LAPPEENRANNAN-LAHDEN TEKNILLINEN YLIOPISTO LUT

School of Energy Systems

Energiatekniikan koulutusohjelma

Otto Puustinen

Systeemiteoreettisen prosessianalyysin hyödyntäminen valmiustoiminnan suunnittelussa

Työn tarkastaja: Professori TkT Juhani Hyvärinen

Työn ohjaaja: DI Tommi Purho

TIIVISTELMÄ

LUT-Yliopisto

School of Energy Systems

Energiatekniikan koulutusohjelma

Otto Puustinen

Systeemiteoreettisen prosessianalyysin hyödyntäminen valmiustoiminnan suunnittelussa

Diplomityö 2020

86 sivua, 20 kuvaa, 7 taulukkoa

Työn tarkastajat: Professori TkT Juhani Hyvärinen

Työn ohjaaja: DI Tommi Purho

Hakusanat: valmiusjärjestelyt, valmiustoiminta, systeemiteoria, STPA

Ydinvoimalaitosten luvanhaltijoiden on varauduttava vakaviin onnettomuuksiin sekä radioaktiivisten aineiden päästöön ydinenergialain vaatimusten mukaisesti. Onnettomuustilanteisiin varaudutaan valmiustoiminnalla, jonka avulla varaudutaan ydinturvallisuutta uhkaaviin epätavallisiin tilanteisiin sekä lievennetään onnettomuuden jälkeisen tilanteen vaikutuksia. Valmiustoimintaan osallistuu ydinvoimalaitoksen luvanhaltijan valmiusorganisaation lisäksi lukuisia viranomaistoimijoita eri tahoilta.

Tässä diplomityössä valmiustoimintaa analysoidaan systeemiteoriaan pohjautuvalla STPA-analyysillä valmiustoimintaa uhkaavien riskien identifioimiseksi. STPA-hasardianalyysi on suhteellisen uusi analysointimenetelmä ja se eroaa perinteisistä luotettavuustekniikkaan liittyvistä analyysimenetelmistä useilla eri tavoilla, joista esimerkkinä voidaan mainita luotettavuuden sekä turvallisuuden määrittely eri ominaisuuksiksi. Systeemiteorian avulla järjestelmää voidaan tarkastella kokonaisuutena järjestelmän ympäröimä organisaatio huomioiden.

Valmiustoiminnan sekä STPA-analyysin esittelyjen lisäksi tässä diplomityössä käydään läpi tutkimuksen eri vaiheita sekä saatuja tuloksia. Työn lopulla pohditaan mahdollisuuksia jatkoanalysoinnille sekä tuloksien hyödyntämiselle.

ABSTRACT

LUT University
School of Energy Systems
Degree Program of Energy Technology

Otto Puustinen

System-Theoretic Process Analysis Applied to Emergency Preparedness Planning

Master's thesis 2020

86 pages, 20 figures, 7 tables

Examiner: Professor Ph.D. (Tech.) Juhani Hyvärinen
Supervisor: M.Sc. (Tech.) Tommi Purho

Keywords: emergency preparedness, emergency response, system theory, STPA

Licensees of nuclear power plants must prepare for severe accidents and to the possible release of radioactive materials accordingly to nuclear energy act's requirements. Emergency response is to anticipate unusual events that could lead to a severe accident. In case of an accident, emergency response is used to mitigate the negative effects of a post-accident situation. Various officials from different fields of activity participate in emergency response act in addition to power plant's license holder's emergency response organisation.

In this master's thesis, emergency response act is analysed with a system-theoretic STPA analysis in a study to identify risks for emergency response. STPA hazard analysis is a fairly new analysation method and it differs from traditional hazard analyses in multiple ways. For example in STPA analysis safety and reliability are seen as two different non-related attributes. With systems theory it is possible to include the surrounding organisation to the analysis of a system.

In this thesis the phases of the study are examined in addition to the results identified. Lastly, possibilities for further analysation and utilisation of the results are discussed.

ALKUSANAT

Tämä työ päättää viiden vuoden mittaisen opiskeluaikani LUT-yliopistossa. Haluan kiittää yliopistoa laadukkaasta poikkitieteellisestä opetuksesta sekä viihtyisästä opiskeluympäristöstä. Erityiskiitokseni menevät professori Juhani Hyväriselle työni tarkastamisesta, mielenkiintoisista luennoista vuosien varrella sekä työstä kotimaisen sekä kansainvälisen ydinvoiman kehityksessä.

Kiitokset Loviisan voimalaitokselta Tommi Purholle hyvästä ja läsnäolevasta työn ohjauksesta sekä mielenkiintoisesta ja sopivan haastavasta diplomityöaiheesta. Haluan kiittää myös koko laitosturvallisuusryhmää hyvästä työilmapiiristä sekä luottamuksesta yhteisten vuosien aikana.

Suuret kiitokset myös kotiväelle jatkuvasta tuesta opintojeni aikana. Kiitokset myös muulle lähipiirille kaikesta saadusta tuesta.

Porvoossa 17.6.2020

Otto Puustinen

SISÄLLYSLUETTELO

SYMBOLI- JA LYHENNELUETTELO

Lyhenteet

FMEA	Failure Mode and Effects Analysis, *vika- ja vaikutusanalyysi*
FSAR	Final Safety Analysis Report, *lopullinen turvallisuusseloste*
IAEA	International Atomic Energy Agency
INSAG	International Nuclear Safety Group
ISO	International Organization for Standardization
IVO	Imatran Voima Oy, *nykyinen Fortum Oy*
PRA	Probabilistic Risk Assessment, *todennäköisyyspohjainen riskianalyysi*
PWR	Pressurised Water Reactor, *painevesireaktori*
SFS	Suomen Standardisoimisliitto ry
STAMP	System-Theoretic Accident Model and Processes
STPA	System-Theoretic Process Analysis
STUK	Säteilyturvakeskus
VVER	Voda-Vodyanoi Energetichesky Reaktor (translitteroitu), *vesi-vesi-tehoreaktori*
YVL-ohje	Ydinturvallisuusohje

1 JOHDANTO

Ydinvoiman käytön taustalla vaikuttaa vahvasti ajatus jatkuvasta ydinenergian tuotannon yleisen turvallisuustason parantamisesta. Jatkuva turvallisuuskehitys näkyy esimerkiksi kansainvälisestä käyttökokemustoiminnasta, jonka avulla ydinvoimalaitokset ympäri maailman voivat oppia toisiltaan huomioiden, virheiden tai muiden tapahtumien kautta. Jatkuva turvallisuuskehitys näkyy myös alati tapahtuvassa uusien voimalaitostyyppien suunnittelussa sekä jo olemassa olevien voimalaitosten turvallisuusjärjestelmien kehittämisessä.

Turvallisuustasoa voidaan parantaa myös toiminnallisuuksien osalta esimerkiksi ottamalla käyttöön uusia menetelmiä tai käytäntöjä. Tässä työssä jatkuvaa turvallisuuskehitystä lähestytään tutkimalla ja testaamalla uutta hasardianalyysimenetelmää valmiustoiminnan suunnittelun yhteydessä aiemmin tunnistamattomien riskien löytämiseksi.

1.1 Työn tausta

Suomessa ydinturvallisuusviranomaisena toimiva Säteilyturvakeskus valvoo ydinturvallisuuden toteutumista ja kehittämistä. Säteilyturvakeskuksen laatimissa ydinturvallisuusohjeissa annetaan ohjeita sekä vaatimuksia ydinvoimalaitosten turvalliseen käyttöön. Tämän työn osalta tärkein ydinturvallisuusohje on C.5, jossa käsitellään ydinvoimalaitoksen valmiusjärjestelyjä.

Vaatimus valmiusjärjestelyjen olemassaololle tulee ydinenergialaista. Valmiusjärjestelyiden avulla ydinvoimalaitoksen luvanhaltija varautuu sellaisiin epätavallisiin tilanteisiin tai onnettomuuksiin, joissa riskinä on vakavan reaktorionnettomuuden tapahtuminen tai radioaktiivisten aineiden leviäminen ympäristöön. Valmiusjärjestelyjen tärkein osa-alue on valmiusjärjestelyjen suunnittelu, johon kuuluvat muun muassa valmiusorganisaation kokoaminen sekä valmiustoiminnan harjoittelu. Valmiussuunnitelmaa on ylläpidettävä koko laitoksen käyttöiän ajan.

Valmiustoimintaan osallistuu henkilöstöä luvanhaltijan organisaatiosta koostuvan valmiusorganisaation lisäksi viranomaisia muun muassa säteilyturvakeskuksesta, pelastuslaitokselta sekä poliisista. Kaikkien näiden toimijoiden on toimittava yhteistyössä

onnettomuuden etenemisen rajoittamisessa sekä onnettomuuden jälkeisen tilanteen vaikutusten lieventämisessä.

Valmiustilanteen vakavuus, tilanteen epäselkeys sekä kommunikaatio-ongelmat saattavat aiheuttaa yksinään tai yhteisvaikutuksena uhkatilanteita valmiustoiminnan objektiiviselle toiminnalle. Mahdollisia uhkatilanteita voivat aiheuttaa esimerkiksi päätösten teko väärien oletuksien pohjalta, kommunikaation puuttuminen tai laitoksen hallinnan menettäminen kriittisen laitevian vuoksi.

Tärkeää valmiustoimintaharjoituksissa on oikeiden asioiden päämäärätietoinen harjoittelu. Muussa tapauksessa valmiustoimintaharjoituksen perusteella saatetaan päätyä esimerkiksi panostamaan vääriin asioihin jättäen tärkeämmät asiat pienemmälle huomiolle. Valmiustoiminnan luonteesta johtuen virheistä oppiminen muutoin kuin harjoituksissa ei ole mahdollinen vaihtoehto, vaan mahdolliset riskit tulee tunnistaa etukäteen. Yksi tapa kohdentaa valmiustoiminnan harjoittelua on analysoida valmiusorganisaatiota sekä muita valmiustoimintaan osallistuvia tahoja sekä näiden keskinäistä toimintaa.

Tällainen systeemin analysointi on osa riskienhallintaprosessia. Riskienhallinta on myös oleellinen osa aiemmin mainittua jatkuvaa turvallisuuden kehittämistä. Oikein toteutettu riskienhallinta toimii apuna voimalaitoksen päätöksenteossa muun muassa strategisten toimenpiteiden priorisoinnissa.

1.2 Tavoite ja rajaukset

Tämän diplomityön tavoitteena on selvittää systeemi- ja säätöteorioihin pohjautuvan STPA-analyysin (System-Theoretic Process Analysis) soveltuvuutta Loviisan voimalaitoksen valmiustoiminnan suunnittelun työkaluna. Tavoitteena työn lopputuloksena on saada käsitys valmiustoimintaa uhkaavista riskiskenaarioista, joita analyysin jälkeen voidaan hyödyntää riskienhallinnassa. Loviisan voimalaitoksen riskienhallintamenettelyt pohjautuvat riskienhallintastandardiin ISO 31000.

Työ rajataan STPA-analyysin laatimiseen. Itse STPA-analyysin yhteensopivuutta valmiustoiminnan analysointiin tullaan arvioimaan työn lopussa. STPA on suhteellisen

uusi hasardianalyysimenetelmä, jolloin menetelmän vertailu paremmin tunnettuihin menetelmiin on oleellista.

Analyysi tullaan toteuttamaan selainpohjaisessa Polarion-ohjelmistossa. Vaikka analyysi toteutetaankin Polarion-ohjelmistossa, ei ohjelmisto tule olemaan kovin suuressa osassa tätä diplomityötä, sillä se toimii ainoastaan alustana analyysin tekemiselle.

1.3 Työn rakenne

Luvussa 2 tarkastellaan Loviisan ydinvoimalaitosta energiantuotannon perusasioista turvallisuusasioihin. Luvussa 2 esitellään syvyyssuuntainen turvallisuusajattelu, joka on yksi perusperiaatteista turvallisuusjärjestelmiä suunnitellessa. Tämän lisäksi luvussa esitellään valmiustoimintaa sekä siihen liittyviä toimijoita yleisesti. Näiden lisäksi Polarion-ohjelmisto esitellään lyhyesti tässä luvussa.

Luvussa 3 käydään läpi STPA-analyysiin oleellisesti liittyviä teorioita sekä niiden syntyperiä. STPA-analyysin sekä yleensäkin systeemiteorian kehityksen taustalla vaikuttavat tietyt ongelmat perinteisiin hasardianalyyseihin liittyen. Luvussa 3 käydään läpi näitä ongelmia sekä STPA-analyysiin liittyvien teorioiden tarjoamia ratkaisukeinoja näille ongelmille. Koska nämä teoriat eivät ole kytköksissä vain ydinvoimatekniikkaan, luvussa 3 käydään asioita läpi yleisellä tasolla eri teollisuusaloihin liittyvien esimerkkien avulla.

Oleellisten teorioiden läpikäynnin jälkeen luvussa 4 käydään läpi STPA-analyysiin kuuluvia elementtejä sekä toimintatapoja käytännössä esimerkkianalyysin muodossa. Esimerkkianalyysi suoritetaan yksinkertaistetulle kemikaalilaitokselle perustuen aiheesta tehtyihin esitelmiin ja muihin lähteisiin. Esimerkkianalyysin lisäksi tässä luvussa käydään läpi mahdollisia ihmiskeskeisten systeemien luomia analysointiongelmia, koska valmiustoiminnassa ihmistoimijoiden keskinäisen toiminnan analysointi on isossa osassa useiden eri osaaottavien organisaatioiden takia.

Luvussa 5 käydään läpi työssä tehty case-tutkimus. Luvussa käydään läpi syitä tutkimuksen laatimisen taustalla, työn tuloksia, tuloksien oikeellisuutta sekä STPA-analyysin soveltuvuutta valmiustoimintaa analysoitaessa. Luvun lopulla esitellään mahdollisia jatkotoimenpiteitä sekä tuloksiin että analyysiin liittyen.

2 LOVIISAN VOIMALAITOS

2.1 Yleiskuvaus

Imatran Voima Oy (IVO) tilasi vuosina 1970 ja -71 ydinvoimalaitoksen kahdella reaktoriyksiköllä neuvostoliittolaiselta Tekhnopromexportilta rakennettavaksi Loviisaan. Tilatut yksiköt olivat VVER-painevesireaktoreita, joiden nettosähköteho oli 440 MW yksikköä kohden. Yksiköt kytkettiin sähköverkkoon vuosina 1977 sekä 1980. (Lehtinen & Sandberg 2004, 17-18.)

IVO sekä Suomen viranomaiset vaativat, että ydinvoimalaitos täyttäisi länsimaalaiset turvallisuusvaatimukset, joten tilattuihin ydinvoimalaitosyksiköihin tuli lisätä muun muassa hätäjäähdytysjärjestelmät sekä suojarakennus (Lehtinen & Sandberg 2004, 16-17). Täysin neuvostoliittolaista suunnittelua Loviisan ydinvoimalaitos ei siis ole, eikä IVO:n alkuperäinen suunnitelma saada voimalaitos käyttöön avaimet käteen -periaatteella toteutunut (Salminen 2007).

Syy siihen, miksi laitos ylipäätään tilattiin Neuvostoliitosta, eikä lännestä, juontaa juurensa tuon ajan poliittiseen ilmapiiriin. Ajateltiin, että tämän kokoluokan investoinnissa alan kansainvälinen herkkyys sekä kauppapolitiikka tulisi ottaa huomioon. Normaalissa liiketaloudellisessa tarjouskilpailussa neuvostoliittolaisten tarjousta ei olisi valittu. (Lehtinen & Sandberg 2004, 16-17.)

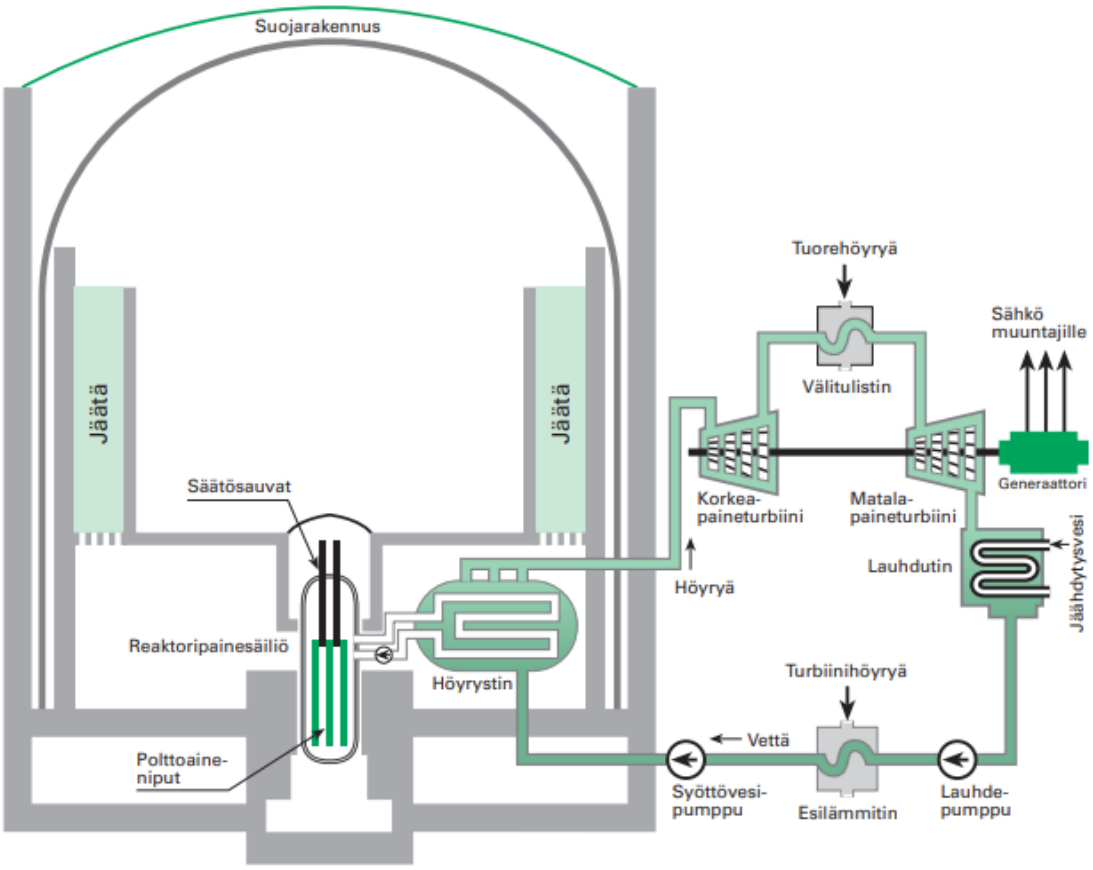
Loviisan voimalaitos oli monin tavoin uutta ydinvoima-alalla. Valmistuttuaan Loviisan ydinvoimalaitos oli ensimmäinen laatuaan Suomessa sekä sen rakennusprojektissa yhdistyivät ensimmäistä kertaa lännen sekä idän ydinvoima-alan osaaminen sekä teknologia. Esimerkiksi kaikki pääkomponentit kuten reaktori, turbiini sekä generaattori ovat neuvostoliittolaista alkuperää, mutta muun muassa suuri osa turvallisuus- sekä automaatiojärjestelmistä ovat länsimaista suunnittelua. (Fortum 2020.)

Monikansallisen vaikutuksen lisäksi myös IVO:n oma kädenjälki näkyy Loviisan voimalaitoksessa, sillä alkuperäisissä VVER-reaktoreissa havaittiin heikkouksia, jotka vaikuttivat koko laitoksen tehokkuuteen. IVO:n suorittamien parannustöiden lopputuloksena saatua VVER-reaktoria markkinoitiin Itä-Eurooppaan ja Pohjois-Afrikkaan yhdessä neuvostoliittolaisen Atomenergoeksportin kanssa. (Michelsen 2007.)

Jatkuvien uudistusten myötä reaktorien nettosähkötehoa on onnistuttu nostamaan alkuperäisestä 440 MW:sta noin 500 MW:iin vuoteen 2011 mennessä (Lahti 2011).

Painevesireaktorit (pressurized water reactor, PWR) ovat maailmanlaajuisesti yleisin reaktorityyppi. PWR-laitoksissa sekä neutronihidasteena että jäähdytteenä käytetään vettä. Polttoaineena käytetään uraania, jonka ^{235}U-isotoopin osuutta on väkevöity hieman alle 5 prosenttiin. Polttoaine on puristettu uraanioksiditableteiksi (UO2) ja ne sijoitetaan kaasutiiviiden polttoainesauvojen sisään. Polttoainesauvat on edelleen niputettu polttoainenipuiksi, joita voimalaitoksilla käsitellään. VVER-440-reaktoreissa käytetään kuusikulmaisia polttoainenippuja. Molempien laitosyksiköiden reaktorisydämiin ladataan kerrallaan 313 polttoainenippua, joista kustakin löytyy 126 polttoainesauvaa. (Eurasto et.al. 2004, 44-46.)

Sähköntuotanto PWR-laitoksissa tapahtuu käyttäen kahta jäähdytyspiiriä; primääripiiriä sekä sekundääripiiriä. Primääripiiri siirtää lämpöä reaktorista höyrystimiin korkeapaineisen jäähdytysveden avulla. Korkean paineen ansiosta primääripiirissä kiertävä vesi ei kiehu. Primääripiirissä ja sekundääripiirissä kiertävät jäähdytysvedet eivät sekoitu keskenään, vaan lämpö siirtyy primääripiirissä kiertävästä jäähdytysvedestä sekundääripiirin jäähdytysveteen höyrystimen lämmönsiirtoputkien läpi. Sekundääripiirissä vallitsee pienempi paine verrattuna primääripiiriin, joten sekundääripiirin vesi kiehuu höyrystimessä. Höyry johdetaan turbiiniin, jossa höyryn lämpöenergia muuntuu turbiinin liike-energiaksi höyryn laajenemisen seurauksena. Turbiinin liike-energia muuntuu edelleen sähköenergiaksi turbiinin akseliin kiinnitetyssä generaattorissa. (Eurasto et.al. 2004, 45.) Alla oleva kuva havainnollistaa edellä mainittua prosessia.



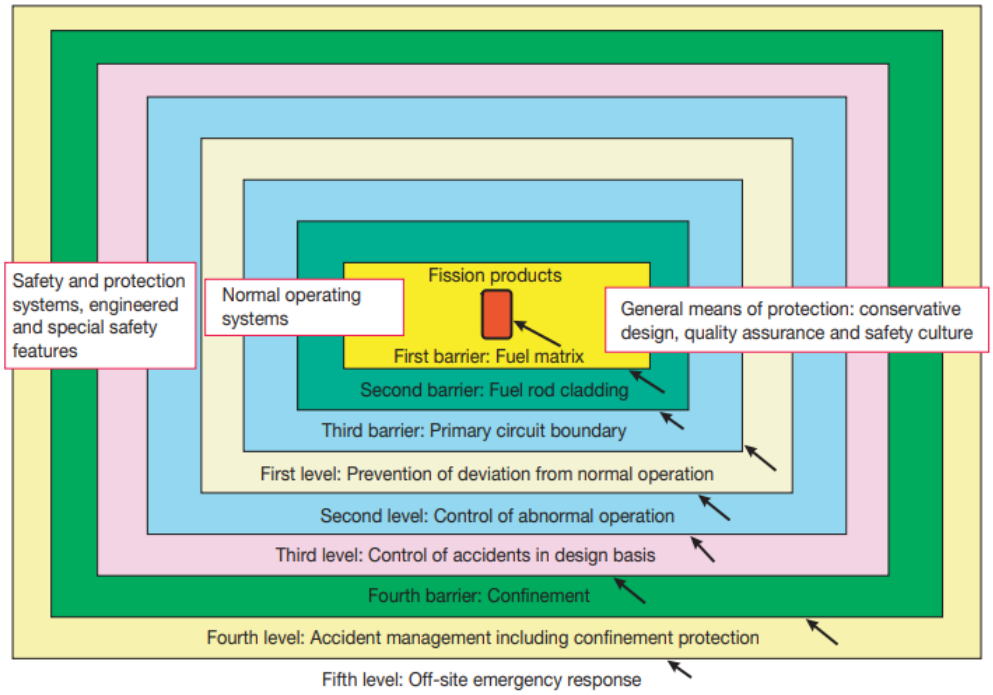
Kuva 1. Loviisan voimalaitoksen periaatekaavio (Eurasto et.al. 2004, 45)

Yllä olevasta kuvasta nähdään lämmönsiirtoprosessin lisäksi alkuperäiseen VVER-440 laitostyyppiin kuulumattomia kohteita, kuten suojarakennus sekä sen sisällä oleva jäälauhdutin. Nämä turvallisuuselementit ovat osa syvyyssuuntaista turvallisuusajattelua, joka on yksi perusperiaatteista ydinvoimalaitoksen turvallisuusjärjestelmiä suunnitellessa.

2.2 Syvyyssuuntainen turvallisuusajattelu

Syvyyssuuntainen turvallisuusajattelu kuvaa ydinvoima-alan kokonaisvaltaista turvallisuusfilosofiaa, jossa kaikki turvallisuuteen vaikuttavat seikat pyritään ottamaan huomioon. Syvyyssuuntainen turvallisuusajattelu kattaa kaikki voimalaitoksen osa-alueet organisaatiosta käytäntöjen kautta laitetasolle. Syvyydellä tarkoitetaan tässä yhteydessä sitä, että yhden turvallisuuselementin pettäminen ei johda välittömään pahimpaan mahdolliseen tilanteeseen, sillä tapahtumaketju pysähtyy seuraavaan turvallisuuselementtiin. (IAEA 1994, 9.) Loviisan voimalaitoksen tapauksessa

ympäristölle haitallisen materiaalin pääsy luontoon tarkoittaisi usean fyysisen esteen menetystä. Kuvassa 1 näitä fyysisiä esteitä ovat polttoaineniput, reaktoripainesäiliö sekä suojarakennus. Alla havainnekuva syvyyssuuntaisesta turvallisuusajattelusta ydinvoimalaitoksissa.



Kuva 2. Syvyyssuuntainen turvallisuusajattelu ydinvoimalaitoksissa (IAEA 2005, 14)

Kuva 2 havainnollistaa syvyyssuuntaisen turvallisuusajattelun ajatusmallia, jossa syvyyssuuntaisen turvallisuusajattelun ”syvyys” ei rajoitu vain fyysisiin esteisiin. Syvyyssuuntaisen turvallisuusajattelun käsitteellä on täten ulottuvuuksia myös toiminnallisella tasolla. Nämä ei-fyysiset tai toiminnalliset tasot luokitellaan niiden turvallisuustavoitteiden mukaan. Syvyyssuuntaisen turvallisuusajattelun tasot on määritelty kansainvälisen atomienergiajärjestön IAEA:n alaisuudessa toimivan kansainvälisen ydinturvallisuusryhmän INSAG:n toimesta. Syvyyssuuntaisen turvallisuusajattelun tasot on määritelty INSAG-10-raportissa (INSAG 1996). Syvyyssuuntaisen turvallisuusajattelun tasot turvallisuusmerkityksineen nähdään yllä olevasta kuvasta.

Turvallisuusajattelun ensimmäisellä tasolla pyritään estämään poikkeamia sekä käyttötapahtumia laitoksen normaalissa käytössä. Tähän tasoon liittyviä turvallisuusseikkoja ovat huolellinen suunnittelu, laadunvarmistus, valvonnalliset

toimenpiteet sekä yleinen turvallisuuskulttuuri. (IAEA 1994, 9.) Tämä taso tunnetaan suomalaisessa kirjallisuudessa ennalta ehkäisevänä tasona (Isolankila et. al. 2004 , 101).

Syvyyssuuntaisen turvallisuusajattelun toiseen tasoon kuuluvat varautuvat toimenpiteet liittyen epänormaaliin laitoskäyttöön tai vikaantuvaan laitosjärjestelmään. Tärkeimpiä turvallisuustavoitteita tällä tasolla ovat tapahtumien lieventäminen sekä onnettomuuksien estäminen. (IAEA 1994, 9.) Tästä tasosta voidaan käyttää suojaavan tason nimitystä (Isolankila et. al. 2004 , 101).

Kolmanteen tasoon liittyvillä toiminnoilla hallinnoidaan onnettomuuden etenemistä, jotta reaktorin sydänvauriota ei tapahtuisi. Kolmannella tasolla käytetyt turvallisuustoiminnot ovat suunniteltu hallinnoimaan oletettuja onnettomuuksia kuten jäähdytteenmenetysonnettomuutta tai kriittisyyden hallinnan menettämistä. Näillä toiminnoilla varmistutaan muun muassa reaktiivisuuden hallinnan ylläpitämisestä sekä polttoaineen jäähdytyksestä. Näiden toimintojen pettäessä on olemassa vakavan reaktorionnettomuuden riski. Reaktorionnettomuuden riskin takia suojarakennuksen tiiveyden varmistaminen on tärkeää. (IAEA 1994, 10.)

Todennäköisyys ympäristön kannalta vakavaan onnettomuuteen on hyvin pieni sellaisessa ydinvoimalaitoksessa, joka toimii ensimmäisen, toisen sekä kolmannen tason periaatteiden mukaisesti. Tällaisiin vakaviin onnettomuuksiin kuitenkin varaudutaan esimerkiksi valmius- sekä pelastusjärjestelyillä. (Isolankila et. al. 2004 , 101.)

INSAG-10-raportissa syvyyssuuntaisen turvallisuusajattelun taso neljä kuvailee erittäin epätodennäköisiä tilanteita, joita alkuperäisessä VVER-440-laitoksen suunnittelussa ei ole otettu huomioon. Tällaisia tilanteita ovat esimerkiksi jonkin turvallisuustoiminnon kaikkien redundanssien äkillinen menettäminen yhdistettynä alkutapahtumaan kuten primääripiirin putkimurtumaan. Tasolla neljä pyritään hallinnoimaan vakavan reaktorionnettomuuden seurauksia. Tason kolme kohdalla mainittujen turvallisuustoimintojen jatkaminen on tärkeää onnettomuuden etenemisen estämiseksi, jotta radioaktiivisten aineiden päästöä ympäristöön ei pääse tapahtumaan. Päästön estämiseksi suojarakennuksen tiiveyden varmistaminen suojarakennuksen painetta hallinnoivin toimenpitein on tärkeää varsinkin vakavan reaktorionnettomuuden jälkeisessä tilanteessa. Näiden toimenpiteiden oikea-aikaiseksi toteuttamiseksi

laitostilanteen tunnistaminen sekä tilanteen hallinnointi on tärkeää. Organisaation laajuinen varautuminen epätavallisiin tilanteisiin sekä onnettomuuksiin on oleellista korkean turvallisuustason saavuttamiseksi. (INSAG 1996, 10-12.)

Syvyyssuuntaisen turvallisuusajattelun tasolla viisi vakava reaktorionnettomuus on jo tapahtunut. Tason viisi toimenpiteet liittyvät onnettomuuden jälkeisen tilanteen seurausten lieventämiseen. Seurausten lieventämiseen sisällytetään muun muassa lähialueen ihmisten evakuointi, ensiavun antaminen sekä säteilytilanteesta tiedottaminen. Tällä tasolla luvanhaltijan organisaatio ei enää toimi yksin, sillä se tekee yhteistyötä eri viranomaistahojen kanssa edellä mainittujen toimenpiteiden toteuttamiseksi. (INSAG 1996, 12.) Yhteistyön puuttuessa tai epäonnistuessa tämä turvallisuustaso on pettänyt, jonka takia yhteistoimintaa on harjoiteltava määräajoin.

2.3 Valmiusjärjestelyt

Yleisesti ottaen radioaktiivisten aineiden päästön todennäköisyys on pieni, mutta koska se kuitenkin on olemassa, tulee vakaviin onnettomuustilanteisiin varautua valmiusjärjestelyin. Aiemmin läpikäydyn INSAG:n määritelmän mukaisesti laitoksen luvanhaltijalla sekä viranomaisella tulee olla suunnitelma onnettomuustilanteen varalle. Valmiusorganisaation sekä valmiussuunnitelman ylläpito on ydinvoimalaitoksen luvanhaltijan vastuulla. (Pöllänen et. al. 2004, 199.)

2.3.1 **Viranomaisvaatimukset**

Suomessa vaatimus valmiusjärjestelyiden olemassaololle tulee ydinenergialain 2 a -luvun 7 p §:stä. Laissa mainitaan, että voimalaitoksen valmiusjärjestelyjen suunnittelussa on varauduttava siihen, että laitokselta voi päästä ympäristöön merkittävä määrä radioaktiivisia aineita. Laissa vaaditaan myös valmiusorganisaation olemassaolo sekä organisaation riittävä toimintakyky koulutuksen, tilojen, varusteiden sekä viestintäjärjestelmien osalta. (L 1987/990.)

Tarkemmin suomalaisten ydinvoimalaitosten valmiusjärjestelyt käsitellään Säteilyturvakeskuksen (STUK) ydinturvallisuusohjeessa (YVL-ohje) C.5. Ohjeessa käydään kattavasti läpi seikat, jotka tulee ottaa huomioon ydinvoimalaitoksen valmiusjärjestelyissä. Näitä seikkoja ovat ydinenergialain säätämien kohtien lisäksi muun

muassa valmiussuunnitelma ja sen laatiminen, toiminta valmiustilanteissa, työntekijöiden turvallisuus sekä valmiuden ylläpito. (STUK 2020.) Loviisan voimalaitoksella YVL-ohjeen C.5 määrittelemät kohteet löytyvät laitoksen sisäisestä valmiuskansiosta, josta löytyvät toimintaohjeet jokaiselle valmiusorganisaation vakanssille (Felin 2019).

Voimalaitoksella valmiusjärjestelyjä edellyttävät tilanteet luokitellaan kolmeen eri luokkaan hallittavuuden perusteella. Valmiustilanteet luokitellaan varautumistilanteeseen, laitoshätätilanteeseen sekä yleishätätilanteeseen. Varautumistilanne määrätään poikkeuksellisissa tilanteissa, kun laitoksen turvallisuustaso halutaan varmistaa. Varautumistilanne voidaan määrätä esimerkiksi sekundääripiirin vuodon tai tulipalon vuoksi. Laitoshätätilanteessa laitoksen turvallisuuden taso on vaarassa heiketä merkittävästi. Laitoshätätilanne määrätään muun muassa primääripiirin vuodon takia. Yleishätätilanteessa tilanne on edennyt siihen pisteeseen, että on olemassa uhka radioaktiivisten aineiden leviämiselle ympäristöön esimerkiksi suojarakennuksen tiiveyden menetyksen yhteydessä. Yhteistä kaikille tilanteille on valmiusorganisaation hälyttäminen, valmiustilanteen julistaminen sekä toimenpiteet tilanteen tunnistamisessa ja hallintaan saamisessa. (Felin 2019.)

2.3.2 **Voimalaitoksen organisaatio**

Loviisan voimalaitoksella valmiusorganisaatio koostuu voimalaitoksella sekä Fortumin pääkonttorilla työskentelevistä asiantuntijoista. Valmiusorganisaatiota johtaa valmiuspäällikkö, jonka vastuulla on säteily- ja ydinturvallisuuteen liittyvien tehtävien johtaminen voimalaitosalueella valmiustilanteen aikana. Valmiuspäällikkö toimii yhteistyössä pelastustoimintaa johtavan viranomaisen kanssa. (Felin 2019.)

Valmiuspäällikön suorassa alaisuudessa toimivat muun muassa käyttöjohtaja, päivystävä turvallisuusinsinööri (PTI), säteilysuojelujohtaja, säteilymittauspäällikkö, korjausjohtaja, suojelujohtaja, sekä tilannekuvaryhmän päällikkö. Valmiustoiminnan aikana suurin osa valmiustoimintaan osallistuvista henkilöistä työskentelee valmiuskeskuksessa pois lukien PTI:n sekä apulaiskäyttöjohtajan, jotka toimivat laitosyksikön valvomossa valmiustoiminnan aikana. (Felin 2019.)

Valmiusorganisaatioon kuuluvat myös edellä listattujen esimiestason vakanssien komentoon kuuluvat ryhmät, joilla jokaisella on oma tehtävänsä valmiustoiminnan

aikana. Valmiusorganisaatioon kuuluu myös muutamia yhdyshenkilöitä, kuten STUK-yhdyshenkilö. Valmiusorganisaatioon katsotaan kuuluvan myös Fortumin pääkonttorilla sijaitseva teknisen tuen ryhmä, jonka tehtävänä on toimia asiantuntijana muun muassa vakavien reaktorionnettomuuksien hallinnassa sekä siihen liittyvissä järjestelmissä. Valmiusorganisaation lisäksi laitoksen sisäisiä valmiustoimintaan osallistuvia tahoja ovat laitosyksiköiden operaattorit sekä voimalaitoksen tehdaspalokunta. (Felin 2019.)

2.3.3 **Viranomaisen organisaatiot**

Valmiustoimintaan liittyy oleellisesti myös useita viranomaistoimijoita, joiden vastuita on kuvattu sisäasiainministeriön (SM) oppaassa. STUK ylläpitää tilannekuvaa säteilytilanteesta samalla toimien säteilyasiantuntijana valmiusorganisaatiolle sekä muille viranomaisille, kuten pelastusviranomaisille. Valmiustilanteessa STUK antaa suositukset väestön suojaamisesta, tiedottamisesta ja muista suojelutoimista perustuen sen ylläpitämään tilannekuvaan. Tilannekuvan muodostamisessa STUK toimii yhteistyössä voimalaitoksen valmiusorganisaation, Ilmatieteen laitoksen sekä pelastusviranomaisten kanssa. (SM 2012, 15.) STUK ylläpitää säteilytilanteen valvontaverkkoa, johon kuuluu 260 jatkuvatoimista automaattista mittausasemaa ympäri Suomea. Myös ydinvoimalaitosten varautumisalueille on määritelty manuaalisia mittapisteitä, joissa valmiustoimintaan osallistuvat tahot suorittavat osaltaan säteilynmittaustoimintaa. (SM 2012, 52).

Pelastustoimintaa johtaa pelastusviranomainen, joka toimii STUK:n suositusten mukaisesti. Valmiustoiminnan aikana pelastustoiminnan johtaja ylläpitää pelastustoimintaa pelastustoiminnan johtokeskuksessa. Pelastustoimi toimii suoraan pelastustoiminnan johtokeskuksen alaisuudessa tai välillisesti pelastustoiminnan johtoelimen alaisuudessa, jos tämän perustamiselle on tarve. Operatiivisia toimenpiteitä pelastustoimintaan liittyen on kuvattu yksityiskohtaisesti turvallisuusluokitellussa ulkoisessa pelastussuunnitelmassa. (SM 2012, 18.) Pelastustoimi suorittaa osaltaan säteilynmittausta vaara-alueen läheisyydessä toimittaen säteilymittaustuloksensa STUK:lle (SM 2012, 54).

Poliisi toimii yleistä turvallisuutta edistävissä tehtävissä myös valmiustoiminnan aikana. Se toimii yhteistyössä muiden viranomaisten kanssa mahdollistaen näiden toiminnan

häiriöittä. Se muun muassa eristää vaara-alueen, ohjaa liikennettä ja osaltaan tiedottaa tapahtumista lähialueen ihmisille. Jos valmiustoiminta on aloitettu rikosperusteisista syistä, on tilanteen vetovastuu kokonaan poliisilla pois lukien säteily- sekä laitosturvallisuuteen liittyvissä asioissa. Muissa tapauksissa poliisi toimii aiemmin mainituissa avustavissa tehtävissä. Tilanteissa, joissa selkeää johtovastuuta on mahdotonta määrittää, häiriöiden torjunta ja tilanteen johtaminen tapahtuu viranomaisten yhteistoimintana. Merialueilla väestön varoittamisen, evakuoinnin sekä meriliikenteen ohjaamisen hoitaa rajavartiolaitos. (SM 2012, 21.)

Edellä mainitut toimijat pelastustoimi, poliisi sekä rajavartiolaitos kuuluvat sisäasiainministeriön alaisuuteen. Sisäasiainministeriöllä on täten merkittävä rooli ydinvoimalaitoksiin liittyvissä valmiustilanteissa. STUK:n ja sisäasiainministeriön lisäksi valmiustoimintaan osallistuu viranomaisia muun muassa sosiaali- ja terveysministeriön, ympäristöministeriön, aluehallintaviraston sekä kunnan alaisuudesta. Näiden kaikkien toimintaan vaikuttaa STUK:n ylläpitämä ja raportoima tilannekuva säteilytilanteesta, joten asianmukaisen tilannekuvan ylläpitäminen on tärkeää. (SM 2012.) Täten valmiusorganisaation turvallinen ja luotettava toimiminen edesauttaa myös näiden viranomaisten toimintaa, sillä valmiusorganisaatio osallistuu osaltaan tämän tilannekuvan luomiseen.

Hätäkeskus on valmiustoiminnan kannalta tärkeässä roolissa, koska se hälyttää valmiusorganisaation sekä muut valmiustoimintaan liittyvät tahot vuoropäällikön ilmoituksesta (Felin 2019, 22). Jos kommunikaatioketju jostain syystä katkeaisi hätäkeskuksen sekä muiden tahojen välillä, voi organisoitumisen aloittaminen vaarantua. Myös hätäkeskus kuuluu sisäasiainministeriön hallinnonalaan. Hätäkeskus hälyttää vastuuviranomaiset sekä tarvittaessa muut tilanteeseen osallistuvat tahot hätäkeskukselle ennalta määritettyjen ohjeistuksien perusteella. (SM 2012, 47).

2.4 Riskienhallinta

Riskienhallinnalla tarkoitetaan koordinoitua toimintaa, jolla organisaatiota johdetaan ja ohjataan riskien osalta (SFS-ISO 31000 2018, 6). Riskienhallinnan on oltava organisaation johtamisjärjestelmään sisällytetty siten, että kaikki organisaation toiminnot on sisällytetty riskienhallintaprosessiin, jotta riskienhallintaa pystytään kehittämään

jatkuvasti koko organisaatiossa. Tämän saavuttamiseksi kaikki organisaation sidosryhmät on otettava mukaan riskienhallintaprosessiin. Riskienhallinta on sovitettava organisaatiolle sopivaksi siten, että se asettuu organisaation toimintaympäristöön. Oikein toteutettu riskienhallinta on ajantasaista ja järjestelmällistä riskienhallinnan tuottamien tulosten vertailun mahdollistamiseksi. Riskienhallinnan on oltava dynaamista, jotta uusien riskien ilmaantuminen, riskien muuttuminen tai poistuminen ei aiheuttaisi ongelmia riskienhallintaprosessissa. (SFS-ISO 31000 2018, 8.)

Tämä diplomityö kuuluu riskienhallintaprosessiin riskien arvioinnin osa-alueeseen riskien tunnistamisen osalta. Tässä riskienhallintaprosessin vaiheessa löydetään, havaitaan sekä kuvataan riskejä, jotka voivat vaikuttaa organisaation tavoitteiden saavuttamisessa. Riskien tunnistamisessa tulee ottaa huomioon useita eri tekijöitä riskin syntytekijöihin liittyen, joista esimerkkinä voidaan mainita prosessin tilaan liittyvät väärät oletukset sekä syyt näiden oletuksien taustalla. (SFS-ISO 31000 2018, 16-17.)

Riskien tunnistamisen jälkeen riskien merkitystä arvioidaan päätöksenteon tukemiseksi. Tällaista riskien merkityksen arviointia suoritetaan vertaamalla tehdyn riskianalyysin tuloksia ennalta määritettyihin riskikriteereihin. Riskien arvioinnin perusteella voidaan päättää jatkoanalyysin tarpeesta, hallintakeinojen vaihtoehdoista tai tavoitteiden uudelleenmäärittämisestä. (SFS-ISO 31000 2018, 18.)

2.5 Polarion-ohjelmisto

Polarion-ohjelmisto on Loviisan voimalaitoksella käytössä oleva alun perin vaatimustenhallintaan suunniteltu ohjelmisto. Ohjelmiston perusominaisuuksiin kuuluu elementtien välinen linkitys ja näiden linkkiroolien visualisointi. Näitä elementtejä kutsutaan ohjelmistossa work itemeiksi ja käytännössä koko ohjelmisto rakentuu näiden elementtien päälle. Work itemeille voidaan määrittää tyyppikohtaisesti eri attribuutteja, joiden avulla work itemeitä voi suodattaa, taulukoida tai visualisoida muussa muodossa. Polarion ohjelmisto taipuu hyvin monentyyppiseen käyttötarkoitukseen ja sitä on käytetty Loviisan voimalaitoksella muun muassa muutamille tarkastuslistoille, toimintasuunnitelmille sekä YVL-ohjeiden kommentointiin ja seurantaan. (Pirinen 2018.)

Work itemeitä voi luoda, muokata ja muutenkin ylläpitää lähes samoin kuin esimerkiksi Word-tekstinkäsittelyohjelmassa. Tällainen ylläpito on mahdollistettu LiveDoc-

asiakirjapohjaan. Yksi work itemien ja LiveDocien mahdollistama ominaisuus on tarkastuskierron suorittaminen kappalekohtaisesti, jolloin koko asiakirjaa ei tarvitse hyväksyttää jokaisen muutoksen kohdalla. (Pirinen 2018). Tämän diplomityön case-tutkimuksessa tehty analyysi laaditaan tällaiseen LiveDoc-pohjaan, johon analyysin elementit luodaan work item -nimikkeinä.

Polarion-ohjelmistossa on mahdollista luoda omia skriptejä ja widgettejä datan visualisointiin. Pääosin skriptejä luodaan JavaScript-kieleen perustuvalla Velocity-kielellä. Useat tämän diplomityön lopussa esitellyt case-tutkimuksen tulokset tullaan esittelemään tällaisten widgettien avulla.

3 TURVALLISUUSTEKNIIKKA

Nykyaikaisissa järjestelmissä on monentyyppistä kompleksisuutta. Järjestelmien sisällä voi olla useita alajärjestelmiä, jotka kaikki vaikuttavat toistensa toimintaan. Järjestelmissä voi olla myös dynaamista kompleksisuutta, jossa muutos tapahtuu suhteessa ajan muutokseen. Järjestelmään voi myös vaikuttaa seikkoja, joita ei ole edes tiedostettu tai syy-seuraus-suhde ei ole muuten selvillä. Näiden seikkojen takia jotkin järjestelmät esimerkiksi voimalaitoksissa voivat olla niin monimutkaisia käyttää ja ymmärtää, että täysimittaseen järjestelmän hallintaan vaaditaan useita eri asiantuntijoita. (Leveson 2011, 4.)

Kompleksisuuteen liittyvä iso muutos nykyaikaisissa järjestelmissä on koneellisten laitteiden, automaation sekä ihmisten välisen yhteistyön lisääntyminen. Ihmistoimijat saattavat tiedostamattaan aiheuttaa koneiden ja laitteiden käytön myötä virhetilanteita esimerkiksi väärien olettamuksien myötä tilanteissa, joissa laitteiden käytöllä on jotain ennalta huomaamattomia vaikutuksia. Toisaalta nykyaikaisissa kompleksisissa järjestelmissä virhetilanne laitetaan usein ihmisoperaattorin syyksi, vaikka todellinen syy on ollut muualla kuten esimerkiksi suunnitteluvirheissä. (Leveson 2011, 5.)

Myös kyky oppia aiemmista virheistä sekä tapahtumista on heikentymässä teknologian nopean kehityksen sekä markkinoilta tulevan paineen myötä. Teknologia kehittyy nopeasti, jolloin vuosien mittaan kerätty data vanhenee nopeammin teknologian muuttumisen myötä. Markkinoilta tuleva paine vähentää yrityksien mahdollisuutta tuottaa kattavaa analysointia sekä testausta järjestelmilleen, koska järjestelmä täytyy saada markkinoille nopeammin. (Leveson 2011, 3.)

Muun muassa nämä edellä mainitut asiat luovat yhteisvaikutuksena uusia uhkatilanteita eri yrityksille sekä niitä ympäröiville yhteisöille. Tieteen ja teknologian kehittyessä ihmiset joutuvat yhä useammin sellaisten aineiden vaikutuksen alaisiksi, joiden vaikutuksia ei täysin tiedetä. Esimerkkinä tästä voidaan mainita lääketeollisuuden tuottamat tuotteet. (Leveson 2011, 4.)

3.1 Perinteinen lähestymistapa turvallisuustekniikkaan

Asioiden suunnittelemattomaan tapahtumiseen on havahduttu jo sivilisaation alkuaikoina. Kuitenkaan kehitystä turvallisuustekniikan tai riskianalyysien osalta ei tapahtunut ennen teollista vallankumousta ja 1800-luvun loppua, jolloin havahduttiin kasvavaan entistä luotettavampien laitteiden tarpeeseen. Toisen maailmansodan myötävaikutuksesta ensimmäisiä luotettavuustekniikan analyysejä alettiin kehittämään luotettavuuteen liittyvien ongelmien ratkaisemiseksi. Samaan aikaan järjestelmät alkoivat olemaan entistä kompleksisimpia, joka vaikutti muun muassa vikapuuanalyysin tai vika- ja vaikutusanalyysin kehitykseen. Näitä hasardianalyysejä käytetään mahdolliseen onnettomuuteen johtavien riskien löytämiseen. Tultaessa 1940-luvun lopulle luotettavuustekniikka oli laajalti hyväksytty ja käytetty tieteenala. (Hollnagel 2012, 3-4.)

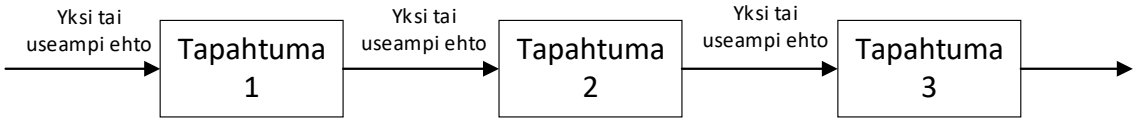
Todennäköisyyspohjaisen riskianalyysin kehitystyö aloitettiin, kun havaittiin, että luotettavuustekniikka ja todennäköisyysteoria toimivat tehokkaasti yhdessä analysoitaessa ja vertaillessa järjestelmien luotettavuustasoja. Todennäköisyyspohjainen riskianalyysi otettiin laajasti käyttöön heti ydinvoimatekniikan alkuajoilta lähtien, sillä sen avulla pystyttiin löytämään mahdollisia onnettomuuksiin johtavia vikaantumisesta tai muista tapahtumista johtuvia alkutapahtumia sekä niiden todennäköisyyksiä. Huomattavaa kuitenkin on se, että ennen Three Mile Islandin (TMI) -onnettomuutta vuonna 1979 luotettavuustekniikan alalla käytetyt analyysimallit kuten vika- ja vaikutusanalyysi sekä vika- ja tapahtumapuut eivät ottaneet huomioon inhimillisiä tekijöitä. TMI:n onnettomuus toimi eräänlaisena uuden ajan aloittajana, jolloin myös inhimillisiä tekijöitä alettiin sisällyttää käytettyihin analyysimenetelmiin. (Hollnagel 2012, 4.)

3.1.1 Periaatteet perinteisissä menetelmissä

Perinteisesti kompleksisuutta hallitaan pilkkomalla tutkittava järjestelmä pienempiin elementteihin, joita on siten helpompi tutkia ja analysoida. Pienemmät elementit siten eristetään muusta järjestelmästä ja järjestelmän kokonaisvaltaisen analysoinnin lopputulos saadaan kokoamalla elementtien analyysit yhteen. (Leveson & Thomas 2018, 5).

Edellä mainittu elementteihin jako on yksi vika- ja vaikutusanalyysin perusperiaatteista, sillä siinä järjestelmän analysointi aloitetaan pilkkomalla järjestelmä komponentteihin, joiden vikaantumistapoja, vikaantumiseen johtavia syitä sekä vikaantumisen vaikutuksia tarkastellaan (Sulaman et. al. 2019). Myös todennäköisyyspohjainen riskianalyysi käyttää tällaista elementteihin pilkkomista riskien analysoinnissa alkutapahtumien avulla (Leveson 2011, 33). Molemmissa analyysimenetelmissä oletetaan, että järjestelmään ei vaikuta näiden elementtien lisäksi muita ulkopuolisia asioita.

Perinteisessä turvallisuustekniikan lähestymistavassa ajatellaan, että esimerkiksi järjestelmän komponentit ovat suoraan linkittyneinä toisiinsa siten, että komponenttien keskinäinen vuorovaikutus on aina tietynlainen. Tässä ajattelumallissa tapahtuma tapahtumaketjun alkupäässä aiheuttaa seuraavan tapahtuman joko yksin tai yhdessä useamman tapahtuman kanssa. (Leveson & Thomas 2018, 5.) Alla havainnollistava kuva tapahtumaketjusta.

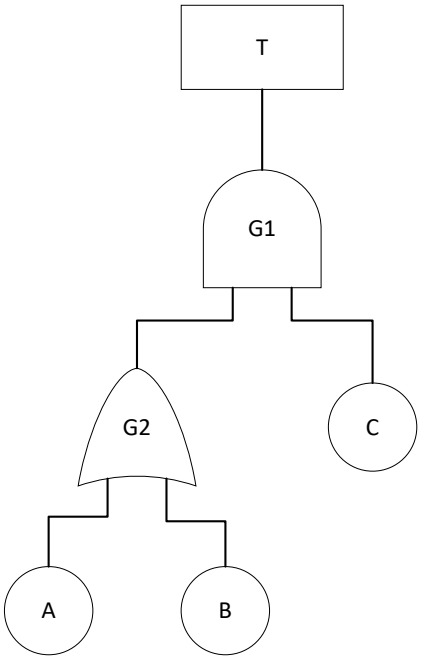


Kuva 3. Tapahtumaketju, jossa alkutapahtuma tapahtuu tiettyjen ehtojen täyttyessä

Kuva 3 havainnollistaa yksinkertaisinta tapahtumaketjuajatusmallia, jota käytetään perinteisissä luotettavuus- sekä turvallisuustekniikan analyysimenetelmissä. Aiemmin mainittujen seikkojen perusteella, perinteisestä turvallisuustekniikasta voidaan todeta, että se perustuu tiettyihin oletuksiin analysoitavan kohteen luonteesta. Perinteisessä turvallisuustekniikassa oletetaan, että rinnakkaiset toiminnot järjestelmän sisällä ovat toisistaan riippumattomia, jos ei voida suoraan osoittaa, että nämä rinnakkaiset toiminnot ovat vuorovaikutuksessa keskenään. Toisaalta myös oletetaan, että mainitut toiminnot toimivat aina samoin riippumatta siitä, tarkastellaanko niitä yksitellen vai yhtenä kokonaisuuden osana. Nämä rinnakkaiset toiminnot eivät tämän lisäksi vaikuta toisiinsa millään epäsuoralla tavalla perinteisissä turvallisuustekniikan analyysimalleissa. (Leveson & Thomas 2018, 6.) Nämä oletukset auttavat yksinkertaistamaan esimerkiksi todennäköisyyspohjaisen riskianalyysin todennäköisyyksien laskentaprosessia, mutta yksinkertaistusten lisääntyessä analyysi erkaantuu reaalimaailmasta. (Leveson 2011, 33).

Vuonna 1931 julkistettu domino-malli on yksi ensimmäisistä onnettomuusmalleista. Domino-mallissa onnettomuuteen johtavat syyt on kuvattu dominopalikoina, eli yhden palikan kaatuminen johtaa automaattisesti seuraavan palikan kaatumiseen. Tämän mallin taustalla vaikuttava ajatusmaailma on tänäkin päivänä nähtävissä turvallisuustekniikkaan liittyvissä onnettomuuden syntyä kuvaavissa malleissa. Tämä voidaan havaita esimerkiksi vika- tai tapahtumapuista, joissa jokin alkutapahtuma aiheuttaa tietyn ehdon toteutuessa seuraavan tapahtuman. Myös aiemmin mainittu syvyyssuuntainen turvallisuusajattelu (kuva 2) pohjautuu domino-malliin, sillä myös siinä tietty tapahtuma johtaa seuraavaan tapahtumaan jonkin turvallisuusjärjestelmän tai -toiminnon pettäessä. (Leveson 2011, 16-17.)

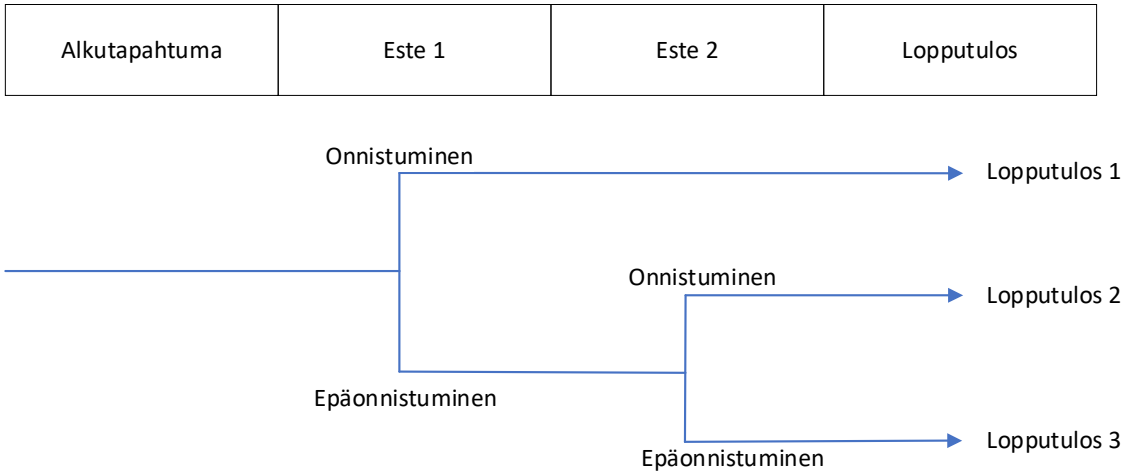
Onnettomuusmallit ovat kehittyneet domino-mallista paljon muun muassa ottamalla huomioon laajempia kokonaisuuksia sekä tekijöitä onnettomuuksien taustalla. Domino-malli on suhteellisen suppea ja se olettaa onnettomuudesta johtuvan loukkaantumisen johtuvan aina tapahtumaketjun aloittaneesta henkilöstä sekä hänen sosiaalisesta ympäristöstään. (Leveson 2011, 16) Nykypäivän yleisimmät onnettomuusmallit kuitenkin kuvaavat onnettomuuksia lukuisien eri tekijöiden tai tapahtumien avulla eikä niissä välttämättä oleteta, että yksi tapahtuma johtaa automaattisesti seuraavaan. Vikapuu on esimerkki tällaisesta onnettomuusmallista. (Leveson 2011, 19) Alla havainnollistava kuva vikapuusta.



Kuva 4. Yksinkertainen vikapuu, jossa on kolme alkutapahtumaa

Kuva 4 visualisoi järjestelmää, jossa puun yläosassa oleva tapahtuma *T* toteutuu, jos tapahtuma *C* tapahtuu yhdessä tapahtuman *A* tai *B* kanssa. Puussa oleva portti *G1* siis vaatii, että sen molemmat haarat tapahtuvat ja portin *G2* tapahtumiseen riittää jommankumman alla olevan alkutapahtuman tapahtuminen.

Huomioitavaa nykyisin yleisesti käytetyissä onnettomuusmalleissa on se, että niiden mukaan onnettomuutta ei tapahdu ilman alkutapahtuman tai tietyn alkutapahtumaryhmän ilmenemistä. Huomioitavaa on myös se, että nämä yleisimmät onnettomuusmallit asettavat onnettomuuden syyksi usein laitteen vikaantumisen, ihmisen tekemän virheen tai energeettisen tapahtuman, kuten räjähdyksen, riippuen täysin siitä miten alkutapahtumat on määritetty. (Leveson 2011, 17.) Alla havainnollistava kuva tapahtumapuusta.



Kuva 5. Yksinkertainen tapahtumapuu, jossa kaksi estettä/turvallisuustoimintoa ja 3 mahdollista lopputulosta

Onnettomuutta analysoidessa onnettomuuden syyksi usein laitetaan se tekijä tai ne tekijät, jotka vaikuttavat syyllisiltä nimenomaan analyysissä käytetyn tapahtumapuun tai muun käytetyn mallin mukaan, vaikka todellisuudessa näihin syyllisiksi todettuihin tekijöihin on voinut vaikuttaa useita muita tai mallin ulkopuolisia tekijöitä (Leveson 2011, 20). Yllä olevan kuvan esittämässä tapahtumapuussa täten onnettomuutta tai muuta lopputulosta ei tapahdu ilman ennalta määritetyn alkutapahtuman ilmenemistä.

3.1.2 Perinteisiin menetelmiin liittyvät ongelmat

Perinteisissä analysointimalleissa ja menetelmissä käytetyt yksinkertaistukset voivat aiheuttaa vääristymiä tai puutteita analyysin lopputuloksissa. Vääristyneiden tuloksien seurauksena analysoitavan järjestelmän luotettavuuden tai turvallisuuden tilasta voidaan saada vääristyneitä tuloksia tai onnettomuuden aiheuttajista voidaan päätyä vääriin johtopäätöksiin.

Tapahtumapuiden alkutapahtumien määritys riippuu käytännössä siitä, miten tarkasti tapahtumia halutaan mallintaa. Alkutapahtuman määritys riippuu analyysiä tekevästä organisaatiosta, sillä eri organisaatioissa voi olla erilainen ohjeistus näihin tapahtumiin liittyen. Eri organisaatio saattavat siis määrittää alkutapahtumat eri tavoin, jolloin eri organisaatioiden tekemät analyysit voivat olla keskenään hyvinkin erilaisia. Tästä voi aiheutua ongelmia, jos analyysin perusteella tehdään toimenpiteitä, jotka todellisuudessa eivät vaikutakaan onnettomuuden tai tapahtuman syntyyn. Esimerkiksi erään Chicagossa vuonna 1979 tapahtuneen DC-10-lentokoneen onnettomuuden syyksi todettiin huoltotyöstä aiheutunut halkeama, vaikka todellisuudessa onnettomuuden aiheutti lentokoneen suunnitteluvirheestä aiheutunut siiven epäkuntoisuuteen liittyvä ongelma. Väärin tunnistetun alkutapahtuman takia tulevia samasta syystä aiheutuneita onnettomuuksia ei voitu ennaltaehkäistä. Tällainen subjektiivisuudesta aiheutunut ongelma pätee alkutapahtumien lisäksi myös muiden prosessin tapahtumien sekä tapahtumien välisen linkityksen määritykseen. (Leveson 2011, 21-22.)

Tapahtumapuut ovat ongelmallisia niiden olettaman suoran syy-seuraus-suhteen takia. Ne eivät havainnollista mallin ulkopuolisten tapahtumien vaikutusta analysoitavaan prosessiin eivätkä ne pysty muiden kuin lineaaristen sekä suorien keskinäisten tapahtumien välisten vaikutusten analysointiin. Lausetta ”tupakointi aiheuttaa keuhkosyöpää” ei olisi sallittua käyttää tapahtumaketjumaisessa ajattelussa, koska näiden välillä ei ole suoraa suhdetta. Näiden asioiden välillä on toki tieteellisesti todistettu kompleksinen ja epäsuora yhteys, mutta tätä yhteyttä ei ole mahdollista kuvata tapahtumapuumalleilla välittömän ja ainoan yhteyden puuttuessa. (Leveson 2011, 19.)

Todenmukaisemman onnettomuusanalyysin aikaansaamiseksi tulisikin olettaa, että onnettomuudet aiheutuvat niin monimutkaisten sosioteknisten prosessien kautta, että

tapahtumapuumalleilla niitä ei täysin kattavasti voi analysoida. Tämä uusi olettamus perustuu luvun alussa mainittuihin haasteisiin, joita eri organisaatiot kohtaavat modernissa yhteiskunnassa. Onnettomuuden juurisyyn käsite voi olla ongelmallinen, koska se ei välttämättä tarjoa tarpeeksi laajaa käsitystä esimerkiksi onnettomuuteen johtaneista todellisista syistä. (Leveson 2011, 31-33.)

Perinteisessä turvallisuustekniikassa oletetaan, että luotettavuuden parantaminen lisää automaattisesti turvallisuutta (Leveson 2011, 7). Tällainen ajattelu on loogista ottaen huomioon sen, että tapahtumapuussa alkutapahtuma tai muu tapahtuma tapahtuu aina tietyllä todennäköisyydellä. Tästä johtuen myös tapahtumapuun yläpäässä oleva onnettomuus tapahtuu myös tietyllä todennäköisyydellä. Näin ollen, jos tapahtumat muuttuvat epätodennäköisemmiksi, myös onnettomuuden todennäköisyys pienenee. Toisin sanoen tällä logiikalla koko järjestelmästä tulee luotettavampi.

On kuitenkin huomattava, että turvallisuus sekä luotettavuus ovat kaksi eri asiaa. Turvallisuus ei vaadi luotettavuutta ja sama toisinpäin. Todellisuudessa jokin järjestelmä tai organisaatio voi toimia luotettavasti, mutta epäturvallisesti. (Leveson 2011, 7)

Englantilaisessa kemikaalilaitoksessa tapahtui onnettomuus, vaikka laitoksen turvallisuusjärjestelmät toimivat täysin turvallisuussuunnittelun mukaisesti. Laitosta ohjasi laitostietokone, jonka vastuulla oli kemikaalin tuottaminen reaktorissa sekä reaktorin jäähdytys. Käytännössä laitosta ohjattiin kahdella venttiilillä, joista toisella aloitettiin tuotanto ja toisella aloitettiin jäähdytys. Laitostietokone oli ohjelmoitu siten, että epätavallisen tilanteen sattuessa venttiilien tuli jäädä paikoilleen. Ennen onnettomuutta laitostietokone sai tiedon epätavallisesta tilanteesta, jolloin tietokone jätti ohjeistuksen mukaisesti venttiilit paikoilleen. Sattumalta kemikaalin tuotanto oltiin juuri aloitettu, jonka takia jäähdytysvesiventtiili oli vasta aukeamassa. Laitostietokone ei jatkanut venttiilin avaamista epätavallisen tilanteen alkaessa, joten reaktorin jäähdytys jäi riittämättömälle tasolle. Onnettomuuden seurauksena kemikaalintuotantoon tarkoitetun reaktorin sisältämä vaarallinen kemikaali pääsi ympäristöön varoventtiilin avautuessa paineen kasvaessa tarpeeksi suureksi. (Leveson 2011, 9.)

Vastaava tilanne on tuttu myös ydinvoima-alalla. Amerikkalaisissa ydinvoimalaitoksissa tapahtui useita tarpeettomia laitoksen alasajoja johtuen vikaantuneista reaktorin tilaa

mittaavista sensoreista. Esimerkiksi reaktorin jäähdytevirtauksen mittarin vikaantuessa reaktori menee pikasulkuun, koska kattavaa tilannetietoa ei enää saatu. Vikaantumisista aiheutuneita pikasulkuja pyrittiin estämään redundanttisilla mittalaitteistoilla, jolloin yhden sensorin vikaantuminen ei vielä aiheuttaisi pikasulkua. Uusi järjestelmä todettiin todennäköisyyspohjaisella riskianalyysillä luotettavammaksi verrattuna edelliseen järjestelmään, mutta analyysi ei kyennyt löytämään järjestelmän muutoksesta aiheutunutta järjestelmätason ongelmaa. Uudessa järjestelmässä laitostietokoneen täytyi vertailla redundanttisia sensoreita toisiinsa, jotta jonkun sensorin vikaantuminen pystyttäisiin havainnoimaan. Näin ollen, jos sensori ilmoittaa normaalia alhaisemman tai normaalia korkeamman virtauksen, sensori todetaan vikaantuneeksi. Suunnitelmassa ei otettu huomioon sitä faktaa, että pääkiertopumpun redundanssia vaihdettaessa esimerkiksi vuosihuollon yhteydessä, reaktoriin virtaava jäähdytevirtaus on hetkellisesti normaalia korkeampi. Tämän seurauksena reaktori meni lähes joka kerta pikasulkuun, kun virtaama oli normaalia tehokäyttöä korkeampi normaalien huoltotoimenpiteiden seurauksena. (Thomas 2019.)

Oleellista luotettavuuden ja turvallisuuden vertailussa on myös ihmisoperaattorin toiminnan tarkastelu. Ihmisoperaattorin tapauksessa luotettavuudella tarkoitetaan toimimista ennalta määritettyjen toimintaohjeistusten mukaisesti. Epäluotettavaksi toiminnaksi luokitellaan taas kaikki toimintaohjeistuksen ulkopuoliset toiminnot. Maailmalla on kuitenkin ollut tapahtumia ja tilanteita, joissa operaattorin toimiminen luotettavasti on johtanut onnettomuuteen sekä tapauksia, joissa poikkeaminen toimintaohjeistuksista on estänyt onnettomuuden tapahtumisen. Näistä ensimmäiseen kuuluu muun muassa TMI-ydinonnettomuus. (Leveson 2011, 10) TMI:n tapauksessa operaattoreita ei oltu koulutettu tilanteeseen, jossa paineistimen varoventtiili ei sulkeudukaan eikä tällaisesta tilanteesta ollut mitään mainintaa operaattorien hätätilanteen toimintaohjeessa. Operaattoreiden tilannetta vaikeutti entisestään se, että heillä ei ollut saatavilla tilatietoa reaktorin paineastian vedenpinnasta, minkä seurauksena operaattorit olettivat reaktorin vedenpinnan tason olevan sallitulla tasolla. Operaattorit toimivat saatavilla olevan ohjeistuksen sekä käytössä olevan puutteellisen ja harhaanjohtavan tilannetiedon mukaisesti. Tämän seurauksena operaattorien toiminta tilanteen parantamiseksi johti käytännössä vain tilanteen huononemiseen. (NRC 2016, 8)

Korkea luotettavuuden taso jollekin järjestelmälle ei siis automaattisesti takaa korkeaa turvallisuuden tasoa. Näin ollen, luotettavuustekniikasta tuttujen menetelmien rinnalla turvallisuutta analysoitaessa tulisikin käyttää muita analyysimenetelmiä, joissa järjestelmätason turvallisuutta pystyttäisiin tarkastelemaan kokonaisvaltaisemmin ottamalla huomioon luotettavuuden ulkopuolisia systeemin normaaliin operointiin liittyviä muutostilanteista aiheutuvia ongelmia. (Leveson 2011, 14.)

Usein onnettomuuksia analysoidessa ja tutkiessa päädytään syyttämään järjestelmän ihmisoperoijia. Tällaisiin virheellisiin syytöksiin saatetaan päätyä varsinkin sellaisissa onnettomuuksissa, joissa operaattori on joutunut toimimaan harhaanjohtavan tai kokonaan puutteellisen tilannetiedon puitteissa. Moderneissa kompleksisissa järjestelmissä on lukuisia komponenteista koostuvia keskenään toimivia järjestelmiä, joiden vikaantuminen saattaa aiheuttaa ennalta arvaamattomia vaikutuksia myös muissa kuin vikaantuneessa komponentissa tai järjestelmässä. Näin ollen operaattori saattaa toimia jälkeenpäin analysoituna täysin epäturvallisella tavalla, jos operaattori on joutunut toimimaan harhaanjohtavan informaation puitteissa, kuten esimerkiksi TMI:ssä tapahtui. (Leveson 2011, 36-39.)

Ehkä tärkein seikka ihmisoperaattorin toiminnan tarkastelussa on se, että ihmisen toimintaan vaikuttaa aina toimintaympäristö. On väärin olettaa, että ihminen tulisi toimimaan aina konemaisesti tietyssä tilanteessa riippumatta ihmisen taustasta tai ympäröivästä ympäristöstä. Yleisesti ottaen on huonoa insinöörityötä suunnitella järjestelmiä huolimattomasti ja syyttää ihmisoperaattoria virheiden sattuessa. (Leveson 2011, 47.)

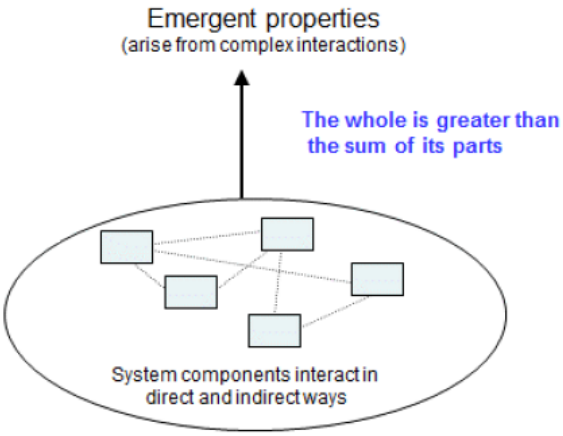
Perinteistä turvallisuustekniikkaa on pyritty asteittain kehittämään edellä mainittujen ongelmien hallinnoimiseksi. Turvallisuustekniikkaa sekä siihen liittyviä analysointimenetelmiä tuleekin jatkuvasti kehittää, jotta jatkuvasti monimutkaisempia järjestelmiä voidaan jatkossakin operoida turvallisesti. (Leveson 2011, 6.) Yksi vaihtoehto uudelle suuntaukselle turvallisuustekniikkaan liittyen on systeemiteorian hyödyntäminen.

3.2 Systeemiteoreettinen lähestymistapa turvallisuustekniikkaan

Uusien analyysimenetelmien tarpeeseen havahduttiin edellä mainittujen ongelmien yleistyessä. Yksi kehitysaskel analyysimenetelmiin inhimillisen tekijän lisäksi oli organisaatioiden mukaan ottaminen analyysien kohteiksi. Vaikka Tšernobylin onnettomuus nähtiin länsimaissa lähinnä Neuvostoliiton omana ongelmana, voi sen silti katsoa myötävaikuttaneen uuteen maailmanlaajuiseen tarpeeseen analysoida isompaa organisaatiota järjestelmien turvallisuutta tarkasteltaessa. Perinteiset analyysimenetelmät, jotka ovat alun perin suunniteltu komponenttitason analysointiin, eivät sovellu tällaiseen organisaatioiden analysointiin, joten tarve uusille ajatusmalleille oli syntynyt. Vaikka Tšernobylin onnettomuudesta ja muista myötävaikuttaneista tapahtumista on jo aikaa, on turvallisuustekniikka tieteenalana edelleen muutosvaiheessa perinteisestä ajatusmallista uusiin malleihin. Tämän muutosvaiheen olemassaolo voidaan edelleen havaita organisaation turvallisuuskulttuurista riippuen tietynlaisena optimistisuutena siihen, että perinteiset ajatusmallit olisivat jollain tapaa muokattavissa ottamaan huomioon myös organisaatioiden vaikutuksen itse analysoitavaan kohteeseen. (Hollnagel 2012, 5-6.)

3.2.1 Systeemiteoria osana turvallisuutta

Systeemiteoriassa analysoitavia kohteita ei pilkota pienempiin erikseen analysoitaviin elementteihin samoin kuin perinteisissä menetelmissä, vaan tarkasteltavaa kohdetta analysoidaan kokonaisuutena. Systeemiteorian taustalla vaikuttavat vahvasti hierarkian sekä emergenttien ominaisuuksien tarkastelu. Emergenteillä ominaisuuksilla tarkoitetaan sellaisia asioita, joita yksittäistä komponenttia tai toimijaa tarkastelemalla ei pystytä havainnoimaan, mutta näistä muodostuvaa kokonaisuutta tarkastelemalla, komponenttien vaikutus aletaan nähdä eri tavalla. Tästä esimerkkinä voidaan mainita aiemmin tarkasteltu luotettavuuden sekä turvallisuuden eroavaisuus. Yksittäisellä komponentilla on selkeästi jokin luotettavuuden taso, mutta pelkästään yhtä komponenttia tarkastelemalla, sen vaikutusta järjestelmän kokonaisvaltaiseen turvallisuuteen ei voida havaita. (Leveson 2011, 61-62.) Alla havainnollistava kuva emergentismistä.



Kuva 6. Emergenttisen ominaisuuden syntyminen systeemin komponenttien yhteisvaikutuksesta (Leveson & Thomas 2018, 11)

Yllä olevan kuvan perusteella voidaan todeta, että komponenttien täytyy jollain tavoin keskustella sekä hallinnoida toisiaan, jotta emergentti ominaisuus eli esimerkiksi turvallisuus ylipäätään syntyy. Hierarkia systeemin sisällä taas määrää sen, miten systeemi toimii. Se linkittää systeemin eri komponentit toisiinsa sekä määrittää niiden väliset vastuut pitäen huolen siitä, että systeemin komponentit toimivat emergenttisen turvallisuuden määrittämissä puitteissa. (Leveson 2011, 62-64.)

Eri hierarkian tasojen välistä yhteyttä voidaan kutsua kommunikaatioksi sekä kontrolliksi. Hierarkiassa ylempänä olevat tahot määrittelevät alempana oleville tahoille rajoitteita tai vaatimuksia, jotta järjestelmätason vaatimus voidaan saavuttaa edellä mainitun emergentin ominaisuuden määritelmän mukaisesti. Ylempänä olevilla tahoilla tulee olla jokin keino kommunikoida alempien tahojen kanssa kontrollin ylläpitämiseksi. Kommunikaation tulee toimia tahojen välillä molempiin suuntiin, jotta ylempi taho voi tarpeen tullen reagoida muuttuneeseen tilanteeseen. (Leveson 2011, 64-65).

Esimerkkinä tällaisesta edellä mainitusta hierarkian eri tasojen välisestä kommunikaatiosta on muun muassa operaattorin sekä kontrolloitavan prosessin välillä. Operaattorin täytyy operoida voimalaitosta turvallisuusparametrien määrittämien rajojen sisällä, mutta operaattorilla täytyy myös olla reaaliaikainen tilannetieto voimalaitoksen tilasta, jotta esimerkiksi epäturvallisissa tilanteissa tilannetta korjaaviin toimenpiteisiin voidaan ryhtyä. Ilman tilannetietoa voimalaitokselta, operaattorilla ei ole mahdollisuuksia reagoida muuttuviin tilanteisiin. Tällainen järjestelmän kontrollointi

järjestelmän tarjoaman takaisinkytkennän puitteissa on osa säätöteoriaa, jota tarkastellaan seuraavassa luvussa tarkemmin. (Guarnieri & Garbolino 2019, 124).

Systeemiteorian lähestymistapa onnettomuuksiin ja niiden analysointiin on erilainen verrattuna aiemmin mainittuihin luotettavuustekniikasta tuttuihin menetelmiin. Sen mukaan onnettomuudet tapahtuvat järjestelmän komponenttien välisestä vuorovaikutuksesta eikä systeemiteoria aina välttämättä määrittele yksittäistä tekijää onnettomuuden aiheuttajaksi. Emergenttisen ominaisuuden määritelmän mukaan turvallisuuden puute johtuu puutteellisesta kontrollista tai hallinnasta. Onnettomuuksia tapahtuu kun komponentti vikaantuu, ulkoinen vaaratekijä ilmenee tai järjestelmän elementit vuorovaikuttavat keskenään epäturvallisella tavalla, eikä näitä ilmiöitä hallinnoida asianmukaisesti. (Leveson 2011, 67-68.)

Ensimmäiset systeemiteoriaan liittyvät projektit olivat osa Yhdysvaltain aseteollisuuden mannertenvälisten ohjusten kehitystyötä 1950- ja 1960-luvuilla. Systeemiteoriaa hyödynnettiin aseteollisuuden ulkopuolella ensimmäisen kerran Apollo-avaruusohjelmassa. (Leveson 2011, 69).

3.2.2 **Säätöteoria systeemiteorian yhteydessä**

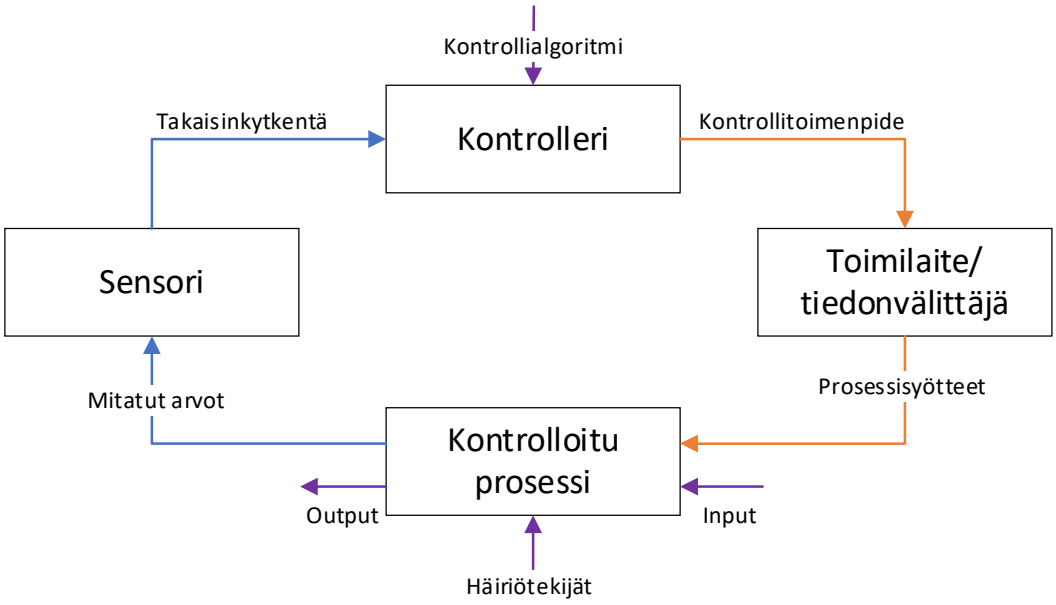
Säätöteorian peruskäsite on takaisinkytkentä, jonka avulla säätöteoria kuvaa dynaamisten järjestelmien operointia. Järjestelmän operoinnissa ilmeneviä ongelmia voidaan kuvailla säätöteorian menetelmiä käyttäen. Säätöteorian mukaan järjestelmän operointiin vaikuttaa lukuisia osa-alueita kuten taloudellisuus, turvallisuus, tehokkuus sekä luotettavuus. Nämä kaikki seikat tulee ottaa huomioon systeemien suunnittelussa sekä niitä käytettäessä siten, että mitään osa-aluetta ei jätetä liian pienelle huomiolle. (Guarnieri & Garbolino 2019, 124.)

Tässä yhteydessä kontrollilla tarkoitetaan järjestelmän saamista haluttuun käyttötilaan tarkoituksenmukaisten toimenpiteiden avulla. Järjestelmän hallinnointia ajatellen on oleellista tietää hallittavaan järjestelmään liittyvät tilamuuttujat, koska näiden muuttujien ymmärtäminen mahdollistaa järjestelmän käytön halutulla tavalla. Jos nämä muuttujat eivät ole tiedossa, järjestelmä saattaa käyttäytyä täysin päinvastoin kuin järjestelmän operaattori oli ajatellut. Täten riskienhallinta voidaan ajatella kontrolliongelmana, sillä järjestelmä pidetään turvallisessa tai muuten halutussa tilassa juuri

kontrollitoimenpiteiden avulla. Järjestelmää hallinnoiville tahoille voidaan täten määrittää myös rajoitteita, joiden puitteissa näiden tahojen tulee toimia, jotta järjestelmä ei ajautuisi ei-haluttuun tilaan. (Guarnieri & Garbolino 2019, 125.)

Säätöteorian mukaan on olemassa avoimia sekä suljettuja säätöpiirejä. Avoin piiri on yksinkertainen kontrollirakenne, jossa systeemin kontrollerilla ei käytännössä ole mahdollisuutta havainnoida kontrollitoimenpiteen vaikutusta itse systeemiin. Tällaisissa systeemeissä edellisillä kontrollitoimenpiteillä ei ole suoranaista vaikutusta tuleviin kontrollitoimenpiteisiin, koska ilman takaisinkytkentää kontrollitoimenpiteen vaikutuksesta ei ole tietoa. (Guarnieri & Garbolino 2019, 126.)

Suljetussa piirissä systeemin kontrollerilla on mahdollisuus reagoida edellisten kontrollitoimenpiteiden tai ulkoisten tapahtumien aiheuttamiin tilamuutoksiin. Kontrolleri voi reagoida ulkoisiin haittatekijöihin ja niiden vaikutuksiin systeemissä takaisinkytkentöjen avulla. Takaisinkytkennän kautta kontrolleri voi reagoida myös puutteellisesti tapahtuneiden kontrollitoimenpiteiden aiheuttamiin vaikutuksiin. Suljetussa kierrossa järjestelmän toiminnan ohjauksessa osallisena ovat kontrollerin ja kontrolloitavan prosessin lisäksi toimilaitteita sekä mittalaitteita tai muita sensoreita. (Guarnieri & Garbolino 2019, 126.) Alla oleva kuva havainnollistaa yksinkertaista suljettua piiriä.



Kuva 7. Suljettu piiri, jossa kuvattuna ovat myös kontrollitoimenpiteen sekä takaisinkytkennän välittäjät

Kuva 7 visualisoi suljettua piiriä, jossa systeemin kontrolleri pystyy vertailemaan systeemin nykytilaa systeemin haluttuun tilaan. Vertailun perusteella kontrolleri pystyy hallinnoimaan systeemiä kontrollitoimenpiteiden kautta, jos prosessi on jostain syystä epätoivotussa tilassa. Tällainen systeemin elementtien välinen kommunikointi on tärkeää säätöteorian lisäksi myös systeemiteoriassa. Säätöteorian mukaan pelkästään avoimia piirejä hyödyntäviä systeemejä ei voida pitää turvallisena niiden hallittavuusongelmien vuoksi. Avointa piiriä käyttävät yksinkertaiset järjestelmärakenteet vaativat takaisinkytkennän saapumista hierarkiassa korkeammalla tasolla olevalle kontrollerille jonkin muun rinnakkaisen kontrollerin kautta, jotta systeemiä voidaan pitää hallittavana ja täten turvallisena. (Guarnieri & Garbolino 2019, 127.)

4 SYSTEEMI- JA SÄÄTÖTEORIAT KÄYTÄNNÖSSÄ

STAMP-malli (System-Theoretic Accident Model and Process) perustuu luvussa 3 läpikäytyihin teorioihin sekä periaatteisiin. STAMP-malli on näiden teorioiden yhteenveto eli se pyrkii kuvaamaan systeemejä turvallisuusrajoitteiden, hierarkkisen kontrollirakenteen sekä prosessimallien avulla. STAMP-mallin ominaispiirre on dynaamisten systeemien kuvaaminen siihen kuuluvan organisaation sisällä. (Leveson 2011, 90.) STAMP-mallin ollessa yhteenveto teorioista tekee siitä itsessään teorian eikä analyysimenetelmän. STAMP-malli toimii perustana muun muassa tässä diplomityössä käytetylle STPA-analyysimenetelmälle.

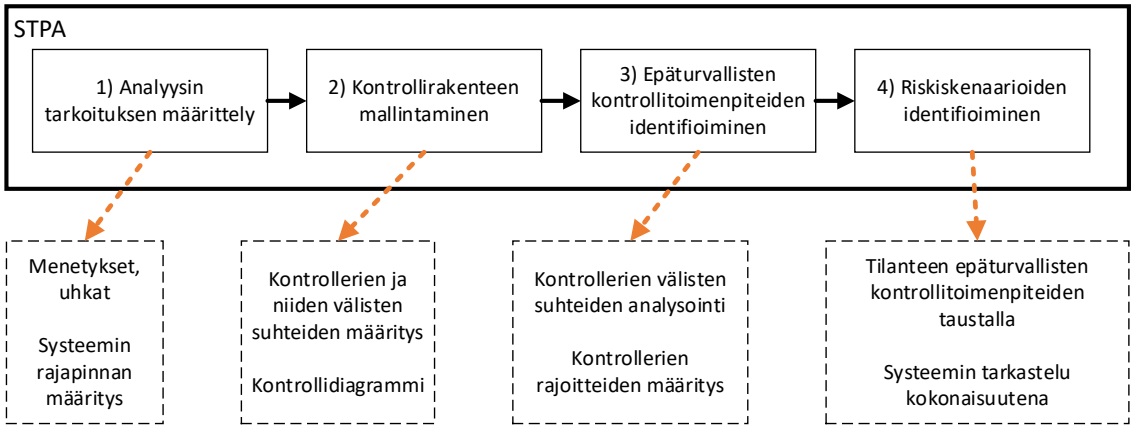
Tässä luvussa käydään läpi STAMP-malliin perustuvaa STPA-analyysiä käytännössä. Tässä luvussa tarkastellaan myös asioita, joita tulisi ottaa huomioon analysoitaessa systeemejä, joissa ihmisen toiminnalla on oleellinen merkitys. Tämän työn case-tutkimus on esimerkki tällaisesta ihmispainotteisesta systeemistä, sillä valmiustoimintaa analysoitaessa tarkastellaan käytännössä ainoastaan ihmisten keskinäistä toimimista.

4.1 Systeemiteoreettinen prosessianalyysi

STPA-analyysi on ennaltaehkäisevä hasardianalyysi, jonka avulla voidaan analysoida kompleksisia sekä ihmispainotteisia systeemejä, joita perinteisillä luotettavuustekniikan menetelmillä ei välttämättä voida analysoida. STPA-analyysin lopputuloksena saadaan riskien kausaalisia tekijöitä kuvaavia skenaarioita, joille voidaan luoda esimerkiksi hallintakeinoja analyysin jälkeen. STPA-analyysin tavoitteet ovat käytännössä identtisiä minkä tahansa muunkin hasardianalyysin kanssa. Näitä tavoitteita ovat esimerkiksi turvallisuustason ylläpitäminen systeemin koko elinkaaren aikana sekä turvallisuuselementtien oleellisuuden kuvaaminen menetyksien estämisessä. (Guarnieri & Garbolino 2019, 146-147.)

STPA-analyysi koostuu neljästä eri vaiheesta. Ensimmäisessä vaiheessa määritetään analyysin tarkoitus sekä tarkasteltavan systeemin rajapinta. Toisessa vaiheessa mallinnetaan systeemin kontrollerit sekä niiden väliset suhteet säätöteoriaan perustuvaan kontrollidiagrammiin. Kontrollidiagrammin perusteella voidaan määritellä epäturvalliset kontrollitoimenpiteet analyysin kolmannessa vaiheessa. Analyysin viimeisessä eli neljännessä vaiheessa määritetään skenaariot, jotka kuvaavat miten aiemmin löydetyt

epäturvalliset kontrollitoimenpiteet voivat tapahtua. Skenaariot voivat liittyä myös suoraan kontrollirakenteeseen liittyviin riskitilanteisiin. (Leveson & Thomas 2018, 14). Alla havainnollistava kuva STPA-analyysin vaiheista.



Kuva 8. STPA-analyysin vaiheet (Leveson & Thomas 2018, 14)

Kuva 8 havainnollistaa miten STPA-analyysi alkaa ylätason menetyksistä ja päättyy alatason skenaarioihin. STPA-analyysi on täten päinvastainen verrattuna esimerkiksi vika ja vaikutusanalyysiin, jossa analysointi aloitetaan alatason komponentteja analysoimalla.

Käydään seuraavaksi STPA-analyysin vaiheet läpi esimerkkien avulla. Esimerkkianalyysin kohteena toimii luvussa 3.1.2 mainittu kemikaalilaitos. Esimerkissä oletetaan kemikaalilaitoksen olevan hyvin yksinkertainen. Kemikaalilaitoksen operaattori operoi laitosta prosessitietokoneen avulla. Prosessitietokone ohjaa kahta laitoksen venttiiliä, joista ensimmäisellä ohjataan katalyyttilinjan virtausta reaktoriin ja toisella reaktorin jäähdytysvesilinjan virtausta. Venttiilin ajaminen ääriasennosta toiseen kestää minuutin, jolloin venttiilin jääminen muuhun kuin ääriasentoon on mahdollista, jos venttiiliä ajetaan liian vähän aikaa.

4.1.1 Analyysin tarkoitus

Ensimmäisessä työvaiheessa tehtävä menetyksien määrittäminen on tärkeää, sillä analyysissä pystytään löytämään vain ja ainoastaan näihin menetyksiin johtavia skenaarioita. Menetyksiä listattaessa on oleellista huomioida kaikkien systeemiin kuuluvien tahojen tarpeet, jotta mikään oleellinen menetys ei jäisi pois analyysistä. Koska menetysten määrittäminen on ensimmäisen vaiheen ensimmäinen askel, ne määritetään yleisessä muodossa eikä niissä tule mainita yksityiskohtaisia asioita kuten komponentteja

tai järjestelmiä. Menetykset voivat olla hyvin eri tyyppisiä keskenään kuten kemikaalilaitokselle määritellyistä menetyksistä voidaan havaita: (Leveson & Thomas 2018, 16.)

- L-1: Henkilövahinko tai -menetys
- L-2: Ympäristövahinko
- L-3: Tuotantomenetys
- L-4: Asiakastyytyväisyyden heikkeneminen

Menetyksien määrityksen jälkeen ensimmäisessä työvaiheessa määritellään uhkat, jotka voivat pahimmassa tilanteessa johtaa menetyksiin. Uhkat voivat olla riippuvaisia useista tekijöistä, joten on huomioitava, että uhkan tapahtuminen ei välttämättä tarkoita menetyksen aiheutumista. Ennen uhkien määritystä tulee tarkasteltava systeemi olla asianmukaisesti identifioitu systeemin rajapinnan osalta. Käytännössä tämä tarkoittaa vain tarkasteltavan kohteen ja muun ympäristön välisen rajan hahmottamista. Uhkien täytyy olla sellaisia, että ne voidaan linkittää menetyksiin sekä uhkien täytyy olla sellaisia, että niiden tapahtumista voidaan rajoittaa käytännön toimenpiteillä. Täten STPA-analyysin uhkat eivät voi olla ulkoisista tapahtumista johtuvia tilanteita. Esimerkkejä uhkatilanteista ovat esimerkiksi: (Leveson & Thomas 2018, 18.)

- H-1: Laitos päästää myrkyllisiä aineita ympäristöön [L-1, L-2, L-4]
- H-2: Laitos vahingoittaa ihmisiä esimerkiksi räjähdyksen seurauksena [L-1, L-2, L-4]
- H-3: Laitosta operoidaan turvallisuusmääräysten vastaisesti [L-1, L-2]

Listatut uhkat ovat sellaisessa systeemitason muodossa, että niitä voidaan analysoida myöhemmässä vaiheessa määrittämällä toimenpiteitä uhkatilanteiden taustalla. Huomioitavaa on, että kaikille menetyksille on määritettävä yksi tai useampi uhka. (Leveson & Thomas 2018, 18.) Täten yllä oleva listaus ei ole täydellinen.

Ensimmäisen työvaiheen viimeisenä määritettävänä kohteena ovat rajoitteet, joiden puitteissa systeemiä tulee ylläpitää, jotta uhkilta ja täten menetyksiltä vältyttäisiin. Rajoitteiden määritys on suoraviivainen prosessi, jossa käytännössä uhkien merkitys

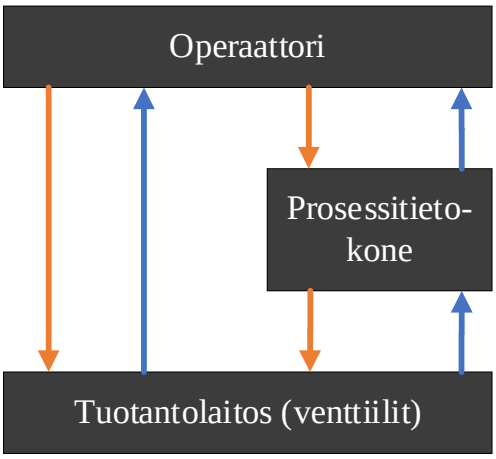
muunnetaan käänteisiksi. Esimerkkejä uhkien rajoitteista ovat: (Leveson & Thomas 2018, 20.)

- SC-1: Laitos ei saa päästää myrkyllisiä aineita ympäristöön [H-1]
- SC-2: Laitoksen käytöstä ei saa aiheutua ylimääräistä haittaa ympäristölle [H-1, H-2]
- SC-3: Laitosta tulee operoida turvallisuusrajoitusten puitteissa (paine ja lämpötila) [H-2, H-3]
- SC-4: Jos myrkyllisten aineiden pääsy ympäristöön tapahtuu, on ryhdyttävä toimenpiteisiin vahinkojen lieventämiseksi [H-1, H-2]

Rajoite voi myös koskea tilannetta, jossa uhkatilanne on jo päässyt tapahtumaan, jolloin rajoitteella rajataan uhkatilanteen etenemistä tai vakavuutta. Esimerkki tällaisesta rajoitteesta on yllä mainittu SC-4. STPA-analyysin neljännessä vaiheessa tullaan löytämään mahdollisia syitä näiden rajoitteiden rikkoutumisen taustalla. (Leveson & Thomas 2018, 20.) Rajoitteet ovat myös oleellinen osa säätöteoriaa.

4.1.2 **Kontrollirakenteen määritys**

Analyysin toisessa vaiheessa mallinnetaan analysoitavan systeemin kontrollerirakenne, joka perustuu luvussa 3.2.2 käsiteltyihin teorioihin sekä elementteihin. Kuva 7 näyttää kaikkein yksinkertaisimman kontrollidiagrammin, jossa on vain yksi kontrolleri sekä kontrolloitava prosessi. Todellisuudessa useimmissa systeemeissä on lukuisia kontrollereita, joilla jokaisella on jokin vaikutusmahdollisuus kontrolloitavaan prosessiin joko suoraan tai toisen kontrollerin kautta. Tärkeä kontrollidiagrammin ominaisuus on hierarkia, jolla mahdollistetaan kontrollerien välisten suhteiden kuvaaminen. (Leveson & Thomas 2018) Esimerkki kahden kontrollerin sekä yhden kontrolloitavan prosessin kontrollidiagrammista on esitettynä alla olevassa kemikaalilaitokseen liittyvässä kuvassa.



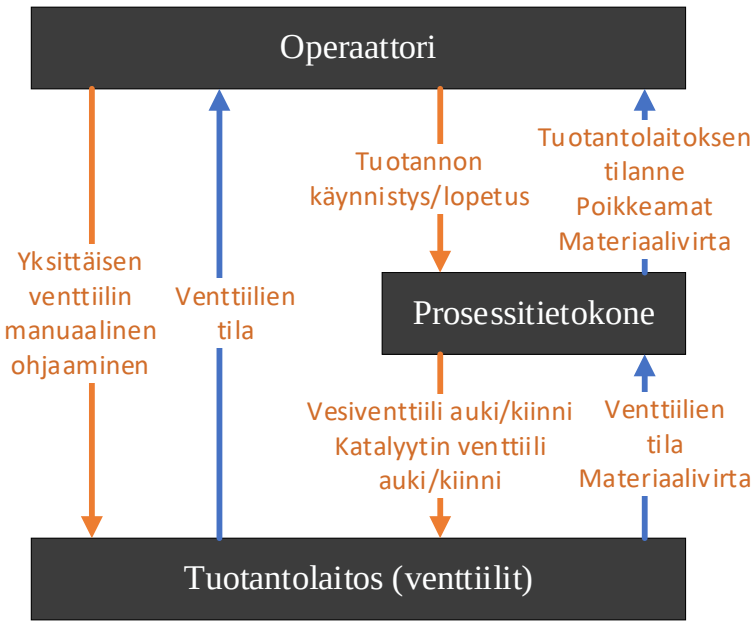
Kuva 9. Esimerkki kontrollidiagrammista

Kuva 9 esittää kontrollidiagrammia, jossa on kontrollereita, kontrolloitu prosessi, kontrollitoimenpiteitä sekä takaisinkytkentöjä. Näiden elementtien lisäksi kontrollidiagrammissa voi olla myös ulkoiselta toimijalta tulevia syötteitä sekä kahden kontrollerin välisiä vuorovaikutuksia. Kontrollitoimenpiteitä sekä takaisinkytkentöjä on kuvailtu luvussa 3.2.2. Vuorovaikutuksella tarkoitetaan kahden hierarkiassa samalla tasolla olevien kontrollereiden keskinäistä vaikutusta. Vuorovaikutuksessa kumpikaan toimija ei pysty suoranaisesti käskemään toisiaan vaan ne kontrolloivat alempana olevaa tahoa yhteisvaikutuksessa. Ulkoinen toimija on taas sellainen taho, joka on tarkoituksella jätetty analysoitavan systeemin ulkopuolelle esimerkiksi analyysin laajuuden rajoittamisen takia, mutta ulkoisen toimijan vaikutusmahdollisuus itse analysoitavaan systeemiin on kuitenkin jollain tapaa mahdollinen. Huomioitavaa diagrammissa on se, että se ei ole fyysinen malli eivätkä sen kontrollitoimenpiteet välttämättä merkitse tottelevaisuutta. Analyysin myöhemmässä vaiheessa tarkastellaan esimerkiksi juuri tottelemattomuudesta aiheutuvia ongelmia tai syitä tottelemattomuuden taustalla. (Leveson & Thomas 2018, 25.)

Kontrollidiagrammin laatimisen jälkeen kontrollereille voidaan määrittää vastuut, joiden avulla systeemitason rajoitteet toteutuvat. Vastuut ja niiden määrittely ovat oleellisessa osassa varsinkin silloin, jos analyysin kohteena on uusi tai kehitteillä oleva systeemi. Tällöin analyysissä laadittuja vastuita voidaan hyödyntää esimerkiksi toimintaohjeiden laatimisessa. Esimerkkejä vastuista kemikaalilaitokselle voivat olla esimerkiksi: (Leveson & Thomas 2018, 28.)

- R-1: Operaattorin on operoitava laitosta turvallisuusrajoitteiden puitteissa [SC-1, SC-2, SC-3].
- R-2: Operaattorin on operoitava laitosta manuaalisesti automaation vikaantuessa [SC-1, SC-2, SC-3]
- R-3: Prosessitietokoneen on ohjattava tuotantolaitosta operaattorien käskyjen mukaan [SC-1, SC-2, SC-3]
- R-4: Prosessitietokoneen on ohjattava tuotantoprosessi turvalliseen tilaan hätätilanteen sattuessa [SC-1, SC-2, SC-3]

Kehitteillä olevien systeemien kohdalla vastuita voidaan hyödyntää myös kontrollidiagrammin kontrollitoimenpiteiden nimeämisessä. Määriteltyjen kontrollitoimenpiteiden perusteella taas määritellään puuttuvat takaisinkytkennät, jotta säätöteorian mukainen prosessin hallittavuus toteutuu. Kontrollidiagrammin laatiminen on täten kehitteillä olevien systeemien osalta iteratiivinen prosessi näiden keskenään vuorovaikuttavien elementtien takia. Jos systeemi on ennestään tuttu, tämä työvaihe on suoraviivaisempi, koska kontrollidiagrammiin voidaan laatia ja nimetä kontrollitoimenpiteet sekä takaisinkytkennät suoraan. Ennestään tutun systeemin tapauksessa vastuita ei tarvitse analyysin aikana laatia varsinkin, jos ne on määritetty aiemmin muussa yhteydessä. (Leveson & Thomas 2018, 28-29.) Yllä oleva listaus vastuista ei ole täydellinen. Valmis kontrollidiagrammi nähdään alla olevassa kuvassa.



Kuva 10. Kemiantuotantolaitoksen kontrollidiagrammi

Yllä olevan kuvan kontrollitoimenpiteet on nimetty suoraan vastuiden asettamista vaatimuksista. Takaisinkytkennät taas nimetään kontrollitoimenpiteiden asettamista vaatimuksista. Esimerkiksi vastuun R-2 mukaan operaattorin tulee tarvittaessa ohjata laitosta manuaalisesti ilman prosessitietokonetta, jolloin operaattorin tulee myös saada venttiilien tilatieto suoraan tuotantolaitokselta.

4.1.3 **Epäturvallisten kontrollitoimenpiteiden identifioiminen**

STPA-analyysin kolmanteen vaiheeseen kuuluu epäturvallisten kontrollitoimenpiteiden (UCA, Unsafe Control Action) määritys. Tässä vaiheessa etsitään uhkatilanteeseen johtavia aiemmin määriteltyihin kontrollitoimenpiteisiin liittyviä seikkoja. STPA-analyysissä kontrollitoimenpide voi olla epäturvallinen neljällä eri tavalla. Nämä UCA-tyypit ovat: ei tehdä, tehdään, tehdään liian aikaisin myöhässä tai väärässä järjestyksessä sekä keskeytetään liian aikaisin tai jatketaan liian pitkään. (Leveson & Thomas 2018, 36.) Kemikaalilaitoksen jäähdytysvesiventtiilin avaamiseen liittyviä epäturvallisia kontrollitoimenpiteitä on kuvattu alla olevassa taulukossa.

Taulukko 1. Kemikaalilaitoksen vesilinjan venttiilin avaamiseen liittyvät UCA:t

Kontrolleri **Kontrolli-toimenpide** **Kohde**	**Ei tehdä, johtaa uhkaan**	**Tehdään, johtaa uhkaan**	**Tehdään liian aikaisin, myöhässä tai väärässä järjestyksessä**	**Keskeytetään liian aikaisin tai jatketaan liian pitkään**
Prosessitietokone Jäähdytysvesi-linjan venttiilin avaaminen Tuotantolaitos	**UCA-1**: Prosessitietokone ei käske vesilinjan venttiilin avaamista operaattorin aloittaessa tuotantokäytön. [H-1, H-2, H-3] **UCA-2**: Prosessitietokone ei käske vesilinjan venttiilin avaamista sellaisessa epänormaalissa tilanteessa, jossa reaktori on vaarassa ylittää turvallisuus-parametrien rajat. [H-1, H-2, H-3]	N/A	**UCA-3**: Prosessitietokone käskee vesilinjan venttiilin avaamisen vasta katalyytin venttiilin avaamisen jälkeen. [H-1, H-2, H-3] **UCA-4**: Prosessitietokone käskee vesilinjan venttiilin avaamisen yli X sekunnin kuluttua sellaisessa epänormaalissa tilanteessa, jossa reaktori on vaarassa ylittää turvallisuus-parametrien rajat. [H-1, H-2, H-3]	**UCA-5**: Prosessitietokone lopettaa käskynantamisen vesilinjan venttiilin avaamiselle liian aikaisin, jolloin venttiili jää vain osittain auki. [H-1, H-2, H-3]

Asianmukaiseen epäturvalliseen kontrollitoimenpiteeseen kuuluu käytännössä neljä eri osa-aluetta, jotka ovat kontrollitoimenpiteen lähde/kontrolleri, vaikutustyyppi, kontrollitoimenpide sekä konteksti. Näistä konteksti on oleellisin, koska se määrittää tilanteen, jossa toimenpide on epäturvallinen. Jos toimenpiteen suorittaminen olisi aina epäturvallista, ei sitä olisi koskaan sisällytetty analysoitavaan systeemiin. (Leveson & Thomas 2018, 36-37.) Nämä epäturvallisiin kontrollitoimenpiteisiin liittyvät elementit voidaan havaita myös yllä olevasta taulukosta.

Kun UCA:t on määritelty, niille voidaan asettaa rajoitteet samoin kuin uhkille. Käytännössä epäturvallisten kontrollitoimenpiteiden merkitykset muunnetaan päinvastaisiksi, jolloin näille saadaan rajoite. Näitä rajoitteita voidaan käyttää vastuiden lisäksi apuna laadittaessa esimerkiksi kontrollerikohtaisia toimintaohjeita. (Leveson & Thomas 2018, 41.) Alla on listattuna muutamia kontrollerikohtaisia rajoitteita:

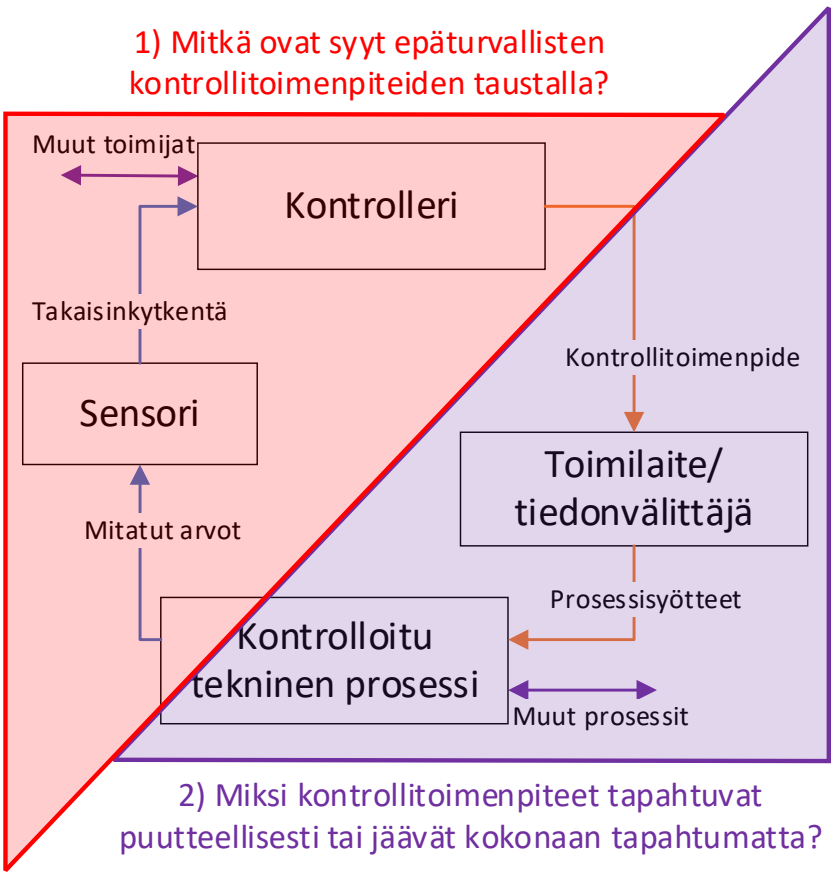
- C-1: Prosessitietokoneen on avattava jäähdytysvesilinjan venttiili ennen/samanaikaisesti katalyytin venttiilin kanssa [UCA-1, UCA-3]

- C-2: Prosessitietokoneen tulee avata jäähdytysvesilinjan venttiili sellaisessa epänormaalissa tilanteessa, jossa reaktori on vaarassa ylittää turvallisuusparametrien rajat [UCA-2]
- C-3: Prosessitietokoneella ei saa kestää yli X sekuntia jäähdytysvesilinjan venttiilin avaamisessa sellaisessa tilanteessa, jossa reaktori on vaarassa ylittää turvallisuusparametrien rajat [UCA-4]
- C-4: Prosessitietokone ei saa keskeyttää käskynantamista jäähdytysvesilinjan venttiilin avaamiselle ennen kuin venttiili on kokonaan auki [UCA-5]

Yllä olevasta listauksesta huomataan, että näitä rajoitteita voidaan soveltaa hyvin systeemin suunnittelun perustana. Näiden rajoitteiden pohjalta suunnittelijat voivat määritellä toimintamenetelmät esimerkiksi koneellisille kontrollereille kuten tietokoneille.

4.1.4 **Skenaarioiden määritys**

Analyysin neljännessä ja viimeisessä vaiheessa määritellään skenaariot. Skenaariolla kuvataan tekijöitä menetykseen johtavan tilanteen taustalla. Skenaariot voidaan jakaa kahteen eri tyyppiin. Ensimmäisen tyypin skenaarioissa määritellään syitä epäturvalliseen kontrollitoimenpiteeseen johtavan tilanteen taustalla kun toisessa skenaariotyypissä identifioidaan syitä kontrollitoimenpiteen tapahtumatta jäämisen taustalla. Lyhyesti sanottuna ensimmäisen tyypin skenaariot liittyvät takaisinkytkentöihin ja kontrollitoimenpiteen lähteeseen (kontrolleriin) ja toisen tyypin skenaariot liittyvät kontrollitoimenpiteen välittäjänä toimiviin toimilaitteisiin sekä itse kontrolloituun prosessiin. (Leveson & Thomas 2018, 42-43.) Alla havainnollistava kuva skenaariotyyppien jaottelusta suljetun kontrollikierron avulla kuvattuna.



Kuva 11. Skenaariotyypit (Leveson & Thomas 2018, 43)

Ensimmäisen tyypin skenaariot voivat siis aiheutua kontrollerista tai takaisinkytkennästä. Itse kontrolleriin liittyvät skenaariot voivat johtua esimerkiksi kontrollerin fyysisestä vikaantumisesta, sähkökatkosta tai muusta vastaavasta. Ihmiskontrollerin kohdalla kyseessä voi olla esimerkiksi sairaskohtaus. Myös kontrollerille määritelty toiminta-algoritmi tai -ohjeistus voi olla virheellinen, jolloin on UCA:n tapahtuminen on mahdollista. Toisaalta kontrolleri saattaa toimia epäturvallisesti myös toisen kontrollerin antaman syötteen takia. Esimerkiksi hierarkiassa alempana oleva toimija saattaa toimia epäturvallisesti tiedostamattaan, jos se on saanut epäturvallisen määräyksen hierarkiassa ylempänä olevalta taholta. Kontrolleri toimii parhaimman mahdollisen tilannetiedon mukaan, jolloin tilannetiedon vääristyessä myös kontrollerin toiminta saattaa muuttua epäturvalliseksi. Tällaiset seikat liittyvät takaisinkytkentöjen puutteisiin ja vikaantumisiin. On myös mahdollista, että kontrolleri tulkitsee saadun takaisinkytkennän väärin, jolloin se tulee tietämättään toimimaan epäturvallisesti. (Leveson & Thomas 2018, 43-44.) Kaikkia näitä seikkoja tulee tarkastella jokaisen UCA:n kohdalla. Näin

ollen yhteen epäturvalliseen kontrollitoimenpiteeseen linkittyy useampia eri tyyppisiä skenaarioita. Alla on listattuna kontrollitoimenpiteeseen UCA-1 liittyviä skenaarioita:

- Skenaario 1: Prosessitietokone ei anna käskyä jäähdytysvesiventtiilin avaamiselle operaattorin antaessa käskyn tuotannon aloittamiselle prosessitietokoneen vian vuoksi. Vian takia jäähdytysvesilinjan venttiili jää suljetuksi, mutta katalyytin venttiili avautuu. [UCA-1]
- Skenaario 2: Prosessitietokone ei anna käskyä jäähdytysvesilinjan venttiilin avaamiselle, koska prosessitietokone luulee katalyyttilinjan venttiilin olevan epäkunnossa, vaikka näin ei todellisuudessa ole vaan katalyyttilinjan venttiili aukeaa normaalisti. Tilanne voi aiheutua esimerkiksi sensorin lähettämästä virhesignaalista prosessitietokoneelle. [UCA-1]
- Skenaario 3: Prosessitietokone ei avaa jäähdytysvesilinjan venttiiliä tuotantokäytön alkaessa ohjelmointivirheen tai muun vastaavan syyn vuoksi esimerkiksi ohjelmistopäivityksen jäljiltä. Tämän seurauksena venttiilit voivat avautua väärässä järjestyksessä. [UCA-1]

Toisessa skenaariotyypissä tarkastellaan uhkiin johtavia kontrollitoimenpiteiden ulkopuolisia tai toimenpidealgoritmiin liittyviä syitä. Toisessa skenaariotyypissä vaaratilanteet syntyvät kontrollitoimenpiteen välittäjänä toimivan toimilaitteen vikaantumisen tai kontrolloidun prosessin tottelemattomuuden takia. Käytännössä tässä vaiheessa tulee tarkastella kontrollitoimenpiteen polkua kontrollerilta kontrolloidulle prosessille asti ja analysoida mahdolliset vikaantumistilanteet. Operaattorin ja prosessitietokoneen välisessä toiminnassa tällaisella vikaantumisella voidaan tarkoittaa esimerkiksi ohjauspaneelin tai -kaapeloinnin epäkuntoisuutta. Jos kontrollitoimenpide kuitenkin kulkeutuu prosessille asti ennalta määritetyllä tavalla, on mahdollista ettei prosessi reagoi kontrollitoimenpiteeseen halutulla tavalla. Tällöin kyseessä voi olla esimerkiksi kontrolloidun kohteen epäkuntoisuus tai jokin ulkoinen haittatekijä. Toisaalta jokin muu kontrolleri on voinut käskeä prosessiin jonkin poikkeavan toimenpiteen, joka estää jatkossa tulevien toimenpiteiden toteutumisen. (Leveson & Thomas 2018, 49-51.) Esimerkkejä jäähdytysvesilinjan virtauksen venttiilin avaamiseen liittyviä toisen skenaariotyypin skenaarioita on listattuna alla:

- Skenaario 1: Prosessitietokone käskee jäähdytysvesilinjan venttiilin avaamisen, mutta venttiili ei aukea prosessitietokoneen ja venttiilin toimilaitteen välisen kaapeloinnin epäkuntoisuuden takia. [H-1, H-2, H-3]
- Skenaario 2: Prosessitietokone käskee jäähdytysvesiventtiilin avaamisen, mutta venttiili ei liiku sen epäkuntoisuuden takia. Venttiili on täten jollain tapaa jumiutunut ja se voi jäädä kiinni. [H-1, H-2, H-3]
- Skenaario 3: Prosessitietokone käskee jäähdytysvesiventtiilin avaamisen, mutta manuaalinen venttiilinohjaus on kytketty päälle, jolloin venttiili ei liiku prosessitietokoneen käskystä. [H-1, H-2, H-3]

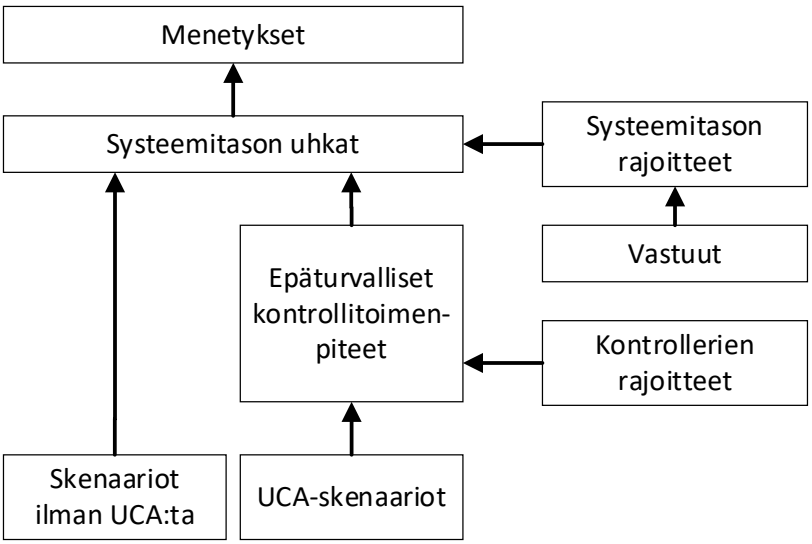
Tällaiset toisen skenaariotyypin skenaariot liittyvät usein laitteistojen epäkuntoisuuteen. Täten STPA-analyysiä voi käyttää myös tärkeimpien komponenttien identifioinnissa ja niiden ylläpidon suunnittelussa.

4.1.5 **Mitä analyysin jälkeen?**

Analyysin tuloksia voi käyttää moneen käyttötarkoitukseen myös riskien hallintatoimenpiteiden lisäksi. Tällaisia kohteita ovat esimerkiksi systeemin arkkitehtuurin luominen, vaatimusten luonti, systeemin testausjärjestelyt sekä riski-indikaattorien luominen. (Leveson & Thomas 2018, 52.)

STPA-analyysin luonteen takia sen voi suorittaa myös iteratiivisesti. Iteratiivisuudella mahdollistetaan kompleksisten systeemien analysointi abstraktisuutta hyödyntäen. Laajojen systeemien analysoinnissa toimijoita sekä niiden välisiä suhteita voidaan tarkastella ryhmittäin. Esimerkiksi analyysissä voidaan määrittää jokin ryhmä kontrolleriksi sen sijasta, että jokainen ryhmän jäsen jaoteltaisiin omiksi kontrollereikseen heti ensimmäisessä analyysi-iteraatiossa. Samanlaista yleistämistä tai abstrahointia voidaan soveltaa myös kontrollitoimenpiteisiin ja takaisinkytkentöihin. Analyysin ensimmäisessä iteraatiossa voidaan esimerkiksi olettaa jonkin kontrollitoimenpiteen olevan paljon yksinkertaisempi kuin se todellisuudessa on. (Leveson & Thomas 2018, 26.) Yleistyksien avulla kompleksistenkin systeemien analyyseistä voidaan saada tuloksia nopeasti, jolloin analyysin käyttökelpoisuutta kyseiseen systeemiin päästään arvioimaan nopeammin ilman suurta taloudellista riskiä.

Yhteenveto analyysin elementeille ja niiden välisille linkitys-suhteille nähdään alla olevasta kuvasta.



Kuva 12. STPA-analyysin linkitysketju eri elementtien välillä (Leveson & Thomas 2018, 52)

Yllä oleva kuva esittää STPA-analyysin elementtejä ja niiden välisiä yhteyksiä, joiden luonti, ylläpito sekä tarkastelu tulee mahdollistaa case-tutkimuksen alussa Polarion-ohjelmistoon. Case-tutkimuksessa tullaan täten luomaan itse analyysin lisäksi myös Polarion-työkalu analyysin laatimiselle ja tulosten tarkastelulle.

4.2 Ihminen kontrollerina

Case-tutkimuksen kohteena oleva valmiustoiminta koostuu suurimmilta osin ihmistoimijoista, jolloin on oleellista käydä läpi oleellisimpia ihmiskontrollereihin liittyviä seikkoja STPA-analyysin osalta. Yleisiä seikkoja muun muassa ihmisoperaattoriin liittyen on kuvailtu kolmannessa luvussa. Tällainen valmiustoiminnalle ominainen ihmiskeskeisyys ei ole este analyysin laatimiselle, mutta se voi tuoda mukanaan omia haasteita sekä huomioonotettavia asioita.

Ihmisen vaikutusta systeemien turvallisuustasoon on alettu panostaa TMI-ydinonnettomuuden jälkeen. Ennen tätä ihmistoimijoita on lähinnä analysoitu tuottavuuden osalta. TMI:n jälkeen muun muassa todennäköisyyspohjaiseen riskianalyysiin on alettu lisäämään siihen aiemmin kuulumattomia osa-alueita ihmistoimijoiden tekemien virheiden ja niiden todennäköisyyksien kattamiseksi. Todennäköisyyspohjaisen riskianalyysin kuitenkin huomattiin olevan jokseenkin

huonosti sopeutuva tällaiseen käyttötarkoitukseen lähinnä siksi, että ihmistoimijat käyttäytyvät huomattavasti eri tavoin kuin koneelliset komponentit. (Hollnagel 2012, 3-5.) Näiden seikkojen myötävaikutuksena STPA-analyysin kehitystyö aloitettiin.

Valmiustoiminnan tyyppiset sosiotekniset systeemit ovat haasteellisia analysoitavia niiden kompleksisuuden ja epälineaarisuuden vuoksi. Tällaisien systeemien turvallisuustason tai luotettavuuden parantamisessa ei voi vain keskittyä yhteen osa-alueeseen, koska muuten systeemitason turvallisuus saattaakin heiketä. Tällainen ilmiö saattaa syntyä varsinkin systeemeissä, joiden toiminta on vahvasti vuorovaikutteista eri toimijoiden kesken. Myös ydinvoimalaitos ja siihen liittyvät hallintatoimet ovat esimerkkejä tällaisesta systeemistä. (Hollnagel 2012, 9-11.)

Jotta sosioteknisten systeemien turvallisuudesta pystytään kattavasti varmistumaan, tulee kyseessä olevan organisaation olla tarpeeksi joustava. Jotta organisaatio voisi olla tarpeeksi joustava, tulee sen turvallisuus-suunnitteluun sekä -ylläpitoon käytetyn analyysin mahdollistaa useiden samanaikaisten haitallisten tapahtumien tarkastelun, turvallisuusteknisten asioiden ennakoinnin sekä turvallisuuden sisällyttämisen organisaation ydinprosessiin. Tällaisten perusperiaatteiden pohjalta syntyy systeemejä, jotka pystyvät reagoimaan useisiin erilaisiin tilanteisiin monitoroinnin, varautumisen sekä oppimisen kautta. (Hollnagel 2012, 15-16.)

Kuten tässä luvussa käydystä STPA-esimerkistä voitiin havaita, STPA-analyysi soveltuu tällaisien sosioteknisten systeemien analysointiin, joissa täytyy tarkastella ihmiskontrollerien ja koneellisten kontrollerien yhteisvaikutusta. Aiemmin käytiin läpi esimerkkien muodossa koneellisten kontrollerien epäturvallisia kontrollitoimenpiteitä sekä näiden taustalla olevia skenaarioita. Tarkastellaan seuraavaksi seikkoja, joita ihmiskontrollerin analysoinnissa tulisi ottaa huomioon.

Oleellisin ero koneellisen- ja ihmiskontrollerin tarkastelun välillä on mentaalimallin hyödyntäminen. Ihmiskontrolleri muodostaa tilannekuvansa systeemin nykytilasta eri tavalla verrattuna koneelliseen kontrolleriin, joka on esimerkiksi ohjelmoitu toimimaan aina samalla tavalla tietyssä tilanteessa. Ihmiskontrollerin itselleen muodostamaan tilannekuvaan liittyy aina joitain uskomuksia ja olettamuksia, mitkä voivat riippua esimerkiksi aiemmista kokemuksista, koulutuksesta, saatavilla olevasta koulutuksesta tai

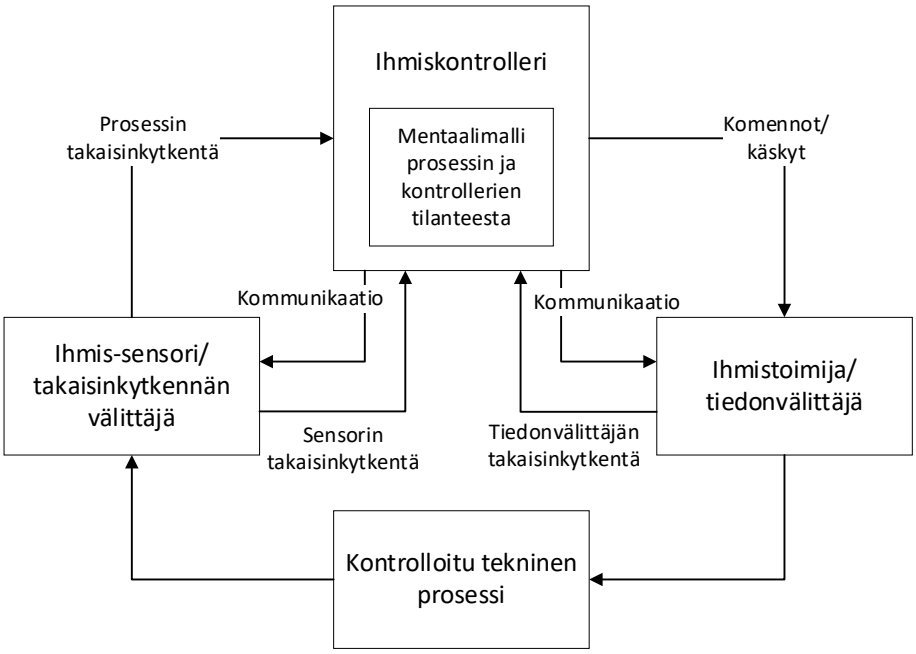
muiden ihmisten toiminnasta. Tällaisen mentaalimallin käyttäminen ihmiskontrollerin toimintaa analysoidessa voi olla oleellista varsinkin monimutkaisten systeemien osalla, joissa ihmiskontrollerin voi olla vaikea hahmottaa jatkuvasti tapahtuvien muutoksien vaikutusta omaan toimintaansa. (France 2015, 32.)

Yksinkertaisimmillaan mentaalimallin käyttö analyysin eri vaiheissa tarkoittaa tilanteiden huomioimista analysoitavan ihmiskontrollerin näkökulmasta. Tällaisen mallin käytöllä pyritään löytämään todellisia syitä ihmiskontrollerien virheellisen toiminnan taustalla. Yleinen turvallisuustaso ei parannu, jos jokaisesta ihmisen tekemästä virheestä syytetään kyseistä henkilöä. Syyttämisen sijasta tulisikin identifioida ja korjata virheellisen toiminnan taustalla vaikuttavia tekijöitä. Yleisesti tällaisista vaikuttavista tekijöistä voidaan mainita koulutus, dokumentaatio ja sen luettavuus, aiemmat kokemukset, takaisinkytkentöjen ymmärrettävyys, epätavalliset kontrollitoimenpiteet muilta toimijoilta, tilannekuvan muodostamiseen vaadittava työpanos sekä systeemin liian hidas reagointi muutoksiin. (France 2015.)

Ihmistoimijoita analysoidessa on syytä huomioida myös eroavaisuudet kontrollitoimenpiteiden sekä takaisinkytkentöjen tiedonsiirron osalta. Koneellisien toimijoiden tapauksessa kontrollitoimenpiteet liikkuvat käytännössä sähköisessä muodossa esimerkiksi tietokoneelta kontrolloituun prosessiin useiden toimilaitteiden kautta. Tällaisessa tilanteessa tiedonkulun kattavan analysoinnin takaamiseksi riittää kaikkien näiden toimilaitteiden vikaantumismahdollisuuksien huomioonottaminen. Ihmistoimijoiden osalta tilanne ei ole aivan näin yksinkertainen sillä esimerkiksi organisaatiota analysoidessa tällainen kontrollitoimenpiteen tai takaisinkytkennän välittäjä saattaa olla ihminen, jolloin tämä välittäjänä toimiva taho on myös altistuvainen aiemmin mainitulle mentaalimallille. Tämän seurauksena näitä välittäjinä toimivia tahoja tulisi myös tarkastella omina kontrollereinaan kattavan analyysin takaamiseksi. (Stringfellow 2010, 86.)

Mentaalimallin lisäksi myös kontrollidiagrammissa tulisi jollain tavoin huomioida keskusteluna tapahtuvan tiedonsiirron olemassaolo. Käytännössä tämän voi toteuttaa luomalla ylimääräisen kontrollikierron hierarkiassa ylempänä olevan kontrollerin sekä tiedonvälittäjän välille mahdollistaen kommunikaation näiden kahden välille. Tällöin tilanne vastaa todenmukaisempaa tilannetta, sillä todellisuudessa tiedonvälittäjä saattaa

pyytää esimerkiksi esimieheltään lisätietoa kontrollitoimenpiteen suorittamiseen. Koneellisten tiedonvälittäjien tapauksessa tällaista kontrollikiertoa ei ole. (Stringfellow 2010, 87-88.) Alla havainnollistava kuva tällaisesta useita kontrollikiertoja sisältävästä yhden kontrollerin kontrollidiagrammista.



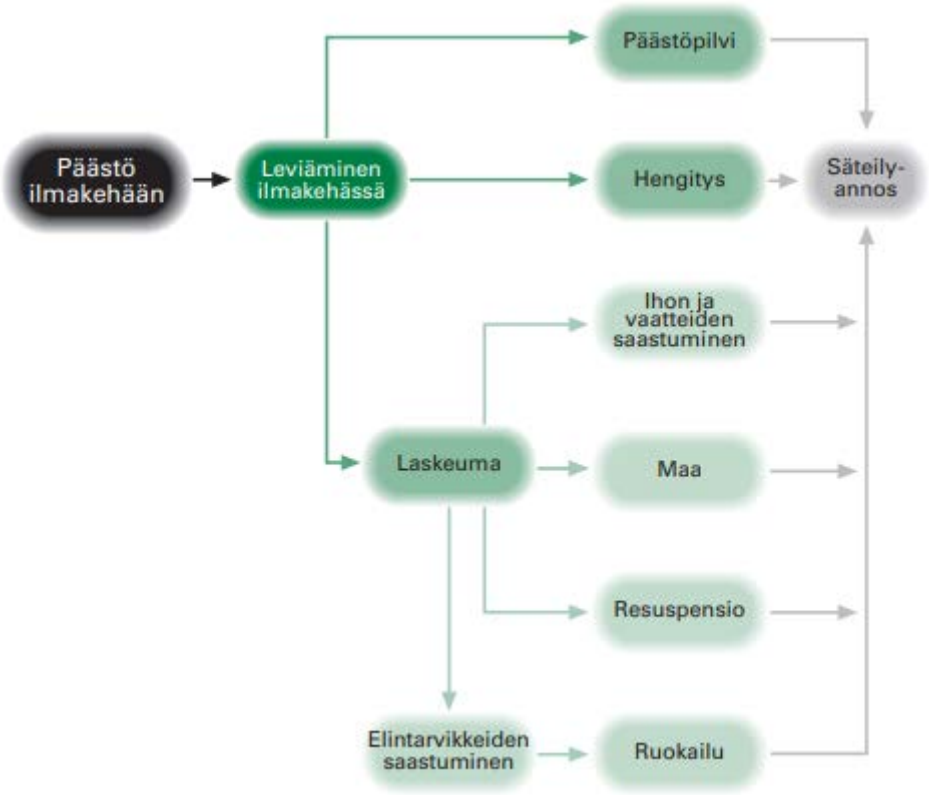
Kuva 13. Ihmistoimijoista koostuva yhden kontrollerin suljettu kontrollikierto (Stringfellow 2010, 88)

Kuva 13 havainnollistaa ihmistoimijoiden keskinäistä toimintaa todenmukaisemmin verrattuna diagrammeihin, joissa ihmisen oletetaan toimivan identtisesti koneiden kanssa. Huomioitavaa ihmistä analysoitaessa STPA-analyysin avulla on myös se, että myös ihminen itsessään koostuu useista kontrollikierroista muodostaen itsessään kompleksisen systeemin (Stringfellow 2010, 86). Näin ollen ihmistä kuvataan poikkeuksetta yleistyksenä itsestään STPA-analyysin kontrollidiagrammeissa.

5 CASE-TUTKIMUS STPA-ANALYYSILLÄ

5.1 Tutkimuksen tausta

Jatkuva valmiusjärjestelyjen kehittäminen on tärkeää niin ydinvoimalaitoksen henkilöstön kuin ympäröivän ympäristön turvallisuuden kannalta. Kuten Tšernobylin ja Fukushiman ydinonnettomuuksista ollaan opittu, vakavalla ydinonnettomuudella on huomattavat vaikutukset laajalla alueella. Alla havainnollistava kuva hallitsemattoman ydinonnettomuuden aiheuttaman mahdollisen säteilypäästön kulkureiteistä väestöön.



Kuva 14. Havainnekuva säteilypäästön kulkeutumisesta väestöön ydinonnettomuuden seurauksena (Pöllänen et. al. 2004, 198)

Ydinonnettomuuden vakavien seurausten takia ydinvoimalaitoksien turvallinen käyttö sekä onnettomuuksiin varautuminen on hyvin tärkeää. Ydinvoima-alan turvallisuuskulttuuri näyttäytyy muun muassa kattavassa ydinvoimalaitoksien turvallisuusjärjestelmien suunnittelussa sekä kansainvälisessä käyttökokemustoiminnassa.

Analyysin käyttökelpoisuuden kannalta on oleellista ottaa huomioon jo käytössä olevat riskienhallintamenettelyt Loviisan voimalaitoksella, jotta analyysin tulokset voitaisiin sovittaa olemassa oleviin menettelyihin. Case-tutkimuksessa tunnistettuja STPA-analyysin skenaarioita voidaan hyödyntää riskienhallinnassa, mikä on toteutettavissa yksinkertaisimmillaan Polarion-ohjelmiston nimikkeiden linkityksillä.

Kaikkein parhaimmassa tapauksessa tällä case-tutkimuksen lopputuloksena saadaan käyttökelpoista dataa valmiustoiminnan suunnittelun avuksi sekä käyttökelpoinen pohja STPA-analyysien laatimiselle ja sen tuottamien tuloksien hyödyntämiselle. Työn lopussa arvioidaan näiden tavoitteiden toteutumista.

5.2 Analyysin vaiheet

5.2.1 **Analyysin alustus**

Ennen itse analyysin aloittamista täytyy laitoksen Polarion-ohjelmistoon luoda pohja analyysin tekoa varten. Pohjan luonti alkaa uuden Polarion-projektin luonnilla, jonka avulla voidaan määrittää eräänlainen rajapinta STPA-analyysin sekä muun ohjelmiston välille. Projektin luonnin jälkeen projektiin tulee määrittää projektikohtaiset määritykset nimiketyypeille, niiden välisille linkityksille sekä muille attribuuteille.

Nimiketyypit määritetään STPA-analyysin määrittämän tyyppijaon mukaisesti. Näin ollen menetykset, uhkat, uhkien rajoitteet, vastuut, epäturvalliset kontrollitoimenpiteet, kontrollerien rajoitteet sekä skenaariot saavat omat nimiketyyppinsä. Tällainen tyyppijako on perusteltua, koska näin jokaiselle STPA-analyysin elementille on oma ”lokeronsa” Polarion-projektissa. Täten analyysiä tehdessä ei tarvitse pohtia, mitä nimiketyyppiä tulisi käyttää missäkin analyysin vaiheessa.

Elementtien väliset linkitykset ovat oleellinen osa STPA-analyysiä. Linkitysketjun avulla voidaan löytää yhteys skenaarioiden ja menetyksien välillä. Tällainen elementtien välinen linkitys on myös yksi Polarion-ohjelmiston perusominaisuuksista. Linkitys-säännöt määritetään Polarion-ohjelmistoon STPA-analyysin linkitysrakenteen mukaisesti. Näin virheellisiä linkityksiä ei voi tapahtua edes vahingossa.

Attribuuttien avulla STPA-elementtejä voidaan tarkastella myös analyysidokumentin ulkopuolella esimerkiksi widgettien avulla. Attribuuttimäärityksien avulla analyysissä laadittuja epäturvallisia kontrollitoimenpiteitä voidaan tarkastella esimerkiksi vain tietyn kontrollerin osalta. Skenaariot perivät siihen linkitetyn epäturvallisen kontrollitoimenpiteen attribuutit, jotta myös skenaarioita voitaisiin taulukoida ja täten tarkastella esimerkiksi juuri kontrollerin perusteella. STPA-elementin tunniste kuten L-1, H-3 tai UCA-17 laaditaan nimikkeen otsikkoon.

Vakavuus määritetään analyysissä ylimpänä olevaan menetykseen. Menetyksiä voi olla monentyyppisiä henkilömenetyksestä asiakastyytyväisyyden putoamiseen, jolloin näille menetyksille voi olla hyvä määrittää jokin vakavuuden taso riippuen systeemiin kuuluvien sidosryhmien näkemyksistä. Vakavuus periytyy menetyksestä kaikkiin alempiin elementteihin skenaariotasolle asti. Täten alimpana olevista skenaarioista voidaan suoraan nähdä sen mahdollisesti aiheuttaman menetyksen vakavuuden taso.

5.2.2 **Menetykset ja uhkat**

STPA-analyysin ensimmäisessä vaiheessa määritetään analyysin laajuus ja tarkoitus. Käytännössä tämä tapahtuu menetyksien sekä niihin johtavien uhkien määrittämisellä. STPA-analyysin menetyksillä tarkoitetaan sellaisia asioita, joita sidosryhmät kokevat mahdottomiksi hyväksyä. Täten menetykset voidaan juontaa esimerkiksi STUK:n YVL-ohjeesta C.5. Ohjeessa mainitaan muun muassa, että valmiustoiminnassa ja sen suunnittelussa tulee huomioida kaikkien voimalaitosalueella olevien yksiköiden yhtäaikainen ydinturvallisuuden vaarantuminen, valmiustoiminnan pitkäkestoisuus sekä väestön säteilyaltistuksen rajoittaminen (STUK 2020). Muun muassa näiden seikkojen pohjalta voidaan laatia yleisellä tasolla olevat STPA-analyysin menetykset, jotka ovat listattuna alla:

- L-1: Onnettomuuden etenemisen estämisen epäonnistuminen
- L-2: Henkilövahinko tai -menetys

Menetys L-1 ei ole aivan yksiselitteinen sillä onnettomuuden etenemisen estämisellä tarkoitetaan erilaisia asioita riippuen valmiustilanteen luonteesta. Esimerkiksi varautumistilanteessa tällä tarkoitetaan tilannetta, jossa laitoksen turvallisuuteen kohdistuvaa uhkaa ei pystytä rajoittamaan, kun taas yleishätätilanteessa vastaavassa

tilanteessa polttoaineen sulamista ei pystytä estämään (Felin 2019, 27). Ydinturvallisuuden takaamisen lisäksi myös henkilöiden suojaaminen, evakuointi ovat valmiustoiminnan perustehtäviä, kuten aiemmin listatuista YVL-ohjeen C.5 määräyksistä tulee ilmi. Näiden epäonnistuessa on riski sellaiselle henkilövahingolle, joka olisi pystytty estämään asianmukaisella valmiustoiminnalla täten aiheuttaen menetyksen L-2. Listataan seuraavaksi menetyksiin johtavat systeemitason uhkatilanteet:

- H-1: Valmiustoimintaan osallistuvat tahot menettävät toimintakykynsä ennen valmiustilanteen päättymistä [L-1, L-2]
- H-2: Polttoaineen lämpötila päästetään liian korkeaksi reaktorissa tai polttoainealtaissa [L-1]
- H-3: Voimalaitos fyysisesti vahingoittaa henkilöstöä/muita ihmisiä virheellisen tai puutteellisen valmiustoiminnan seurauksena [L-2]
- H-4: Henkilöstön tai ulkomaailman ihmisten suojaamisen epäonnistuminen [L-2]

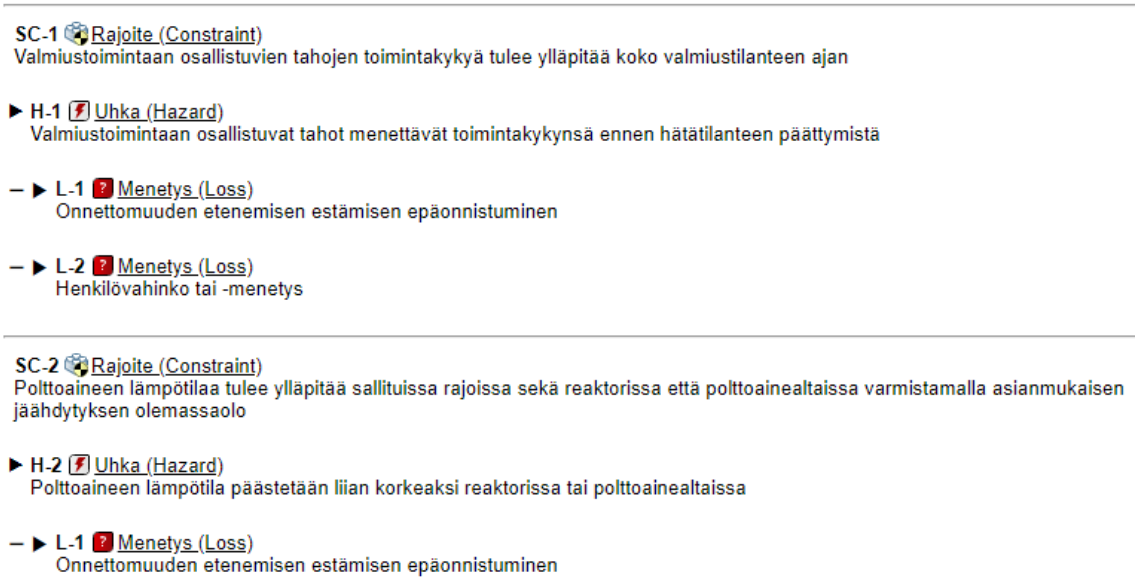
Valmiustoiminnan katsotaan epäonnistuneen, jos valmiustoimintaan osallistuvat tahot eivät kykene enää ylläpitämään toimintakykyään. Uhka H-1 toteutuu, jos esimerkiksi kommunikaatio eri tahojen välillä menetetään tai valmiuskeskus muuttuu käyttökelvottomaksi esimerkiksi kontaminoitumisen tai tarvikkeiden loppumisen seurauksena tilanteessa, jossa korvaavaa sijaintia ei ole saatavilla. Voisi myös ajatella, että uhka H-1 johtaisi myös muihin listattuihin uhkiin, mutta uhkat H-2, H-3 sekä H-4 on hyvä pitää erillään, jotta analyysissä löydetään skenaarioita mahdollisimman monentyyppiseen uhkatilanteeseen liittyen.

Säätöteorian mukaan onnettomuus aiheutuu rajoitteiden rikkomisesta. Muunnetaan seuraavaksi uhkatilanteet rajoitteiksi, jotta nähdään millaisien systeemitason rajoitteiden rikkomisesta menetykset johtuvat valmiustoiminnassa:

- SC-1: Valmiustoimintaan osallistuvien tahojen toimintakykyä tulee ylläpitää koko valmiustilanteen ajan [H-1]
- SC-2: Polttoaineen lämpötilaa tulee ylläpitää sallituissa rajoissa sekä reaktorissa että polttoainealtaissa varmistamalla asianmukaisen jäähdytyksen olemassaolo [H-2]

- SC-3: Valmiustoiminta ei saa olla siten virheellistä tai puutteellista, että voimalaitos tulee vahingoittamaan henkilöstöä tai muita lähialueen ihmisiä esimerkiksi räjähdyksen seurauksena yksinomaan valmiustoiminnan seurauksena [H-3]
- SC-4: Henkilöstön sekä ulkopuolisten ihmisten suojaamisen on oltava kattavaa valmiustoiminnan aikana. On varmistuttava siitä, että suojaustoimenpiteet on tehty vaaditulla laajuudella sekä vaadituin menetelmin [H-4]
- SC-5: Jos polttoaineen lämpötila päästetään liian korkeaksi, on ryhdyttävä välittömästi toimenpiteisiin lämpötilan laskemiseksi [H-2]

Lisätietona rajoitteeseen SC-4 mainittakoon, että kattavaan suojaukseen liittyvät toimenpiteet on esitetty YVL-ohjeessa C.5. Rajoitteista SC-5 on ainoa, jossa rajoitetaan menetyksen vakavuutta uhkatilanteen aiheutuessa. Tässä tapauksessa uhka H-2 tapahtuu, koska rajoitetta SC-2 ei pystytty noudattamaan. Nämä systeemitason rajoitteet voidaan nyt suoraan linkittää rajoitteiden vaikuttamiin menetyksiin. Alla olevassa kuvassa havainnollistetaan linkitysketjun muodostumisen lisäksi myös Polarion-ohjelmiston tuomia mahdollisuuksia tulosten havainnollistamiseen.



Kuva 15. Linkitysrakenteen muodostuminen rajoitteesta menetyksiin

Yllä olevasta kuvasta nähdään yhteenvetona kahden rajoitteen linkittyminen ylätason menetyksiin. Samantyyppistä linkitysrakennetta käytetään koko STPA-analyysin ajan, jolloin analyysin lopussa identifioitujen skenaarioiden yhteys menetyksiin voidaan

havainnollistaa samaan tapaan kuin yllä esitetyt rajoitteet. Linkitysketjun voi myös kuvata päinvastaisessa järjestyksessä menetyksistä alaspäin, jolloin linkitysketju ei tule sisältämään liikaa toistoa.

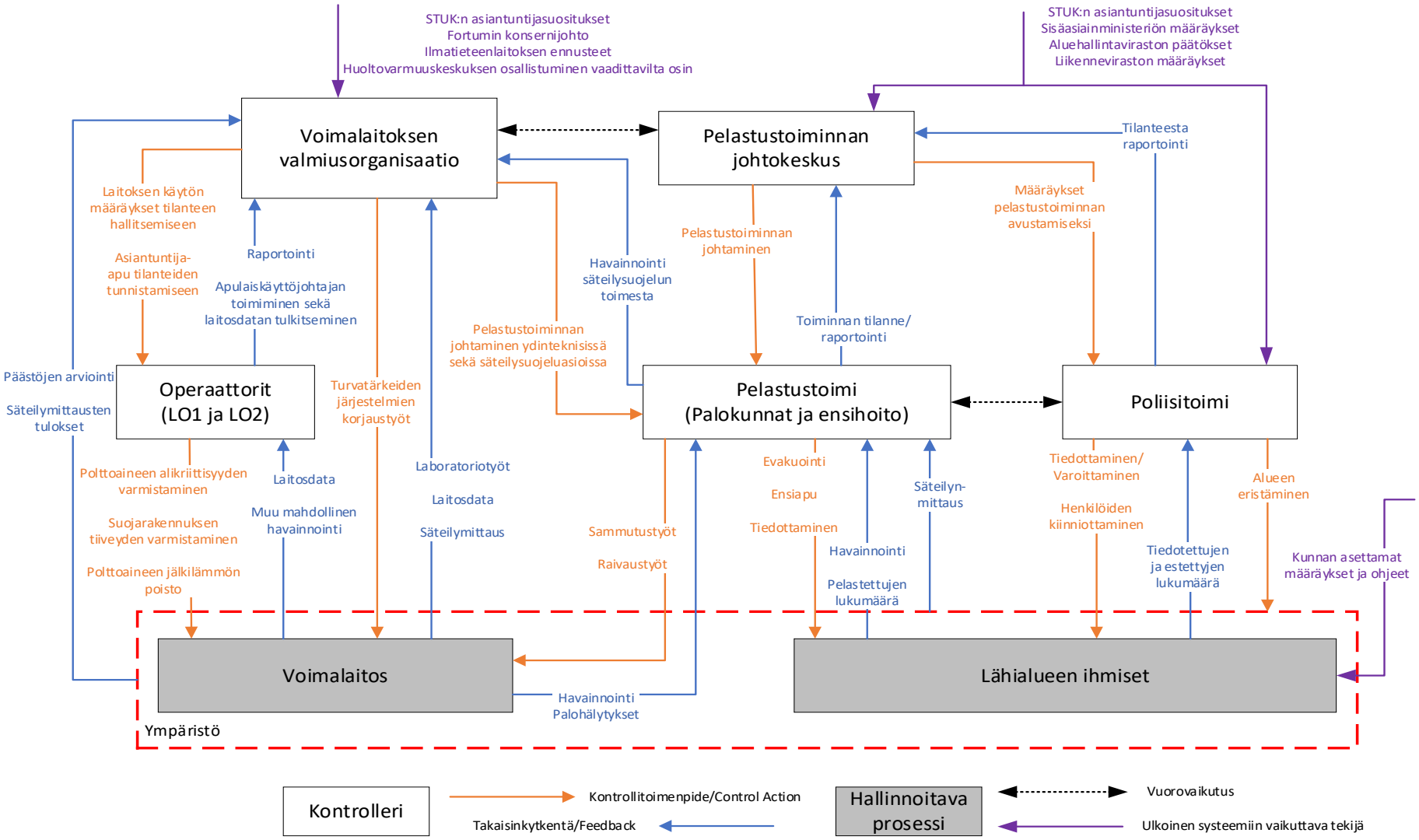
Rajoitteiden määrittämisen jälkeen analyysissä voitaisiin määrittää vastuut eri toimijoille systeemin sisällä. Valmiustoiminnan tahojen vastuut on kuitenkin jo kuvattuna voimalaitoksen lopullisessa turvallisuusselosteessa sekä valmiuskansiossa. Täten vastuita ei tulla erikseen listaamaan analyysissä. Valmiusorganisaation vakansseja sekä valmiustilanteeseen oleellisesti liittyviä viranomaisia on kuvailtu myös tämän työn luvussa 2.3. Vastuiden määrittäminen on vaihtoehtoinen työvaihe STPA-analyysissä varsinkin jo olemassa olevien systeemien osalta, joten sen poisjättäminen ei ole este analyysin jatkamiselle.

5.2.3 **Kontrollerien sekä niiden välisten suhteiden kuvaaminen**

STPA-analyysin toisessa vaiheessa mallinnetaan systeemin kontrollirakenne. Kontrollirakenne määritetään diagrammina, josta näkee systeemin mallinnettavat toimijat, niiden väliset suhteet sekä hierarkian. Mallinnettavia toimijoita on kuvailtu aiemmin luvussa 2. Näistä toimijoista oleellisimpia tämän työn kannalta ovat valmiusorganisaatioon liittyvät toimijat, operaattorit sekä pelastustoimintaan ja poliisiin liittyvät tahot. STUK:n rooli valmiustilanteen kokonaiskuvan kannalta on oleellinen, mutta koska se on puhtaasti asiantuntijaroolissa, ei sitä määritellä kontrolleriksi kontrollidiagrammiin. Toisaalta STUK:n ja useiden muiden viranomaisten toimintaa on käytännössä mahdotonta analysoida tässä työssä yksityiskohtaisempien toimintaohjeiden puuttuessa.

STPA-analyysin luonteesta johtuen voi analyysin suorittaa iteratiivisesti kuten luvussa 4.1.5 mainittiin. Käytännössä tämä tarkoittaa siis sitä, että analyysin ensimmäisen iteraation voi laatia hyvinkin yleisessä muodossa menemättä yksityiskohtaisuuksiin. Ensimmäisen analyysi-iteraation jälkeen analyysiä voi detaljoida koko systeemin tai vain tietyn osa-alueen osalta muissa iteraatioissa. Tässä työssä analyysin ensimmäinen iteraatio pyritään saamaan mahdollisimman tehokkaasti tehtyä, jolloin STPA-analyysin tuottamia tuloksia päästään arvioimaan ja käsittelemään mahdollisimman aikaisessa vaiheessa. Toisaalta yksityiskohtaisen analyysin tuottamiseen ei ole mahdollisuuksia

tarkasteltaessa valmiustoiminnan kaltaista suurta kokonaisuutta diplomityön laajuisessa työssä. Käytännössä yleistäminen näyttäytyy kontrollidiagrammissa abstraktiointina sekä kontrollerien että niiden välisten suhteidenkin osalta. Valmiustoiminnan kontrollidiagrammi nähdään alla olevassa kuvassa.



Kuva 16. Valmiustoiminnan kontrollidiagrammi

Kuva 16 havainnollistaa luvussa 2.3 mainittuja valmiustoimintaan osallistuvia tahoja sekä niiden välisiä suhteita valmiustoiminnan aikana. Kuvassa ylimpänä olevat kontrollerit ovat hierarkiassa korkeammalla kuin alempana olevat kontrollerit täten havainnollistaen johtoasemassa olevia kontrollereita. Aiemmin mainittu abstraktisuus näkyy kuvassa kontrollerien osalta siten, että esimerkiksi voimalaitoksen valmiusorganisaation kontrolleriin kuuluvat kaikki luvussa 2.3 mainitut vakanssit. Toinen vaihtoehto olisi ollut eritellä kaikki vakanssit erikseen, jolloin vakanssien väliset suhteet olisivat tulleet näkyviin myös kontrollidiagrammissa, mutta tällöin analyysistä olisi tullut huomattavasti laajempi täten ylittäen työlle asetetun rajauksen. Kontrollerimäärityksiä voi tarkentaa myöhemmissä iteraatioissa, jos sille koetaan tarvetta.

Valmiustoiminnan ydin- ja säteilyteknistä osa-aluetta johtaa valmiusorganisaatio, jonka suorassa alaisuudessa valvomoissa olevat operaattorit toimivat. Valmiusorganisaatio toimii osaltaan myös pelastustoimen johtamisessa sellaisissa pelastustehtävissä, joissa vaaditaan ydintekniikan tai säteilysuojelun asiantuntijuutta. Muilta osin pelastustoimintaa johtaa pelastustoiminnan johtokeskus, jonka oleellisimpana toimijana on pelastustoiminnan johtaja. Poliisitoimi-kontrolleriin sisällytetään poliisin johtoelementti sekä kenttätoiminta. Ei-rikosperusteisissa valmiustilanteissa poliisitoimi toimii avustavissa tehtävissä pelastustoimen rinnalla.

Huomioitavaa kontrollidiagrammissa on se, että kaikki kontrollerit ovat inhimillisiä, eikä koneellisia kontrollereita ole tunnistettu ollenkaan siitä huolimatta, että operaattorit operoivat voimalaitosta laitostietokoneen välityksellä. Laitostietokoneen sisällyttäminen kontrolleriksi ei katsota kuuluvan valmiustoiminnan analyysiin. Jos tutkimuksessa olisi analysoitu operaattoreiden toimintaa esimerkiksi voimalaitoksen normaalikäytössä, olisi laitostietokonetta oleellista tarkastella.

Ihmiskontrollerien analysoinnin haasteellisuutta lisää kontrollerien abstraktisuus, sillä abstraktia kokonaisuutta on vaikeampi analysoida mentaalimallin mukaisesti, koska isossa kokonaisuudessa on hankalampi hahmottaa kontrollitoimenpiteisiin ja takaisinkytkentöihin liittyvää tiedonvälittymistä. Mentaalimalli ei toisaalta yksinkertaisimmassa muodossaan vaadi muuta kuin analysoijan subjektiivista näkemystä. Isoa kokonaisuutta on hankalampi analysoida verrattuna yksittäisen ihmiseen myös siksi, että kokonaisuuteen on hankalampi samaistua analysoinnin aikana.

Kommunikaatio eri toimijoiden välillä on oleellista ja tärkeää turvallisen toiminnan takaamiseksi. Kommunikointia tapahtuu kontrollitoimenpiteiden, takaisinkytkentöjen sekä vuorovaikutuksen muodossa. Toimivalla kommunikaatiolla taataan luotettava tilannekuva, jonka perusteella kontrollerit voivat suorittaa kontrollitoimenpiteitä hierarkiassa alempana oleville tahoille. Valmiusorganisaatio esimerkiksi suunnittelee ja määrää laitokseen kohdistuvat korjaustoimenpiteet yhdessä operaattoreiden kanssa. Jos kommunikaatio puuttuu, ei valmiusorganisaatio välttämättä pysty toteuttamaan korjaustoimenpiteitä turvallisuuden kannalta vaaditulla tavalla, jolloin onnettomuuden etenemisen rajoittaminen voi vaarantua.

Kontrollidiagrammista on oleellista huomioida myös analysoitavan systeemin ulkopuolelle rajatut ulkopuoliset toimijat, joista oleellisin on STUK. Edellä mainitun kommunikaation avulla STUK pystyy luomaan tilannekuvan ja antamaan asiantuntijasuosituksensa tämän tilannekuvan perusteella. Jos STUK:n tilannekuva on jostain syystä vääristynyt, voi se antaa epäturvallisia suosituksia esimerkiksi pelastustoiminnan johtokeskukselle. On siis tärkeää, että myös valmiusorganisaatio raportoi toiminnastaan ja havainnoistaan asianmukaisesti STUK:lle. Vaikka jokin toimija onkin rajattu analysoitavan systeemin ulkopuolelle, ei se tarkoita sitä, etteikö se voisi jollain tapaa vaikuttaa analysoitavaan systeemiin. Näiden ulkopuolisten toimijoiden olemassaolo tulee huomioida skenaarioita määritettäessä.

Kontrollidiagrammissa mainitut laboratoriotyöt, päästöjen arviointi sekä säteilyn mittaus on merkitty diagrammiin takaisinkytkentänä, vaikka ne ovatkin sinänsä aktiivista suorittamista. Syy tälle on se, että niillä ei ole suoranaista vaikutusta kontrolloitavaan kohteeseen, joka on näissä tapauksissa voimalaitos tai sen ympäristö. Esimerkiksi säteilyä mitattaessa voimalaitoksen ympäristöä ei kontrolloida tai muokata millään tavoin, joten nämä eivät voi olla STPA-analyysissä kontrollitoimenpiteitä. Säteilyn mittauksen sekä muiden vastaavien toiminnallisten takaisinkytkentöjen puutteellinen toteutus tai puutteellinen tulkinta tulee huomioida täten vasta riskiskenaarioita määritettäessä. Tällaisia riskitekijöitä tullaan pohtimaan työn myöhemmässä vaiheessa.

Kontrollidiagrammi on erittäin hyvä perusta analysoitavan kohteen ymmärtämiselle, joten diagrammin todenmukaisuus sekä asiaankuuluvuus on tärkeää. Jos jokin osa diagrammista ei ole todenmukainen, myös analyysi tuottaa epätodenmukaisia tuloksia.

Toisaalta on muistettava, ettei diagrammi kerro koko kuvaa analysoitavasta systeemistä. Esimerkiksi ulkoisten toimijoiden lisäksi systeemiin voi vaikuttaa hyvin myös ulkoiset uhkat. Tällainen ulkoinen uhka voi olla esimerkiksi jokin valmiustoiminnan laukaissut tapahtuma kuten öljyonnettomuus Suomenlahdella (Felin 2019). Ulkoinen uhka voi itse valmiustilanteen aikana aiheuttaa lisäongelmia sellaisissa tilanteissa, joissa jokin ulkoinen uhka on päässyt vaikuttamaan valmiustoimintaan osallistuvien organisaatioiden ja tahojen toimintaan.

5.2.4 Epäturvalliset kontrollitoimenpiteet valmiustoiminnan aikana

Kuva 16 määrittelee kontrollitoimenpiteet, joita seuraavaksi tarkastellaan epäturvallisten kontrollitoimenpiteiden identifioimisen yhteydessä. Tässä STPA-analyysin kolmannessa vaiheessa perusperiaatteiden sekä yleisen toiminnan ymmärtäminen analysoitavaan kohteeseen liittyen on oleellista, jotta kontrollitoimenpiteiden vaikutuksia pystytään tarkastelemaan mahdollisimman todenmukaisesti. Esimerkiksi on syytä tiedostaa, mitä milläkin toimenpiteellä pyritään saavuttamaan ja että voiko jonkin toimenpiteen suorittamiseen tai suorittamatta jättämiseen liittyä epäturvallisuutta.

Käytännössä epäturvallisten kontrollitoimenpiteiden määritys on suoraviivainen prosessi, jossa jokaiselle kontrollidiagrammin kontrollitoimenpiteelle käydään läpi taulukon 1 osoittamat neljä UCA-tyyppiä. Jokaisesta UCA:sta tulee käydä ilmi kontrollitoimenpiteen suorittaja (kontrolleri), kontrollityyppi, itse kontrollitoimenpide sekä konteksti. Analyysi on alun perin suunniteltu englannin kielellä tehtäväksi, jolloin tiettyjä kielellisiä haasteita saattaa ilmentyä analyysin eri vaiheissa. Käydään seuraavaksi läpi esimerkkien avulla epäturvallisia kontrollitoimenpiteitä valmiusorganisaation sekä operaattorien osalta. Esimerkki-UCA:t löytyvät alla olevasta taulukosta.

Taulukko 2. Epäturvallisia kontrollitoimenpiteitä valmiusorganisaatiolle sekä operaattoreille

Kontrolleri Kontrolli-toimenpide Kohde	**Ei tehdä, johtaa uhkaan**	**Tehdään, johtaa uhkaan**	**Tehdään liian aikaisin, myöhässä tai väärässä järjestyksessä**	**Keskeytetään liian aikaisin tai jatketaan liian pitkään**
Valmius-organisaatio Kriittisen kohteen korjaus-toimenpide Voimalaitos	**UCA-1**: Valmius-organisaatio ei suorita kriittisen kohteen korjaus-toimenpidettä tilanteen vaatiessa. [H-2, H-3]	**UCA-2**: Valmius-organisaatio suorittaa kriittisen kohteen korjaustoimen-piteen, mutta toimenpiteellä on negatiivinen turvallisuus-vaikutus. [H-2, H-3]	**UCA-3**: Valmius-organisaatio suorittaa kriittisen kohteen korjaus-toimenpidettä liian aikaisin siten, että korjattava kohde ei ole vielä turvallinen toimen-pidettä varten. [H-1]	**UCA-4**: Valmius-organisaatio on suorittamassa korjaustoimen-pidettä, mutta toimenpide lopetetaan liian aikaisin ennen kuin se on saatu päätökseen. [H-2, H-3]
Operaattorit Polttoaineen alikriittisyyden varmistaminen Voimalaitos	**UCA-5**: Operaattorit eivät suorita polttoaineen alikriittisyyden varmistamiseen liittyviä toimenpiteitä tilanteen niin vaatiessa. [H-2, H-3]	**UCA-6**: Operaattorit suorittavat polttoaineen alikriittisyyden varmentamista pumppaamalla booraamatonta vettä reaktoriin. [H-2, H-3]	**UCA-7**: Valmius-organisaatio suorittaa kriittisen kohteen korjaus-toimenpiteen liian aikaisin siten, että korjattava kohde ei ole vielä turvallinen toimen-pidettä varten. [H-2, H-3	**UCA-8**: Operaattorit lopettavat polttoaineen alikriittisyyden varmentamisen liian aikaisin, jolloin reaktori voi mennä uudelleen-kriittiseksi. [H-2, H-3]

Yllä oleva taulukko pitää sisällään vain osan identifioiduista epäturvallisista kontrollitoimenpiteistä. Kaikkien muidenkin kontrollitoimenpiteiden epäturvallisuus analysoidaan samalla tavalla. Tässä työvaiheessa ei vielä mietitä syitä epäturvallisten kontrollitoimenpiteiden taustalla, vaan keskitytään identifioimaan epäturvallisia toimenpiteitä systemaattisesti UCA-tyyppien avulla. Alla olevasta taulukosta nähdään identifioitujen epäturvallisten kontrollitoimenpiteiden tyyppijakautuminen.

Taulukko 3. Epäturvallisten kontrollitoimenpiteiden tyyppijakautuminen

UCA-tyyppi	**Lukumäärä**
Ei tehdä, johtaa uhkaan	16
Tehdään, johtaa uhkaan	19
Tehdään liian aikaisin, myöhässä tai väärässä järjestyksessä	19
Keskeytetään liian aikaisin tai jatketaan liian pitkään	15
Yhteensä	*69*

Yllä olevasta taulukosta nähdään, että UCA:t jakautuvat lukumäärältään suhteellisen tasaisesti eri tyyppeihin. Osaltaan tähän vaikuttaa analyysin laadinta yleisellä tasolla. Esimerkiksi valmiusorganisaation ja operaattorien väliset kontrollitoimenpiteet eli käytön määräykset sekä asiantuntija-apu ovat epäturvallisien kontrollitoimenpiteiden osalta samankaltaisia. Jos analyysi olisi yksityiskohtaisempi, nähtäisiin luultavasti suurempia eroja kontrollitoimenpiteissä sekä UCA-tyyppijaossa.

Yllä olevaan taulukkoon listattujen toisen ja kolmannen UCA-tyypin suurempi lukumäärä selittyy sillä, että tiettyjen kontrollitoimenpiteiden osalta itse toimenpiteen voi suorittaa väärin useammalla eri tavalla tai useampaan kohteeseen liittyen. Tähän verrattuna ensimmäinen UCA-tyyppi on suppeampi, koska yhdellä UCA:lla voidaan käsittää toimenpiteen kokonaan pois jättäminen riippumatta kontrollitoimenpiteen kohteesta tai suoritustavasta. Kolmanteen UCA-tyyppiin liittyen joillekin kontrollitoimenpiteille on mahdollista, että toimenpiteen suorittaminen liian aikaisin tai liian myöhässä voivat johtaa eri uhkiin tai syyt tällaisten toimenpiteiden taustalla voivat olla keskenään erilaiset. Neljänteen UCA-tyyppiin on löydetty vähäisin määrä epäturvallisia kontrollitoimenpiteitä siitäkin huolimatta, että tässä UCA-tyypissä toimenpide voi olla kahdellakin tapaa epäturvallinen. Tämä johtuu siitä, että epäturvallisia toimenpiteitä ei juuri ole määritelty tilanteille, joissa toimenpidettä jatketaan liian kauan. Tämä johtuu siitä, että suuri osa määritellyistä kontrollitoimenpiteistä on kommunikointia eri tahojen välillä, jolloin kommunikoinnin jatkaminen liian kauan tilanteesta riippumatta on hankala määritellä uhkaksi.

Kontrollereille määritellään seuraavaksi rajoitteet vastaamaan jokaista epäturvallista kontrollitoimenpidettä. Kontrollerikohtaisten rajoitteiden määritys tässä yhteydessä ei sinänsä olisi oleellinen työvaihe, koska näillä rajoitteilla ei juuri ole muuta jälleenkäyttöarvoa kuin kontrollerikohtaisten vaatimusten tai toimintaohjeiden laatimisessa. Toisaalta tässä tapauksessa näitä kontrollerikohtaisia rajoitteita voidaan vertailla jo olemassa oleviin vaatimuksiin mahdollisten puutteiden tai ristiriitaisuuksien löytämiseksi. Kuten aiemminkin, rajoitteet laaditaan kääntämällä epäturvalliset kontrollitoimenpiteet päinvastaiseksi siten, että rajoitetta noudattamalla epäturvallisia kontrollitoimenpiteitä ei pääse tapahtumaan. Alle on listattu muutamia taulukon 2 esittämien epäturvallisten kontrollitoimenpiteiden rajoitteita.

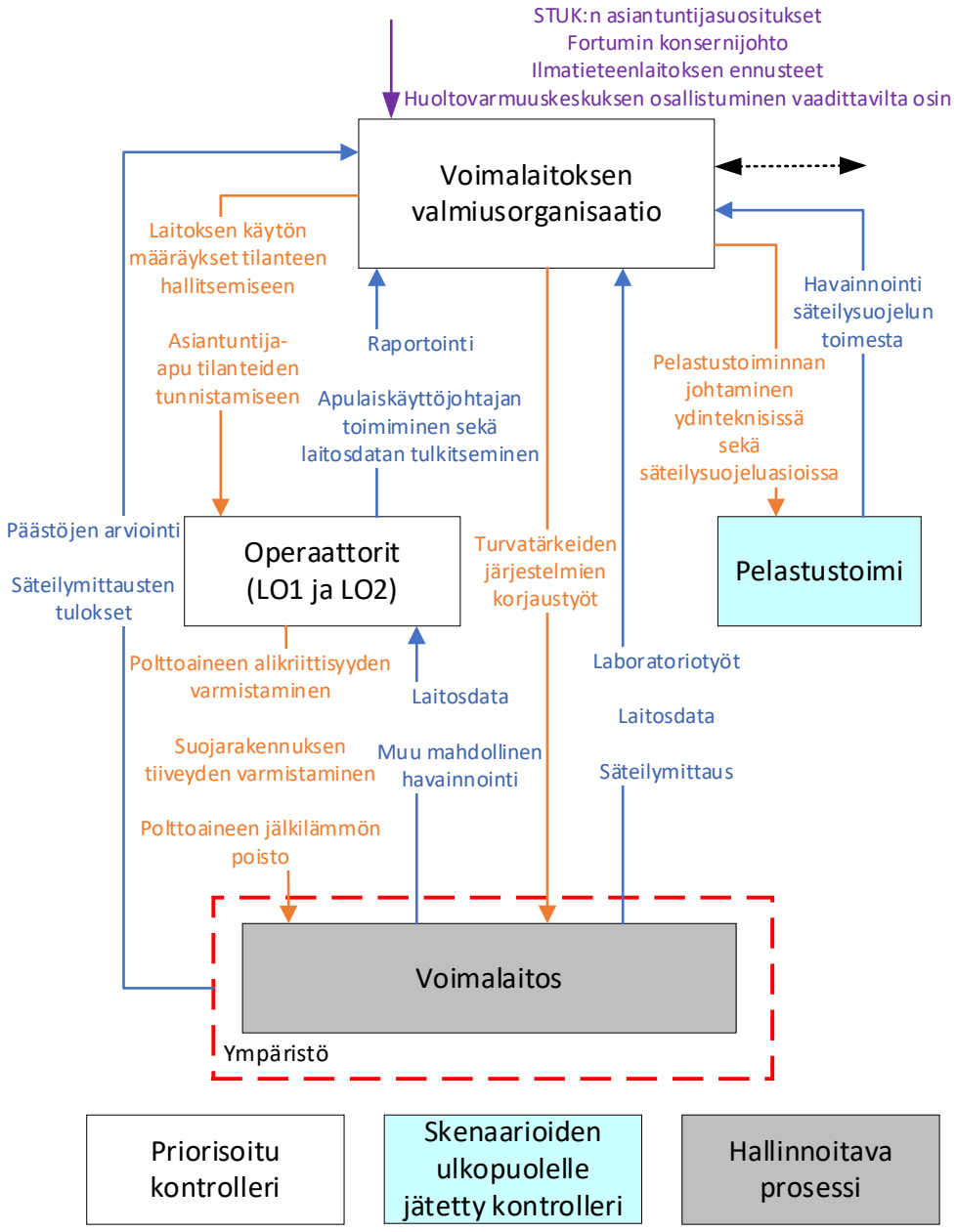
- C-1: Valmiusorganisaation tulee korjata vikaantuneet voimalaitoksen turvallisuuden kannalta kriittiset kohteet [UCA-1]
- C-2: Valmiusorganisaation suorittamalla korjaustyöllä ei saa olla negatiivista turvallisuusvaikutusta. [UCA-2]
- C-3: Valmiusorganisaation tulee varmistua siitä, että korjaustoimenpiteen kohde sekä sen ympäristö ovat tilanteeseen nähden turvallisia korjaustoimenpidettä varten. [UCA-3]
- C-6: Operaattorien suorittaman polttoaineen alikriittisyyden varmentamiseen liittyvän toimenpiteen tulee alentaa polttoaineen reaktiivisuutta [UCA-6]
- C-7: Operaattoreilla ei saa kestää liian kauan aikaa polttoaineen alikriittisyyden varmentamisen aloittamisessa [UCA-7]
- C-8: Operaattorit eivät saa lopettaa polttoaineen alikriittisyyden varmentamiseen liittyviä toimenpiteitä liian aikaisin, jolloin polttoaine voi palata kriittiseksi [UCA-8]

Yllä olevat esimerkkirajoitteet havainnollistavat hyvin sekä valmiusorganisaation että operaattoreiden toimintaan liittyviä vaatimuksia turvallisen toiminnan takaamiseksi. Rajoitteet luovat syvyyttä analyysin oikeellisuuden arviointiin tutkimuksen lopulla sillä, jos yllä olevat rajoitteet eivät olisi ollenkaan linjassa laitoksella olevien käytäntöjen kanssa, on syytä epäillä, että analyysi ei tuota todenmukaisia tuloksia.

5.2.5 Skenaarioiden identifioiminen

Analyysin viimeiseen vaiheeseen kuuluu skenaarioiden identifiointi. Skenaariot muun muassa kuvailevat kausaalisia syitä edellisessä vaiheessa löydetyille epäturvallisille kontrollitoimenpiteille. Skenaariot voidaan jakaa kahteen eri tyyppiin. Jako näiden skenaariotyyppien välillä nähdään kuvasta 11.

Luvussa neljä käydystä esimerkistä nähdään, että yhteen epäturvalliseen kontrollitoimenpiteeseen linkittyy vähintään kolme skenaariota. Taulukon 3 perusteella voidaan todeta, että tässä analyysissä epäturvallisiin kontrollitoimenpiteisiin liittyviä skenaarioita tullaan määrittämään noin 250 kappaletta. Tästä syystä tässä työssä on päädytty määrittämään skenaariot ainoastaan valmiusorganisaatiolle sekä operaattoreille. Alla olevasta kontrollidiagrammin osaa esittävästä kuvasta nähdään ne kontrollerit sekä kontrollitoimenpiteet, joiden osalta skenaariot tullaan määrittämään.



Kuva 17. Valmiusorganisaation sekä operaattoreiden kontrollidiagrammi

Yllä oleva kuva esittää niitä kontrollereita sekä kontrollitoimenpiteitä joiden osalta riskiskenaariot tullaan identifioimaan tässä case-tutkimuksessa. Skenaariot liittyvät useisiin eri tekijöihin aina kontrollerin omasta toiminnasta kontrollidiagrammin muiden tai mahdollisesti ulkopuolisten kontrollereiden toimintaan saakka. Skenaarioita laatiessa tulee miettiä väärän tilannekuvan vaikutusmahdollisuutta kontrollerin päätöksentekoon. Tämän lisäksi väärän tilannekuvan aiheuttajia on oleellista pohtia skenaarioita laadittaessa. Vääriin olettamuksiin liittyvien kausaalisten tekijöiden analysoinnin apuna

voidaan hyödyntää aiemmin käsiteltyä mentaalimallia. Skenaarioiden laadintaa on käyty läpi myös luvussa 4.1.4.

Laaditaan seuraavaksi taulukon 2 epäturvallisten kontrollitoimenpiteiden taustalla olevat skenaariot. Alla olevasta taulukosta löytyy korjaustoimenpiteen epäturvallisiin kontrollitoimenpiteisiin liittyviä skenaarioita.

Taulukko 4. Korjaustoimenpiteeseen liittyviä skenaarioita

Kontrolleri Kontrolli-toimenpide Kohde	**Ei tehdä, johtaa uhkaan**	**Tehdään, johtaa uhkaan**	**Tehdään liian aikaisin, myöhässä tai väärässä järjestyksessä**	**Keskeytetään liian aikaisin tai jatketaan liian pitkään**
Valmius-organisaatio Kriittisen kohteen korjaus-toimenpide Voimalaitos	**Skenaario 1**: Valmius-organisaatio ei suorita korjaus-toimenpidettä voimalaitokselle korjaus-toimenpiteeseen osallistuvan tahon inhimillisen syyn tai ulkoisen häiriötekijän vuoksi. Seurauksena korjaustoimen-pidettä ei saada suoritettua. [UCA-1]	**Skenaario 2**: Valmius-organisaatio suorittaa korjaus-toimenpiteen epä-turvallisesti. Tilanne voi aiheutua pitkit-tyneestä valmius-tilanteesta aiheutuneesta uupumuksesta. Tilanteen seurauksena korjaustoimen-pide suoritetaan vajavaisesti tai epäturvallisesti korjaajille itselleen. [UCA-2]	**Skenaario 3**: Valmius-organisaatio lähtee suorittamaan korjaustoimen-pidettä kohteelle liian aikaisin siten, että kohde ei ole vielä turvallinen korjausta varten esimerkiksi prosessierotuksen osalta. Tilanne voi aiheutua esimerkiksi kommunikaatio-ongelmista valmiusorganisaati on sisällä. [UCA-3]	**Skenaario 4**: Valmius-organisaatio lopettaa korjaus-toimenpiteen suorittamisen liian aikaisin puut-teellisen tieto-taidon vuoksi. Korjausta suorit-tava taho olettaa korjauksen olevan valmis työn ollessa vielä kesken. Tilanne voi aiheutua esimerkiksi puutteellisesta koulutuksesta, ohjeistuksesta tai kokemuksesta. [UCA-4]

Yllä olevasta taulukosta nähdään, että korjaustoimenpiteen epäturvallisiin kontrollitoimenpiteisiin liittyy ainakin hypoteettisesti useita eri syitä. Yllä oleva taulukko pitää sisällään vain osan korjaustoimenpiteen identifioiduista skenaarioista. Analyysissä on identifioitu noin viisi skenaariota jokaiselle korjaustoimenpiteen epäturvalliselle kontrollitoimenpiteelle.

On ainakin teoriassa mahdollista, että korjauksen suorittajat tai korjausjohtaja ovat jollain tavalla estyneet, jolloin korjaustoimenpiteet jäisivät kokonaan suorittamatta joko

henkilökohtaisesta inhimillisestä syystä kuten sairaskohtauksesta tai ulkoisen tekijän takia.

Korjaustoimenpide suorittaminen saattaa myös johtaa epäturvallisiin tilanteisiin, jos korjaustyöllä ei olekaan vaadittua lopputulosta. Yllä olevan taulukon skenaarion 2 mukaan tällainen tilanne voi aiheutua esimerkiksi työn teon tarkkuuden heikkenemisestä pitkäkestoisesta tilanteesta aiheutuen. Tämän skenaarion hallintatoimenpiteenä voisi esimerkiksi varmistaa, että korjausryhmän vuoroja ja henkilöstöä on varmasti tarvittava määrä.

Korjaustoimenpiteen suorittamiseen liittyy epäturvallisuutta myös vääräaikaisen suorittamisen suhteen sellaisissa kohteissa, joissa prosessierotus on tärkeää tehtävä ennen korjaustyön aloittamista. Tällaisissa tilanteissa korjaajat saattavat joutua hengenvaaraan, jos ennalta vaadittuja valmisteluja ei ole tehty ennen korjaustyön aloittamista. Yllä olevan taulukon esimerkin mukaan onnettomuus saattaa tapahtua kommunikaatio-ongelmien seurauksena, jolloin korjausjohtaja tai korjaajat itse ovat siinä käsityksessä, että työn kohde on turvallinen korjausta varten. Toisaalta on mahdollista, että itse erotus on toteutettu väärin, jolloin korjaajien ja korjausjohtajan lisäksi myös muulla henkilöstöllä on epätodenmukainen tilannekuva tilanteesta.

Kaikkien epäturvallisten kontrollitoimenpiteiden taustalla voidaan katsoa olevan ihmiskontrollerin koulutuksen, ohjeistuksen tai kokemuksen puute. Näissä skenaarioissa kontrollitoimenpiteen suorittajalla on puutteellinen tietotaito, jonka seurauksena saatetaan ajautua ainakin teoriassa epäturvallisiin tilanteisiin. Alla olevassa taulukossa esitetään esimerkkiskenaarioita operaattoreiden suorittamalle polttoaineen alikriittisyyden varmistamiselle.

Taulukko 5. Alikriittisyyden varmistamiseen liittyviä skenaarioita

Kontrolleri **Kontrolli-toimenpide** **Kohde**	**Ei tehdä, johtaa uhkaan**	**Tehdään, johtaa uhkaan**	**Tehdään liian aikaisin, myöhässä tai väärässä järjestyksessä**	**Keskeytetään liian aikaisin tai jatketaan liian pitkään**
Operaattorit Polttoaineen alikriittisyyden varmistaminen Voimalaitos	**Skenaario 5**: Operaattorit eivät eivät suorita alikriittisyyden varmistamiseen liittyviä toimenpiteitä valmius-organisaation antaman harhaanjohtavan määräyksen takia. Tilanteen seurauksena alikriittisyyden varmentamista ei ole suoritettu. [UCA-5]	**Skenaario 6**: Operaattorit pumppaavat booraamatonta vettä reaktoriin puutteellisen tilannetiedon vuoksi. Tilanne voi liittyä esimerkiksi valmius-organisaation antamaan harhaanjohtavaan ohjeistukseen. Tilanteessa operaattorit eivät ole tietoisia pumpattavan veden booraamatto-muudesta. [UCA-6]	**Skenaario 7**: Operaattorit aloittavat alikriittisyyden varmentamiseen liittyvät toimenpiteet myöhässä kontrollerin sisäisen hitauden vuoksi. Tilanne voi johtua esimerkiksi valvomon kommunikaatio-ongelmista. [UCA-7]	**Skenaario 8**: Operaattorit lopettavat alikriittisyyden varmentamisen liian aikaisin kriittisen tahon inhimillisen syyn tai ulkoisen häiriötekijän takia. Kyseessä voi olla valvomossa tapahtunut häiriö. Tilanteen seurauksena polttoaine voi palata kriittiseksi tai mennä ylikriittiseksi. [UCA-8]

Yllä olevan taulukko esittää polttoaineen alikriittisyyden varmistamiseen liittyvien epäturvallisten kontrollitoimenpiteiden taustalla olevia skenaarioita. Kuten taulukossa 4, myös tässä taulukossa on esitettynä vain osa analyysissä identifioiduista skenaarioista. Myös tässä tapauksessa skenaarioita on identifioitu noin viisi kappaletta jokaista epäturvallista kontrollitoimenpidettä kohden.

Kontrollitoimenpiteen tekemättä jättämiseen liittyvän esimerkkiskenaarion 5 taustalla on, että hierarkiassa operaattoreiden yläpuolella oleva valmiusorganisaatio on jollain tavalla päässyt vaikuttamaan operaattoreiden toimintaan. Tässä tapauksessa ei kuitenkaan tarkoiteta sitä, että valmiusorganisaatio estäisi tai kieltäisi alikriittisyyden varmistamisen tarkoituksenmukaisesti tai muuten tietoisesti. Tällaisen skenaarion tapahtuessa on hyvin, mahdollista, etteivät operaattorit tule noudattamaan kyseistä epäturvalliseen toimintaan ohjaavaa määräystä, vaan he tulevat noudattamaan omaa ohjeistustaan.

Polttoaineen alikriittisyyden varmentamiseen liittyvien toimenpiteiden suorittamisessa vaaran paikka on silloin, jos reaktoriin pumpataan booratun veden sijasta booraamatonta vettä. Tämän seurauksena reaktiivisuus kasvaa ja polttoaineesta voi tulla nopeasti ylikriittinen aiheuttaen polttoaineen lämpötilan nopean nousemisen. Lämpötilan nousun seurauksena polttoaine voi vaurioitua, jolloin tilanne voi johtaa analyysin alussa määritettyyn menetykseen L-1. Yllä olevan taulukon esittämän esimerkkiskenaarion 6 mukaan tällainen tilanne voi tapahtua silloin, jos operaattorit eivät ole tietoisia siitä, että reaktoriin pumpataan booraamatonta vettä. Tällainen tilanne voi syntyä esimerkiksi silloin, jos operaattoreilla on harhaanjohtavaa tietoa jonkin säiliön veden booripitoisuudesta. Harhaanjohtavaa tietoa voi tulla suoraan laitokselta laitosdatan muodossa tai valmiusorganisaatiolta kommunikaation muodossa esimerkiksi kontrollitoimenpiteeseen tai takaisinkytkentään liittyvien ongelmien seurauksena.

Esimerkkiskenaario 7 on esimerkki hypoteettisestä skenaariosta, jonka tapahtumisen todennäköisyys on todellisuudessa erittäin pieni. Skenaarion 7 kuvaamaa tilanne ei liity pelkästään valmiustoimintaan, koska kyseisen skenaarion kuvaama kommunikaatio-ongelmiin liittyvä kausaalinen tekijä voi tapahtua myös voimalaitoksen normaalikäytön aikana. Tämän perusteella voidaan olettaa, että kommunikaatio-ongelmiin liittyviä ongelmia on analysoitu ja hallittu koko voimalaitoksen käyttöiän ajan. Analyysin aikana havaittiin muitakin vastaavia skenaarioita, jotka liittyvät myös voimalaitoksen normaalikäyttöön.

Yleisesti ottaen taulukoiden 4 ja 5 esittämien skenaarioiden kausaalisia tekijöitä voidaan soveltaa kaikkien epäturvallisten kontrollitoimenpiteiden taustalla oleviin skenaarioihin. Toistuvien kausaalisten tekijöiden takia näissä taulukoissa on esitetty vain osa identifioiduista skenaarioista. Jokaisen UCA:n kohdalla tuleekin käytännössä pohtia, että soveltuuko tietty ennalta määritetty taustatekijä analysoitavaan epäturvalliseen kontrollitoimenpiteeseen vai ei.

Epäturvallisten kontrollitoimenpiteiden taustalla olevien skenaarioiden jälkeen analyysissä laaditaan toimenpidealgoritmiin liittyvät toisen tyypin skenaariot. Kuva 11 havainnollistaa eroja ensimmäisen ja toisen skenaariotyypin välillä. Alla olevasta taulukosta nähdään sekä korjaustoimenpiteeseen että alikriittisyyden varmentamiseen liittyviä toimenpidealgoritmin epäturvallisuuteen liittyviä toisen tyypin skenaarioita.

Taulukko 6. Valmiusorganisaation sekä operaattoreiden toisen tyypin skenaarioita

Kontrolleri **Kontrolli-toimenpide** **Kohde**	**Ei tehdä, johtaa uhkaan**
Valmius-organisaatio Kriittisen kohteen korjaus-toimenpide Voimalaitos	**Skenaario 9**: Valmiusorganisaatio lähtee suorittamaan korjaustoimenpidettä, mutta ei pysty tekemään sitä puuttuvien varaosien tai työkalujen vuoksi. Tilanteen seurauksena korjaustoimenpidettä ei saada suoritettua kokonaisuudessaan. [H-2, H-3] **Skenaario 10**: Valmiusorganisaatio lähtee suorittamaan korjaustoimenpidettä, mutta ei pysty suorittamaan sitä kokonaisuudessaan ilman asiantuntija-apua. Tilanteesta epäturvallisen tekee kommunikaatio-ongelmat korjaajien sekä asiantuntijan välillä. Tilanne voi aiheutua esimerkiksi radiopuhelimen käyttöön liittyvistä ongelmista. [H-2, H-3]
Operaattorit Polttoaineen alikriittisyyden varmistaminen Voimalaitos	**Skenaario 11**: Operaattorit suorittavat polttoaineen alikriittisyyden varmistamiseen liittyvän toimenpiteen voimalaitokselle, mutta operoitava järjestelmä/komponentti ei reagoi halutulla tavalla puutteellisesti toimivan tiedonvälitysjärjestelmän vuoksi. Tilanteen seurauksena polttoaineen alikriittisyyttä ei ole varmistettu. [H-2, H-3] **Skenaario 12**: Operaattorit suorittavat polttoaineen alikriittisyyden varmistamiseen liittyvän toimenpiteen voimalaitokselle, mutta operoitava järjestelmä/komponentti on epäkunnossa, jolloin se ei reagoi. Tilanteessa polttoaineen alikriittisyyttä ei saada varmennettua ennen korjaustyötä. [H-2, H-3]

Yllä olevista esimerkkiskenaarioista nähdään korjaustoimenpiteelle sekä alikriittisyyden varmentamiselle identifioituja toimenpidealgoritmiin liittyviä toisen tyypin skenaarioita. Analyysissä on identifioitu neljä skenaariota kumpaakin ylläolevan taulukon esittämää kontrollitoimenpidettä kohden. Toisen tyypin skenaarioita on siis identifioitu keskimäärin yksi vähemmän verrattuna vastaaviin ensimmäisen tyypin taulukon 4 sekä 5 esittämiin skenaarioihin.

Korjaustoimenpiteen suorittamisen osalta on mahdollista, että työhön vaadittuja varaosia tai työkaluja ei ole saatavilla esimerkiksi varaosien saatavuuden takia. Tilanne voi aiheutua esimerkiksi pitkään jatkuneen valmiustilanteen seurauksena. Korjaustoimenpide saattaa jäädä suorittamatta myös kommunikaatio-ongelmien takia, jos kommunikointivälineitä ei ole saatavilla tai niiden käyttöä ei ole koulutettu. Tilanteesta epäturvallisen tekee se, jos korjaajat joutuvat korjaustyötä suorittaessa tilanteeseen, jossa heidän on kysyttävä asiantuntemusta valmiusorganisaation muilta toimijoilta.

Korjaustoimenpiteen osalta vastaavat skenaariot on mahdollista löytää myös ensimmäisen skenaariotyypin kohdalla sellaisien epäturvallisten kontrollitoimenpiteiden osalta, jossa toimenpidettä ei tehdä. STPA-analyysissä on täten mahdollista, että samankaltaisia skenaarioita löydetään analyysin eri vaiheissa.

Polttoaineen alikriittisyyden varmentamiseen liittyvissä skenaarioissa nähdään selkeämmin miten toisen tyypin skenaariot muodostuvat. Käytännössä kaikki operaattoreille identifioidut skenaariot liittyvät siihen, että laitoksen ohjauspaneeli tai siitä lähtevät signaalit ovat epäkuntoisia tai väärin toimivia. Voimalaitokseen kohdistuvat operointitoimenpiteet epäonnistuvat myös silloin, jos operoitava järjestelmä tai komponentti on epäkuntoinen. Tällaisessa tilanteessa operaattoreiden tulee ilmoittaa tilanteesta valmiusorganisaatiolle, joka ilmoituksen perusteella suorittaa korjaustoimenpiteen vikaantuneelle kohteelle.

Suuri osa kaikista identifioiduista skenaarioista liittyy kontrollerien estymisiin tai vastaaviin esimerkiksi sairastumisien seurauksena, jolloin skenaarioissa on suhteellisen paljon toistuvia tekijöitä. Sairastumiset on määritetty skenaarioiksi siitäkin huolimatta, että valmiusorganisaatiossa sekä yksiköiden valvomossa sairastuneet henkilöt voidaan korvata olemassa olevin menettelyin. Tässä työssä valittu lähestymistapa ei ota kantaa jo olemassa oleviin valmiustoimintaan liittyvien riskien hallintakeinoihin, jonka takia myös sellaisia skenaarioita on identifioitu, joille hallintakeino on jo otettu käyttöön. Tämä lähestymistapa on valittu, koska riskienhallintaan liittyvien hallintakeinojen määritys on jätetty työn rajauksen ulkopuolelle.

Taulukoiden 4, 5 ja 6 sisältämät skenaariot on valittu siten, että ne edustaisivat mahdollisimman hyvin eri tyyppisiä skenaarioita ja niiden taustoja. Alla olevassa taulukossa on esitelty skenaarioiden lukumääräinen jakautuminen.

Taulukko 7. Identifioitujen skenaarioiden lukumäärät skenaariotyypeittäin

Skenaariotyyppi	**Lukumäärä**
Epäturvallisiin kontrollitoimenpiteisiin liittyvät skenaariot (1. tyyppi)	130
Toimenpidealgoritmiin liittyvät skenaariot (2. tyyppi)	27
Yhteensä	*157*

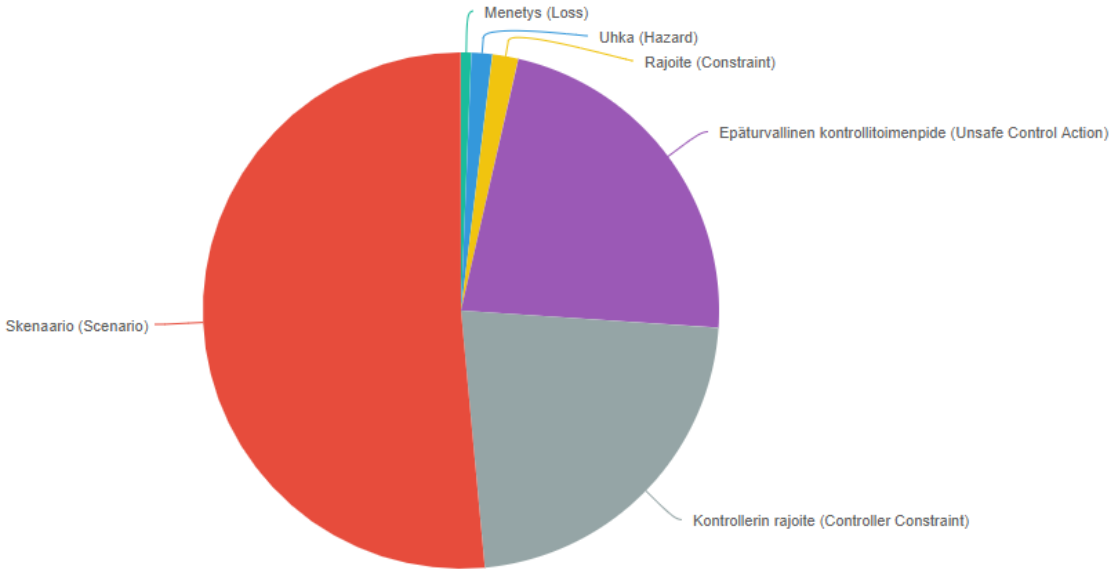
Yllä olevasta taulukosta nähdään, että ensimmäisen tyypin skenaarioita on noin viisinkertaisesti verrattuna toisen tyypin skenaarioihin. Tämä johtuu siitä, että toisen tyypin skenaariot määritetään kontrollitoimenpidekohtaisesti samoin kuin epäturvalliset kontrollitoimenpiteet, joille vielä määritellään omat ensimmäisen tyypin skenaarionsa. Näin toisen tyypin skenaarioiden määrityksessä on yksi työvaihe vähemmän verrattuna ensimmäisen tyypin skenaarioihin.

Verrattuna useisiin luotettavuustekniikan analyyseihin, STPA-analyysissä skenaarioiden laatimista helpottaa huomattavasti todennäköisyyksien arvioinnin puuttuminen. Suuri osa identifioiduista skenaarioista on sellaisia, ettei niiden tapahtumisen todennäköisyyttä pysty arvioimaan luotettavasti. Tällainen STPA-analyysin mukainen lähestymistapa skenaarioihin saattaa tuoda lisää syvyyttä tai informaatiota sellaisiin riskeihin liittyen, joita aiemmin ei ole otettu ollenkaan huomioon niiden hypoteettisuuden tai erittäin pieneltä vaikuttavan todennäköisyyden vuoksi. Tämä siksi, STPA-analyysissä ei karsita skenaarioita tai tapahtumia niiden pienen todennäköisyyden takia, sillä STPA-analyysissä tarkastellaan pahimpia mahdollisia tilanteita.

5.3 Case-tutkimuksessa esiin tulleet asiat

Tässä luvussa esitellään työn tuloksia diagrammien avulla samalla esittäen mahdollisuuksia valmiustoiminnan jatkoanalysoinnille. Tässä luvussa arvioidaan myös tuloksien oikeellisuutta sekä STPA-analyysin soveltuvuutta. Analysoinnin kohteena oleva valmiustoiminta osoittautui monin paikoin haasteelliseksi analysoitavaksi sen monimutkaisten kontrollilogiikoiden takia.

Alla oleva diagrammi havainnollistaa STPA-elementtien lukumääräisen jakautumisen tehdyssä analyysissä. Diagrammi havainnollistaa analyysin eri vaiheiden tekoon vaadittavaa työpanosta. Toisaalta diagrammista ei näe STPA-elementtien ulkopuolisia asioita kuten kontrollidiagrammia, joka voi olla hyvinkin isotöinen riippuen analysoitavasta kohteesta.



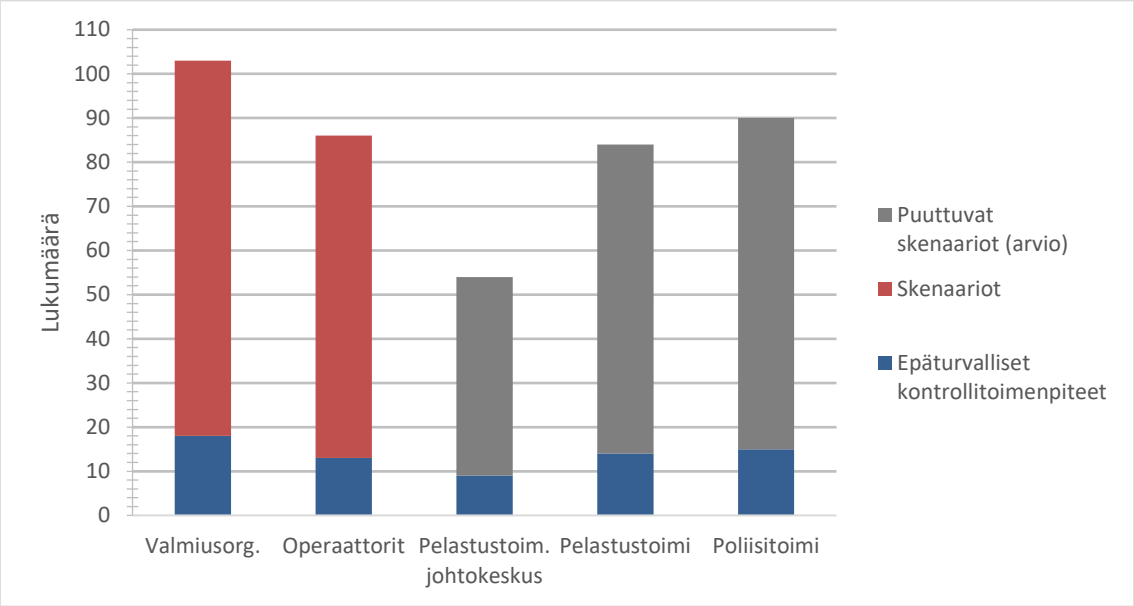
Kuva 18. STPA-elementtien kappalemääräinen jakautuminen

Yllä olevasta kuvasta nähdään, että skenaarioita on määritetty kappalemääräisesti hieman yli 50% verrattuna kaikkien muiden elementtien yhteenlaskettuun määrään, vaikka työssä ei edes laadittu skenaarioita kaikille mahdollisille kontrollereille. Vaikka skenaarioita on lukumääräisesti eniten, on syytä huomioida se, että varsinkin ensimmäinen analyysivaihe vaatii systeemiin osallistuvien toimijoiden sekä sidosryhmien välistä yhteistyötä menetyksien ja uhkien määrittelemiseksi. Täten tilanteesta riippuen muutaman menetyksen sekä uhkan laatimiseen saattaa kulua yhtä paljon aikaa kuin satojen skenaarioiden määrittelyyn.

5.3.1 Ehdotukset jatkoanalyysille

Laadittua analyysiä voi siis suoraviivaisesti jatkaa laatimalla skenaariot myös muille kontrollereille valmiusorganisaation sekä operaattoreiden lisäksi. Näiden skenaarioiden määrityksen myötä myös valmiusorganisaation sekä operaattoreidenkin toimintaan voitaisiin tunnistaa uusia skenaarioita. Esimerkkinä tällaisesta valmiusorganisaatioon

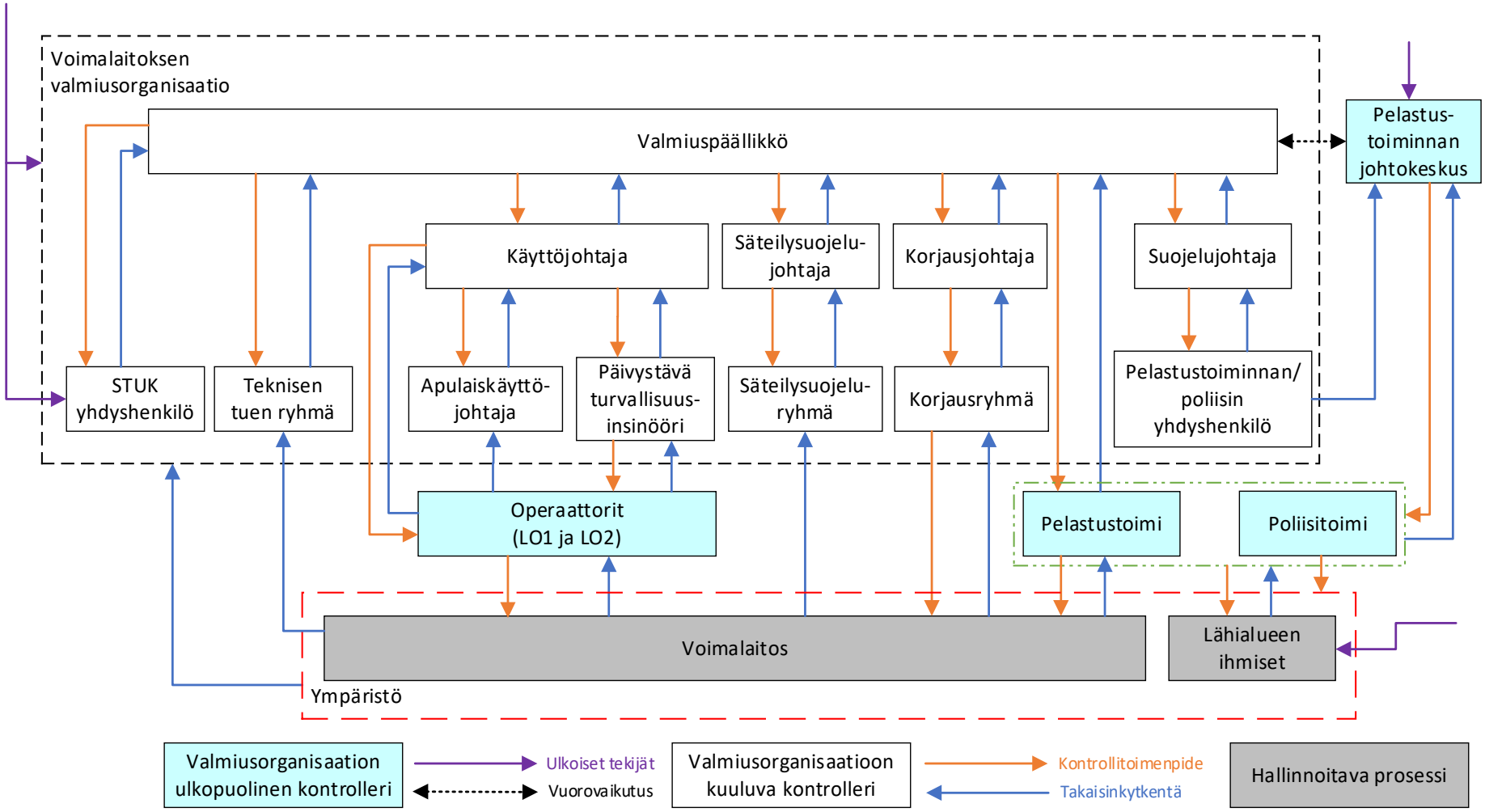
liittyvästä skenaariosta voisi liittyä pelastustoiminnan epäturvalliseen toimimiseen valmiusorganisaation antaman epäturvallisen määräyksen seurauksena. Alla oleva diagrammi esittää toteutuneiden epäturvallisten kontrollitoimenpiteiden sekä skenaarioiden lisäksi arvioitujen skenaarioiden lukumääriä.



Kuva 19. Epäturvallisten kontrollitoimenpiteiden sekä toteutuneiden ja arvioitujen skenaarioiden kontrollerikohtaiset lukumäärät

Yllä olevan kuvan esittämän arvion mukaan koko analyysin skenaarioiden valmiusaste on noin 45 %. Skenaarioiden lukumäärä on suoraan riippuvainen sekä kontrollitoimenpiteiden että niistä määritettävien epäturvallisten kontrollitoimenpiteiden lukumäärästä. Tämän seurauksena toteutumattomien riskiskenaarioiden määrä muuttuu, jos esimerkiksi kontrollitoimenpiteitä tullaan lisäämään jollekin pelastustoimintaan liittyvälle kontrollerille.

Analyysiä voi jatkaa myös uuden analyysi-iteraation muodossa. Seuraavassa iteraatiossa ensimmäinen askel olisi kontrollerien jakaminen useampiin kontrollereihin kontrollidiagrammissa. Tässä analyysissä käytetyt kontrollerit ovat todellisuudessa useampien kontrollerien kokonaisuuksia. Tällainen kontrollerien tarkentaminen on perusteltua, koska STPA-analyysi ei juuri pysty analysoimaan kontrollerin rajapinnan sisäpuolella tapahtuvaa toimintaa. Esimerkiksi valmiusorganisaation kontrollerin jakaminen useampiin kontrollereihin mahdollistaisi valmiusorganisaation sisäisen toiminnan analysoinnin. Alla oleva kuva on hahmotelma siitä, miten useamman uuden kontrollerin voi sisällyttää jo olemassa olevaan kontrollidiagrammiin.



Kuva 20. Hahmotelma valmiusorganisaatiokontrollerin jakamisesta useisiin kontrollereihin

Yllä oleva kuva on hahmotelma kontrollidiagrammista, jossa tässä analyysissä käytetty valmiusorganisaatiokontrolleri on kuvattu tarkemmin useampana kontrollerina. Yllä olevasta kuvasta löytyvät käytännössä kaikki alkuperäisessäkin kontrollidiagrammissa olevat kontrollerit sekä niiden väliset suhteet. Kuvan luettavuuden takia kontrollitoimenpiteitä tai takaisinkytkentöjä ei ole nimetty. Kuvaa on myös yksinkertaistettu muun muassa kontrollitoimenpiteiden sekä takaisinkytkentöjen osalta sekä siitä puuttuu joitain työryhmiä kuten tilannekuvaryhmä.

Yllä oleva kuva esittää yhtä mahdollista tapaa suorittaa valmiusorganisaation sisältämien kontrollerien jako useampiin kontrollereihin. Toinen tapa suorittaa sama asia olisi esimerkiksi yhdistämällä ryhmän johtajan sekä itse ryhmän saman kontrollerin sisälle. Tällainen kontrollerijako jättäisi johtajan sekä vastaavan ryhmän välisen toiminnan tarkastelun analyysistä pois, mutta tämä voisi olla esimerkiksi väli-iteraatio tämän tutkimuksen ja yllä olevan kuvan välillä.

Yllä olevasta hahmotelmasta on kuitenkin tärkeää havaita se, että alkuperäistä kontrollidiagrammia ei tarvitse luoda alusta asti uudelleen, vaan sitä voi käyttää hyvänä perustana uusien kontrollidiagrammi-iteraatioiden laatimisessa. Toki useat kontrollitoimenpiteet tai takaisinkytkennät tulevat muuttumaan niiden lähteen tai kohteen osalta varsinkin tässä esimerkissä, jolloin myös laadittuja epäturvallisia kontrollitoimenpiteitä sekä skenaarioita tulee päivittää muuttuneen kontrollidiagrammin perusteella. Tällainen iteraatioittain analysointi vaikuttaa kuitenkin olevan ainoa tapa analysoida näin laajaa kokonaisuutta.

5.3.2 STPA-analyysin sovittaminen Loviisan voimalaitoksen riskienhallintamenettelyihin

Identifioituja skenaarioita voi käyttää Loviisan voimalaitoksen riskienhallintasovelluksessa riskeinä, joille voidaan määrittää hallintatoimenpiteitä. Hallintakeinot voivat liittyä esimerkiksi lisäkoulutukseen, työtapojen muuttamiseen tai ääritapauksessa organisaation muuttamiseen.

Polarion-ohjelmiston tuomien yhteensopivuusominaisuuksien avulla STPA-analyysin sovittaminen yhteen jo olemassa oleviin menetelmiin ei ole ongelma. Käytännössä tällainen yhteensovittaminen ei vaadi suurta panostusta, sillä STPA-analyysin tulosten

yhteensovittaminen riskienhallintamenettelyihin on suoraviivainen prosessi Polarion-ohjelmistossa.

5.3.3 Analyysin soveltuvuuden sekä tulosten arviointi

Esitellyistä esimerkkitapauksista voidaan todeta, että identifioidut epäturvalliset kontrollitoimenpiteet, kontrollerien rajoitteet sekä skenaariot ovat todenmukaisia sekä perusteltuja ottaen huomioon analyysin alussa määritetyt menetykset sekä uhkat. Tosin jotkin skenaariot jättävät tulkinnan varaa todellisesta kausaalisesta tekijästä, jolloin ne saattavat vaatia lisäanalysointia ennen riskienhallintamenettelyjen aloittamista. Skenaarioiden ja muiden elementtien lopullinen arviointi sekä kausaalisten tekijöiden lopullinen tulkitseminen tapahtuu muissa työvaiheissa kuten analyysin lisäiteraatioissa tai riskienhallinnassa.

Edellä mainittua monitulkintaisuutta olisi voitu vähentää varsinkin identifioitujen skenaarioiden osalta esimerkiksi asiantuntijahaastatteluiden avulla. Työn rajauksen vuoksi tällaista kenttätyön mahdollisuutta ei otettu käytäntöön. Rajauksen takia osa työn tuloksista vaikuttaa ympäripyöreiltä, mutta jos työssä olisi panostettu enemmin tähän osa-alueeseen, jokin muu analyysivaihe olisi jäänyt pienemmälle huomiolle. Täten STPA-analyysiä itsessään ei voi syyttää tuloksien ympäripyöreydestä tai hypoteettisuudesta.

Luvussa 4.2 tarkasteltua mentaalimallia hyödynnettiin tutkimuksessa mahdollisuuksien mukaan. Valmiustoiminnan kompleksisuus, kontrollerien abstraktisuus sekä asiantuntijuuden puute asetti mentaalimallin hyödyntämiselle haasteita. Mentaalimallin kokonaisvaltainen hyödyntäminen vaatii syvempää ymmärrystä analysoitavan ihmiskontrollerin työympäristöstä.

Polarion-ohjelmisto toimi hyvänä alustana STPA-analyysin laatimiselle sekä analyysin tulosten esittämiselle. Analyysin pohjan sekä itse analyysin laatiminen selainpohjaiseen Polarion-ohjelmistoon oli suoraviivainen prosessi kattavan ohjelmistoon tutustumisen jälkeen. Case-tutkimuksen lopputuloksena saatiin laaditun analyysin lisäksi myös käyttökelpoinen pohja STPA-analyysin laatimiselle. Luotua analyysipohjaa voi soveltaa myöhemmissä vaiheissa myös muihin käyttötarkoituksiin.

STPA-analyysi vaikutti olevan helppo hasardianalyysi sisäistää sekä laatia siitäkin huolimatta, että valmiustoiminta on hyvin ihmispainotteista sekä kompleksista. Voi olla, että useilla systeemiteoriaan liittymättömillä hasardianalyyseillä vastaavan tutkimuksen laatiminen olisi ollut huomattavasti haasteellisempaa selkeän syy-seuraus-suhteen puuttuessa. STPA-analyysin helppouden, suoraviivaisuuden sekä vapaasti saatavien ohjeistuksien (Leveson & Thomas 2018) vuoksi sen voisi hyvin ottaa laajempaankin käyttöön Loviisan voimalaitoksella.

6 YHTEENVETO

Tämän diplomityön tavoitteena oli tutkia STPA-analyysin soveltuvuutta Loviisan voimalaitoksen valmiustoiminnan suunnittelun työkaluna. STPA-analyysin soveltuvuutta tutkittiin case-tutkimuksena, jolloin soveltuvuuden tutkimisen lisäksi tuloksena saatiin analyysissä identifioituja skenaarioita.

Työn toisessa luvussa käytiin läpi Loviisan voimalaitoksen yleiskuvausta sekä syvyyssuuntaista turvallisuusajattelua, joka on turvallisuusjärjestelmien suunnittelun perusperiaatteen lisäksi myös valmiustoimintaan oleellisesti liittyvä ajatusmalli. Toiminnallisella tasolla syvyyssuuntainen turvallisuusajattelu jaetaan viiteen eri tasoon, joista valmiustoiminta liittyy tasoihin neljä sekä viisi. Nämä toiminnalliset tasot on määritelty kansainvälisen atomienergiajärjestön alaisuudessa toimivan INSAG-ryhmän toimesta.

Valmiusjärjestelyjen avulla ydinvoimalaitosorganisaatiot pystyvät varautumaan epätavallisiin tilanteisiin. Valmiusjärjestelyihin oleellisesti liittyvä valmiustoiminta voidaan jakaa eri luokkiin tilanteiden vakavuustason mukaan. Varautumistilanteessa valmiustoiminnalla pyritään ylläpitämään yleistä turvallisuustasoa epätavallisten tilanteiden sattuessa kun taas yleishätätilanteessa radioaktiivisten aineiden päästö on tapahtunut tai sille on merkittävä riski suojarakennuksen tiiveyden menetyksen yhteydessä. Valmiustoimintaan osallistuu henkilöstöä sekä voimalaitoksen omasta valmiusorganisaatiosta että lukuisista muista viranomaistoimijoista kuten säteilyturvakeskuksesta, pelastuslaitoksesta sekä poliisista. Kaikkien näiden toimijoiden yhteistoiminta sekä toimintakyvyn ylläpito on tärkeää kattavan ja tarkoituksenmukaisen valmiustoiminnan takaamiseksi.

Työn kolmannessa luvussa käytiin läpi STPA-analyysiin liittyviä taustatekijöitä sekä teorioita. Luvussa kerrottiin seikkoja perinteisestä turvallisuustekniikasta, sen historiasta ja siihen liittyvistä analysointiongelmista moderneihin ja kompleksisiin järjestelmiin. Ensimmäisien hasardianalyysien taustalla vaikutti ajatus siitä, että järjestelmän komponenttien korkea luotettavuuden taso takaisi myös korkean järjestelmän turvallisuuden. Tällainen ajatus nähdään nykypäivänäkin laajalti käytössä olevista analyysimalleista kuten vika- ja tapahtumapuista.

Luotettavuus sekä turvallisuus eivät kuitenkaan ole samoja ominaisuuksia kuten luvussa kolme mainituista esimerkeistä käy ilmi. STPA-analyysissä systeemin turvallisuutta ei nähdä luotettavuudesta riippuvana ominaisuutena vaan turvallisuus nähdään emergenttisenä ominaisuutena. Emergentti turvallisuus näyttäytyy eri tavoin systeemissä eri hierarkian tasoilla oleville tahoille. Hierarkiassa ylempänä olevat tahot pystyvät vaikuttamaan turvallisuuteen määrätietoisemmin verrattuna alempana oleviin tahoihin. STPA-analyysissä analyysiin sisällytetään systeemin lisäksi myös sitä ympäröivän organisaation vaikutus.

Luvussa neljä STPA-analyysiä havainnollistettiin yksinkertaistetulle kemikaalilaitokselle laaditun esimerkkianalyysin avulla. Esimerkkianalyysissä käytiin läpi STPA-analyysin eri vaiheita sekä analyysiin liittyviä elementtejä. Käytännössä analyysi tehdään neljässä eri vaiheessa, joista ensimmäisessä määritetään tarkasteltavan systeemin rajapinta sekä systeemiin liittyvät menetykset ja niihin johtavat systeemitason uhkat. Analyysin toisessa vaiheessa laaditaan kontrollidiagrammi, josta tulee ilmi kaikki systeemin kontrollerit sekä niiden väliset suhteet kuten kontrollitoimenpiteet sekä takaisinkytkennät. Analyysin kolmannessa vaiheessa identifioidaan epäturvallisia kontrollitoimenpiteitä systemaattisesti eri kontrollitoimenpiteille. Näille epäturvallisille kontrollitoimenpiteille määritellään skenaarioita analyysin viimeisessä vaiheessa. Epäturvallisen kontrollitoimenpiteen lisäksi skenaario voi liittyä myös kontrollidiagrammiin.

Valmiustoiminnan case-tutkimuksessa määritettiin kaksi menetystä. Ensimmäinen menetys liittyy onnettomuuden etenemisen epäonnistumiseen ja toisen menetyksen tapahtuessa on tapahtunut joko henkilövahinko tai -menetys. Näihin menetyksiin johtavia uhkia määritettiin yhteensä neljä kappaletta ja ne liittyvät valmiustoimintaan osallistuvien tahojen toimintakyvyn menetykseen, jälkilämmön poiston menetykseen sekä lähialueen henkilöstön sekä muiden ihmisten vahingoittamiseen tai heidän evakuoinnin epäonnistumiseen.

Analyysissä määritettiin viisi kontrolleria, jotka toimivat yhteisvaikutuksessa sekä voimalaitoksen, että lähialueen ihmisten hallinnoimisessa. Kontrollerit määritettiin yleiseen muotoon siten, että esimerkiksi kaikki valmiusorganisaatioon kuuluvat tahot niputettiin yhteen kontrolleriin. Jatkoehdotusten osalta esitettiin mahdollisia lähestymistapoja kontrollerimääritysten tarkentamiselle.

Analyysissä identifioitiin yhteensä 69 epäturvallista kontrollitoimenpidettä. Työssä valmiusorganisaation sekä voimalaitoksen operaattoreiden analysointi priorisoitiin etusijalle ja näille kontrollereille määritettiin yhteensä 157 skenaariota. Skenaariot liittyvät valmiusorganisaation osalta määräyksien antamiseen operaattoreille tai pelastustoimelle sekä operaattoreille annettavaan asiantuntija-apuun tilanteiden tunnistamiseen liittyen. Skenaarioiden todettiin olevan osaltaan monitulkintaisia, joten skenaarioiden jatkojalostamiselle on tarvetta. Osasyyksi tulosten monitulkinnaisuudelle mainittiin työn rajauksesta johtuva asiantuntijahaastattelujen puute.

Case-tutkimuksen tuloksena saatujen skenaarioiden todettiin olevan sovitettavissa käytössä oleviin riskienhallinnan menettelyihin Polarion-ohjelmiston teknisenä ratkaisuna. Skenaarioiden lisäksi tutkimuksen sivutuotteena Polarion-ohjelmistoon laaditun pohjan todettiin olleen käyttökelpoinen STPA-analyysien laatimiselle sekä tulosten esittämiselle.

STPA-analyysin todettiin olevan toimiva hasardianalyysi erityyppisten sosioteknisten systeemien ja kokonaisuuksien analysointiin. STPA-analyysi mahdollistaa analysoitavan kohteen ympäröivän organisaation huomioimisen analyysin eri vaiheissa. Tulosten arvioinnissa mainittiin, että vastaavanlaisen tutkimuksen laatiminen systeemiteoriaan kuulumattomilla hasardianalyyseillä olisi ollut huomattavasti haasteellisempaa varsinkin sellaisissa analyysimenetelmissä, joissa analyysimalli perustuu suoran syy-seuraus-suhteen oletukseen. Syy-seuraus-suhteen muodostaminen valmiustoimintaa analysoidessa olisi ollut erittäin haasteellista valmiustoiminnan kompleksisuudesta johtuen.

LÄHDELUETTELO

Eurasto Tapani, Hyvärinen Juhani, Järvinen Marja-Leena, Sandberg Jorma, Sjöblom Kirsti-Liisa. 2004. Ydinvoimalaitostekniikan perusteita. Teoksessa: Ydinturvallisuus/Jorma Sandberg. Hämeenlinna: Säteilyturvakeskus, Karisto Oy. ISBN 951-712-507-0.

Felin Jonna. 2019. FSAR 13.3 Valmiusjärjestelyt Loviisan voimalaitoksella. Loviisan voimalaitos: Fortum Power and Heat Oy. LO1-K852-00931. [Ei julkinen]

Fortum. 2020. Loviisa Nuclear Power Plant History. [www-lähde]. Saatavissa: https://www.fortum.com/about-us/our-company/our-energy-production/our-power-plants/loviisa-nuclear-power-plant/history [viitattu 20.1.2020]

France Megan. 2017. Engineering for Humans: A New Extension to STPA. Diplomityö. MIT, Department of Aeronautics and Astronautics. Partnership for Systems Approaches to Safety and Security. 71 sivua.

Guarnieri Franck, Garbolino Emmanuel. 2019. Safety Dynamics: Evaluating Risk in Complex Industrial Systems. 1. painos. Cham: Springer International Publishing. 234 sivua. ISBN: 978-3-319-96258-0.

Hollnagel Erik. 2012. An Application of the Functional Resonance Analysis Method (FRAM) to Risk Assessment of Organisational Change. Stråk Säkerhets Myndigheten (SSM). Report number: 2013:09. 73 sivua. ISSN: 2000-0456.

IAEA. 1994. Design Basis and Design Features of WWER-440 Model 213 Nuclear Power Plants. Wien, Itävalta. Engineering Safety Section International Atomic Energy Agency. 155 sivua. ISSN 1011-4289.

IAEA. 2005. Safety Reports Series no. 46: Assessment of Defence in Depth for Nuclear Power Plants. Wien, Itävalta. International Atomic Energy Agency. ISBN: 92–0–114004–5.

INSAG. 1996. Defence in Depth in Nuclear Safety: INSAG-10. Wien, Itävalta. International Atomic Energy Agency. 155 sivua. ISSN 1025-2169.

Isolankila Arto, Järvinen Marja-Leena, Keskinen Rauli, Niemelä Ilkka, Ojanen Matti, Rantala Rainer, Sandberg Jorma, Tiippana Petteri, Valtonen Keijo, Virolainen Reijo, Åstrand Kaisa. 2004. Ydinturvallisuuden varmistaminen. Teoksessa: Ydinturvallisuus/Jorma Sandberg. Hämeenlinna: Säteilyturvakeskus, Karisto Oy. ISBN 951-712-507-0.

L 11.12.1987/990. Ydinenergialaki.

Lahti Tero. 2011. Loviisa 1 ja 2 , nimellistehot. Loviisan voimalaitos: Fortum Power and Heat Oy. LO1-K300-00024. [Ei julkinen]

Lehtinen Jarmo, Sandberg Jorma. 2004. Ydinvoiman taival Suomessa: Atomi-innostuksesta ydinrealismiin. Teoksessa: Ydinturvallisuus/Jorma Sandberg. Hämeenlinna: Säteilyturvakeskus, Karisto Oy. ISBN 951-712-507-0.

Leveson Nancy G. 2011. Engineering a Safer World: Systems Thinking Applied to Safety. Moses Joel, de Neufville Richard, Heitor Manuel, Morgan Granger, Paté-Cornell Elisabeth, Rouse William. Lontoo/Cambridge (MA): The MIT Press. 560 sivua. ISBN: 978-0-262-01662-9.

Leveson Nancy G., Thomas John P. 2018. STPA Handbook. Partnership for System Approaches to Safety and Security. MIT. 188 sivua. Saatavissa PDF-muodossa: http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

Michelsen Karl-Erik. 2007. Project Eastinghouse: Teknologinen haaste Loviisassa. ATS Ydintekniikka, 2007: nro 3, sivut 14-16. ISSN-0456-0473.

NRC. 2016. Three Mile Island Accident of 1979 Knowledge Management Digest: Overview. Division of Risk Analysis: NUREG/KM-0001, Revision 1. Washington DC. Saatavissa: https://www.nrc.gov/docs/ML1616/ML16166A337.pdf

Pirinen Janne. 2018. LoCore, Polarion alkuperehdytys. Polarion-koulutus, Loviisa 1.6.2018. Fortum Power And Heat Oy.

Pöllänen Lauri, Ristonmaa Suvi, Sandberg Jorma, Vilkamo Olli. 2004. Varautuminen häiriöihin ja onnettomuuksiin ydinvoimalaitoksilla. Teoksessa: Ydinturvallisuus/Jorma Sandberg. Hämeenlinna: Säteilyturvakeskus, Karisto Oy. ISBN 951-712-507-0.

Salminen Kai. 2007. Loviisan projekti oli hankala mutta opettava. ATS Ydintekniikka, 2007: nro 3, s.17. ISSN-0456-0473.

SFS-ISO 31000. 2018. Riskienhallinta: Ohjeet. Suomen Standardisoimisliitto SFS ry. 2. painos. Helsinki: SFS ryhmä. 39 sivua. Standardi on suomennos kansainvälisestä standardista ISO 31000.

SM. 2012. Säteilyvaaratilanteet - toimijoiden vastuut ja tehtävät. Opas. Helsinki: Monistamo. 91 sivua. ISBN 978-952-491-785-8.

Stringfellow Margaret. 2010. Accident Analysis and Hazard Analysis for Human and Organizational Factors. Väitöskirja. MIT, Department of Aeronautics and Astronautics. Partnership for Systems Approaches to Safety and Security. 231 sivua.

STUK. 2020. Ydinvoimalaitoksen valmiusjärjestelyt, 20.1.2020 YVL C.5. Saatavissa PDF-muodossa: https://www.stuklex.fi/fi/ohje/YVLC-5.

Sulaman Sardar Muhammad, Beer Armin, Felderer Michael, Höst Martin. Software Quality Journal, 2019: volume 27, sivut 349-387. ISSN-1574-1367.

Thomas John. 2019. STPA Hazard Analysis Introduction and Application. European STAMP Workshop and Conference, Helsinki/Espoo, 18-20.9.2019. Aalto-yliopisto.