization) ja toteutuksia (generalization). Assosiaatiot voidaan esittää myös koostesuhteena lohkojen välillä. Suhteiden esitystavat on esitetty kuviossa 4.



Kuvio 4. Lohkojen väliset suhteet (Järvelä &Puusaari 2005, 4)

Vaatimusten väliset suhteet muihin mallielementteihin ovat tärkeimpiä seikkoja, jotka täytyy ottaa huomioon vaatimuksia mallinnettaessa. Yleisimmin käytetyt vaatimusten väliset suhdetyypit ovat: containment, trace, derive requirement, refine, satisfy ja verify. Nämä suhteet muodostavat jäljitettävyyden vaatimuksille:

- **Containment-**sisältyvyyssuhteessa vaatimuselementeillä on selitetty mihin toiseen elementtiin vaatimuksella on riippuvuussuhde. Yksi tai useampi vaatimus sisältyy ylemmän tason vaatimukseen.

- **Trace**-riippuvuussuhde ilmaisee vaatimuksen jäljitettävyyden johonkin mallielementtiin.

- **Derive requirement**-riippuvuussuhteella ilmaistaan, että vaatimus on johdettu jonkin toisen vaatimuksen pohjalta. Riippuvuus on kuvattu kaaviossa avainsanalla <<derive-Reqt>>. Tämän riippuvuussuhteen täytyy mallissa olla aina kahden vaatimuksen välinen.

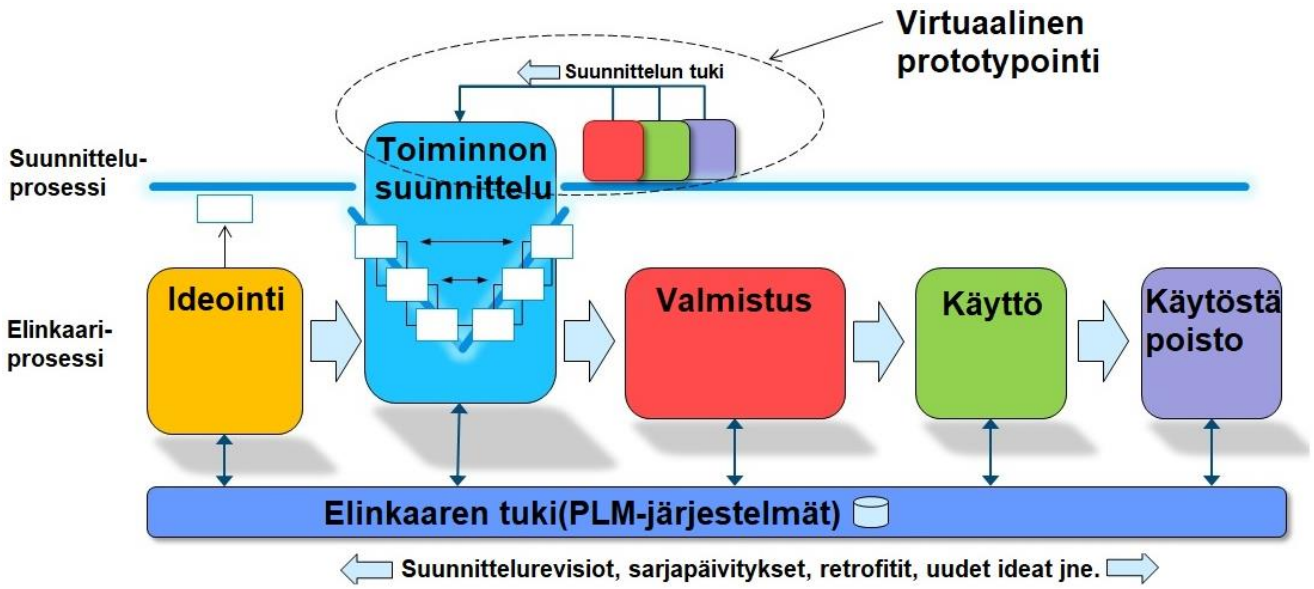
- **Refine**-riippuvuussuhteella ilmaistaan suhdetta johonkin toiseen mallielementtiin, jonka avulla voidaan selventää vaatimusta.

- **Satisfy**-riippuvuussuhteella esitetään, että mallielementti täyttää vaatimuksessa esitetyt asiat. SysML-kielessä ei eritellä, minkälainen mallielementin täytyy olla, mutta sen täytyy toteuttaa vaatimus. Satisfy-riippuvuussuhde on ainoastaan tapa osoittaa vaatimus rakenne-elementille. Vaatimuksen lopullinen toteutuminen varmistetaan testitapauksen avulla.

- **Verify-**riippuvuussuhteella voidaan ilmaista, kuinka mallielementti varmistaa vaatimuksen toteutumisen. SysML-kielessä ei ole rajoituksia, mikä toteuttavan mallielementin täytyisi olla, mutta useimmiten se on testitapaus. Testitapaus on SysML-kielessä jokin käyttäytymistä kuvaava mallielementti eli aktiviteetti, vuorovaikutus tai tilakone. (Delligatti 2013, 205-209.)

3.5 Turvatoiminnon virtuaaliprototypointi ja elinkaari

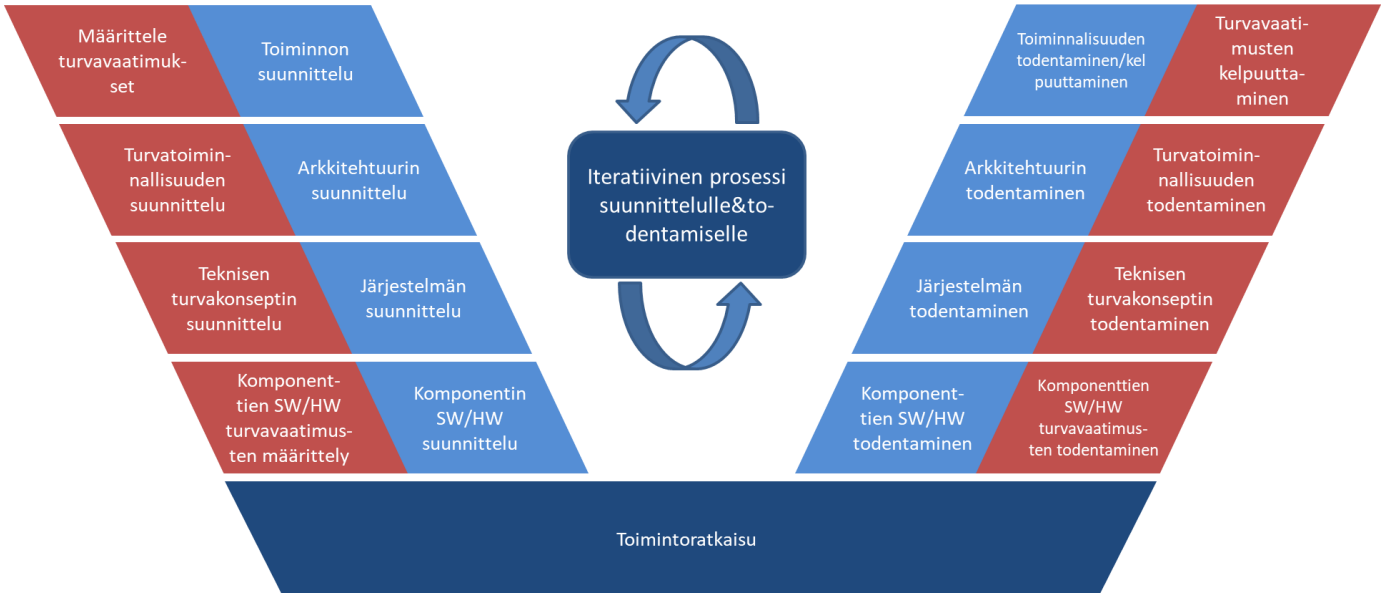
Nykyään esiintyy myös käsite ”laajennettu mallipohjainen SE” (”Extended MBSE”). Tämä tarkoittaa sitä, että mallipohjaisuuden käsitettä on laajennettu kattamaan virtuaaliprototypointi eli simulointimalleihin ja visualisointeihin. Virtuaaliprototypointi on tässä yhteydessä termi, jolla tarkoitetaan joukkoa digitaalista tuotetietoa tuottavia, analysoivia ja hyödyntäviä työkaluja ja menetelmiä, esimerkiksi erilaisia simulointeja, virtuaaliympäristöjä ja CAE-työkaluja. Virtuaaliprototypointi käsittelee käyttäytymistä kuvaavia malleja. Virtuaaliprototypointia voidaan hyödyntää mm. abstraktien ja kompleksisten mallien visualisoinnissa ja tulkinnassa, vaatimusten määrittelyssä ja suunnitelmien arvioinnissa. (VTT 2013, 38.)



Kuvio 5. Turvatoiminnon elinkaari (VTT 2013, 38).

Perinteisesti virtuaaliprototypointia on sovellettu usein järjestelmän teknisten ratkaisujen todentamiseen hyvin myöhäisessä tuoteprosessin vaiheessa suunnittelun jatkeena. Ajattelun pitäisi olla kuitenkin päinvastainen, eli dokumenttien sijaan malleilla ja simuloinneilla lähdetään määrittelemään tarpeita, tavoitteita ja vaatimuksia, jotka sitten konkretisoituvat suunnittelussa (kuvio 5). Tämän prosessin kehittäminen ja hallinta on haastavaa, mutta kehitys on jo ottanut askeleita siihen suuntaan. (VTT 2013, 38.)

Kuviossa 5 on esitettynä toiminnon suunnittelun sisällä V-malli. Tämä kuvaa tuotekehityksen prosessia uuden toiminnon kehittämiseen. Uutta toimintoa suunnitellessa täytyy turvavaatimusten kulkea koko ajan toiminnon kehittämisen rinnalla. Kuviossa 6 on esitettynä toiminnallisuuden kehittämisen monimuotoinen prosessi, jossa vasemmalla puolella on esitettynä rinnakkainen suunnittelu ja oikealle rinnakkainen todentaminen.



Kuvio 6. Toiminallisuuden rinnakkaisen kehittämisen V-malli (Skoglund, Warg & Sangchoolie 2018, 5).

3.6 SafeML-profiili vaarojen mallintamiseen

Vuonna 2017 OMG-yhtymässä (Object Management Group) muodostettiin uusi ryhmä sekä teollisuuden että korkeakoulujen osaajista määrittelemään UML:lle uusi standardiprofiili, joka käsittelee järjestelmän turvallisuus- ja luotettavuusnäkökohtia. Tämä on tärkeä osa järjestelmätekniikkaa, johon SysML-kieli ei kyennyt. (Biggs, Juknevicius, Armonas & Post 2018, 2.)

SafeML on profiili, joka tarjoaa SysML-kielelle mahdollisuuden mallintaa turvallisuustietoja, kuten vaaroja ja niiden mahdollisesti aiheuttamia haittoja, mallintaa luotettavuusanalyyseja, mukaan lukien vikapuuanalyysia (FTA) ja vaikutusten analyysia (FMEA) ja käyttää rakenteellista argumentointia mallin järjestämiseen ja varmennustapausten määrittämiseen. (Biggs & Kotoku 2014, 3-4.)

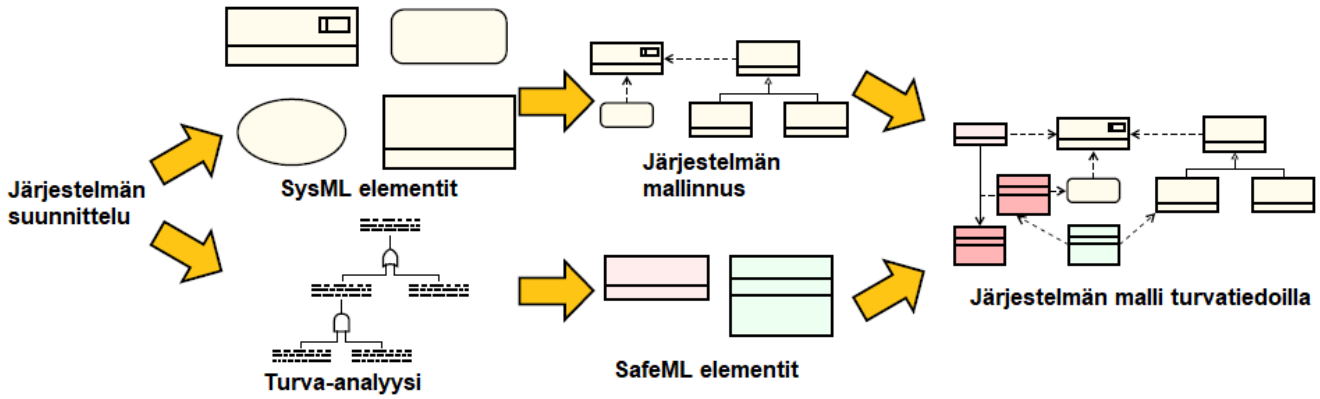
Selkeämpi viestintä liittyen turvallisuuteen tukee kriittistä turvajärjestelmän kehittämistä:

1. Se tukee kehittäjiä auttamalla heitä ymmärtämään, mitkä riskit järjestelmälle ja sen osiin ovat merkityksellisiä

2. Se tukee testaajia auttamalla ymmärtämään riskejä, joita järjestelmä käsittelee ja miten niitä käsitellään

3. Dokumentaatio tukee sertifiointiviranomaisia määrittämällä selkeästi huomioon otettavat riskit ja niiden suhdetta järjestelmän suunnitteluun, mikä auttaa sertifioijaa tekemään päätöksiä siitä, onko järjestelmä toiminnaltaan ja ominaisuuksiltaan riittävän turvallinen. (Biggs & Kotoku 2014, 2.)

SafeML-profiil on kohdistettu käytettäväksi turvallisuuden kannalta kriittisiin järjestelmiä varten, jotka on rakennettu sekä turvalaitteista että ohjelmistoista, jotka on suunniteltu ohjaamaan turvalaitteistoa. SafeML:n tavoitteena on mahdollistaa yhdenmukaisten turvallisuusanalyysien tulokset ja turvatoimenpiteet järjestelmän mallintamisessa. SafeML keskittyy tekemään näistä tiedoista näkyviä järjestelmäsuunnittelussa. SafeML on suunniteltu käytettäväksi yhdessä SysML:n kanssa. SysML tarjoaa tarvittavat kaaviot ja elementtityypit, joita tarvitaan mallin suunnittelussa. SafeML tarjoaa elementtityypit, joita tarvitaan turvallisuustietojen lisäämiseen malliin. Tämä on esitettynä kuviossa 7. (Biggs & Kotoku 2014, 8.)



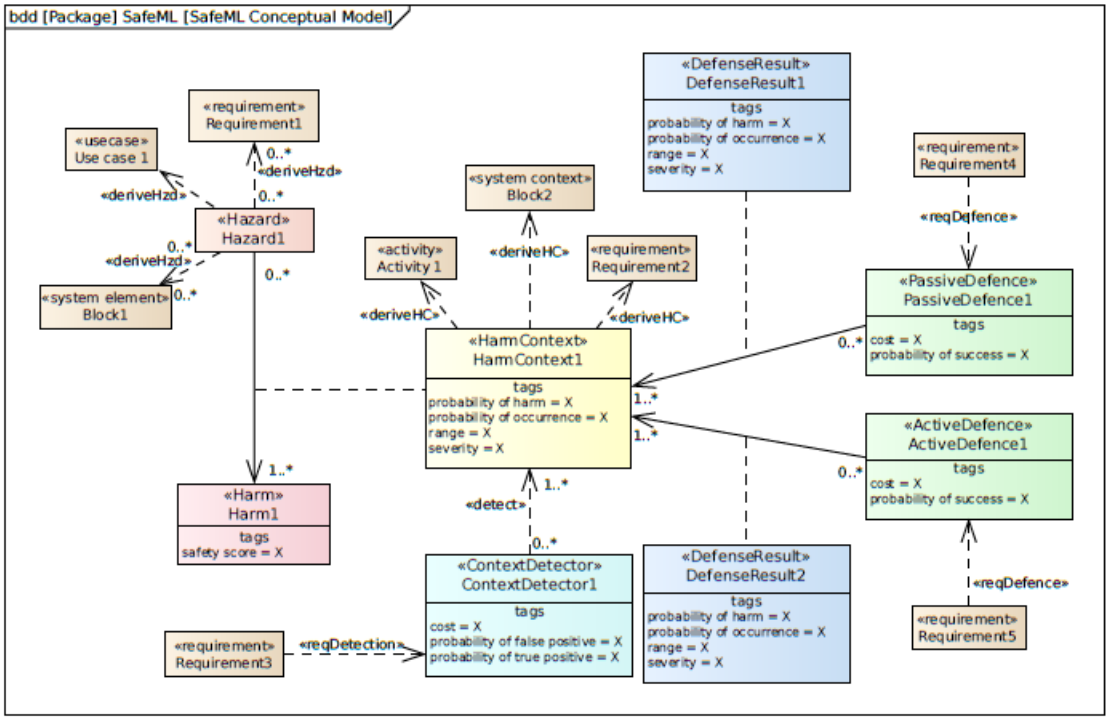
Kuvio 7. SafeML:n käytön konsepti (Biggs & Kotoku 2014, 9).

3.6.1 SafeML-elementit

SafeML-profiilissa elementtityypit määrittävät turvakonsepteja, joiden vaaran ja vahingon yhteyttä ja niiltä suojaavan suojan yhteyttä vaatimuslohkoon mallinnetaan. SafeML-profiilissa on seitsemän elementtityyppiä. Elementtityypit jaotellaan kahteen osioon.

Ensimmäinen osio käsittää vaaran (Hazard), vahingon (Harm) ja vahingon esiintymisen (HarmContext) yhteyden. (Biggs & Kotoku 2014, 11-15.)

Toinen osio käsittää turvallisuuden mitoituksen (PassiveDefence/ActiveDefence), joka SafeML profiilissa esitetään vaarallisen tilanteen estäjänä (DefenceResult), jotta vaara ei aiheuta vahinkoa. Turvallisuusstandardeissa määritellään käsite vaaratilanteen seuranta. Syynä tähän on se, että turvatoimien ei välttämättä tarvitse olla aktiivisina koko ajan. Näissä tapauksissa järjestelmällä on oltava valmiudet havaita erityistilanne, joka vaatii erityistä turvallisuutta toimenpiteiden aktivoimiseksi. SafeML-profiiliin sisältyy tämä käsite vahingontunnistaja (ContextDetector) elementtinä. (Biggs & Kotoku 2014, 15-18.)

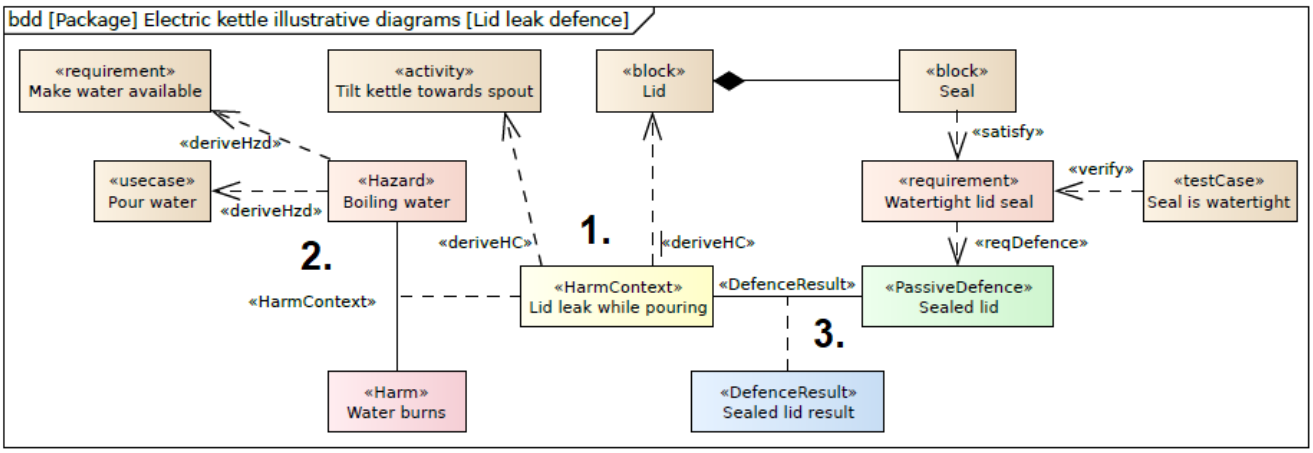


Kuvio 8. SafeML-profiilin elementit liittyen vaaralliseen tapahtumaan (Biggs& Kotoku 2014, 12.)

SafeML-elementtejä sisältävässä mallinnuksessa käytetään myös SysML-profiilista tuttuja elementtejä, kuten vaatimuskaavio (sisältäen myös turvavaatimuksen), käyttötapauskaavio

ja lohkokaavio. Yksinkertaisena esimerkkinä Biggs esittää SafeML-profiilin eri elementtien suhteen vedenkeittimen suojien mallintamisella. (Biggs & Kotoku 2014, 30.)

Ensimmäisenä esimerkkinä kuviossa 9 on vedenkeittimen kannen tiiviste, jolla estetään kuuman veden vuotaminen kaadettaessa:



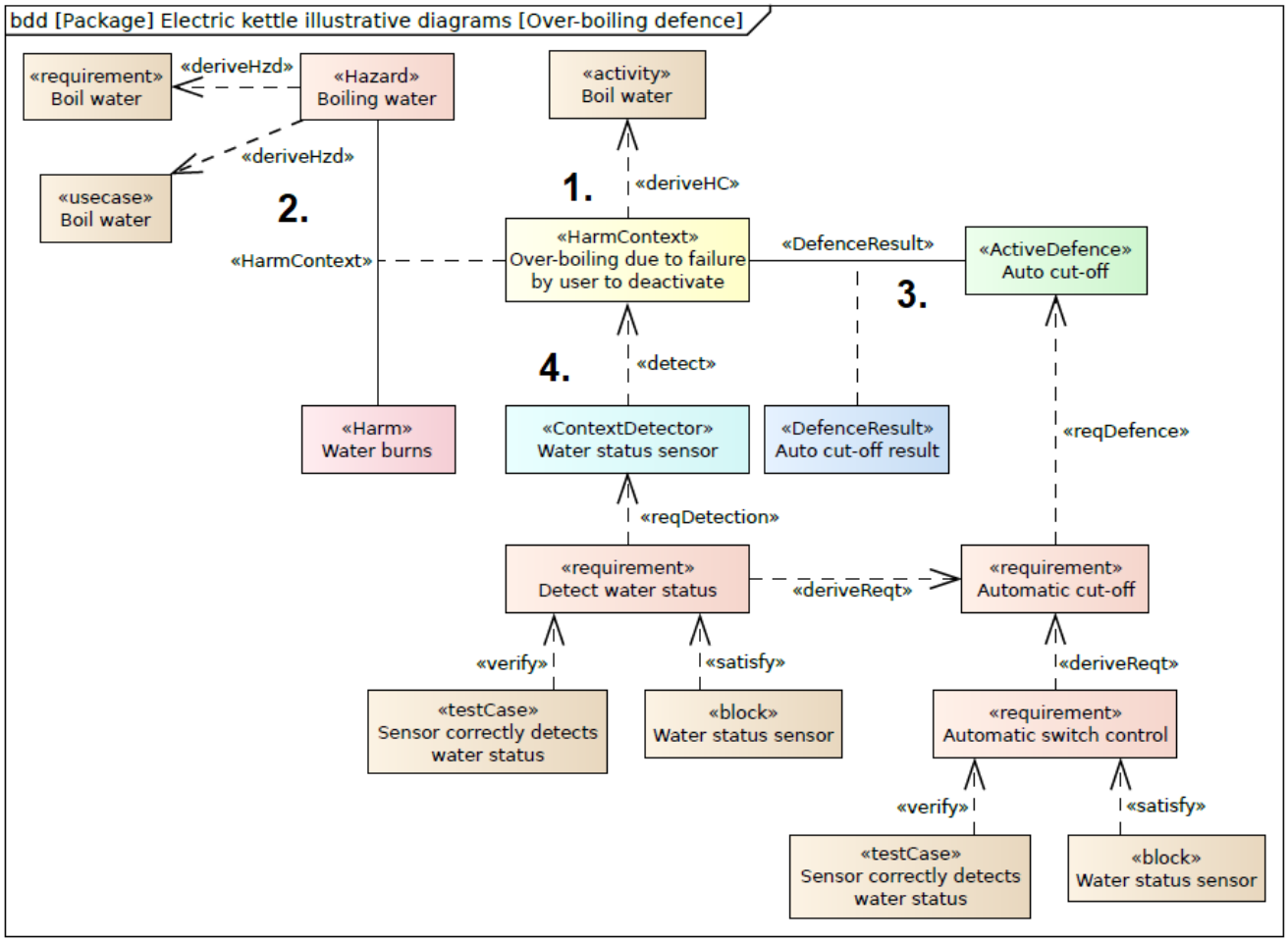
Kuvio 9. Passiivinen suojaus esitettynä SafeML-elementeillä (Biggs & Kotoku 2014, 30).

1. Vahingonyhteytenä (HarmContext) on kansi, joka vuotaa kaadettaessa. Tämä vaatii toimintona keittimen kaatamista nokan suuntaan ja lohkoelementtinä kannen.

2. Vaarana (Hazard) on kiehuva vesi ja vahinkona palovamma (Harm). Vaaran vaatimuksena tietenkin on, että vettä pitää olla keittimessä ja käyttäjä kaataa vettä.

3. Vaarallisen tilanteen suojana (DefenceResult) toimii tiivistetty kansi, joka on passiivinen suoja (PassiveDefence). Suojavaatimuksena tiivisteen on oltava vedenpitävä, joka on todennettu. (Biggs & Kotoku 2014, 29.)

Toisena esimerkkinä on esitettynä kuviossa 10 ylikiehuminen, joka vaatii monimutkaisemman suojan. Suojana on esitettynä automaattinen katkaisu.



Kuvio 10. Aktiivinen suojaus esitettynä SafeML-elementeillä (Biggs & Kotoku 2014, 30.)

1. Vahingonyhteytenä (HarmContext) on ylikiehuminen, joka tapahtuu käyttäjän virheestä. Tämä vaatii toimintona vedenkeittämisen.

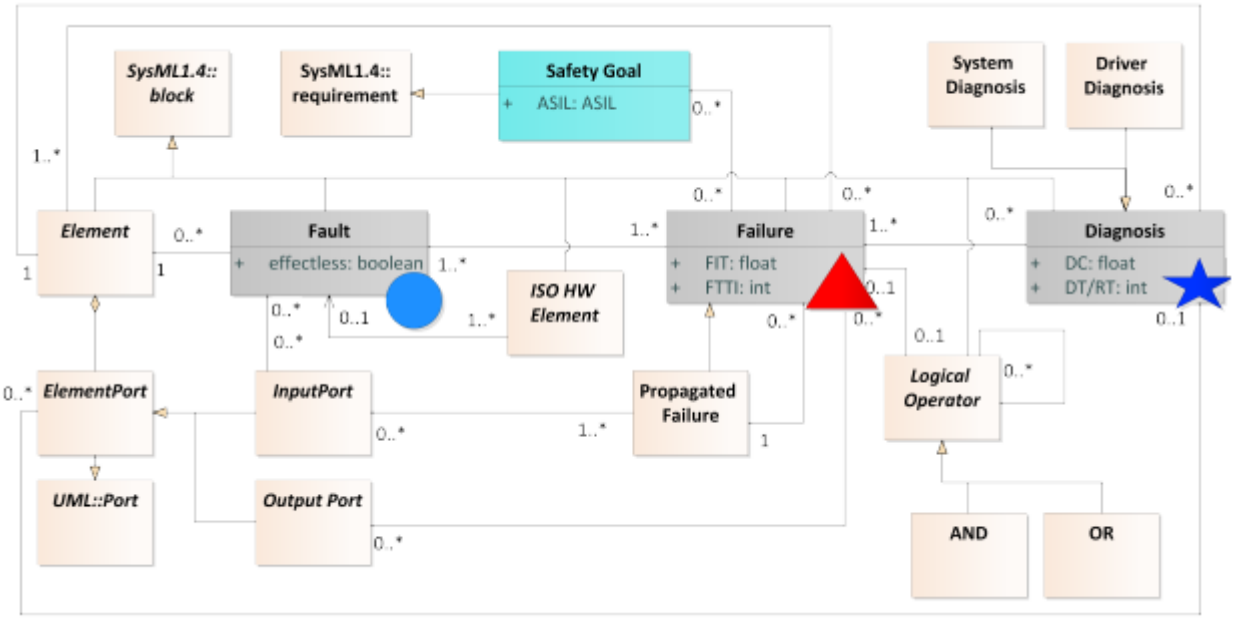
2. Myös tässä vaarana (Hazard) on kiehuva vesi ja vahinkona palovamma (Harm). Vaatimuksena on kiehuva vesi, jota käyttäjä haluaa.

3. Vaarallisen tilanteen suojana (DefenceResult) on automaattinen katkaisu, joka on aktiivinen suoja (ActiveDefence). Suojavaatimuksena on automaattisen katkaisun toiminto, joka toimiakseen vaatii automaattisen kytkintoiminnon. Tämä vaatii veden lämpötilan mittaaja-anturin, joka on todennettu, että se toimii halutulla tavalla.

4. Vahingontunnistajana (Contextdetector) toimii myös veden lämpötilan mittaaja-anturi, joka tunnistaa veden lämpötilan, joka johtaa automaattiseen katkaisuun ylikiehuessa. (Biggs & Kotoku 2014, 31.)

3.7 Vika-analyysin mallintaminen

Gonschorekin mukaan SafeML ainoastaan integroi turvasuunnittelun tulokset mukaan systeemin mallintamiseen. SafeML ei kuitenkaan tue itse varsinaista suunnitteluprosessissa käytävää riskien analysointia. Kun SafeML mahdollisesti integroidaan SysML-profiiliin tulevissa versioissa, Gonschorek toisi mukaan myös suunnittelua tukevan SafeDeML-profiilin elementtejä. Mallin integrointia varten esitellään neljä peruselementtiä: virhe (Fault), vika (Failure), diagnosointi (Diagnosis) ja turvan päämäärä (Safety Goal) laajennuksina SysML-profiiliin. (IMBSA 2019, 97.)



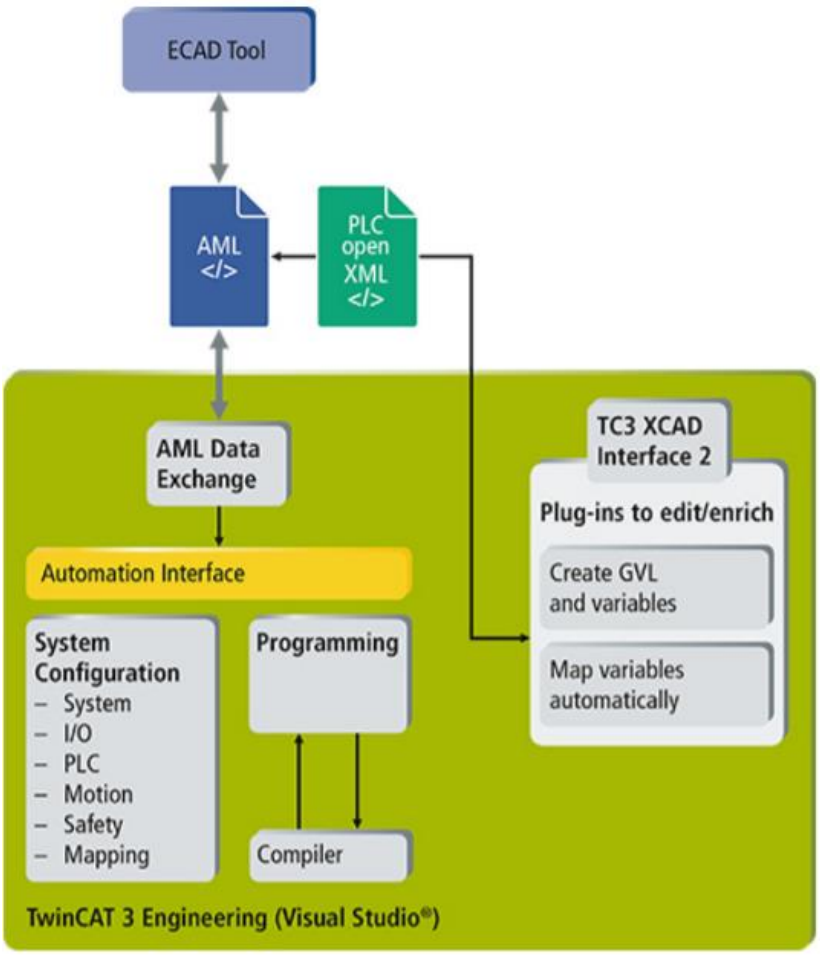
Kuvio 11. SafedeML-elementit (IMBSA 2019, 96).

SafedeML on kehitetty enemmänkin tukemaan autoteollisuuden standardia ISO 26262. Nykyajan autot ovat niin monimutkaisia, että auton eri järjestelmien osien mahdolliset viat on mallinnettava. (IMBSA 2019, 95.)

3.8 AutomationML

AutomationML (Automation Markup Language) on avoin xml-pohjainen standardi, joka perustuu digitaalisen tehtaan tuomaan käsitteeseen. Sen tarkoituksena on kytkeä yhteen epäyhtenäinen valmistavan teollisuuden automaation laitteisto siten, että todellisen tehtaan komponentit esitetään niiden luonnetta kuvastavina objekteina. Tyypilliset objektit sisältävät informaatiota topologiasta, geometriasta, liikkumisesta ja logiikoista. (Collin & Saarelainen 2016.)

Myös turvajärjestelmien objekteja on mahdollista siirtää suunnittelusovellusten välillä. Esimerkkinä Beckhoff tajoaa TwinCat 3 -PLC-ohjelmistoon TC3 XCAD -rajapintalaajennusta, jonka avulla pystytään siirtämään automationML-kieltä tukevasta sähkösuunnitteluohjelmistosta valmis HW-konfiguraatio PLC-ohjelmointiympäristöön (Beckhoff, [viitattu 23.3.2021]).



Kuvio 12. AutomationML-rajapinta (Beckhoff, [viitattu 23.3.2021])

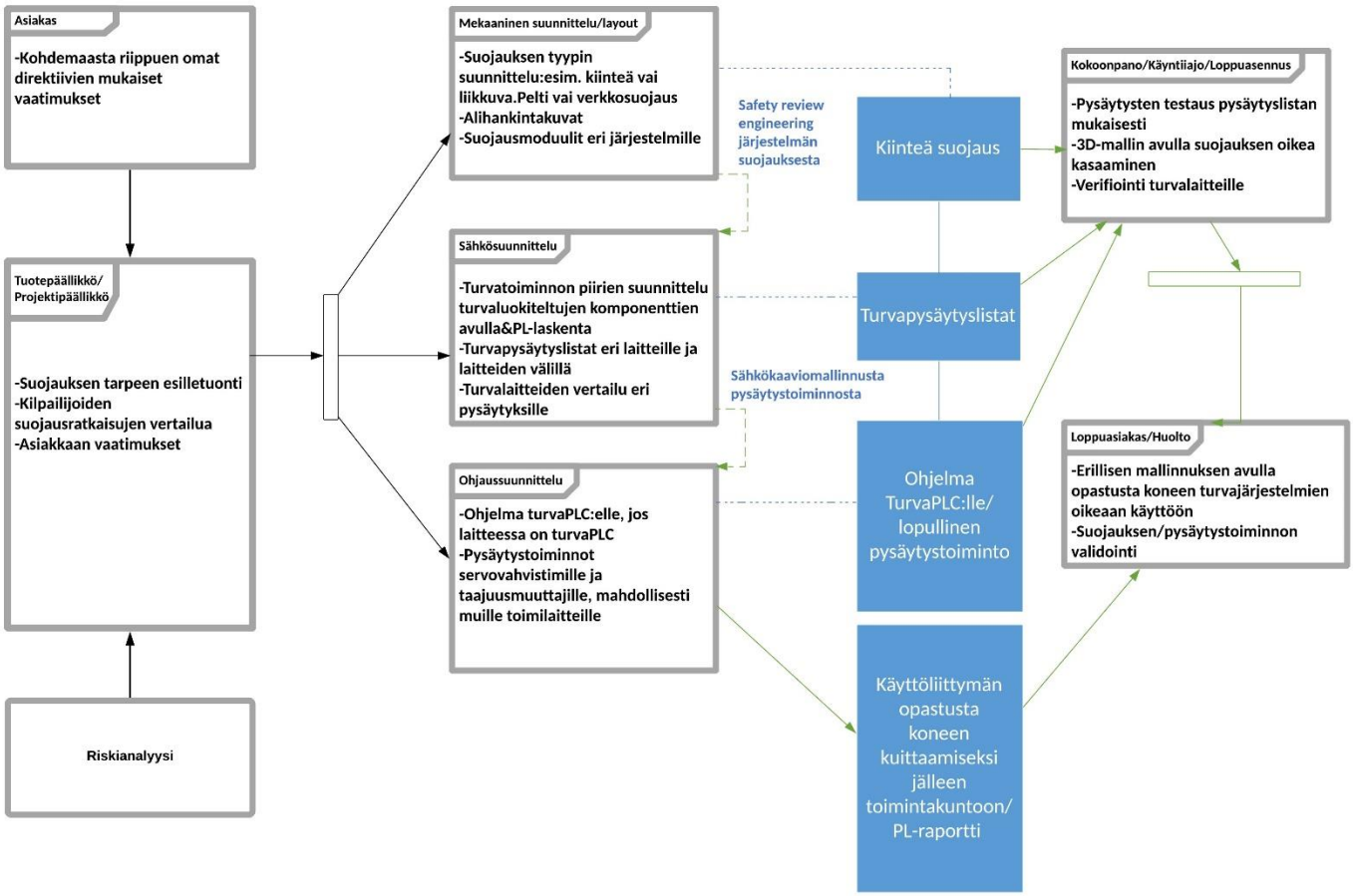
XCAD-rajapintalaajennus lukee tiedon luodusta XML-tiedostosta ja luo TwinCAT 3-projektin, joka sisältää elementtejä I/O-konfiguraatiosta, sisältäen kaikki I/O- ja NC-laitteet muuttujineen. Lisäksi I/O-parametrien linkit PLC-ohjelmalle ovat valmiina määriteltynä. (Beckhoff, [viitattu 23.3.2021])

AutomationML-kielen vahvuutena on siis alakohtainen ja yksityiskohtainen suunnittelu sekä siihen liittyvän tiedon mallintaminen. SysML-kieli soveltuu paremminkin korkean tason systeemisuunnitteluun.

4 Tutkimusmenetelmä ja aineisto

4.1 Nykytilanne

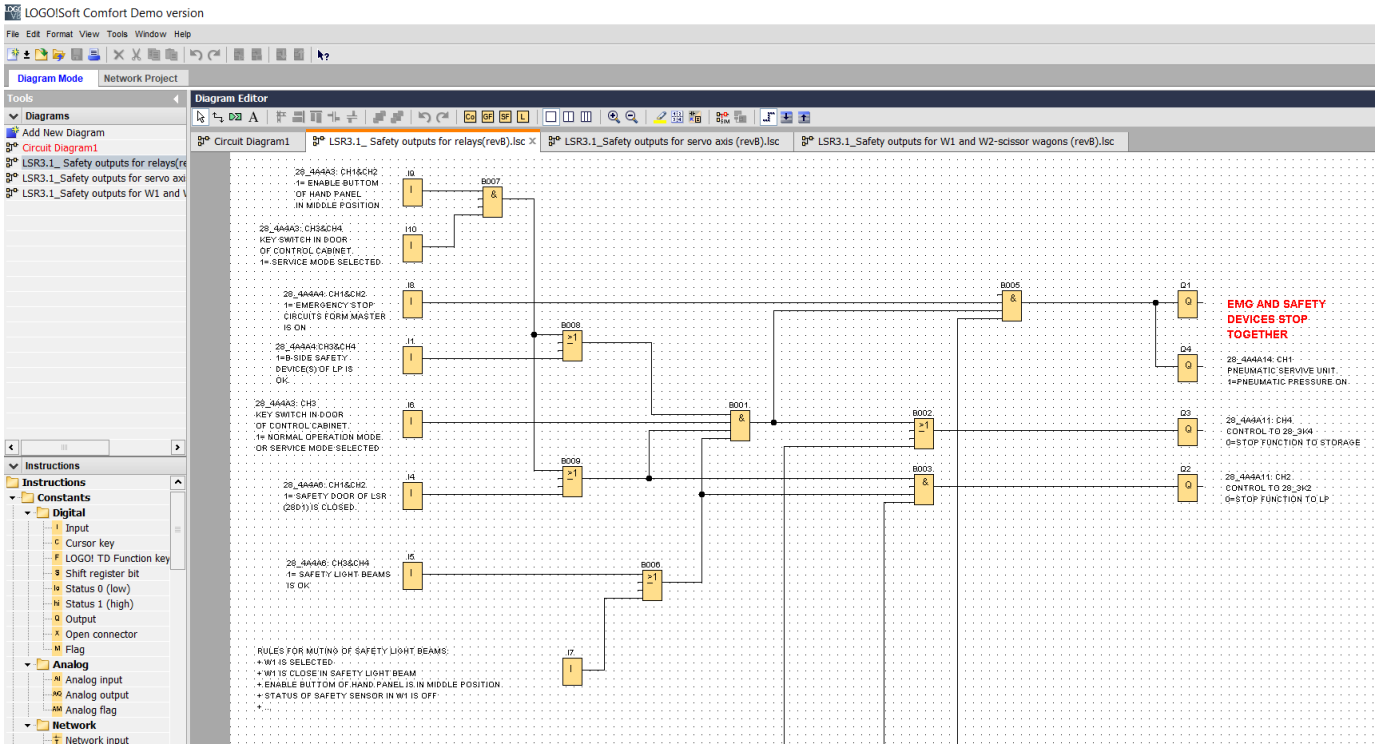
Finn-Powerin tuotekehityksen turvallisuuden suunnitteluprosessi on esitettynä kuviossa 13.



Kuvio 13. Finn-Power Oy tuotekehityksen prosessi suojaukselle

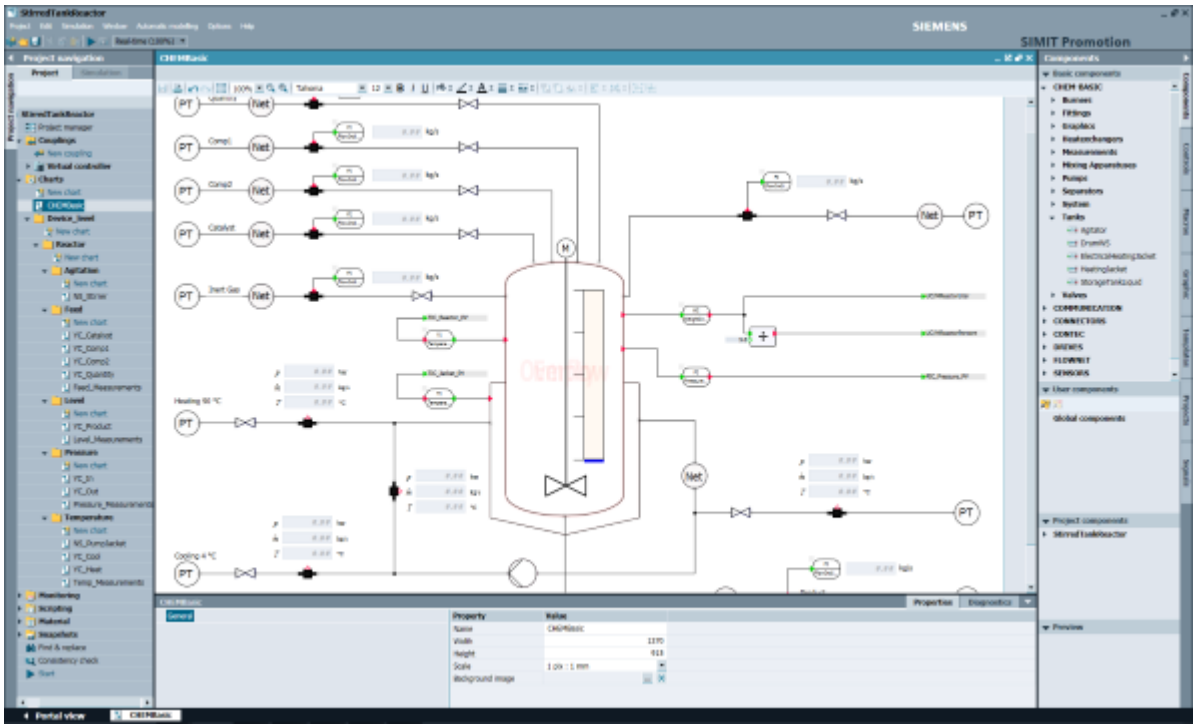
Tarkempaa mallinnusta turvavaatimuksesta tai toiminnoista ei käytännössä ole. Sähkösuunnittelu ja mekaniikkasuunnittelu laativat suunnittelun aikana yhteistyössä safety review engineering-dokumentin, johon on koottu tilattavat rakenteet asiakaskohtaista suojausta varten. Dokumentti on laajentunut nykyään käytettäväksi myös loppuasennukselle, kun asentajat haluavat selvittää suojausten suunniteltua asennusta. Sähkösuunnittelun ja ohjaussuunnittelun välillä on mallintamisen keinona periaatteessa ainoastaan laitekohtaiset sähkökuvat. Osassa laitteiden ohjauksessa on mukana

turvalogiikkaa, jonka turvapiiriä sähkösuunnittelu on alustavasti mallintanut tikapuukaavion avulla Siemensin kehittämällä ilmaisohjelmalla Logo!.



Kuva 3. Logo!-demo-ohjelmisto

Ohjaussuunnittelussa on koulutustarkoitukseen kehitetty simulointiohjelmiston Simitin avulla konelayoutin pohjalle mallinnus. Simuloidut turvatulot on emulaattorin kautta yhdistetty todelliseen PLC-kokoonpanoon. Beckhoffin ohjaimilta saa yhteyden Simitiin ainoastaan OPC UA-rajapinnan kautta. Testauksen simulointia on yritetty myös yhdistämällä Solidworks-suunnitteluohjelmalla luotua 3D-mallia Beckhoffin ohjaukseen. Tämän digitaalisen kaksosen luominen on hyvin alkutekijöissään.



Kuva 4. Simit-simulaattori (Siemens 2017)

4.2 Avoin haastattelu ja kysely

Haastattelulla tietoa kerätään tutkimuskysymyksiin:

- Mikä olisi paras tapa mallintaa turvatoimintoja?
- Millä tavalla nyt on mallinnettu turvatoiminnalisuutta?
- Voisiko nykyistä mallia kehittää palvelemaan useampaa sidosryhmää?

Kvalitatiivisen tutkimuksessa haastattelu on päämenetelmänä tiedonkeruussa. Haastattelun suurena etuna verrattuna muihin tiedonkeruumuotoihin on, että siinä voidaan säädellä aineiston keruuta joustavasti tilanteen edellyttämällä tavalla. Haastattelusta saatavasta aineistosta on mahdollisuuksia enemmän tulkita vastauksia kuin kyselystä. Tutkimuksen haastattelumuotona käytettiin avointa haastattelua. Avoimessa haastattelussa selvitetään asiantuntija haastateltavan ajatuksia, mielipiteitä, tunteita ja käsityksiä sen mukaan, kuin ne tulevat aidosti vastaan keskustelun kuluessa. (Hirsjärvi, Remes, Sajavaara & Sinivuori 2009,205-209.) Avoimet haastattelut toteutettiin parihaastatteluina. Tutkimuksen

alkuvaiheessa esiteltiin turvatoiminnon mallintamisen menetelmiä sähkösuunnitteluosaston esimiehelle ja pääsuunnittelijalle. Kun mallintamisessa oli edetty valitulla ohjelmalla, lopuksi haastateltiin ohjaussuunnittelun kahta pääsuunnittelijaa tulosten esittelyn jälkeen. Avoimessa haastattelussa sähkösuunnitteluosaston esimiehen ja pääsuunnittelijan kanssa esiin nousivat seuraavat turvatoiminnon mallintamiseen liittyvät asiat:

- Mallinnussovellukseen olisi hyvä saada simulointi mukaan ja sillä pitää saada kuvattua laajakin järjestelmä, vaikka erillisinä osina
- Sovelluksen tulisi olla helppo, nopea ja havainnollinen käyttää dokumentin luomisessa
- Mallin tulisi olla riittävän havainnollinen lopputuloksen (testaustuloksen) esittämiseen
- Toiminnon mallintamisen täytyisi olla yleiskattava ja mallissa ei eriteltäisi, että onko turvatoiminnon toteuttajana turvarele tai turvalogiikka
- Turvapiirien toimintakuvaus olisi hyvä olla asiakkaan ymmärtämällä kielellä

Lisäksi simulointi pitäisi olla aluksi yksinkertaistettu eli ei ole tarvetta saada jokaista kuittauspainiketta ja paneelin toiminnallisuutta esiin. Turvatoiminnallisuuden lisäksi halutaan myös simuloida energiansyötöistä erottamista, koska tulevaisuudessa useammin laajempikin linjasto on oltava eroteltavissa eri työstösoluihin, joita voidaan käyttää muun linjaston osien ollessa huollossa. Esille tuli myös, että turvalaitteiden vikaantumista ei olla erikseen dokumentoitu, koska ne täyttävät luokkansa vaatimukset ja vikaantuvat turvallisesti. Ohjelmistovirheet luokitellaan samoin, eli softaa valvotaan redundanttisesti.

Ohjaussuunnittelijoiden haastattelussa esille nousi tarve rajapintojen mallintamisesta eri laitteiden välillä eli kuinka laajasti turvatoiminto vaikuttaa. Ohjaussuunnitellussa ei ole hyödynnetty mallintamista aikaisemmin kuin lähinnä tikapuumallilla huoltoa varten. Asiakkaalle ei ole tarvinnut lähettää turvalogiikan ohjelmasta raporttia kuin erittäin harvoin.

Järjestelmien kehittämisen aikainen kommunikaatio on tehokkainta kasvokkain. Nyt kuitenkin vallitsevassa tilanteessa suunnittelijat ovat joutuneet siirtymään pääosin etätyöskentelyyn. Tulevaisuudessa pandemian loputtuakin, etätyö muuttuu enemmän uudeksi normaaliksi tietoliikenneyhteyksien nopeutuessa ja toisaalta ylimääräistä autolla liikkumista halutaan

vähentää. Tulevaisuuden turvatoimintojen suunnittelun prosessia ja mallinnustyökalun määrittelyä lähdettiin kartoittamaan verkkokyselyllä nykytilannetta. Kyselyn avulla kerättiin tietoa tutkimuskysymykseen: Kuinka mallinnusta ylläpidettäisiin järjestelmän elinkaaren ajan?

Kyselytutkimus on laajimmin levinnyt muoto hankkia sellainen tutkimusaineisto, joka kuvaa laajojen joukkojen käsityksiä, mielipiteitä, asenteita jne. Aineistosta pidemmälle analysoitua tietoa voidaan käyttää edelleen yksityiskohtaisempiin tutkimuksiin johtavana lähtökohtatietona ja yleensä kuvaamaan, mitä johonkin ilmiöön sisältyy, missä määrin sitä ilmenee ja missä yhteydessä se esiintyy. Lopullinen kyselylomake pidettiin niin lyhyenä ja suoraviivaisena kuin mahdollista. Kyselyssä käytetään suljettuja kysymyksiä, koska tutkimuksessa halutaan tilastollisesti mitattavissa olevaa tietoa. Suljettujen kysymysten suurin hankaluus on siinä, että tämän tutkimustyön tekijällä on kysymyksiä laatiessa jo selkeä näkemys aiheesta ja siitä, kuinka kysymykset liittyvät tutkimuskysymykseen yleensä. (Anttila 2014)

Kysely toteutettiin Google Forms kyselynhallintaohjelmistolla ja kysely lähetettiin Finn-Powerin sähkösuunnitteluosaston 8 henkilölle. Kyselyn kysymykset olivat seuraavat:

1. Onko laitekohtaisen uuden suojauksen turvallisuusvaatimukset selkeitä sähkösuunnittelun alusta alkaen?

2. Onko mielestäsi suunnittelun aikainen tiedonkulku eri osastojen välillä etätyössä yhtä tehokasta kuin toimistolla?

3. Onko mielestäsi etätyöskentelyn aikana tiedon jäljitettävyys myös selkeää koko valmistusprosessin ajan liittyen laitekohtaiseen suojaukseen ja turvatoimintoon?

4. Onko mielestäsi suojauksien ja turvatoimintojen suunnittelun aikana usein tiedonhukkaa eli epäselvyyttä oikeasta tiedonlähteestä?

5. Löydätkö helposti jo toteutuneita ratkaisuja, joita voi käyttää uuden suunnittelun pohjana?

6. Mitä tiedonlähdettä käytät useimmin jo toteutuneiden suojausratkaisujen tiedon etsimiseen?

7. Sähkösuunnittelutehtävän jälkeen, tuleeko jälkikäteen yleensä muutoksia jo kertaalleen suunniteltuun turvatoimintoon, esimerkiksi: kolmannen osapuolen laitteen rajapinnalle?

8. Onko mielestäsi turvapysäytyslista yleensä tarpeeksi havainnollinen pysäytystoiminnon todentamiseen?

Kyselyyn vastasi 7 henkilöä. Vastausten jakautuminen on tämän opinnäytetyön liitteessä 1. Kyselystä kävi ilmi seuraavat asiat tiivistetysti:

- Uuden suojauksen vaatimukset ovat osittain selkeitä suunnittelun alusta alkaen.

- Etätyöskentelyn aikainen kommunikaation tehokkuus verrattuna toimistolla olemiseen jakautui tasaisesti puolesta ja vastaan.

- Suunnitellun turvatoiminnon tiedon jäljitettävyys on selkeää suurilta osin.

- Tiedonhukkaa liittyen turvatoiminnon suunnitteluun on toisinaan. Tätä kysymystä olisi voinut tarkentaa koskemaan täysin uuden turvatoiminnon suunnittelua. Suunnittelun alussa tietoa löydetään edellisistä jo toteutuneista ratkaisuista.

- Jo toteutuneiden suojaratkaisujen tietoja löydetään helposti.

- Jo toteutuneiden suojausratkaisujen tiedon etsimiseen käytetään tehtävienhallintaohjelmisto Jiraa ja tämän lisäksi voidaan kysyä toiselta suunnittelijalta.

- Selkein vastaus tuli jo uuden toiminnon suunnittelutehtävän jälkeiseen muutostarpeeseen, melkein aina näin joutuu tekemään. Kysymyksessä tosin oli esimerkkinä mainittu liittyvä kolmannen osapuolen laite, joka aiheuttaa usein jälkikäteen muutosta. Kolmannen osapuolen laitteen vakiorajapintadokumenttien tekeminen on osastolla vielä työn alla. Tarkennuksena kysymys olisi pitänyt jakaa koskemaan Prima Power-laitetta ja kolmannen osapuolen laitetta.

- Sähkösuunnitteluosaston tekemää turvapysäytyslistaa testaajaa varten pidettiin havainnollisena.

Tiedonhukka ja suunnittelun jälkeinen muutostarve nousivat kyselyn perusteella ongelmakohdiksi turvatoiminnon suunnitteluprosessissa. Muutostarpeet liittyvät myös olennaisesti suunnittelun määrittelyyn. Jos uusi turvallisuuteen liittyvä kehityskohde on määritelty kunnolla dokumentoiden, niin muutoksia tuskin ilmenee. Tutkimukseen lähdettäessä simulointia oli tarkoitus hyödyntää mahdollisesti myös turvatoiminnon todentamisen työkaluna, joka korvaisi testauksen pysäytyslistat. Tätä ei kuitenkaan kyselyn perusteella nähdä tarpeellisena. Mallintamista ja simulointia halutaan käyttää enemmän suunnittelun tukena ja mahdollisesti asiakkaalle määritellyn toiminnon esittämisenä. Prosessin kannalta mallinnusohjelmisto olisi luontevinta olla integroituna Jira-ohjelmistoon. Tätä tukee myös asentajien ja käyntiinajajien tottuminen Jiran käyttämiseen ja sieltä asiakasprojektien tietojen etsimiseen.

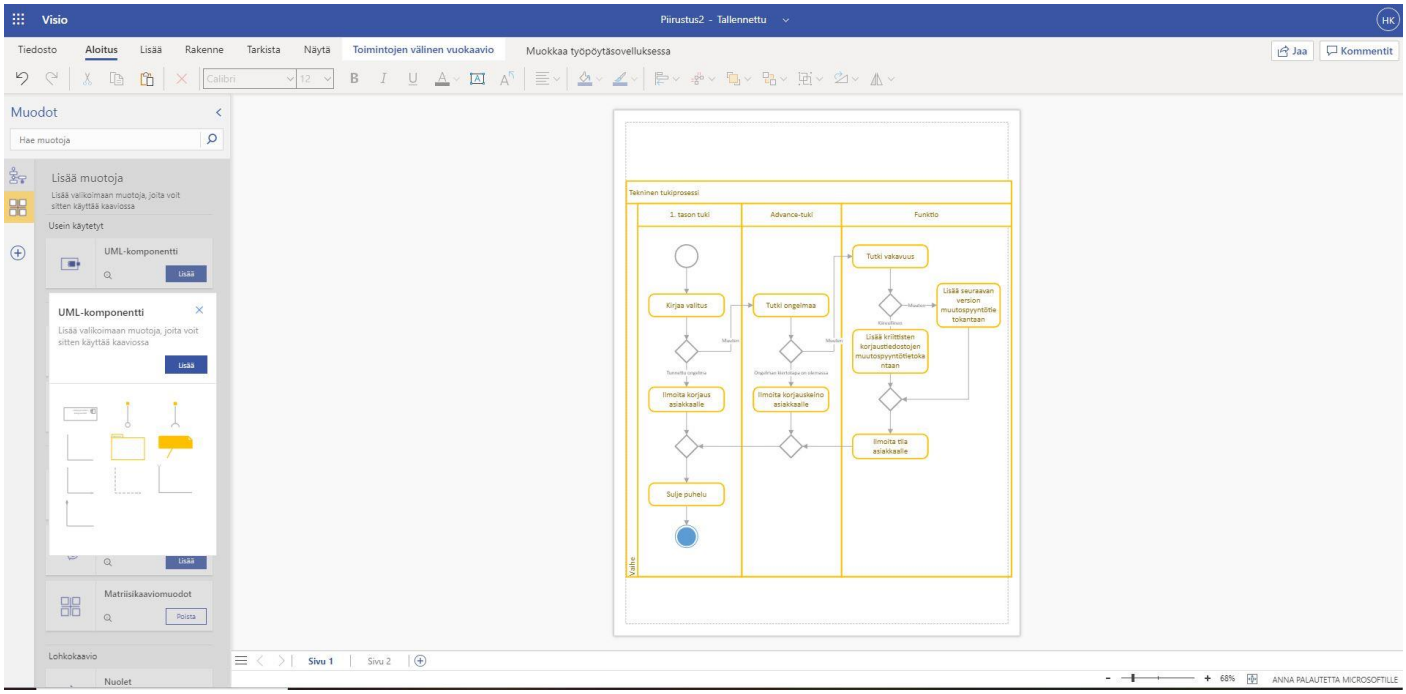
4.3 Mallinnussovellusten vertailu

Tässä työssä vertailuun otetaan mallinnussovelluksia, joita voidaan käyttää selaimessa. Verkossa voidaan tarkastella, luoda ja muokata pilvipalveluun tallennettuja kaavioita. Tutkimuskyselyn perusteella myös mallinnusohjelman integroiminen Jira-tehtävienhallintaohjelmistoon on olennaista. Yhteistä tarkasteltavissa kaaviosovelluksissa on, että niiden avulla pystyy mallintamaan:

- Vuokaaviot
- UML/SysML-kaaviot
- ERD (Entity Relationship) -kaaviot
- Verkkokaaviot
- Liiketoimintamallit
- Organisaatiokaaviot
- Elektroniset piirit
- Rautalankamallintaminen ja simulaatiot.

4.3.1 Microsoft Visio Online

Microsoft Visio (aikaisemmin Microsoft Office Visio) on Microsoftin kehittämä 2D-objekti-piirustusohjelma, joka on osa Microsoft Officea. Verkkosovellus sisältyy Vision palvelupaketteihin 1 ja 2. Projektien tallennus suoraan on mahdollista ainoastaan OneDrive-tiedosto säilytyspalveluun ja Visio Onlinen saa laajennusosana ainoastaan Office365-pilvipohjaiseen palvelukokonaisuuteen. (Microsoft, [viitattu 3.4.2021].) Visio Onlinessa oli suppea valmiiden mallien ja kaaviopohjien kirjasto. Lisäksi Visio Onlinella ei ole integroitavaa laajennussovellusta Jira-tehtävienhallintaohjelmistoon.

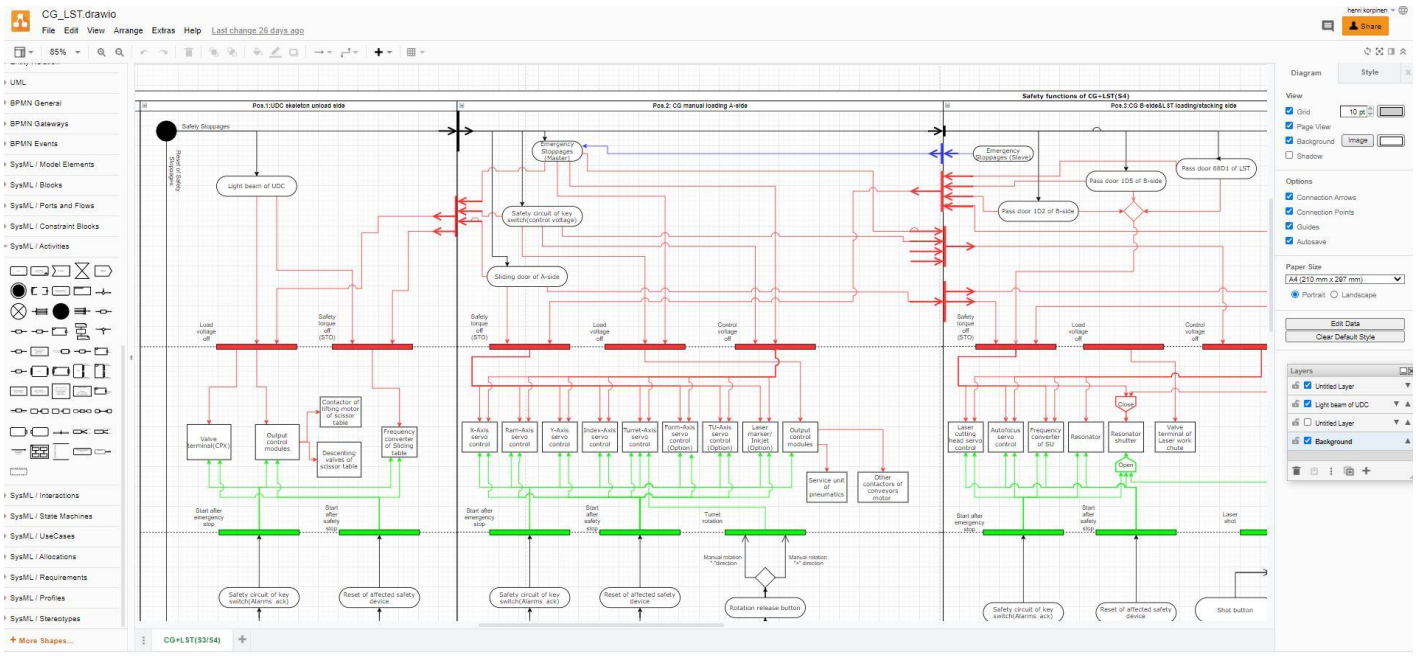


Kuva 5. Microsoft Visio Online

4.3.2 Diagrams.net

Diagrams.net (aikaisemmin draw.io) on kokonaan ilmainen ja maailman eniten käytetty verkossa toimiva kaavio-ohjelma. Ohjelman kehittäjänä toimii //SEIBERT/MEDIA, joka on organisaatio-ohjelmistoja tekevä yrityksen Atlassianin suurimpia yhteistyöyrityksiä. Atlassian on kehittänyt Jira-tehtävienhallintaohjelmiston, joten Diagrams.net-ohjelman saa myös integroitua maksullisesti Jiraan. (Atlassian Marketplace, [viitattu 3.4.2021].) Diagrams.Net tarjoaa laajasti elementtikirjastoja ja valmiita kaavioita. Diagrams.net-ohjelman saa myös ladattua työpöytäsovelluksena. Interaktiivisten mallien tekeminen ei testaamisen aikana

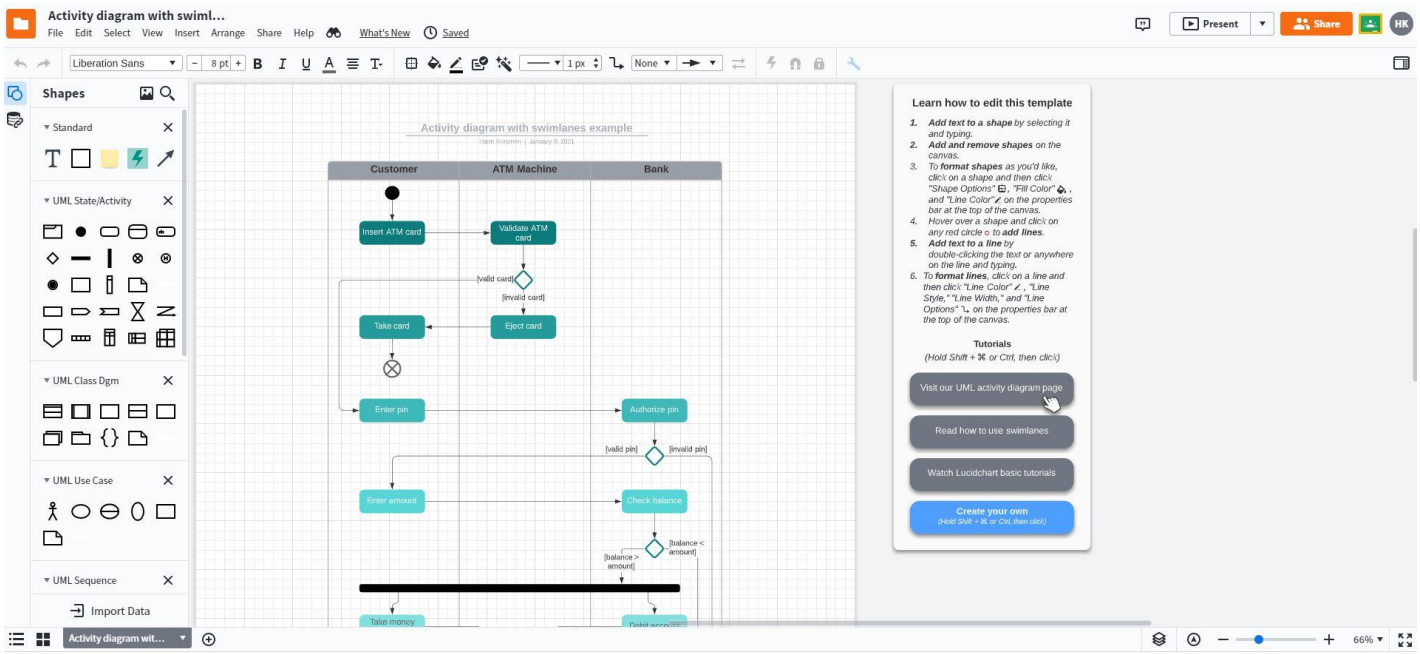
kuitenkaan ollut helppoa, koska ohjelmasta ei löydy valmista toimintoa tälle, vaan mallien datakenttään piti kirjoittaa JSON-formaatin mukainen koodi ennen kuin sai muutettua esimerkiksi mallin näkyvyyttä eri tasoille.



Kuva 6. Diagrams.net

4.3.3 Lucidchart

Lucidchart-ohjelmisto on Lucid Software Inc. kehittämä. LucidChart toimii selaimessa, joka tukee HTML5-merkintäkieltä, eli se ei vaadi erillisiä päivityksiä kolmannen osapuolen ohjelmistoilta kuten Adobe Flashilta. Lucidchart työpöytäohjelman saa ladattua Google Apps MarketPlacesta. LucidChart on maksullinen ja LucidChartin saa integroitua Jiraan maksua vastaan. (Google Workspace Marketplace, [viitattu 3.4.2021].) LucidChart on kaikista tutkimuksen aikana verratuista ohjelmista käyttäjäystävällisin. Ohjelmassa on myös hyvin laaja kirjasto ja runsas määrä valmiita kaaviopohjia. Oman kirjaston luominen on helppoa. Myös interaktiivisten mallien tekeminen oli helppoa ohjelmiston valmiin toiminnon myötä. Tosin toiminnolla pystyi ainoastaan piilottamaan ja vaihtamaan elementtejä eri kerroksilta toiselle, enemmänkin toiminnallista esittämistä ja simulaatiota voisi olla.



Kuva 7. Lucidchart

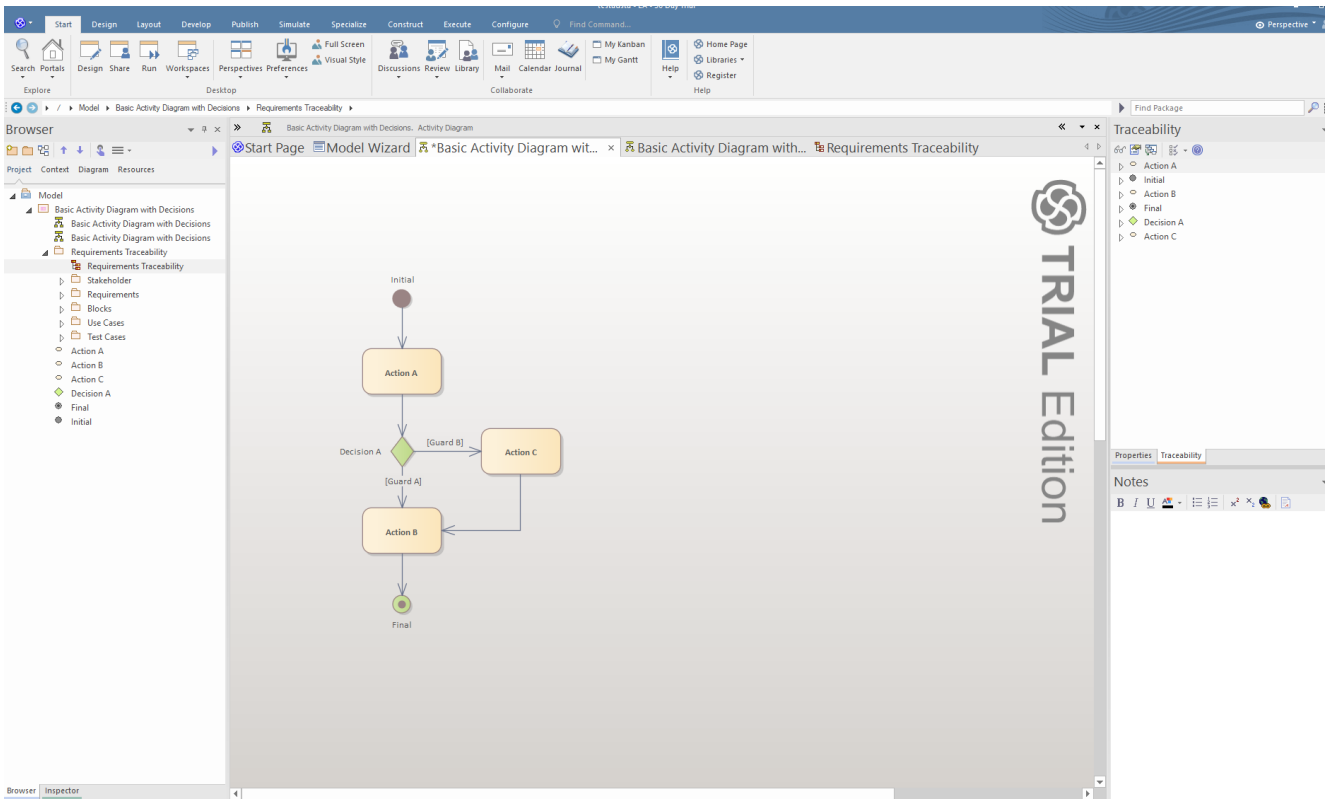
4.3.4 Enterprise Architect

Sparx Systems, joka on jäsenenä Object Management Group (OMG) -konsortiossa, on kehittänyt Enterprise Architectin. Vuonna 2006 yhtiö oli ensimmäisten valmistajien mukana tukemassa OMG:n kehittämää SysML-kieltä. (Sparx systems, [viitattu 3.4.2021].) Enterprise Architect -ohjelmaa pystyy käyttämään ilman rajoituksia kuukauden ajan, jonka jälkeen ohjelma on maksullinen. Ohjelmasta on saatavilla corporate-, unified-, professional- ja ultimate-lisenssit. Lisensseissä on eri määrä ominaisuuksia tarjolla, unified-lisenssi tarjoaa eniten vastinetta järjestelmän suunnittelijalle. Enterprise architect on kaikista verratuista sovelluksista kallein.

Enterprise Architect-ohjelma on työpöytäsovellus, mutta WebEAn, joka toimii osana Sparx Systems Pro Cloud Server -pilvilpalvelua, avulla valmiita mallinnuksia pystyy reaaliaikaisesti jakamaan verkkoon. Sparx Systems Pro Cloud Server- pilvilpalvelussa on mukana myös Prolaborate-työkalu, jonka avulla Enterprise Architect-ohjelman mallit saa linkitettyä Jiraan. (Sparx systems, [viitattu 3.4.2021].)

Käyttöliittymältään Enterprise Architect muistuttaa Microsoft Visiota. Ohjelman käyttäminen vaati eniten opettelua tutkimuksessa mukana olleista ohjelmista. Elementtikirjasto ei ole kovin

havainnollinen ja esimerkiksi elementin kopioiminen samaan kaavioon ei ole mahdollista, vaan jokainen elementti täytyy erikseen luoda kaavioon. Pohjakaavioita on kuitenkin runsaasti. Simulaatiotoimintoa pystyy käyttämään toimintaa kuvaavissa kaavioissa, joissa simulaatio etenee esittäen kaavion elementit totetutussuhteiden kautta. Tämä toiminto on enemmänkin tarkistusta varten kaavion laatijalle kuin kaavion lukijalle.



Kuva 8. Enterprise architect

5 Turvatoimintojen mallintaminen

5.1 Turvavyöhykkeiden määrittely

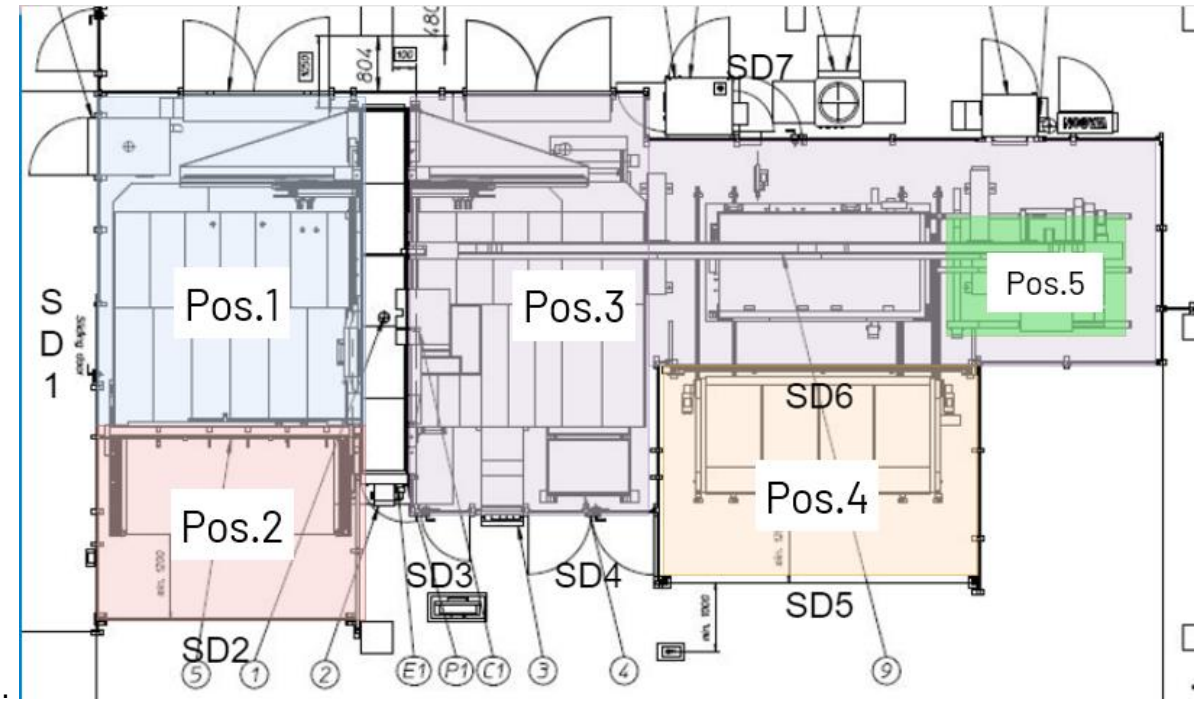
Sovelluksista käyttöön otettiin Lucidchart käyttäjäystävällisyyden ja toiminnallisuuden rakentamisen helppouden vuoksi. Tutkimuksessa käytetään mallintamisen esimerkkinä koneyhdistelmää CombiGenius-työstökonetta, jossa on liitettynä LST-lastaus/pinontarobotti. Ennen turvatoimintojen mallinnusta eri suojaukset on hyvä määritellä eri luokkiin, eli A-, B- ja C-suojauksiin:

- A-suojausprojektit olisivat yksinkertaiset standalone-koneet suppealla automaatiolla, ovat aina ns. vakiosuojauksia. A-suojausprojektille tehtäisiin vain kerran mallinnus turvatoiminnoista laitteen elinkaaren alussa.

- B-suojausprojektit olisivat combi-koneet laajemmalla automaatiolla ja mahdollisesti varastoon liitettynä. Vakio-B-suojausprojektille tehtäisiin kerran mallinnus turvatoiminnoista ja tarkistettaisiin asiakasprojektien kohdalla mallinnuksen päivityksen tarve

- C-suojausprojektit olisivat monimutkaisia useamman linjaston suojausjärjestelmiä. C-suojausprojekteille tehtäisiin aina oma asiakaskohtainen turvatoimintojen mallintaminen

CombiGenius +LST olisi B-suojausprojekti, josta voisi syntyä vakiosuojaus.



Kuva 9. CombiGeniuksen turvavyöhykkeet

Kuvassa 9 on esitettynä CombiGenius+LST layoutin turvavyöhykkeet. Aluksi layoutin pohjalle määritellään turvavyöhykkeet standardin SFS-EN ISO 12100 mukaisesti selkeästi esitettynä ja annetaan sijaintinumero. Jokainen turvalaite on myös merkitty SD (safety device)-merkinnällä ja jokaisella turvalaitteella on oma numero.

Taulukko 1. Turvavyöhykkeet

Position	Description
Pos. 1	CG manual load A-side
Pos. 2	UDC skeleton unload side
Pos. 3	CG B-side&LST loading/stacking side
Pos. 4	Load/Unload wagon area
Pos. 5	LST Gripper

Taulukko 2. Turvalaitteet

Safety device	Description
SD1	Sliding door 1D1 of A-side
SD2	Light beam of UDC
SD3	Pass door 1D2 of B-side
SD4	Pass door 1D5 of B-side
SD5	Light beam of Unload/load wagon
SD6	Lifting door of Unload/load wagon
SD7	Pass door 68D1 of LST

Lopuksi voidaan taulukoida pysäytysten vaatimukset turvavyöhykkeiden välillä.

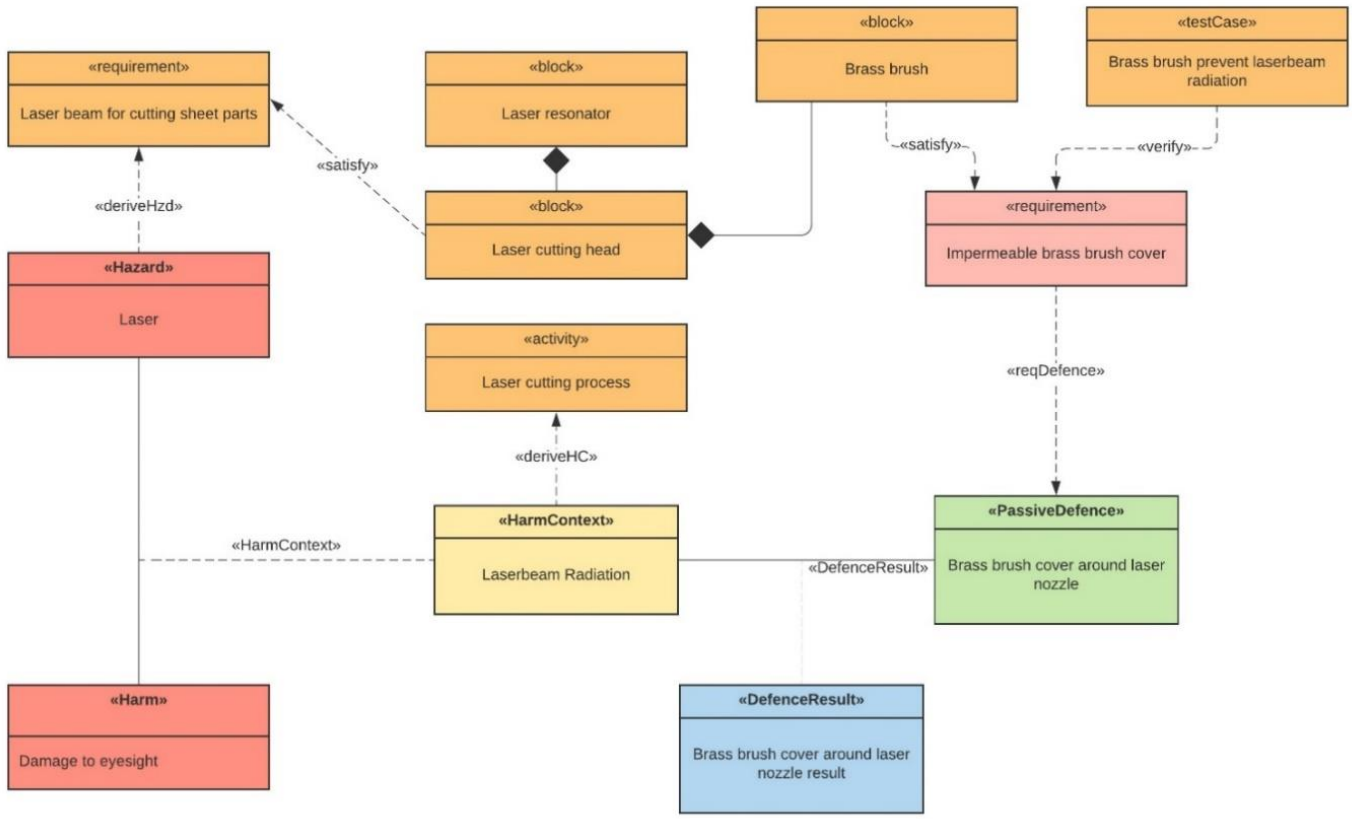
Taulukko 3. Turvavyöhykkeiden pysäytykset

Tripped safety device	Safety zone stop	Notice!
SD1	Pos. 1 + Pos. 5	
SD2	Pos. 2	
SD3	Pos. 3 + Pos. 5	SD6 will close
SD4	Pos. 3 + Pos. 5	SD6 will close
SD5	Pos. 4	If SD6 open Then also Pos.3 and Pos.5 will stop
SD6	-	If also SD5 or SD3/SD4 tripped then Pos.3, Pos, 5 and Pos. 4 will stop
SD7	Pos.3+Pos. 5	SD6 will close

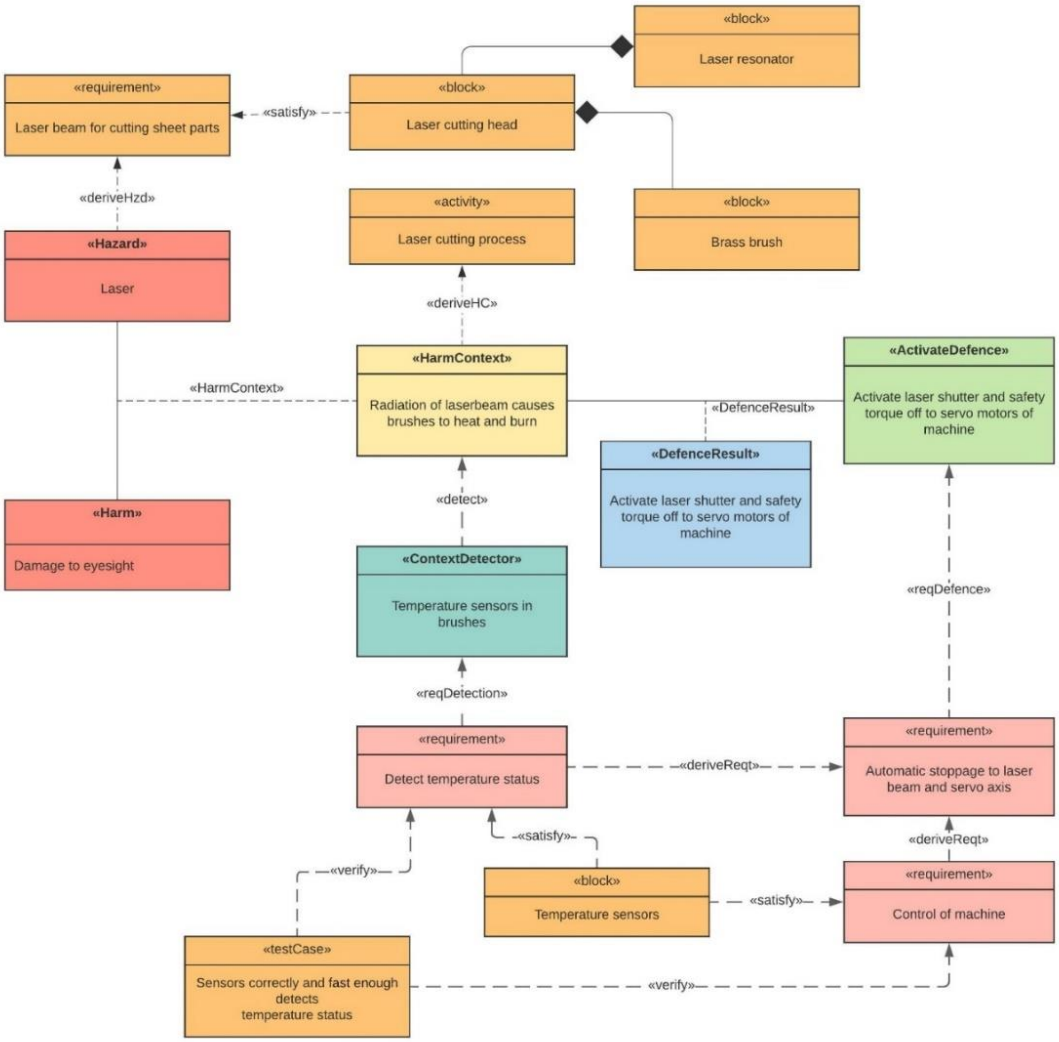
5.2 Turvavaatimusten määrittely

Riskianalyysin Excel-tiedostosta mallinnetaan haluttuja elementtejä SafeML-profiilin mukaan. CombiGeniukselta otettiin esimerkkinä leikkuupää, jossa on sekä passiivinen ja aktiivinen suojaus. Leikkuupään lasersäde voi heijastuessaan aiheuttaa pysyviä silmävammoja. Passiivisena suojauksena toimii leikkuusäteen ympärillä sisin messinkiharjas-suojakerros, jonka ensisijainen tehtävä on suojata ulompia suojakerroksia kuumuudelta ja työstöstä aiheutuvilta roiskeilta. Suojauksen toissijainen tehtävä on pitää säteilyä mahdollisimman paljon sisällä, mutta tämän lisäksi tarvitaan myös muutakin näkösuojaa.

Yhtenä aktiivisena suojana leikkuupäässä toimivat lämpötilasensorit, joiden on reagoitava ympäröivään ilmaan nopeasti. Mikäli säde virhetilanteessa kohdistuisi kohti harjaksia muodosta tai irtokappaleesta heijastuneena, olisi säteen kohdistusaika harjaksiin lyhytaikainen. Tällöin lämpötilasensorin on ehdittävä havaita harjaksiin kohdistuva säde nopeasti.



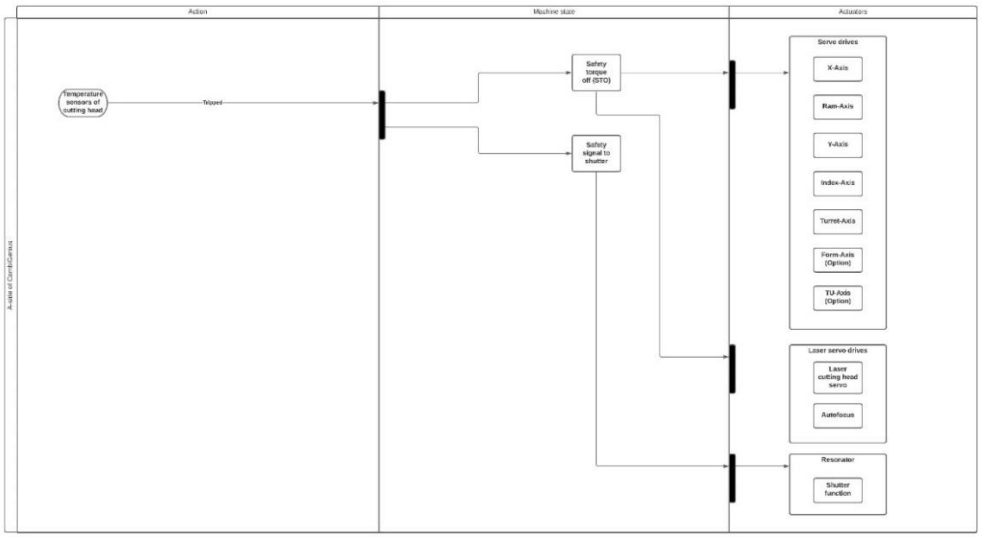
Kuvio 14. Passiivinen suoja



Kuvio 15. Aktiivinen suoja

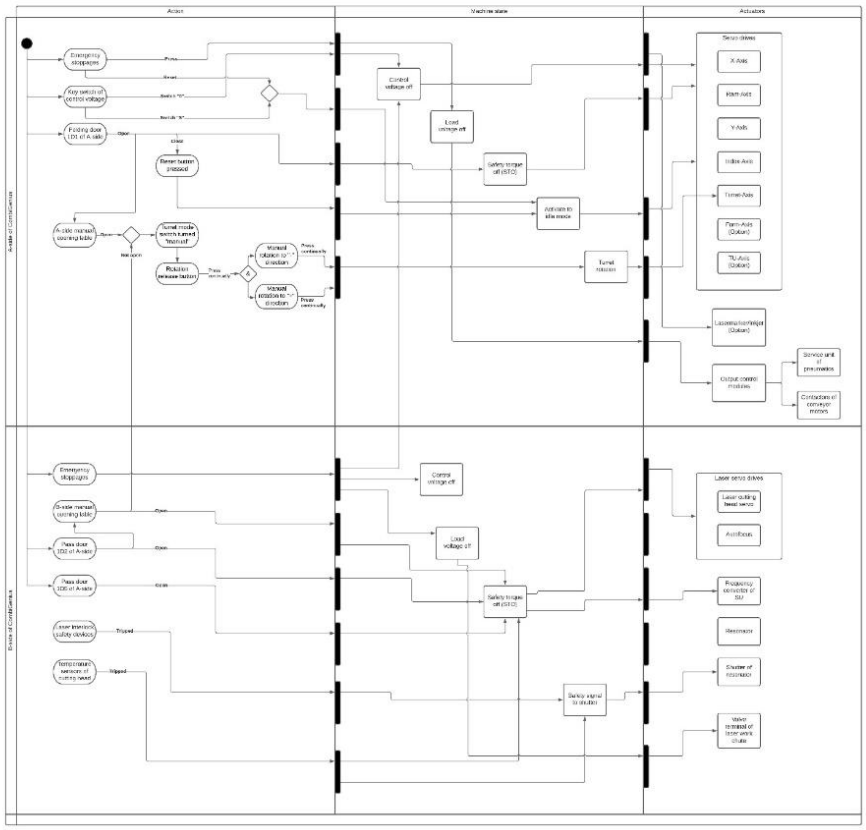
5.3 Aktiviteettikaavion avulla turvatoimintojen todentaminen

Vaatimuskaavion avulla saatu <<ActivateDefence>> -elementti ja <<ContextDetector>> -elementti voidaan sijoittaa seuraavaksi aktiviteettikaavioon. Aktiviteettikaavio voidaan jakaa pystysuunnassa kolmeen eri sarakkeeseen luokan mukaan, näiden välillä on selkeä yhteysviivoja kokoava rajapintahaara. Toimintoelementtejä sisältävät kolme saraketta jaetaan toimintasarakkeeseen, koneen tilan sarakkeeseen ja toimilaitteiden ohjauksen sarakkeeseen (kuvio 16).



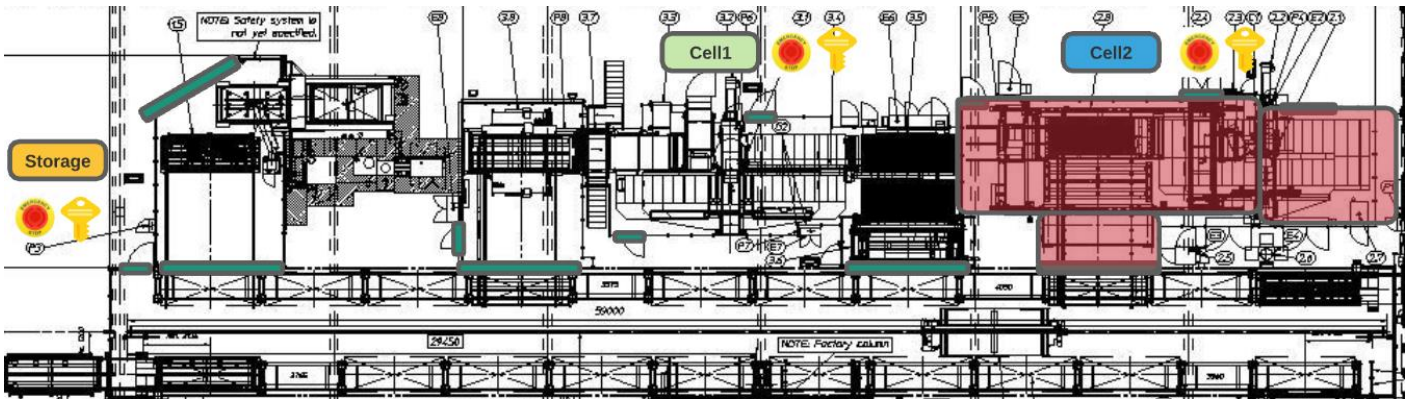
Kuvio 16. Aktiviteettikaavion jako

Jokaiselle vyöhykkeelle varataan oma rivi kaaviotaulukkoon. Kaavioiden rivien välillä voi kulkea eri turvalaitteiden pysäytykset, jolloin selviää turvalaitteen pysäytyksen laajuus (kuvio 17).



Kuvio 17. Useamman vyöhykkeen aktiviteettikaavio

Useita turvavyöhykkeitä sisältävien laitteiden väliset suhteet ovat tehokkainta havainnollistaa esittämällä interaktiivisen mallintamisen keinolla. Lucidchart-sovelluksen avulla saa helposti luotua konelinjan layoutin päälle eri vyöhykkeiden ja turvalaitteiden muodot, jotka jaetaan eri tasoihin. Itse tehdyille muodoille voi laatia oman kirjastonsa. Tasoihin linkitetään eri toimintoja, joilla piilotetaan tai tuodaan esiin eri vyöhykkeitä. Kuvassa 10 on kaksi eri työstösolua kiinni junavarastojärjestelmässä. Ohjausjännite on sammutettuna työstökonesolusta CombiGenius ja lastausportaalirobotista LSR solun avainkytkimeen vaikuttamalla. Jokaisessa solun ja varaston kuvaustekstissä on hyperlinkki suoraan aktiviteettikaavioon, joka koskee kyseistä solua tai varastoa. Aktiviteettikaaviossa on yksityiskohtaisemmin kuvattuna solun tai varaston toimilaitteiden pysäytyksen taso.



Kuva 10. Turvavyöhykkeiden sijoitus konelayoutiin

Lopuksi koko dokumentista voi julkaista pysyvän URL-osoitteen, jossa dokumenttia pystyy käyttämään interaktiivisesti. Tämä URL-osoite on pysyvä, johon dokumentin näkymä päivittyy reaaliaikaisesti, jos kaavio-ohjelmassa dokumenttiin tekee jälkikäteen muutoksia.

6 Johtopäätökset ja loppupohdinta

Ennen mallintamista suunnittelijalla täytyy olla laaja tuntemus eri järjestelmistä. Jos aktiviteettikaavioiden laatiminen otetaan osaksi suunnitteluprosessia, työkalun täytyy olla helposti hallittavissa. Suurimpia kompastuskiviä ovat liiallinen mallintaminen kerralla ja se, että mallintamista ei nähdä suunnitteluprosessin aikaisena tehtävänä, vaan lähinnä saman työn tekemisenä kahteen kertaan. Mallipohjainen systeemisuunnittelu on hyvin alkutekijöissään suomalaisessa koneteollisuudessa. Tämä johtunee mallinnustyökalujen opettelun ja SysML-kielen omaksumisen vaatimasta ajasta. Esimerkin vaatimuskaaviota esiteltäessä ohjaussuunnittelun pääsuunnittelijoille kyseistä mallikaaviota ei pidetty kovin havainnollisena, tai vähintään lukija tarvitsee koulutusta mallin esitystavasta. Lisäksi vaatimuskaaviota luettaessa täytyy ymmärtää kokonaiskonteksti. Vaatimuskaaviolla nähtiin ehkä hyötyä, jos se luodaan heti riskianalyysin jälkeen, josta suunnittelu voi alkaa. Esitetyistä malleista eniten kiinnosti aktiviteettikaavio ja eri vyöhykkeiden väliset suhteet. Tämän nähtiin auttavan suunnittelijaa, testaajaa ja myös huoltoa. Myös visuaalista esitystapaa layoutin päällä pidettiin hyvin havainnollistavana ja hyvänä työkaluna uutta työntekijää perehdyttäessä. Vaikka turvatoimintojen yksinkertainen simulaatio ei korvaisi yksityiskohtaisempaa turvatarkastuslistaa, sen nähtiin ehkä jatkossa tukevan listan lisäksi turvatarkastusta, varsinkin isommassa järjestelmässä.

Jos tulevaisuudessa tulee käyttöön sähkösuunnitteluohjelmisto, joka tukee AutomationML-siirtotiedostoa, tämän avulla voitaisiin luoda yksinkertaisia laitekokoonpanoja turvalogiikalle. Kokoonpanojen rakentamisen pohjana voisi käyttää eri laitteiden vakioratkaisuja, joten siksi suojaukset on hyvä jakaa eri monimutkaisuuden tasoihin. Turvaohjelma pysyisi aina samana ja parametreja muuttamalla saataisiin eri turvahaaroja käyttöön. AutomationML hyöty nähtiin lähinnä vielä teoreettisena, jonka avulla siirtotiedostoon luotu lopullinen laitekokoonpano vaatinee kuitenkin ohjaussuunnittelijan myös määrittelyä.

SysML-profiilista on kehitteillä versio 2.0, jonka pitäisi tulla käyttöön vuoden 2021 aikana. Tämä profiili tuo mukanaan mahdollisesti uusia kaavioita, joilla järjestelmää voidaan kuvata entistäkin tarkemmin. Mahdollisesti riskejä kuvataan omalla kaaviolla uudessa profiilissa. SysML 2.0 olisi tulevaisuudessa itsenäinen kieli, jonka pohjalla olisi uudestaan kehitetty käyttöjärjestelmän ydin, jota kutsutaan KerML (Kernel Modeling Language) -ytimeksi. Tämä mahdollistaa

SysML 2.0 -mallien elementeille ja ulkopuolisille elementeille, kuten CAD-malleille, suhteen esittämisen havainnollisemmin. (Weilkiens 2019)

Mahdollisesti vasta tämän versiopäivityksen myötä aika on kypsä SysML-kaavioiden käyttämiseen enemmän myös osana dokumentaatiota. Tutkimuksessa tutkittiin turvatoiminnon määrittelyä mallipohjaisen systeemisuunnittelun avulla suunnittelijoita ja testaajia varten. Tulevaisuudessa kehitystä kohdistetaan myös enemmän prosessien, menetelmien, organisaatioiden ja informaation hallinnan kehittämiseen. Prima Powerin tuote- ja suunnittelutiedon hallintajärjestelmänä on käytössä TeamCenter, johon on mahdollista integroida System Modeling Workbench -laajennus (Siemens 2019). Tämän integraation myötä suunnittelijat pystyisivät yhdistämään TeamCenterin mallit SysML-profiilin mallinnukseen.

Opinnäytetyön aihepiiri oli hyvin laaja. Tutkimuksen myötä mallipohjainen systeemisuunnittelu tuli tutummaksi työn tekijälle ja myös käsitteenä suunnitteluosastojen pääsuunnittelijoille. Työn tavoitteena oleviin tutkimuskysymyksiin saatiin ratkaisu turvatoiminnon tehokkaammalla esitystavalla mallintamisen keinoihin. Finn-Powerin strategian mukaisesti laitteiden pitää olla liitettävissä kolmannen osapuolen laitteisiin, jonka myötä myös turvatoiminnallisuuden määrittely ja esittäminen eri sidosryhmille kehittynee tulevaisuudessa. Ketterän kehityksen hallitsemiseen mallipohjaisuus ja siihen liittyvät menetelmät voisivat tuoda helpotusta. Mallipohjaisuus mahdollistaa läpinäkyvyyttä myös asiakkaille ja muille sidosryhmille järjestelmien kehittämisen aikana. Eri järjestelmien mallien ylläpitämiseen koko elinkaaren ajan vaatii tämän tutkimustyön jälkeen lisätutkimusta. Mallipohjaisen systeemisuunnittelun edut nousevat esiin, jos sen avulla uusi suunnittelija ja testaaja oppii nopeammin eri toiminnot järjestelmässä. Tulevaisuudessa myös turvaratkaisut todennäköisesti monimutkaistuvat, joten ehkä myös vian analysointi mallintamisen keinoin täytyy ottaa huomioon. Nykyisten turvapiirien vikojen taajuuden analysointi pystytään ottamaan huomioon jo turvapiirien suoritustasoa laskettaessa.

Nykyään eri laitteissa on käytössä erilaisia turvaratkaisuja. Sähkösuunnittelijan rooli on tulevaisuudessakin määrittää riskianalyysin perusteella turvatoimintojen laajuus. Trendi kehittyy jatkuvasti enemmän ohjelmistopuolen ohjauksiin ja todennäköisesti siirrytään useammassa koneessa turvalogiikkaan, jota pystytään hallinnoimaan etäkäytön avulla ja tarkistelemaan vikatietoja turvapiireistä ilman asentajan käyntiä. Määrittelyn aikana luotujen

mallikaavioiden avulla turvaohjelman toiminnallisuus on helpommin luettavissa, joten vertailu turvalogiikasta saatavaan raporttiin on helpompaa.

LÄHTEET

A 12.6.2008/400 Valtioneuvoston asetus koneiden turvallisuudesta.

Anttila, P. 2014. Tutkimisen taito ja tiedon hankinta. [www-dokumentti]. [Viitattu 30.4.2021]. Saatavissa: https://metodix.fi/2014/05/17/anttila-pirkko-tutkimisen-taito-ja-tiedon-hankinta/

Atlassian Marketplace. Ei päiväystä. draw.io Diagrams for Jira. [www-dokumentti]. [Viitattu 3.4.2021]. Saatavissa: https://marketplace.atlassian.com/apps/1211413/draw-io-diagrams-for-jira?hosting=cloud&tab=overview

Beckhoff. Ei päiväystä. TE1120|TC3 XCAD Interface 2. [www-dokumentti]. [Viitattu 23.3.2021]. Saatavissa: https://download.beckhoff.com/download/Document/Catalog/Main_Catalog/english/separate-pages/twincat/te1120.pdf

Biggs, G. & Kotoku,T. 2014. A profile and tool for modelling safety information with design information in SysML. [www-dokumentti]. [Viitattu 23.3.2021]. Saatavissa: https://www.researchgate.net/publication/271923239_A_profile_and_tool_for_modelling_safety_information_with_design_information_in_SysML

Biggs, G., Juknevicius, T., Armonas, A. & Post,K. 2018. Integrating Safety and Reliability Analysis into MBSE: overview of the new proposed OMG standard. [www-dokumentti]. [Viitattu 23.3.2021]. Saatavissa: https://www.researchgate.net/publication/327071441_Integrating_Safety_and_Reliability_Analysis_into_MBSE_overview_of_the_new_proposed_OMG_standard

Collin, J. & Saarelainen, A. 2016. Teollinen internet. [Verkkokirja]. Helsinki: Talentum. [Viitattu 23.3.2021]. Saatavana Alma Talent bisneskirjasto -palvelusta. Vaatii käyttöoikeuden.

Delligatti, L. 2013. SysML Distilled: A Brief Guide to the Systems Modeling language. USA: Addison-Wesley Professional

Google Workspace Marketplace. Ei päiväystä. Lucidchart Diagrams. [www-dokumentti]. [Viitattu 3.4.2021]. Saatavissa: https://workspace.google.com/marketplace/app/lucidchart_diagrams/7081045131

Graessler, I., Hentze, J. & Bruckmann, T. 2018. V-models for interdisciplinary systems engineering. [www-dokumentti]. [Viitattu 17.3.2021]. Saatavissa: https://www.designsociety.org/publication/40489/V-MODELS+FOR+INTERDISCIPLINARY+SYSTEMS+ENGINEERING

Huhtala, P. & Pulkkinen, A. 2009. Tuotettavuuden kehittäminen: Parempi tuotteisto useasta näkökulmasta. Helsinki: Teknologiainfo Teknova.

Hirsjärvi, S., Remes, P., Sajavaara, P. & Sinivuori, E. 2009. Tutki ja kirjoita. 15. uud. p. 22. painos. Helsinki: Tammi.

DGUV. 2019. IFA report 2/2017e: Functional safety of machine controls, application of EN ISO 13849-1. [www-dokumentti]. Germany, Berlin: German Social Accident Insurance (DGUV) [Viitattu 22.3.2021]. Saatavissa:https://www.dguv.de/medien/ifa/en/pub/rep/pdf/reports-2019/report0217e/rep0217e.pdf

IMBSA. 2019. Model-Based Safetyand Assessment 6th International Symposium, IMBSA 2019 Thessaloniki, Greece, October 16–18, 2019 Proceedings. [Verkkokirja]. Switzerland: Springer Nature AG. [Viitattu 12.2.2021]. Saatavana Springerling -palvelusta. Vaatii käyttöoikeuden.

INCOSE. 2014. System engineering vision 2025. [www-dokumentti]. [Viitattu 23.3.2021]. Saatavissa: https://www.incose.org/docs/default-source/aboutse/se-vision-2025.pdf

Liu, D. 2015. Systems Engineering: Design Principles and Models 1st Edition. New York: CRC Press.

Malmén, Y., Nissilä, M., Wallin, K. & Virolainen, K. 2012. Ulkopuolisen suunnittelijan rooli ja vastuu prosessilaitoksen turvallisuudesta. [www-dokumentti]. [Viitattu 17.3.2021]. Saatavissa: https://oma.tsr.fi/api/projects/57c05513-11dd-4c77-89c6-a9b03ea78651/attachment/fab9bc86-034d-4524-9266-a66ff9007c65

Microsoft. Ei päiväystä. Visio Työskentele visuaalisesti missä ja milloin tahansa. [www-dokumentti]. [Viitattu 3.4.2021]. Saatavissa: https://www.microsoft.com/fi-fi/microsoft-365/visio/flowchart-software

Powell-Morse, A. 2016. V-model: what is it and how do you use it. [Blogi]. [Viitattu 24.1.2021]. Saatavissa: https://airbrake.io/blog/sdlc/v-model

Prima Power Mediabank. 2020. The System. [www-dokumentti]. [Viitattu 23.3.2021]. Saatavissa: https://mediabank.primapower.com/f/twkn Vaatii käyttöoikeuden.

Prima Power. Ei päiväystä. Laser- ja levyntyöstöteknologian johtava yritys. [www-dokumentti]. [Viitattu 23.3.2021]. Saatavissa: https://www.primapower.com/fi/prima-power/

Prima Power. 2019. Safety device layout document 21.11.2019.

SFS-EN 62061. 2005. Koneturvallisuus. Turvallisuuteen liittyvien sähköisten, elektronisten ja ohjelmoitavien elektronisten ohjausjärjestelmien toiminnallinen turvallisuus. Helsinki: Suomen standardisoimisliitto.

SFS-EN ISO 12100. 2010. Koneturvallisuus. Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen. Helsinki: Suomen standardisoimisliitto.

SFS-EN ISO 13849-1. 2015. Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet. Helsinki: Suomen standardisoimisliitto.

SFS-EN ISO 14118. 2018. Odottamattoman käynnistyksen estäminen. Helsinki: Suomen standardisoimisliitto.

Sheard, S. & Mostashari, A. 2008. Principles of Complex Systems for Systems Engineering. [www-dokumentti]. [Viitattu 17.3.2021]. Saatavissa: https://www.academia.edu/26719547/Principles_of_Complex_Systems_for_Systems_Engineering

Siemens 2019. New System Modeling Workbench for Teamcenter enables multi-domain digital twin [www-dokumentti]. [Viitattu 3.4.2021]. Saatavana: https://www.plm.automation.siemens.com/global/en/our-story/newsroom/system-modeling-workbench-teamcenter/43935

Siemens. 2017. Process simulation with SIMIT CHEM BASIC library and SIMATIC PCS 7. [www-dokumentti]. [Viitattu 3.4.2021]. Saatavissa: https://support.industry.siemens.com/cs/document/109745800/process-simulation-with-simit-chem-basic-library-and-simatic-pcs-7?dti=0&lc=en-US

Siirilä, T. & Tytykoski, K. 2016. Koneturvallisuuden käsikirja. Helsinki: Inspecta.

Siirilä, T. 2009. Koneturvallisuus: Ohjausjärjestelmät ja turvalaitteet. 2. uud. p. Espoo: Inspecta.

Skoglund, M., Warg, F. & Sangchoolie, B. 2018. In Search of Synergies in a Multi-Concern Development Lifecycle: Safety and Cybersecurity. [www-dokumentti]. [Viitattu 23.3.2021]. Saatavissa: https://www.researchgate.net/publication/327113600_In_Search_of_Synergies_in_a_Multi-concern_Development_Lifecycle_Safety_and_Cybersecurity_SAFECOMP_2018_Workshops_ASSURE_DECSoS_SASSUR_STRIVE_and_WAISE_Vasteras_Sweden_September_18_2018_Proceedings

Sparx systems. Ei päiväystä. Enterprise architect. [www-dokumentti]. [Viitattu 3.4.2021]. Saatavissa: https://sparxsystems.com/products/ea/index.html

STSARCES - Standards for Safety Related Complex Electronic Systems- 2014. [www-dokumentti]. Standardization and European regulations. [Viitattu 20.3.2021]. Saatavissa: http://www.industry-finder.com/machinery-directive/stsarces-annex-5-common-mode-faults-safety-systems.html

VTT. 2013. Katsaus kompleksisten järjestelmien elinkaaren suunnitteluun. [www-dokumentti]. [Viitattu 5.3.2021]. Saatavissa: https://www.vttresearch.com/sites/default/files/pdf/technology/2013/T121.pdf

Weilkiens, T. 2007. Systems engineering with SysML/UML: Modeling, analysis, design. Amsterdam; Boston: Morgan Kaufmann OMG Press/Elsevier.

Weilkiens, T. 2019. SysML v2 – The Next Generation. [www-dokumentti]. [Viitattu 3.4.2021]. Saatavissa: https://www.microtool.de/en/requirementsengineering/sysml-v2-the-next-generation/

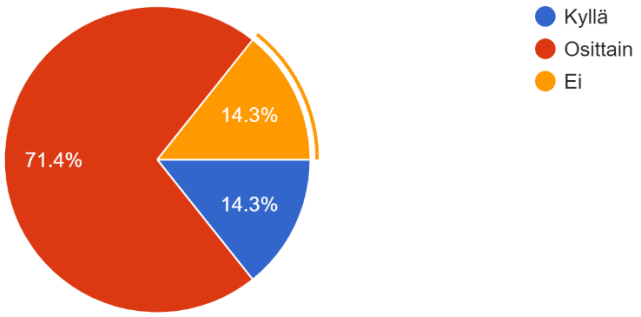
LIITTEET

Liite 1. Kysely turvatoiminnon suunnitteluprosessista sähkösuunnitteluosastolla

LIITE 1. Kysely turvatoiminnon suunnitteluprosessista sähkösuunnitteluosastolla

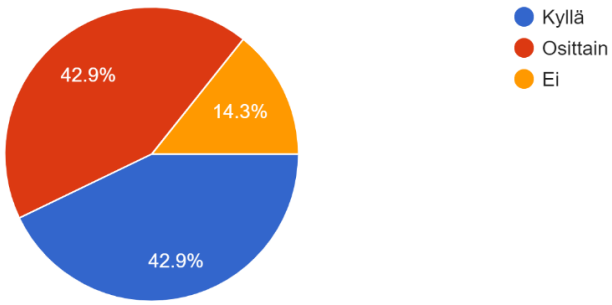
1. Onko laitekohtaisen uuden suojauksen turvallisuusvaatimukset selkeitä sähkösuunnittelun alusta alkaen?

7 responses



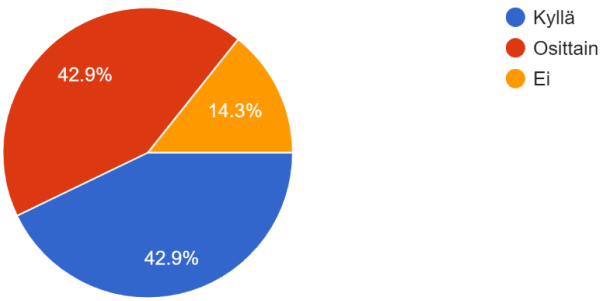
2. Onko mielestäsi suunnittelun aikainen tiedonkulku eri osastojen välillä etätyössä yhtä tehokasta kuin toimistolla?

7 responses



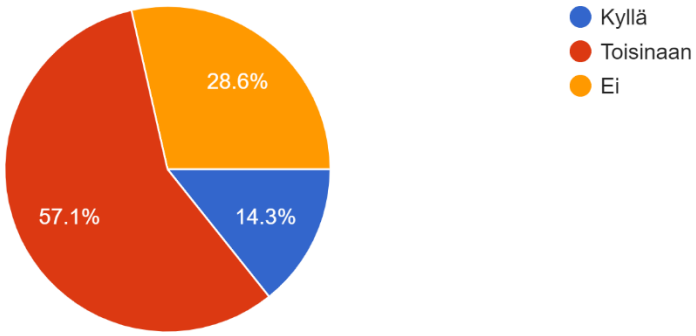
3. Onko mielestäsi etätyöskentelyn aikana tiedon jäljitettävyys myös selkeää koko valmistusprosessin ajan liittyen laitekohtaiseen suojaukseen ja turvatoimintoon?

7 responses



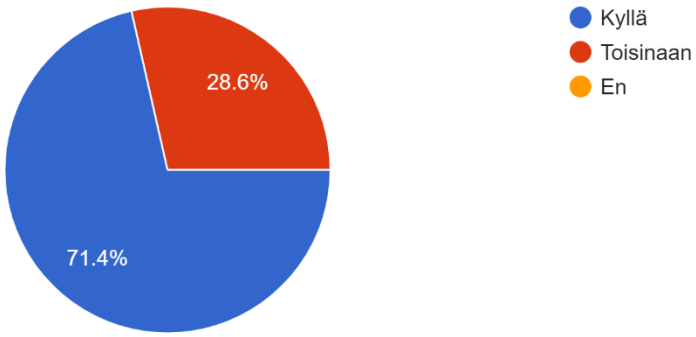
4. Onko mielestäsi suojauksien ja turvatoimintojen suunnittelun aikana usein tiedonhukkaa eli epäselvyyttä oikeasta tiedonlähteestä?

7 responses



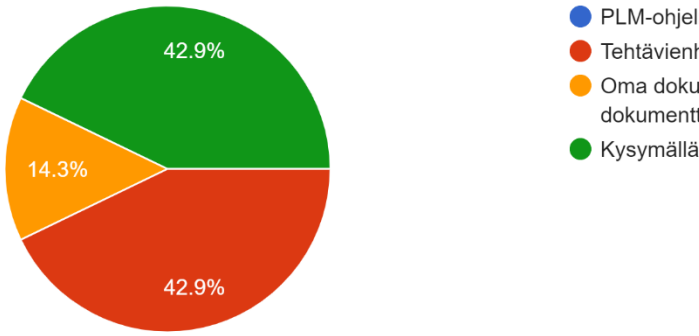
5. Löydätkö helposti jo toteutuneita ratkaisuja, joita voi käyttää uuden suunnittelun pohjana?

7 responses



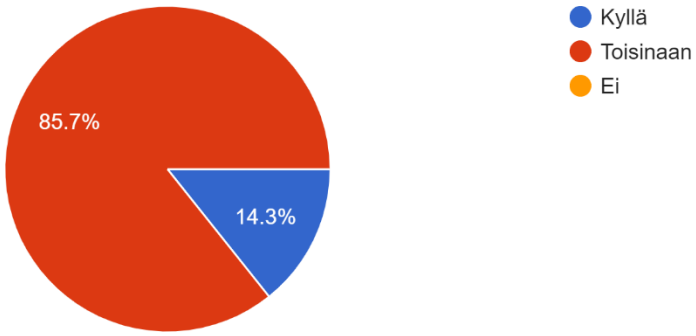
6. Mitä tiedonlähdettä käytät useimmin jo toteutuneiden suojausratkaisujen tiedon etsimiseen?

7 responses



7. Sähkösuunnittelutehtävän jälkeen, tuleeko jälkikäteen yleensä muutoksia jo kertaalleen suunniteltuun turvatoimintoon, esimerkiksi: kolmannen osapuolen laitteen rajapinnalle?

7 responses



8. Onko mielestäsi turvapysäytyslista yleensä tarpeeksi havainnollinen pysäytystoiminnon todentamiseen?

7 responses