VAASAN YLIOPISTO

TEKNILLINEN TIEDEKUNTA

SÄHKÖTEKNIIKKA

Hanna-Kaisa Kemppainen

YDINVOIMALAN OHJELMISTOPOHJAISTEN SÄHKÖ- JA AUTOMAATIOJÄRJESTELMIEN KELPOISTUSPROSESSIMALLI

Diplomityö, joka on jätetty tarkastettavaksi diplomi-insinöörin tutkintoa varten

Vaasassa 1.10.2014

Työn valvoja	Professori Kimmo Kauhaniemi
Työn ohjaaja	DI Matti Vaaheranta
Työn tarkastaja	Professori Timo Vekara

ALKULAUSE

Tein diplomityöni Teollisuuden Voima Oyj:n (TVO) Olkiluodon sähkötekniikan toimistossa. Aihe oli mielenkiintoinen ja moniulotteinen, mikä teki siitä myös haastavan. Erityisen mielenkiintoista oli havaita miten laajasta kokonaisuudesta kelpoistuprosessissa on kyse ja miten monet organisaatiot osallistuvat prosessin eri vaiheisiin.

Työni aiheesta, ohjauksesta, neuvoista ja kannustuksesta haluan kiittää esimiestäni ja ohjaajaani Matti Vaaherantaa. Lisäksi kiitos kuuluu TVO:n työntekijöille, jotka auttoivat ja neuvoivat minua kelpoistusprosessimallia kehittäessäni.

Haluan kiittää myös Vaasan yliopiston valvojaani, professori Kimmo Kauhaniemeä, saamastani opastuksesta ja neuvoista.

Lämmin kiitos kuuluu poikaystävälleni, perheelleni ja ystävilleni saamastani tuesta ja kannustuksesta opintojen sekä tämän työn aikana.

Rauma 13.8.2014

Hanna-Kaisa Kemppainen

SISÄLLYSLUETTELO

SYMBOLI- JA LYHENNELUETTELO

ALARA	As Low As Reasonably Achieavable
AGR	Advanced Gas-Cooled Reactor, kaasujäähdytteinen grafiittimoderoitu reaktori
BWR	Boiling Water Reactor, kiehutusvesireaktori
CI	Cinfiguration Item, konfiguraatioyksikkö
CM	Configuration Management, konfiguraationhallinta
COTS	Components Off the Shelf, ”suoraan hyllyltä” otettavat tuotteet
DID	Defence-In-Depth, syvyyspuolustus periaate
ETA	Ennakkotarkastusaineisto
EYT	Ei ydinteknisesti turvallisuusluokiteltu
FBR	Fast Breeder Reactor, hyötyreaktori
GCR	Gas Cooled Reaktor, kaasujäähdytteinen reaktori
HCM	Hardware Configuration Management, laitteiston konfiguraation-hallinta
HWR	Heavy Water Reactor, raskasvesireaktori
IAEA	International Atomic Energy Agency, kansainvälinen atomiener-giajärjestö
ICRP	International Commission on Radiological Protection, kansainvälinen säteilyturvakeskus
IEC	International Elecrotechnical Commission, kansainvälinen sähköalan standardiorganisaatio
IEEE	Institute of Electrical And Electronics Engineering, kansainvälinen tekniikan alan järjestö
ISO	International Organization for Standardization, kansainvälinen standardijärjestö
ITP	Inspection and Testing Plan, tarkastus- ja testaussuunnitelma
LOCA	Loss Of Coolant Accindent, jäähdytteenmenetysonnettomuus
LWR	Light Water Reactor, kevytvesireaktori
OL1	Olkiluodon voimalaitosyksikkö 1
OL2	Olkiluodon voimalaitosyksikkö 2
OL3	Olkiluodon voimalaitosyksikkö 3
OL4	Olkiluodon voimalaitosyksikkö 4
PRA/ PSA	Probabilistic Risk/Safety Assessment, todennäköisyyspohjainen riski-

	analyysi
PWR	Pressurized Water Reactor, painevesireaktori
RBMK	Reaktor Bolshoy Moshchnosti Kanalnyy, Neuvostoliiton aikainen grafiittimoderoitu paineputkireaktori
RE	Requirement Engineering, vaatimustenhallinta
SAHARA	Safety As High As Reasonably Achievable
SAM	Severe Accident Management, vakavien onnettomuuksien hallinta
SCM	Software Configuration Management, ohjelmiston konfiguraation-hallinta
SFS	Suomen Standardisoimisliitto ry
SIL	Safety Integrity Level, turvallisuuen eheyden taso
STUK	Säteilyturvakeskus
TET	Turvallisuuden eheyden taso
TVO	Teollisuuden Voima Oyj
TVONS	TVO Nuclear Services Oy
VCS	Version Control System, versionhallintajärjestelmä
WTC	World Trade Center
YVL	Ydinvoimalaitos

VAASAN YLIOPISTO
Teknillinen tiedekunta
Tekijä: Hanna-Kaisa Kemppainen
Diplomityön nimi: Ydinvoimalan ohjelmistopohjaisten sähkö- ja automaatiojärjestelmien kelpoistusprosessimalli
Valvoja: Professori Kimmo Kauhaniemi
Ohjaaja: Diplomi-insinööri Matti Vaaheranta
Tarkastaja: Professori Timo Vekara
Tutkinto: Diplomi-insinööri
Oppiaine: Sähkötekniikka
Opintojen aloitusvuosi: 2009
Diplomityön valmistumisvuosi: 2014 **Sivumäärä:** 91

TIIVISTELMÄ

Teollisuuden voima Oyj:lle (TVO) turvallisuuskriittisen ajattelun noudattaminen niin ydinvoimakäytössä kuin järjestelmien kunnossapidossa on tärkeä Voimalaitoksen toiminnan turvallisuus taataan jo suunnitteluvaiheessa noudattamalla säädettyjä lakeja sekä viranomaisten laatimia määräyksiä ja ohjeita, joita noudatetaan myös ydin-voimalan käytössä. Ydinvoimalan järjestelmien ja laitteiden turvallisuus, luotettavuus ja sopivuus tarkoitettuun tehtävään todetaan kelpoistuksen avulla.

Diplomityössä perehdyttiin kelpoistusprosessin etenemiseen sekä standardeihin ja Säteilyturvakeskuksen laatimiin uusiin YVL (ydinvoimalaitos) -ohjeisiin, joita kelpoistuksessa tulee noudattaa. Tavoitteena oli luoda TVO:n käyttöön ohjelmistopohjaisille sähkö- ja automaatiojärjestelmille tarkoitettu kelpostusprosessimalli, jota pystyttäisiin hyödyntämään myös muissa sovelluksissa tapauskohtaiset muutokset huomioiden. Kelpoistusprosessimalli luotiin helpottamaan kelpoistuksen etenemisen seurantaa sekä selkeyttämään kelpoistuksen eri vaiheissa toteuttettavien tehtävien roolijakoa.

Kelpoistusprosessimallin toimivuutta testattiin kolmella case-tyyppisellä testillä, joiden avulla prosessimallin toimivuus laitteelle, ohjelmapohjaiselle laitteelle sekä järjestelmälle saatiin selvitettyä. Tarkastelukohteina olivat suojarele, ultraäänivirtausmittari ja päähöyryputken säteilynmittausjärjestelmä. Tarkasteluista saatujen tulosten perusteella voidaan todeta kelpoistusprosessimallin täyttävän tehtävänsä. Joitakin muutoksia prosessimalliin kuitenkin oli tehtävä, jotta se soveltuisi paremmin esimerkiksi yksittäisille laitteille. Kehitetty kelpoistusprosessimalli noudattaa YVL E.7 -ohjetta ollen linjassa muiden TVO:n prosessimallien kanssa.

AVAINSANAT: Kelpoistusprosessimalli, ohjelmistopohjainen järjestelmä, ydinturvallisuus

UNIVERSITY OF VAASA
Faculty of technology
Author: Hanna-Kaisa Kemppainen
Topic of the Thesis: Qualification Process Model for Programmable Electrical and Automation systems of Nuclear Power Plant
Supervisor: Professor Kimmo Kauhaniemi
Instructor: M. Sc. Tech. Matti Vaaheranta
Evaluator: Professor Timo Vekara
Degree: Master of Science in Elctrical Egineering
Major of Subject: Electrical Engineering
Year of Entering the University: 2009
Year of Completing the Thesis: 2014 **Pages:** 91

ABSTRACT

Following safety critical thinking in the nuclear power plant's use and in the maintenance of its systems is important for Teollisuuden Voima Oyj (TVO). The safety of the nuclear power plant is guaranteed already in the design stage by following the relevant laws, specifications and rules composed by authorities. These are also followed in the use of the nuclear power plant. The safety, reliability and suitability of a nuclear power plant's system for its intended purpose and its conformance to the aforementioned rules are proved by qualification.

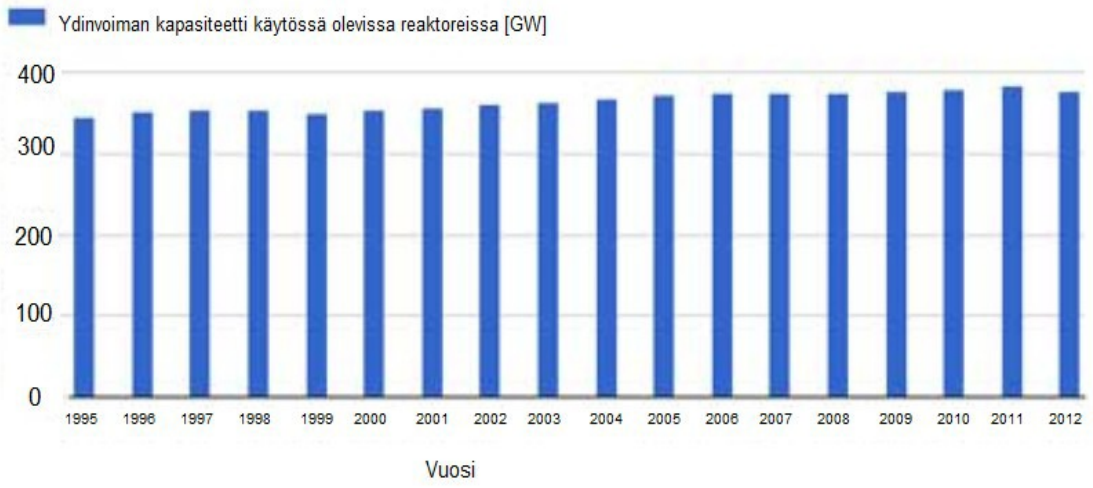
This thesis explored how the qualification process proceeds and the standards that have to be obeyed. It also investigated the new YVL-guidelines composed by Finnish Radiation and Nuclear Safety Authority, and how they have to be applied to the qualification process. The goal was to provide TVO with a qualification process model for programmable electrical and automation systems, which could be also used in other applications by taking their differences into account on a case-by-case basis. The qualification process model was created for ease of monitoring a system's advancement in the qualification process and to clarify the division of labour in the different stages of the qualification process.

The qualification process was tested using three case-type tests, which demonstrated the suitability of process for qualifying programmable and non-programmable devices as well as larger systems. Among the test targets were a relay, an ultrasound flow meter and a radiation measurement system of main steampipe. According to results of the test, the qualification process model works as it should. However, some changes had to be done so it would be more suitable to, for example, the individual devices. The qualification process model follows YVL E.7 -reference and is also in line with other TVO's process models.

KEYWORDS: Qualification process model, programmable system, nuclear safety

1 JOHDANTO

Ydinvoimaa alettiin käyttää sähköntuotantoon 1950-luvulla. Maailman ydinvoimaloiden kapasiteetti kasvoi noin 1 GW:stä yli 100 GW:hen tultaessa 1970-luvulle. Kapasiteetin kasvuun ovat vaikuttaneet sähkönkäytön lisääntyminen sekä 1970-luvulla tapahtunut öljykriisi, jolloin ydinvoimaa lisäämällä pyrittiin öljyriippumattomuuteen. Tultaessa vuoteen 2011 maailmalla oli käytössä 436 ydinreaktoria, joiden yhteinen kapasiteetti oli 370 GW. Kuvassa 1 voidaan nähdä ydinvoimaloiden yhteisen kapasiteetin kehitys vuosilta 1995–2012. European Nuclear Societyn (2014) mukaan ydinvoimaloiden yhteinen kapasiteetti on kasvanut vuoteen 2014 mennessä 372 GW:iin. Tästä kapasiteetista Suomen voimalaitokset tuottivat noin 2,8 GW, josta Olkiluodon kummankin käyvän voimalaitoksen nettoteho on 880 MW ja Loviisan voimalaitosten nettoteho puolestaan 496 MW. (Kessler 2012: 1−2; Vattenfall 2014; TVO 2014e; European Nuclear Society 2014; Henriksson 2012.)



Kuva 1. Maailman ydinvoimaloiden yhteisen kapasiteetin kehittyminen vuosina 1995–2012. (Muokattu lähteestä European Nuclear Society 2014.)

Ydinvoiman historiaan kuuluu myös kolme suurta ydinvoimalaonnettomuutta (*Three Mile Island, Tšernobil* ja *Fukushima*), joista on otettu oppia ydinturvallisuuteen. Viranomaiset ovat uudistaneet ohjeitaan ja määräyksiään muun muassa näiden onnettomuuk-

sien myötä, jotta ydinvoimaloiden turvallisuus pystyttäisiin takaamaan paremmin eikä vastaavia onnettomuuksia tapahtuisi enää. (Vattenfall 2014.)

Jotta ydinvoimalan toiminta olisi turvallista ja luotettavaa, tulee järjestelmien ja sen laitteiden ja ohjelmistojen luotettava ja turvallinen toiminta pystyä takaamaan. Turvallisen toiminnan osoittamisessa käytetään kelpoistusta, jonka tarkoituksena on osoittaa tuotteen täyttävän sille asetetut vaatimukset. (Wang, Azarian & Pecht 2008.) Tässä työssä keskitytään kelpoistamiseen ja kelpoistusprosessimallin kehittämiseen. Kehitettävän kelpoistusprosessimallin testaukseen käytetään ohjelmistopohjaista ultraäänivirtausmittaria, suojarelettä sekä päähöyryputken säteilymittausjärjestelmää. Näiden avulla pyritään tarkastelemaan prosessimallin toimivuutta ja soveltuvuutta erilaisille ohjelmistopohjaisille tuotteille

1.1 Työn tausta

Tämä diplomityö on tehty Teollisuuden Voima Oyj:lle (TVO), jolle ydinvoimalaitosten turvallisen ja luotettavan toiminnan varmistaminen on yhtiön toiminnan pääkriteeri. Ydinvoimalan turvallisuutta on ylläpidettävä sekä kehitettävä jatkuvasti, jotta voimalan järjestelmät laitteineen ja ohjelmistoineen pysyisivät ajan tasalla. Kehityksessä on huomioitava aikaisemmat käyttökokemukset, tekniikan kehittyminen ja turvallisuustutkimustulokset sekä lainsäädännöt ja viranomaisen ohjeet. (Työ- ja elinkeinoministeriö 2010: 9–13; TVO 2014 f.)

Viime vuosikymmenten aikana sähkö- ja automaatiotekniikka ovat kehittyneet ja automaatiolaitteissa nojataan enemmän ohjelmoitavaan elektroniikkaan. Lisäksi ohjelmistotuotteet ja -tekniikka ovat kehittyneet muun tekniikan rinnalla ja tarjoavat uusia mahdollisuuksia. Tekniikan kehittymisen myötä ydinvoimaloiden vanhalla tekniikalla toimivat järjestelmät ja niiden laitteistot ovat haastavia ylläpitää, koska varaosien saatavuus ja tekninen tuki ovat heikentyneet. Tämän takia ydinvoimalan järjestelmiä ja laitteistoja on jouduttu uusimaan ikääntymisen lisäksi. Osa uusista järjestelmistä ja laitteista on ohjelmistopohjaisia, joissa toiminnot toteutetaan ajamalla suorittimella ohjelmakoodi. Osa

ohjelmistopohjaisista järjestelmistä ja laitteista ei kuitenkaan ole uudelleen ohjelmoitavissa valmistuksen jälkeen. (YVL E.7 2013: 28; Halminen 2001: 8.)

Uudet turvallisuusluokkien 2 ja 3 järjestelmät ja laitteet on todettava luotettaviksi ja soveltuviksi niille suunniteltuun käyttöympäristöön, mikä toteutetaan kelpoistamalla. Ohjelmistopohjaisten laitteiden kelpoistaminen on haastavaa, sillä ohjelmiston testaaminen on vaikeaa monien testitapausten ansiosta. Turvallisuuskriittisten järjestelmien ja laitteiden luotettavuus on kuitenkin pystyttävä todistamaan, minkä takia ohjelmistopohjaisten järjestelmien ja laitteiden ohjelmistokehitykseltä vaaditaankin korkealaatuista suunnittelutyötä. Järjestelmien kelpoistamisen onnistumisen takaamiseksi on noudatettava paitsi viranomaisen määräyksiä myös soveltuvia standardeja, joiden avulla suunnittelutyö ja tuotteen kelpoistus toteuttavat kaikki vaaditut vaatimukset. (VTT 2003: 12; Kasurinen 2013: 10–13; Halminen 2001: 8.)

1.2 Teollisuuden Voima Oyj

Teollisuuden Voima Oyj (TVO) on vuonna 1969 perustettu listaamaton julkinen osakeyhtiö, jota perustamassa oli 16 suomalaista teollisuus- ja ydinvoimalaitosyhtiötä. Tällä hetkellä TVO:n omistajuus jakautuu kuuden yhtiön kesken, jotka ovat Pohjolan Voima Oy, Fortum Power and Heat Oy, Oy Mankala Ab, EPV Energia Oy, Kemira Oyj sekä Karhu Voima Oy. Näistä TVO:n suurin omistaja on Pohjolan Voima, jonka konserniin kuuluvat myös TVO:n tytäryhtiöt TVO Nuclear Services Oy (TVONS), Olkiluodon Vesi ja Perusvoima sekä yhteistyöyritys Posiva Oy. Posiva Oy rakentaa muun muassa Fortumin ja TVO:n ydinvoimaloiden ydinjätteiden loppusijoitusonkaloa. (Yli-Nikkilä 2012: 9; Posiva 2014; TVONS 2014; TVO 2014d.)

TVO:n tarkoituksena on tuottaa omistajilleen sähköä omakustannushintaan. Sähköä yhtiö tuottaa kahdella omistamallaan ydinvoimalaitoksella, Olkiluoto 1 (OL1) ja Olkiluoto 2 (OL2), jotka sijaitsevat Olkiluodon voimalaitosalueella. Voimalaitosyksiköiden kaupallinen käyttö aloitettiin vuosina 1979 (OL1) ja 1982 (OL2). OL1 ja OL2 ovat molemmat kiehutusvesireaktorilaitoksia (*Boiling Water Reactor*, BWR). Näiden rinnalle rakennetaan kolmatta voimalaitosyksikköä, Olkiluoto 3 (OL3), joka on painevesireakto-

rilaitos (*Pressurized Water Reactor*, PWR). Olkiluodon voimalaitosalueen kolmen laitosyksikön lisäksi suunnitteilla on Olkiluoto 4 (OL4). Vuoden 2010 heinäkuussa eduskunta vahvisti valtioneuvoksen myönteisen periaatepäätöksen OL4:n rakentamisesta. (TVO 2013a: 5; Yli-Nikkilä 2012: 9.)

1.3 Työn tavoitteet ja rajaus

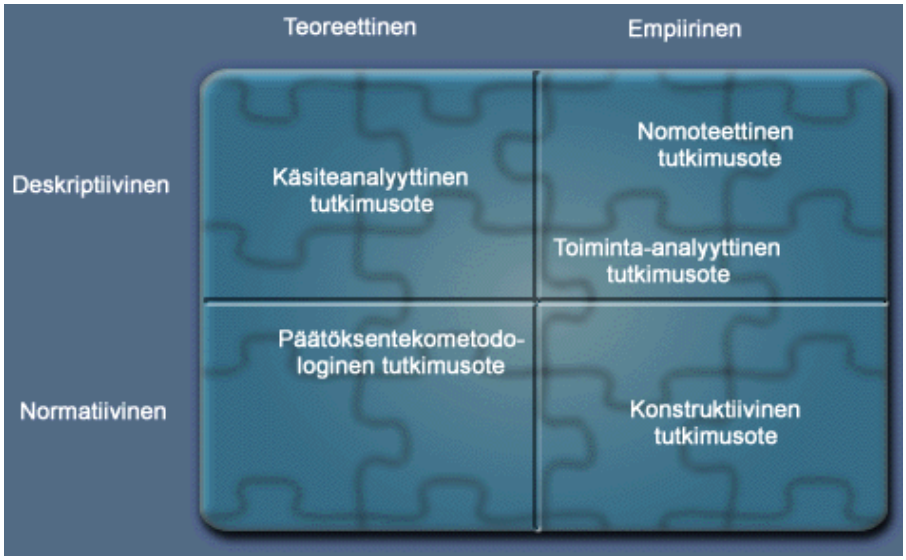
Työn tarkoituksena on kehittää TVO:lle kelpoistusprosessimalli, jota käytettäisiin osoitettaessa ohjelmistopohjaisen järjestelmän ja sen laitteiston sekä ohjelmiston luotettavuus ja toimivuus tarkoitetussa käyttöympäristössä. Kelpoisusprosessimallia tulisi voida soveltaa tarvittaessa myös ei-ohjelmistopohjaisille sähkö- ja automaatiolaitteille ja -järjestelmille tapauskohtaiset muutokset huomioiden, esimerkiksi vaativuusaste. Työssä selvitetään kelpoistuksen kannalta tärkeät standardit ja noudatettavat YVL-ohjeet, joita on noudatettava laitoksella käyttöönotettavien järjestelmien ja sen laitteiden kelpoistuk-sessa. Erityisesti tutkittavana ovat ohjeet ja vaatimukset, jotka vaikuttavat vaatimusmäärittelyyn, kelpoistusprosessin etenemiseen ja itse kelpoistukseen.

Kelpoistusprosessimallin tehtävänä on helpottaa kelpoistusprosessin toteuttamista ja auttaa vaiheiden ja etenemisen seurannassa. Lisäksi kelpoistusprosessimallin avulla selvennetään roolien jakoa TVO:n, viranomaisen ja toimittajan välillä sekä TVO:n sisäisessä suunnittelussa. Prosessimallin tehtävä on auttaa alusta alkaen hahmottamaan, mitä dokumentteja tulee laatia ja lähettää viranomaiselle.

Tässä työssä keskitytään turvallisuuskriittisiin ohjelmistopohjaisiin sähkö- ja automaatiojärjestelmiin. Lisäksi kelpoistusprosessimallissa pääpaino on TVO:n tehtävissä ja suunnittelussa eikä niinkään esimerkiksi toimittajan suunnittelutyössä, vaikka mallin avulla pyritään varmistamaan myös toimittajan työnlaadun olevan halutulla tasolla.

1.4 Tutkimusmenetelmä

Tutkimusmenetelmiä ja erilaisia lähestymistapoja on useita ja ne soveltuvat erilaisille tutkimuskohteille. Esimerkiksi metodologisia tutkimusotteita ovat kuvassa 2 esitetyt tutkimusotteet, joista tässä diplomityössä sovelletaan konstruktiivista tutkimusotetta. Alun perin konstruktiivinen tutkimus kehitettiin liiketalouden alalle, mutta sitä on alettu soveltaa yhä enemmän myös teknisillä aloilla, lääketieteessä sekä matematiikassa laajan potentiaalinsa takia. Se on innovatiivista, kokeellista ja soveltavaa tutkimusta, jossa hyödynnetään aikaisempaa teoreettista tietämystä tutkittavasta ongelmasta. Ratkaisu ongelmaan pyritään löytämään kehitettävän konstruktion avulla. Konstruktio voi olla esimerkiksi malli, kaavio tai suunnitelma. Sen tärkein tavoite on toimivuus. (Rohweder & Virtanen 2008: 11; Eskelinen 2010: 17; Aho 2006: 5−6; Lukka 2001; Lauronen 2003: 3.)



Kuva 2. Metodologisen tutkimuksen eri tutkimusotteet. (Lukka 2001.)

Konstruktiivisessa tutkimuksessa on hieman päätöksentekometodologisen tutkimuksen piirteitä. Molemmissa muun muassa teoreettinen päättely ja analysointi ovat tärkeässä roolissa konstruktiota kehitettäessä. Erona näillä menetelmillä on, että konstruktiivisessa tutkimuksessa halutaan testata kehitetyn konstruktion käytännön toimivuutta. Lisäksi konstruktiiviseen tutkimusotteeseen sisältyy myös käsiteanalyyttisiä tutkimuksen piirteitä. Käsiteanalyyttinen tutkimus on kuvailevaa ja teoriapainotteista tutkimusta, jossa pyritään määrittämään tutkimuksen keskeinen käsite. Se piirteet näkyvät konstruktiivi-

sessa tutkimuksessa erityisesti tutkimusaiheen ja käsitteiden määrittelyssä. (Aho 2006: 5−6; Alanko 2010: 12; Metsävainio 2013: 19; Lukka 2001; Lauronen 2003: 3; Eskelinen 2010: 17.)

Konstruktiivinen tutkimus on rinnastettavissa tapaustutkimukseen eli case-tutkimukseen yhtenäisten piirteiden ansiosta. Konstruktiivisessa tutkimuksessa muun muassa kehitetyn ratkaisun toimivuus testataan tapaustutkimukselle ominaisesti vain muutamalla tutkimuskohteella. Lisäksi konstruktiivisessa tutkimuksessa käytetään tapaustutkimuksen tavoin havainnointia, haastatteluja ja arkistojen analysointia tiedon keruussa. Lukka (2001) kuitenkin huomauttaa, että konstruktiivisessa tutkimuksessa pyritään tekemään teoreettisia johtopäätöksiä empiiriseen työhön perustuen. Tutkimukselle ominaista onkin selvittää, miten ennalta tiedetty päämäärä voitaisiin saavuttaa. Lisäksi konstruktiiviselle tutkimukselle keskeiset elementit ovat kuvan 2 mukaisesti tosielämän ongelmaan keskittyminen, teorian kytkeminen osaksi kehitettävää konstruktiota, konstruktion testaaminen käytännössä sekä tutkimuksesta saadun teoreettisen kontribuution kytkeminen osaksi teoriaa. (Aho 2006: 5−6; Lukka 2001; Lauronen 2003: 3)

Kuva 3. Konstruktiivisen tutkimusotteen ydinpiirteet. (Lukka 2001.)

Aineisto kelpoistusprosessimallin kehittämiseen kerätään aikaisempien kokemuksien, aihetta koskevan teorian, standardien ja uusien YVL-ohjeiden avulla. Tällä tavoin pyritään määrittämään keskeisin käsite, kelpoistus, sekä ymmärtämään tutkimuskohdetta. Lisäksi huolella kootun teorian avulla varmistetaan kehitettävän prosessimallin lopputuloksen laadullisuus ja toimivuus. Näiden lisäksi konstruktioon vaikuttavat myös idea valmiista kelpoistusprosessimallista sekä sille esitetyt vaatimukset ja tavoitteet. Kehite-

tyn kelpoistusprosessimallin toimivuutta käytännössä arvioidaan valittujen, kolmen tapauskohtaisen tarkastelun avulla sekä analysoimalla saatuja tuloksia. Tarkastelujen yhteydessä toteutetaan myös haastattelu, jossa pyritään selvittämään tarkasteluun osallistuneen henkilön mielipide mallin toimivuudesta ja kehittämistarpeista. Toimivan ja onnistuneen konstruktion piirteitä ovat helppokäyttöisyys, yksinkertaisuus sekä asianmukaisuus (Blinnikka 2002: 5). Tältä työltä ei odoteta teoreettista kontribuutiota olemassa olevaan teoriaan.

1.5 Työn rakenne

Työssä perehdytään aluksi lyhyesti Olkiluodon ydinvoimalayksiköiden toimintaan ja hieman tarkemmin voimalaitosten turvallisuuden varmistamiseen muun muassa riskianalyysien ja turvallisuussuunnittelun avulla. Tavoitteena on antaa yleiskäsitys ydinvoimalaitoksen toiminnasta, toiminnan turvallisuuden varmistamisesta ja siihen liittyvistä, noudatettavista turvallisuus- ja vaatimusmääräyksistä, jotka tulee huomioida niin kelpoistusprosessissa kuin voimalaitoksen toiminnassa.

Tämän jälkeen selvitetään kelpoistukseen kuuluvat elementit kuten kelpoistusmenetelmät sekä vaatimusmäärittelyt, jotka on huomioitava kelpoistusprosessissa. Tarkoituksena on antaa yleinen kuva siitä, mitä kaikkea tulee huomioida kelpoistusprosessissa, ja miten moniulotteinen prosessi on. Työssä pyritään myös selventämään, mikä rooli itse kelpoistuksella on koko prosessissa.

Mallin testaamisesta kerrotaan kolmen esimerkkitapausten avulla. Tarkasteluihin on valittu suojarele, ultraäänivirtausmittari ja päähöyryputken säteilynmittausjärjestelmä. Näiden avulla pyritään selvittämään, miten hyvin luotu kelpoistusprosessimalli soveltuu tehtäväänsä kussakin tarkastelutapauksessa. Saatujen tulosten perusteella voidaan pohtia, miten prosessimallia voisi kehittää tulevaisuudessa. Ennen tarkasteluja esitellään kelpoistusprosessimalli ja kerrotaan sen kehittämisestä ja kehityksen aikana ilmenneistä haasteista. Lopuksi nivotaan koko työ yhteen sekä kerrotaan näkemyksiä ja parannusehdotuksia tulevaisuutta varten.

2 YDINVOIMALAT JA TURVALLISUUS

Maailmalla kaupalliseen käyttöön suunniteltuja ja rakennettuja voimalaitosreaktoreita on seitsemää eri tyyppiä, jotka voidaan luokitella muun muassa hidastimen, polttoaineen tai jäähdytteen mukaan. Yleisimpiä reaktorityyppejä ovat painevesireaktori ja kiehutusvesireaktori, joista käytetään yhteistä nimitystä kevytvesireaktori (*Light Water Reactor,* LWR). Muita käytössä olevia reaktoreita ovat muun muassa raskasvesijäähdytteinen reaktori (*Heavy Water Reactor*, HWR), kaasujäähdytteinen grafiittimoderoitu reaktori (*Advanced Gas-Cooled Reactor*, AGR), kaasujäähdytteinen reaktori (*Gas Cooled Reactor*, GCR), hyötyreaktori(*Fast Breeder Reactor*, FBR) sekä Neuvostoliitossa kehitetty grafiittimoderoitu paineputkireaktori (*Reaktor Bolshoy Moshchnosti Kanalnyy,* RBMK) (Kessler 2012: 73−108; TVO 2014c; World Nuclear Association 2010: STUK 2013e.)

Reaktorien tehtävänä on tuottaa lämpöä polttoaineesta. Lämpö saadaan reaktoreissa tapahtuvalla fissioreaktiolla, jota ylläpidetään ja säädetään. Vikatilanteissa reaktiota pyritään hidastamaan tai pysäyttämään. Vaikka fissioreaktio saadaan pysäytettyä, reaktoria joudutaan jäähdyttämään noin vuoden ajan, sillä polttoainesauvoissa tapahtuvasta korkea-aktiivisesta halkeamisesta syntyvä lämpöenergia kykenee sulattamaan reaktoriytimen. (Honkanen 2013; Kessler 2012: 4−6.) Vikatilanteiden varalle ydinvoimalat on varustettu moninkertaisilla turvallisuustoiminnoilla ja turvallisuuslaitteilla, joiden avulla voimalaitosten ydinturvallisuus pystytään takaamaan.

Tässä luvussa perehdytään kevytvesireaktorivoimalaitosten toimintaperiaatteeseen lyhyesti sekä käydään läpi ydinturvallisuuteen liittyviä tekijöitä, joiden avulla varmistetaan ydinvoimaloiden turvallinen ja luotettava toiminta. Lisäksi osiossa keskitytään ohjelmistopohjaiseen tekniikkaan, jonka käyttöön ydinvoimaloissa siirrytään vähitellen.

2.1 Ydinvoimalan toimintaperiaate

Suomen ydinvoimaloiden reaktorit ovat kevytvesireaktoreita, joissa veden tehtävänä on toimia hidasteena ja jäähdyttimenä. Kevytvesireaktoreiden toimintaperiaate vastaa tavanomaisen höyryvoimalaitoksen toimintaa, jossa vesihöyryn avulla pyöritetään turbii-

nia. Se puolestaan pyörittää samalla akselilla olevaa sähkögeneraattoria, jonka tehtävänä on muuttaa turbiinista saatavan liike-energia sähköenergiaksi. Voimalaitoksien erona on veden höyrystymiseen tarvittavan lämpöenergian syntyminen. Höyryvoimaloissa lämpöenergia saadaan polttoaineen, kuten öljyn tai hiilen polttamisella. Ydinvoimaloissa lämpöenergia syntyy fissio- eli halkeamisreaktiosta ja kontrolloidulla fissioiden ketjureaktiolla. Fissioreaktiossa polttoaineena käytettävää uraania pommitetaan neutroneilla, jotka osuessaan uraaniytimeen halkaisevat sen kahdeksi pienemmäksi atomiytimeksi. Näitä kutsutaan fissiotuotteiksi. Reaktiosta vapautuu lämpöenergian ja fissiotuotteiden lisäksi lisää neutroneja, jotka kykenevät halkaisemaan uusia uraaniytimiä. (Eurasto, Hyvärinen, Järvinen, Standberg & Sjöblom 2004: 26−28; Korpelainen 2000; Korpelainen 2008; TVO 2013a: 7; TVO 2009: 10.)

Kevytvesireaktoreiden erot ovat rakenteellisia. Painevesireaktorilla on primääripiiri ja sekundäärispiiri, kun taas kiehutusvesireaktorilla on ainoastaan primääripiiri. Lisäksi painevesireaktorissa on höyrystin, joka puuttuu kiehutusvesireaktorista, sillä vesi höyrystyy jo kiehutusvesireaktorin reaktorissa. Painevesireaktorin etu kiehutusvesireaktoriin on sen helpompi ohjattavuus jäähdytteeseen liuotettavalla boorihapolla sekä reaktorin yläosasta säätösauvoilla, koska kaikki vesi on reaktorin primääripiirissä nesteenä korkean paineen ansiosta. Höyrystimessä paineistettu vesi siirtyy sekundääripiiriin, jossa vesi höyrystyy matalamman paineen ansiosta. Höyrystimen ansiosta painevesireaktorissa tapahtuu lämpöhäviöitä jonkin verran enemmän kuin kiehutusvesireaktorissa ennen höyryn kulkeutumista turbiiniin. (Eurasto yms. 2004: 48−49; Kessler 2012: 75−100; STUK 2013e.)

2.2 Ydinturvallisuus

Ydinturvallisuuden katsotaan maailmanlaajuisesti olevan päävaatimus rauhanomaisen ydinenergian käyttöön. Ydinturvallisuus ja sen suunnittelu perustuvat lainsäädäntöjen (ydinenergialaki), säädösten ja ohjeiden noudattamiseen. Esimerkiksi Suomen ydinenergialaissa (990/1987) 6§:ssa on määritelty, ettei ydinvoimalan käytöstä saa aiheutua minkäänlaisia vahinkoja ihmisille, ympäristölle tai omaisuudelle (Finlex 2014). Asetet-

tuja säädöksiä ja ohjeita ylläpitävät paikalliset ja kansainväliset viranomaiset, jotka myös valvovat, että ohjeet ja kansalliset säädökset ovat päivitetty ydinvoimaloissa ja niitä noudatetaan kaikessa toiminnassa. (Koutaniemi, Reponen, Salminen, Sandberg & Varjoranta 2004: 356–359; Hölttä 2012: 14−15.)

Suomessa ydinvoimatoimintaa ja säteilyturvallisuutta valvova viranomainen on Säteilyturvakeskus (STUK). Kansainvälisellä tasolla rauhanomaisen ydinenergian käyttöä edistämässä on Kansainvälinen atomienergiajärjestö (*International Atomic Energy Agency*, IAEA) ja kansainvälisellä tasolla yleistä säteilyturvallisuutta edistämässä on Kansainvälinen säteilysuojakeskus (*International Commission on Radiological Protection*, ICRP). Virastot harjoittavat yhteistyötä keskenään ja yhdessä ydinvoimaloiden kanssa. (Paile 2002: 152; Hölttä 2012: 14−15; IAEA 2014; ICRP 2014.)

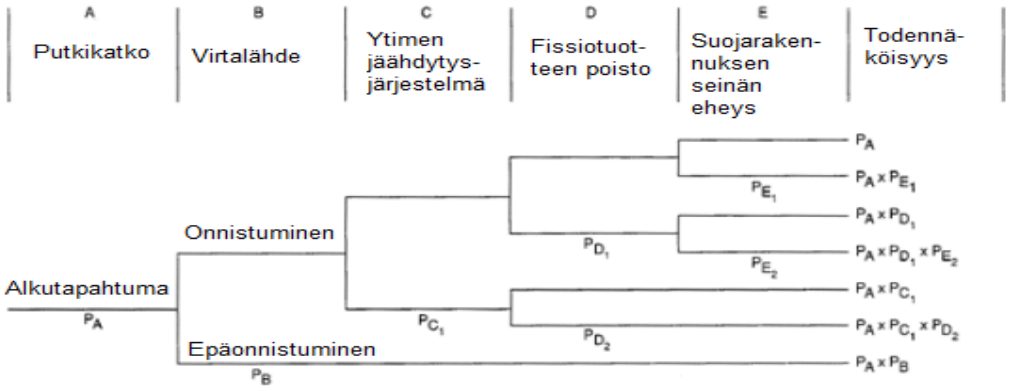
Teollisuuden Voima Oyj noudattaa toiminnassaan viranomaisten määräyksiä ja turvallisuuskriittistä ajattelumallia, jonka tavoitteena on varmistaa ydinvoimaloiden turvallinen ja luotettava toiminta heti suunnittelusta lähtien. Ydinvoimaloissa turvallisuussuunnittelu ja turvallisuustoimintojen suunnittelu lähtee reaktorisydämen suunnittelusta. Häiriötilanteiden varalle ydinvoimala on varustettu moninkertaisilla turvallisuusjärjestelmillä ja -laitteilla, joiden tehtävänä on ehkäistä häiriö- ja onnettomuustilanteiden syntyminen ja lieventää mahdollisesta onnettomuudesta syntyviä seurauksia. Lisäksi vikoja pyritään ennaltaehkäisemään turvajärjestelmien ja suunnittelun lisäksi laitteiston huollolla, testauksilla, koulutetun henkilökunnan ja toimintaohjeiden avulla. Erityisesti vakavat onnettomuudet, kuten jäähdytteenmenetysonnettomuus (*Loss of Coolant Accident*, LOCA), huomioidaan aina ydinvoimalan suunnittelussa. (Isolankila, Järvinen, Keskinen, Niemelä, Ojanen, Rantala, Sandberg, Tiippana, Valtonen, Virolainen & Åstrand. 2004: 91−92; TVO 2013a: 51; Koskiniemi 2005: 3.)

2.2.1 Riski- ja turvallisuusanalyysi

Riskianalyysien avulla tuodaan esille ne asiat, jotka vaikuttavat negatiivisesti aiottuun toimintaan ja sen onnistumiseen. Riski- ja turvallisuusanalyysit ovatkin tärkeä osa ydinvoimalan turvallisuussuunnittelua ja turvallista toimintaa. Ydinvoiman turvallisuussuunnittelussa noudatetaan todennäköisyyspohjaista riskianalyysia (*Probabilistic*

Risk/Safety Assessment, PRA/PSA) ja determinististä turvallisuusanalyysia yhdessä käytettynä. (Sistonen 2012: 19; Hölttä 2012: 17; YVL A.7: 4.)

PRA-analyysi on alun perin kehitetty ydinvoimalan turvallisuussuunnitteluun, mutta myöhemmin sitä on alettu soveltaa laajemmin myös muilla tekniikan alueilla, kuten ohjelmistojen kehityksessä. Myös NASA (*National Aeronautics and Space Administration*) käyttää PRA-analyysiä riskienhallinnassaan. PRA-analyysin avulla voidaan tarkastella laajoja teknisiä järjestelmiä ja keskittyä tutkimaan tärkeimpien turvallisuuslaitteiden, järjestelmien sekä toimintojen luotettavuutta. PRA-analyysin mallit perustuvat useimmiten joko vikapuu- tai tapahtumapuumenetelmään, josta on esitettynä esimerkki kuvassa 4. Lisäksi PRA-analyysissä arvioidaan onnettomuuksien esiintymistodennäköisyyttä ja -taajuutta. PRA-analyysissä tavoitteena on tunnistaa erilaisten teknisten järjestelmien häiriöistä aiheutuvat onnettomuudet. (Isolankila ym. 2004: 126−135; Heikkilä 2007: 14−16; YVL A.7: 8; Apthorpe 2001; NEA 2002; NASA 2014.)



Kuva 4. Esimerkki PRA-analyysin tapahtumapuusta. (NEA 2002.)

Deterministinen turvallisuusanalyysi täydentää PRA-analyysiä. Deterministisessä turvallisuusanalyysissa kyse on häiriöiden ja onnettomuuksien analysoinnista, jossa tietyt viat, kuten LOCA, oletetaan tapahtuvaksi huolimatta vikojen todennäköisyydestä. Analyysillä osoitetaan, että vikojen varalle suunnitellut turvallisuustoiminnot täyttävät niille osoitetut tehtävät ja vaatimukset. Hyvä esimerkki deterministisen analyysin käytöstä on turvallisuusjärjestelmien suunnittelu, jossa käytetään erilaisia deterministisen analyysin

menetelmiä. Näitä ovat moninkertaisuusperiaate, erilaisuusperiaate ja erotteluperiaate. (Isolankila ym. 2004: 96−97, 126; Heikkilä 2007: 16; NEA 2002.)

2.2.2 Turvallisuussuunnittelu

Turvallisuussuunnittelu perustuu vikatilanteisiin ja onnettomuustilanteisiin varautumiseen. Turvallisuussuunnittelussa pyritään varmistaman ydinvoimalan turvallinen, luotettava ja häiriötön toiminta erilaisten ja monikertaisten turvallisuusjärjestelmien ja toimintojen avulla. Lisäksi turvallisuussuunnittelun tähdätään voimalaitoksen vikasievoisuuteen, eli turvallisuustoimintojen toimivuuteen niille asetettujen vaatimusten mukaisesti tilanteesta riippumatta. Toiminnon on saatettava voimala hallittuun tilaan ja pidettävä laitos tuossa tilassa, vaikka järjestelmässä ilmenisi vika. (Hölttä 2012: 15−16; Isolankila ym. 2004: 95−96.)

Turvallisuussuunnittelu pohjautuu vikojen ja häiriöiden ennakoimisen lisäksi viranomaisten säätämien lakien ja ohjeiden noudattamiseen. Näitä ohjeita päivitetään maailmalta saatavan ydinturvallisuuteen ja ydinvoimalan käyttöön liittyvän uuden tiedon myötä. Myös onnettomuusraportit ovat tärkeitä tietolähteitä turvallisuussuunnittelulle. Erityisesti kolme suurinta ydinvoimalaonnettomuutta, *Three Mile Island* vuonna 1979, *Tšernobil* vuonna 1986 ja *Fukushima* vuonna 2011, ovat opettaneet ja antaneet paljon tietoa, jotta vastaavat onnettomuudet voitaisiin välttää tulevaisuudessa. Myös muut tapahtumat maailmalla, kuten *World Trade Center* (WTC) -isku vuonna 2001 on vaikuttanut ydinvoimalan turvallisuuden ja turvallisuussuunnittelun ohjeisiin. Esimerkiksi OL3-voimalaitoksen kaksiseinäisen suojarakennuksen teräsbetoninen ulkorakenne on suunniteltu kestämään matkustajalentokoneiden törmäyksen ja sisäinen seinä on varustettu teräsvuorauksella. Suojarakennus on esitettynä kuvassa 6 b), jossa esitellään OL3:n vapautumisesteet. (Hölttä 2012: 15–16; Karjunen, Suksi & Tossavainen 2004: 219−220; Isolankila ym. 2004: 97; TVO 2009: 21.)

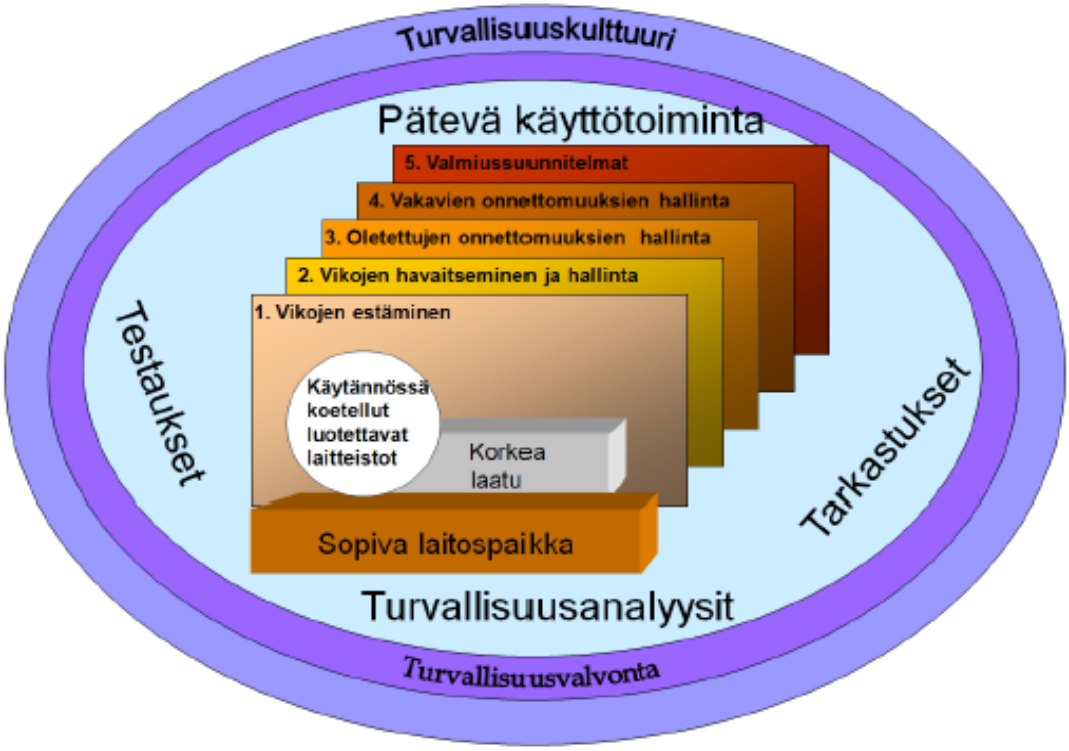
Myös uusituissa YVL-ohjeissa esitetään muutamia pääperiaatteita, joita edellytetään turvallisuussuunnittelusäädöksiltä. Näitä ovat syvyyssuuntainen turvallisuusperiaate tai syvyyspuolustusperiaate (*Defence-In-Depth*, DID), moninkertaiset vapautumisesteet, erilaisuusperiaate (diversiteetti, *diversity*), rinnakkaisperiaate (redundanssi, *redundancy*)

ja erottelu. Lisäksi turvallisuussuunnittelussa noudatetaan myös SAHARA (*Safety As High As Reasonbly Achievable*) -periaatetta. Periaatteen tavoitteena on saada turvallisuustaso niin korkeaksi kuin käytännössä on mahdollista. (Hölttä 2012: 9, 15−6; Isolankila ym. 2004: 91, 95–106; STUK YVL B.1 2013: 11−14.)

Lueteltujen menetelmien lisäksi turvallisuustavoitteiden täyttyminen edellyttää myös ALARA (*As Low As Reasonably Achievable*) -periaatetta, jota käytetään säteilyaltistusrajoista. Niiden on oltava ydinvoimalaitoksen normaalikäytön aikana niin alhaiset kuin on mahdollista saavuttaa käytännöllisillä toimilla. ALARA-periaatteesta käytetään myös nimitystä optimointiperiaate. (STUK 2007; Isolankila ym. 2004: 91.)

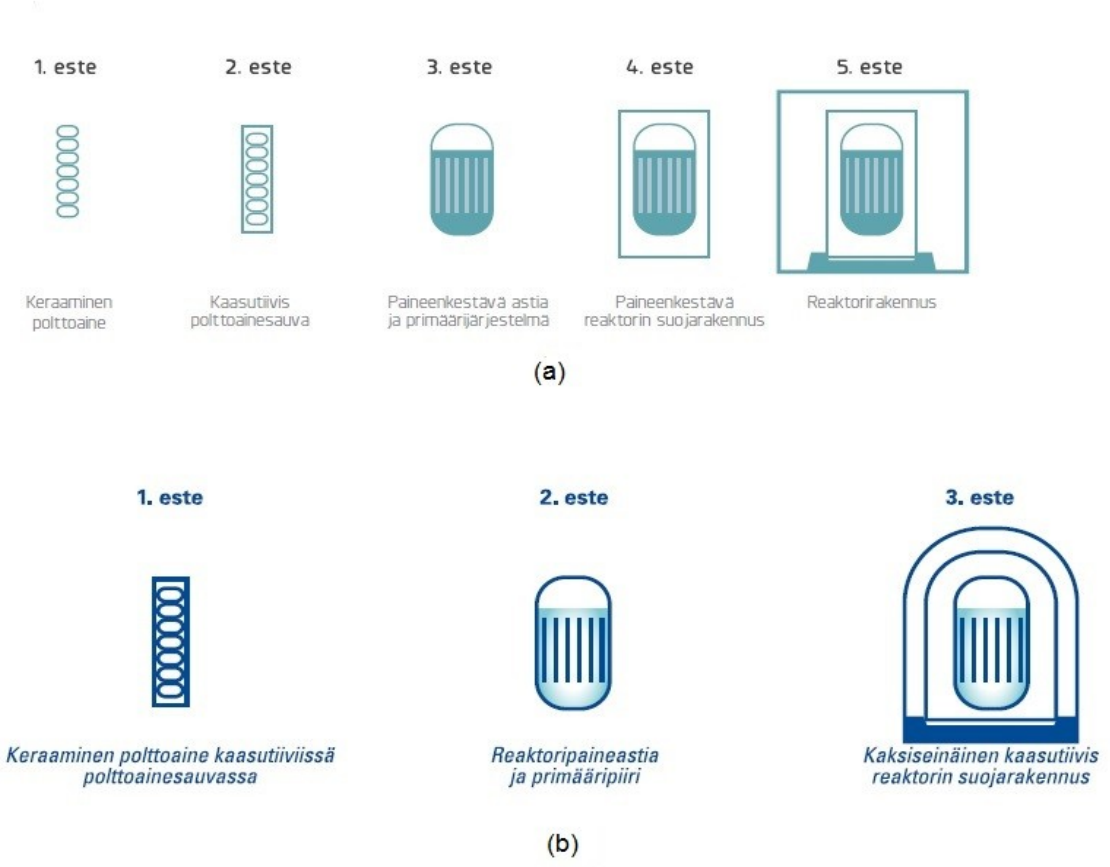
Syvyyssuuntainen puolustusperiaate on ydinvoimaloissa yksi turvallisuuden perusta. Sen puolustustasot on luokiteltavissa viiteen peräkkäiseen, toisiaan tukevaan tasoon kuvan 5 mukaisesti. Puolustustasoista kaksi ensimmäistä ehkäisevät onnettomuuksia ja loppujen tehtävänä on suojata laitosta, sen käyttäjiä sekä ympäristöä onnettomuuksien vaikutuksilta. Lisäksi tasojen on oltava toisistaan mahdollisimman riippumattomia. Tällöin yhden tason menetys ei haittaa muiden puolustustasojen toimintaa. Tasojen riippumattomuus perustuu toiminnalliseen erotteluun erilaisuusperiaatteeseen ja moninkertaisiin vapautumisesteisiin. Erilaisuusperiaatteesta ja toiminnallisesta erottelusta kerrotaan enemmän kappaleessa 2.2.3. (Ahonen 2011: 11; Valtonen 2011; YVL B.1 2013: 11.)

Vapautumisesteiden avulla estetään radioaktiivisten aineiden pääsy ympäristöön. Esteitä ovat polttoaine, primääripiiri ja suojarakennus. Kuvan 6 mukaisesti vapautumisesteet voidaan jakaa vieläkin yksityiskohtaisemmin. Ensimmäisenä vapautumisesteenä on rakenteeltaan keraaminen polttoaine, joka on kaasutiiviissä, metallisessa polttoainesauvassa. Keraamisenpolttoaineen metalliset polttoainesauvat ovat toinen vapautumiseste. Kolmantena esteenä on reaktorin paineastia ja siihen liittyvien putkien sekä venttiilien muodostama tiivis, paineenkestävä jäähdytyspiiri eli primääripiiri. Neljäntenä vapautumisesteenä on reaktoria ympäröivä, paineen kestävä ja kaasutiivis suojarakennus. (Isolankila ym. 2004: 97; TVO 2013a: 52; TVO 2014b.)



Kuva 5. Syvyyssuuntaisen puolustusperiaatteen toimintaperiaate. (Ahonen 2011: 13.)

Uloimpana esteenä on reaktorirakennus, jonka tulee suojata reaktoria ulkoisilta suojatekijöiltä. WTC-iskun jälkeen koettiin tärkeäksi paitsi rakentaa OL3 voimalaitosyksiköstä törmäyskestävä, mutta myös selvittää OL1 ja OL2 voimalaitoksien törmäyskestävyys. Laitosyksiköiden alkuperäisiin vaatimuksiin törmäyskestävyys ei kuulunut, joten selvityksessä on analysoitu teräsbetonirakenteen vahvuutta, joka selvityksessä todettiin kestäväksi. (Isolankila ym. 2004: 97; TVO 2013a: 52; TVO 2014b.)



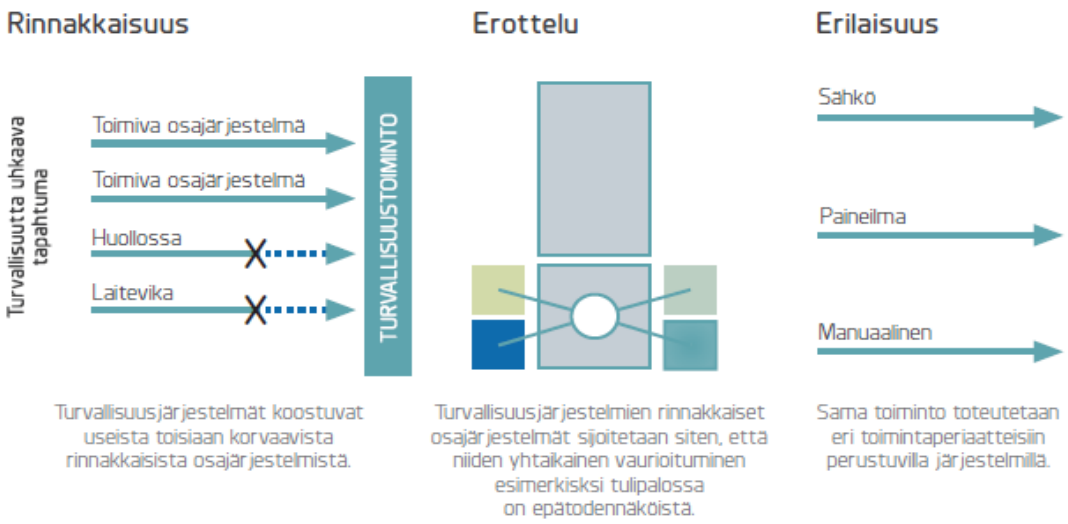
Kuva 6. Moninkertaiset vapautumisesteet Olkiluoto 1 ja Olkiluoto 2 voimalaitosyksiköissä (a) ja Olkiluoto 3 voimalaitosyksikössä (b). (Muokattu alkuperäisistä lähteistä TVO 2013a: 51 ja TVO 2010: 41.)

OL3-laitoksen ensimmäiset vapautumisesteet ovat samat kuin OL1- ja OL2-voimalaitoksilla. Tämän lisäksi OL3-laitoksessa on varauduttu maanjäristyksiin reaktorirakennuksen perustuksena olevalla, kolme metriä paksulla teräsbetonilaatalla. Pohjalaatan päälle on rakennettu kuva 6 b) mukaisesti kaksiseinäinen ja kaasutiivis reaktorin suojarakennus. (TVO 2009: 21; TVO 2010: 41.)

2.2.3 Turvallisuusjärjestelmien suunnittelu

Turvallisuusjärjestelmien suunnittelussa tavoitteena on varmistaa turvallisuuden kannalta tärkeiden toimintojen tapahtuminen luotettavasti, jotta vältyttäisiin vakavilta onnettomuuksilta. Suunnittelussa tulee myös varautua onnettomuuksiin. Tällöin toimintojen,

joiden tehtävä on lieventää onnettomuuden aiheuttamia seurauksia, on toimittava luotettavasti ilman häiriöitä. Turvajärjestelmien suunnittelussa noudatetaan muutamia pääperiaatteita, jotka auttavat pääsemään tavoitteisiin. Käytettyjä periaatteita ovat kappaleessa 2.2.2 mainitut rinnakkaisuusperiaate, erotteluperiaate ja erilaisuusperiaate. Kuvassa 7 selvennetään näiden periaatteiden ajatusta ja toimintaideaa vikatilanteiden varalle.



Kuva 7. Turvallisuusjärjestelmien suunnittelussa käytettyjen periaatteiden toimintaperiaate. (TVO 2013a: 52.)

Erotteluperiaate koostuu fyysisestä ja toiminnallisesta erottelusta. Fyysisellä erottelulla tarkoitetaan turvallisuusjärjestelmien rinnakkaisten ja toisiaan täydentävien osajärjestelmien sijoittamista eri tiloihin. Poikkeustapauksissa erottelu voidaan toteuttaa sijoittamalla osajärjestelmät riittävän kauaksi toisistaan siten, että kutakin osajärjestelmää ympäröi suojarakenne. Toiminnallisessa erottelussa vältetään rinnakkaisten ja toisiinsa liittyvien järjestelmien vuorovaikutus. Esimerkiksi sähkö- ja automaatiojärjestelmät on erotettu toisistaan sähköisesti ja toiminnallisesti. (Koskiniemi 2005: 5; Isolankila ym. 2004: 103−104.)

Rinnakkaisuusperiaatteessa turvallisuusjärjestelmä jaetaan useisiin rinnakkaisiin ja toisiaan korvaaviin osajärjestelmiin. Osajärjestelmät suorittavat samaa toimintoa, joten niiden on kyettävä toteuttamaan turvallisuustoimintonsa riippumatta siitä, onko jokin

yksittäinen laite järjestelmästä vioittunut tai huollon takia poissa käytöstä. Tätä kutsuntaan N+2 -vikakriteeriksi, jonka täyttämiseksi kutakin toimintoa kohden on neljä rinnakkaista laitetta. Näistä jo kaksi riittää varmistamaan turvallisuusjärjestelmän käynnistymisen ja ohjaamisen. Toisin sanoen N+2 -vikakriteeri tarkoittaa, ettei yksi vikasignaali aiheuta välttämättä vikatoimintojen laukaisua. (Hölttä 2012: 16; Koskiniemi 2005: 4; Isolankila ym. 2004: 102.)

Erilaisuus- eli diversiteettiperiaatteella tarkoitetaan saman turvallisuustoiminnon toteuttamista eri toimintaperiaatteisiin ja mekanismeihin perustuvilla järjestelmillä ja laitteilla. Tällä tavoin parannetaan turvallisuustoiminnon luotettavuutta ja vältetään yhteisvihkojen mahdollisuus. Hyvä esimerkki diversiteetistä on reaktorin sammuttaminen säätösauvoilla ja boorihappoliuoksella. Sama turvallisuustehtävä, reaktorin sammuttaminen, pystytään suorittamaan kahdella eri tavalla. (Koskiniemi 2005: 6; Hölttä 2012: 16; Isolankila ym. 2004: 104.)

2.2.4 Turvallisuusjärjestelmät

Ydinvoimaloiden järjestelmät ja laitteet jaetaan turvallisuusluokkiin niiden turvallisuusmerkityksen mukaan. STUK:n laatimassa YVL B.2 -ohjeessa määritellään turvallisuusluokat 1-3 ja EYT (ei ydinteknisesti turvallisuusluokiteltu), joista turvallisuusjärjestelmät voidaan ryhmitellä turvallisuusluokkiin 2, 3 tai EYT. Mitä korkeampi turvallisuusluokka on, sitä tärkeämpi järjestelmä on laitoksen turvallisuuden kannalta. Turvallisuusluokka kertoo, mitkä asetetut vaatimukset ja ominaisuudet järjestelmä tai laite täyttää. Samalla se kertoo myös, kuinka paljon vaaditaan suunnittelulta, valmistukselta ja kunnossapidolta. Esimerkiksi turvallisuusluokan 2 järjestelmät on suunniteltu ehkäisemän vahinkoja onnettomuustilanteissa. Niiden avulla laitos saatetaan hallittuun tilaan ja pidetään siinä kunnes turvalliseen tilaan siirtyminen voidaan varmistaa. (YVL B.2 2013: 3−6; Halminen 2001: 13.)

Ydinvoimaloiden turvallisuusjärjestelmät kuuluvat tärkeytensä vuoksi turvallisuusluokkaan 2 tai 3. Turvallisuusjärjestelmät on Olkiluodon laitosyksiköissä jaettu yksittäisvikaantumisen varalle neljään rinnakkaiseen osajärjestelmään, jotka ovat fyysisesti eri tiloissa. Niiden tärkein tehtävä on ehkäistä häiriö- ja vikatilanteiden syntyminen sekä

varmistaa, etteivät seuraukset pääse leviämään. Prosessinmittausjärjestelmä, reaktorinsuojausjärjestelmä, pikasulkujärjestelmät ja hätäjäähdytysjärjestelmät ovat voimalaitosten keskeisimmät turvallisuusjärjestelmät. Lisäksi OL1:n ja OL2:n reaktoreissa tärkeisiin turvallisuusjärjestelmiin kuuluu myös SAM (*Severe Accident Management*) -suodatin, jonka tehtävänä on alentaa kiehutusvesireaktorissa painetta vakavan onnettomuuden aikana. (Halminen 2001: 18; Koskiniemi 2005: 7; TVO 2013a: 52; TVO 2010: 41; Canadian Nuclear Safety Commission 2006: 1.)

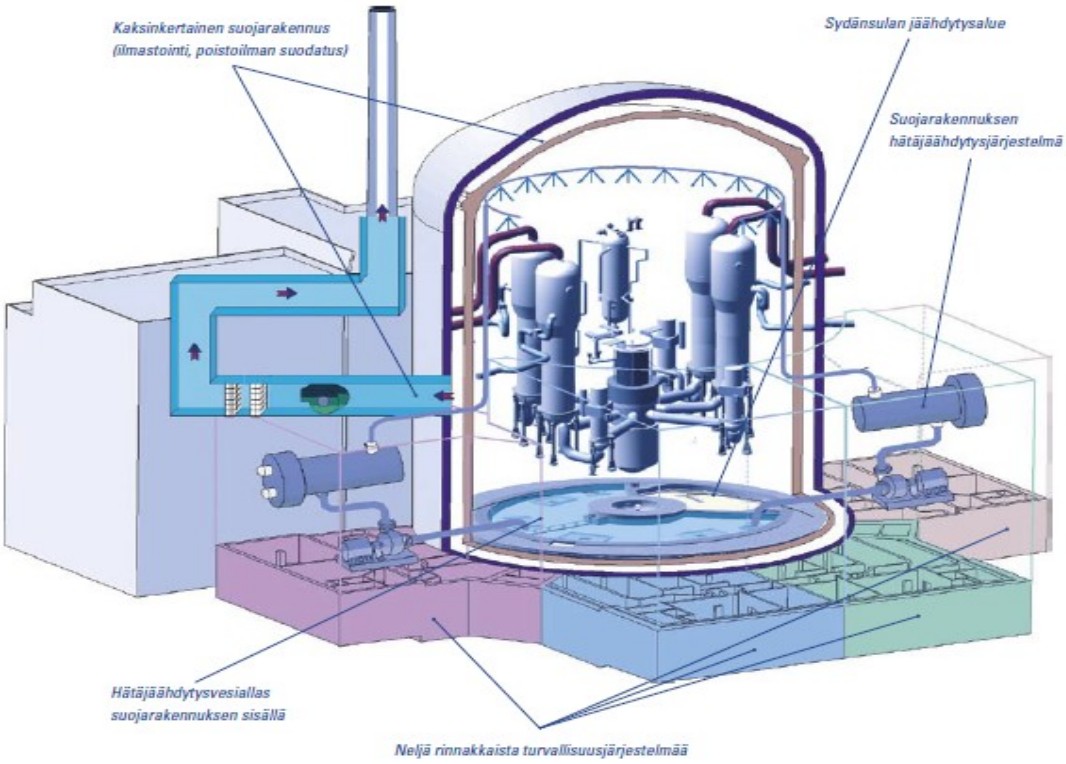
Prosessimittausjärjestelmä mittaa ja valvoo reaktorin toiminnan kannalta tärkeitä suureita, esimerkiksi painetta, virtaamaa, pinnan tasoa ja sähkönjohtavuutta. Järjestelmän turvallisuustehtävänä on toimittaa tarvittavat signaalit hälytysjärjestelmälle ja suojausjärjestelmälle mitattujen arvojen saavuttaessa ennalta määritellyt raja-arvot normaalien käyttöarvojen ulkopuolella. Reaktorinsuojausjärjestelmä puolestaan käynnistää reaktorin turvallisen sammuttamisen ja siihen liittyvät toiminnot, kuten pikasulkujärjestelmät. Lisäksi järjestelmän tehtävänä on estää käyttöhäiriöiden ja mahdollisten onnettomuustilanteiden kehittyminen. (Halminen 2001: 18.)

Ydinvoimalan reaktorin pikasulku voidaan suorittaa kahdella menetelmällä. Ensisijaisesti reaktori pyritään sammuttamaan säätösauvoilla. Ne työnnetään reaktoriin joko hydraulisesti tai sähkömekaanisen järjestelmän avulla. Jos pikasulku säätösauvojen avulla epäonnistuu, hätäbooraus käynnistyy, jolloin boorivettä pumpataan reaktorin jäähdytysveteen. Näin saadaan reaktorin veden booripitoisuus nousemaan ja fissioreaktio pysähtymään. Boorivesi on kuitenkin toissijainen vaihtoehto, koska sen käytön jälkeen reaktorin paineastia täytyy puhdistaa. (TVO 2008: 43; Koskiniemi 2005: 6)

Olkiluodon voimala-alueen käyvien reaktoreiden hätäjäähdytysjärjestelmä koostu apuvesisyöttöjärjestelmästä ja reaktorin sydämen ruiskutusjärjestelmästä, joista apuvesisyöttöjärjestelmä toimii korkeapaineessa ja reaktorisydämen ruiskutusjärjestelmä matalapaineessa. Molemmat järjestelmät on suunniteltu ylläpitämään reaktoripaineastian vesitasapainoa jäähdytteenmenetysonnettomuudessa. Apuvesisyöttöjärjestelmän avulla pystytään pitämään reaktorinsydän veden peitossa, mikäli veden syöttöjärjestelmä ei ole toiminnassa. Sen avulla pystytään syöttämään vettä kovassakin paineessa. Reaktorisydämen ruiskutusjärjestelmää aletaan käyttää vasta reaktorin paineen laskettua

riittävän alas. Järjestelmä suojaa reaktoria ylikuumenemiselta apuvesisyöttöjärjestelmän ja ulospuhallusjärjestelmän kanssa reaktorisydämen yläpuolisessa putkikatkossa. (TVO 2013a: 52; Halminen 2001: 19; Koskiniemi 2005: 7)

Olkiluodon voimala-alueen rakenteilla olevan OL3-laitoksen reaktorin hätäjäähdytysjärjestelmä koostuu matala- ja keskipaineisesta hätäjäähdytysjärjestelmästä, typellä paineistetuista paineakuista sekä reaktorin suojarakennukseen sijoitetuista hätäjäähdytysvesialtaista. Lisäksi voimalaitoksen turvatoimissa on varauduttu reaktorisydämen sulamiseen rakentamalla reaktorin sydänsulalle leviämisalue, jossa sulan annetaan jäähtyä. OL3:n keskeisimmät turvallisuustoiminnot on esitettynä kuvassa 8 olevasta laitoksen poikkileikkauksesta. (TVO 2008: 43; TVO 2009: 21−22.)



Kuva 8. Olkiluoto 3:n keskeisimmät turvallisuustoiminnot. (TVO 2008: 42.)

Onnettomuustilanteiden varalle ydinvoimalaitosyksiköiden sähkönsaanti on turvattu usealla eri tavalla, muun muassa hätäjäähdytys- ja jälkilämmönpoistojärjestelmille. Päägeneraattorin ollessa pois käytöstä, saadaan sähkö joko toiselta laitosyksiköltä tai valta-

kunnan sähköverkosta joko 400 kV:n tai 110 kV:n sähköverkosta. Lisäksi laitoksilla on neljä dieselgeneraattoria, jotka käynnistyvät automaattisesti sähkönmenetystilanteessa. Dieselgeneraattoreiden avulla pystytään syöttämään sähköä laitosyksiköltä toiselle niiden välisen yhteyden kautta turvallisuuden kannalta olennaisille järjestelmille. Olkiluodossa on myös varavoimalaitos, kaasuturbiinilaitos, jonka avulla voidaan syöttää sähköä laitosyksiköille joko maakaapeliyhteyden tai 110 kV sähköaseman kautta. Näiden varmistusten lisäksi sähköä voidaan saada suoraan joko Harjavallan vesivoimalaitoksilta tai Paneliankosken Voiman 20 kV:n verkosta erikoisjärjestelyillä. Lisäksi akkuvarmennetut järjestelmät saavat sähköä akustoilta. OL3-laitos tulee valmistuttuaan saamaan kuusi dieselgeneraattoria ja se tullaan liittämään OL1:n ja OL2:n kanssa samaan sähkönsyöttörenkaaseen. (Koskiniemi 2005: 7; TVO 2014b; TVO 2013a: 36; TVO 2010: 41.)

2.3 Ohjelmistopohjaiset järjestelmät ja laitteet

Ohjelmistopohjaista tekniikkaa käytetään nykyään enenevässä määrin ydinvoimaloiden sähkö- ja automaatiojärjestelmissä ja -laitteissa. Ajan kuluessa ja tekniikan kehittyessä vanhan, käytössä olevan tekniikan osaaminen heikkenee ja varaosien saanti vähenee, sillä niiden tekeminen ei ole tekniikan kehittymisen myötä enää kannattavaa. Varaosien puutteiden myötä ydinvoimaloiden vanhat laitteet ja järjestelmät on korvattava uusilla laitteilla, jotka voivat sisältää ohjelmistoa. (Halminen & Nevalainen 2007: 559.)

Ohjelmistopohjainen tekniikan myötä laitteiden ja järjestelmien käytöstä on tullut helpompaa ja joustavampaa. Ohjelmiston avulla saadaan toteutettua halutut toiminnot sekä laitteistojen huolto ja kunnossapito on nopeampaa. Lisäksi ohjelmoitava tekniikka mahdollistaa järjestelmien ja laitteiden turvallisuuden parantamisen. Ohjelmistopohjaisten järjestelmien ja laitteiden turvallisuus ja luotettavuus on kuitenkin pystyttävä osoittamaan ydinvoimakäyttöä varten. Perinteisesti tähän on käytetty kelpoistamista, mutta se on havaittu vaikeaksi ja suuritöiseksi ohjelmistoille. Lisäksi ohjelmiston testaaminen on haastavaa ja melkein mahdotonta useiden testitapausten ansiosta. Testauksessa käytettäviä työkaluja on useita samoin ohjelmiston suunnittelutyökaluja. Tähän mennessä ydin-

voimaloiden turvallisuuskriittisten laitteiden ja järjestelmien ohjelmiston turvallisuus ja luotettavuus on pystytty takaamaan yhtenäisellä ja hallitulla suunnittelu- ja kehitysprosessilla, joka tarkastetaan luvanhaltijan toimesta. Jotta ohjelmistopohjaisten laitteiden turvallisuutta ja luotettavuutta saataisiin parannettua, ohjelmiston testausmenetelmiä ja -työkaluja on kehitettävä muun suunnittelu- ja kehitysprosessin rinnalla. (Halminen ym. 2007: 559; Kasurinen 2013:19.)

Ohjelmistopohjaiset laitteet voidaan luokitella ohjelmiston perusteella. Se voi olla alusta asti kehitettävä uusi ohjelmisto tai valmis tuote, joka on valmiiksi asennettu laitteeseen. Laitteeseen valmiiksi asennettuihin ohjelmistoihin on vaikea vaikuttaa, mutta useimmiten niihin pystytään lisäämään ohjelmistosovelluksia asiakkaan tarpeiden ja käyttötarkoituksen mukaan. Esimerkiksi automaatiojärjestelmissä ja -laitteissa ohjelmistot voidaan rakentaa laitealustan ohjelmistosta, joihin pystytään lisäämään asiakkaan toiveiden mukaisia ohjelmistosovelluksia. Ohjelmistosovelluksien lisäämismahdollisuudet kuitenkin riippuvat paljon kyseessä olevasta laitteesta ja järjestelmästä. Tilattaessa ohjelmistopohjaista laitetta ydinvoimalaan on tiedettävä minkä tyyppinen ohjelmisto laitteessa on. Tämä vaikuttaa muun muassa laitteen varaosien tilaukseen sekä huoltoon. (Webster 2008.)

3 OHJELMISTOPOHJAISEN JÄRJESTELMÄN KELPOISTAMINEN

Ydinvoimalaitoksen turvallisuuskriittisten järjestelmien kelpoistamisella on tärkeä rooli niiden kehitysprosessissa. Sen avulla osoitetaan järjestelmän, sen ohjelmiston ja laitteiden toimivan halutulla tavalla. Kelpoistamisen avulla osoitetaan asetettujen vaatimusten, niin toiminnallisten kuin ei-toiminnallisten, toteutuminen luotettavasti ilman ei-toivottuja toimintoja, joista aiheutuu vain haittaa ja pahimmillaan häiriötilanteita. Kelpoistaminen on kuitenkin osa isompaa prosessia, kuten laitosmuutostyöprosessia tai luvitusprosessia, josta tehty prosessimalli on esitettynä liitteessä 1. Liitteestä laatikko *qualification material elaboration* kuvaa kelpoistusmateriaalia, joka välitetään luvanhaltijalle. (Wang ym. 2008.)

Kelpoistaminen jakaantuu järjestelmän ja sen ohjelmiston ja laitteiden elinkaaren ajalle jokaisen elementin ja komponentin suunnittelusta koko järjestelmän toiminnallisiin testeihin ja suorituskykytesteihin. Tällä tavoin varmistetaan jokaisen suunnittelu- ja toteutusvaiheen noudattavan virmanomaisen asettamia ohjeita ja standardeja, joihin myös itse kelpoistusprosessi pohjautuu. (VTT 2003.)

Kelpoistuksesta vastuussa on aina luvanhaltija, jolle viranomainen on myöntänyt luvan ydinenergialain mukaiseen ydinenergian käyttöön. Luvanhaltijan vastuulla on varmistaa kelpoistuksen toteuttaminen laadittujen testisuunnitelmien ja laatusuunnitelman mukaisesti. Laitostoimittajan tehtävänä on toimittaa järjestelmästä kelpoistukseen tarvittavaa tietoa luvanhaltijalle. (VTT 2003.)

Tässä osiossa käsitellään kelpoistukseen liittyviä tärkeitä tekijöitä, kuten kelpoistussuunnitelma sekä yleisimmät kelpoistusmenetelmät. Lisäksi esitellään kelpoistuksessa noudatettavat standardit ja ohjeet sekä käsitellään vaatimusmäärittelyn, konfiguraation hallinnan ja dokumentoinnin merkitystä kelpoistusprosessille. Lopuksi esitellään yleinen kelpoistusproseduuri, eli miten kelpoistamisprosessi yleisesti etenee.

3.1 Kelpoistussuunnitelma

Kelpoistussuunnitelma laaditaan kelpoistettavalle turvallisuusluokan 2 tai 3 järjestelmälle, laitteelle tai ohjelmistolle. Se on järjestelmä tai laitekohtainen dokumentti, jossa kuvataan tarkasti, miten järjestelmän tai laitteen osoitetaan soveltuvan käyttötarkoitukseensa ja täyttävän asetetut turvallisuusvaatimukset. Ohjelmoitavan järjestelmän kelpoistussuunnitelmaan on kuuluttava niin perusjärjestelmän kelpoistussuunnitelma kuin sovelluksen ohjelmiston kelpoistus. (YVL E.7 2013: 12−13, 22; VTT 2003.)

Kelpoistussuunnitelmaa laadittaessa ja tarkistettaessa on varmistettava kaikkien turvallisuusvaatimusten tulevan testatuiksi ja analysoiduiksi. Siinä tulee ilmetä, mitä kelpoistusmenetelmää tai menetelmien yhdistelmää kelpoistuksessa käytetään sekä kelpoistukseen osallistuvat organisaatiot. Lisäksi suunnitelmassa tulee esittää kelpoistuksessa sovellettavat standardit sekä suunnittelussa ja toteutuksessa käytettävät työkalut. Suunnitelmasta on käytävä myös ilmi järjestelmälle, laitteelle tai ohjelmistolle asetetut luotettavuusvaatimukset sekä niiden turvallisuusmerkitys voimalaitokselle. Jos kyseessä on turvallisuusluokan 2 järjestelmä tai laite, tulee kelpoistussuunnitelmasta ilmetä menettelytapa, jolla riippumaton asiantuntija-arvioija arvioi kelpoistustoimenpiteiden hyväksyttävyyden. (YVL E.7 2013: 12; Hietikko, Alanen & Tiusanen 1996: 15; Urunga, Sözbir, Özyildirim 2013.)

Kelpoistussuunnitelman sisältö poikkeaa riippuen siitä, onko tuote uusi, alusta asti kehitettävä vai onko se standardituote. Jos tuote kehitetään alusta alkaen, tulee suunnitelmasta käydä ilmi jokainen suunnittelu- ja toteutusprosessi sekä vaiheiden jälkeen tehtävät tarkastukset ja arvioinnit. Lisäksi kelpoistussuunnitelmalla pystytään vaikuttamaan tuotteen kehitykseen ja sille asetettaviin vaatimuksiin. Mikäli tuote on standardituote, sen kehitykseen tai vaatimuksiin ei voida vaikuttaa enää kelpoistussuunnitelmassa. Tällöin se tulee kelpoistaa niille ominaisuuksille, jotka sillä jo on. Standardituotteen kelpostussuunnitelmassa on huomioitava, miten osoittaa sen soveltuvan tarkoitettuun käyttötarkoitukseen sekä tuotteen täyttävän käyttötarkoituksesta sille kohdistuvat vaatimukset. (Halminen 2001: 29.)

Kelpoistussuunnitelma on laadittava luvanhaltijan ohjeiden mukaisesti ja dokumentin laatimisesta vastaa luvanhaltija. Suunnitelma lähetetään toimittajalle ja siitä on käytävä ilmi toimittajalta kelpoitusprosessin aikana ja itse kelpoistuksessa odotettavat tehtävät. Kelpoistussuunnitelmassa tulee olla myös kirjattuna kaikki kelpoistukseen vaikuttavat tekijät, kuten vaatimukset, jotta kelpoistusprosessin jokainen vaihe pystyttäisin toteuttamaan ja sen etenemistä olisi helpompi seurata. Kelpoistussuunnitelma päivitetään kelpoistusprosessin edetessä tarpeen vaatiessa. Suunnitelman päivittymiseen voi vaikuttaa esimerkiksi vaatimusmäärittelyjen muuttuminen, joka vaikuttaa kelpoistukseen, tai jokin muu kelpoistusprosessiin vaikuttava tekijä, jolla on vaikutusta suunnitelmaan, kuten tilanne, jossa kelpoistussuunnitelmassa havaitaan puutteita tai tehdastestit epäonnistuvat. Kaikki kelpoistussuunnitelmat, niin järjestelmä- kuin laitekohtaisetkin, tulee välittää viranomaiselle. Siinä on käytävä ilmi laadittavat soveltuvuusarviot. (YVL E.7 2013: 12−13; VTT 2003; Hietikko ym. 1996: 15; Piensalo 2013: 10−11.)

3.2 Kelpoistusmenetelmät

Kelpoistamisen avulla osoitetaan alkuperäisten vaatimusten toteutuminen. Se voidaan toteuttaa joko testeillä, vertaamalla saatuja testituloksia dokumentoituihin tuloksiin tai näiden yhdistelmänä. Tyypillisesti järjestelmän kelpoistaminen suoritetaan erillisissä vaiheissa. Ensin testataan järjestelmän yksittäiset komponentit tai osajärjestelmien kokoonpanot, jonka jälkeen testataan vasta koko järjestelmä. (IEC 61513 2011: 71; IEC 60780 1998: 19−21; Havuajo 2012: 32.)

Yleisimpiä käytettyjä kelpoistusmenetelmiä yksittäisille komponenteille ja osajärjestelmien kokoonpanoille ovat tyyppitestit tai tyyppihyväksynnät, toiminnalliset testit, analyysit, käyttökokemukset, jatkuva kelpoistaminen tai mainittujen menetelmien yhdistelmä. Ohjelmistojen kelpoistaminen pelkän testin avulla on erittäin haastavaa, minkä takia sen laatu pyritään osoittamaan pääasiassa laadukkaalla kehitystyöllä sekä muun muassa analyysien avulla. Käytettävästä menetelmästä huolimatta kelpoistamisessa on noudatettava viranomaisten laatimia ohjeita, erityisesti sähkö- ja automaatiokomponenttien sekä turvallisuusluokiteltujen laitteiden ohjelmien kelpoistukseen laadittua YVL

E.7 -ohjetta sekä kelpoistusta koskevia IEC standardeja esimerkiksi IEC 60780. (IEC 60780 1998: 19–21; Havuajo 2012: 32; IEC 61513 2011: 71; YVL E.7 2013: 13–17.)

Osajärjestelmille ja komponenteille valittavaan kelpoistusmenetelmään vaikuttavat useat eri tekijät, erityisesti järjestelmän ja sen laitteiden käyttöolosuhteet, vanheneminen sekä vikojen alkutapahtumat. Näiden tekijöiden lisäksi on kyettävä osoittamaan, että kelpoistukseen valittu menetelmä tai menetelmien yhdistelmä on riittävän kattava ja vaativa osoittamaan järjestelmän ja laitteiden täyttävän asetetut vaatimukset. (YVL E.7 2013: 13; Halminen 2001: 22; Yli-Nikkilä 2012: 25.)

Yleisimmin kelpoistuksessa käytetty menetelmä on tyyppitesti, jossa käytetään laitteen käyttöolosuhteita vastaavia simuloituja olosuhteita osoittamaan järjestelmän täyttävän asetetut vaatimukset. Testin aikana simuloidaan laitteen käytöstä sen käyttöympäristössä ja häiriötilanteissa sekä mitataan sen suorituskykyä. Lisäksi tyyppitesteissä selvitetään ikääntymisen aiheuttamia haittoja laitteelle. Ohjelmoitavan tekniikan tyyppitestauksen on katettava niin ohjelmisto kuin laitekin. Tyyppitestejä täydentämässä käytetään joskus käyttökokemuksia, jotka eivät ole yksin riittävä kelpoistusmenetelmä. Niiden avulla pystytään kuitenkin selvittämään yleiskuva järjestelmän ja sen laitteiden toiminnasta todellisessa käyttökohteessa. Lisäksi käyttökokemukset kuvaavat hyvin järjestelmän ja sen laitteiden käyttäytymistä käyttöympäristössään, esimerkiksi käyttökokemuksien perusteella voidaan selvittää järjestelmän ja sen laitteiden vikaantumishistoria. (IEC 60780 1998: 17–19; YVL E.7 2013: 16–17; VTT 2003.)

Mikäli toiminnallisten ja suorituskykyvaatimusten täyttymistä ei kyetä osoittamaan tyyppitestien ja käyttökokemuksien avulla, käytetään analyysejä. Tämä menetelmä tarvitsee kelpoistettavaa laitetta tai järjestelmää kuvaavan mallin, joka perustuu todistettaviin testien tuloksiin, käyttökokemuksiin, fysikaalisiin lakeihin tai näiden yhdistelmiin. Myös analyysit voivat olla osa yhdistettyä kelpoistusmenetelmää. Analyysien avulla kelpoistamista käytetään muissa kelpoistusmenetelmissä tukena, jos esimerkiksi koko tai jokin muu käytännön vaatimus rajoittaa tyyppitestin suorittamista. (IEC 60780 1998: 19; YVL E.7 2013: 16.)

Jatkuvaa kelpoistusta puolestaan käytetään edellä mainittujen kelpoistusmenetelmien antaessa järjestelmälle ja sen laitteille haluttua lyhyemmän käyttöajan. Toteutustavat menetelmässä ovat toistuva toimiva laitteen testaus ja sen korvaaminen uudella. Lisäksi laitteen rinnalle voidaan asentaa toinen yksilö, joka poistetaan ennen kuin kelpoistetun käyttöaika päättyy. Rinnalle asennettavan laitteen on oltava tyyppitestattu, jotta laitteille voitaisiin määrittää lisää käyttöaikaa. (IEC60780 1998: 21.)

Valitusta kelpoistusmenetelmästä riippumatta testien tulokset on raportoitava ja dokumentoitava. Tällä tavoin voidaan osoittaa järjestelmän soveltuvan suorittamaan vaaditut toiminnot, täyttävät vaatimusmäärittelyt sekä soveltuvan suunniteltuun käyttötarkoitukseen. Tehtyjen testien tulosten dokumentoinnin on oltava kattava, yksiselitteinen ja tarkastettavassa muodossa muun muassa viranomaisille esitettäväksi ja liitettäväksi lopulliseen soveltuvuusarvioon. (Halminen 2001: 23; Yli-Nikkilä 2012: 25.)

3.3 Standardit ja YVL-ohjeet

Kelpoistuksessa on noudatettava viranomaisten asettamia YVL-ohjeita sekä standardeja. Standardit ovat kuitenkin vain suosituksia, eivät lakeja. Niiden avulla esitetään suositus, miten jokin asia, tässä tapauksessa kelpoistus, tulisi toteuttaa. Standardien avulla pystytään luomaan yhtenäinen toiminta sekä arvioimaan yritysten toimintaa. (SFS 2014a; SFS 2014b.) YVL-ohjeet puolestaan ovat perustuslain, ydinenergialain (990/1987), ydinenergia-asetusten (161/1988) ja valtioneuvoston asetusten (717/2013) mukaisia yksityiskohtaisia turvallisuusvaatimuksia, joissa esitetyt vaatimukset tulee toteuttaa ja niitä tulee noudattaa niin ydinvoimalan toiminnassa kuin laitteistojen uusinnoissa. YVL-ohjeissa voidaan viitata noudatettaviin standardeihin, ohjeistoihin ja lakeihin. Standardit ja YVL-ohjeet täydentävät toisiaan tehden kelpoistusprosessista laadukkaan sekä varmistaen, että lopputuloksena ovat vaatimukset täyttävä järjestelmä, jonka laitteisto ja ohjelmisto on testattu määritettyjen vaatimusten ja menetelmien mukaisesti. (Koutaniemi ym. 2004: 356; YVL E.7 2013: 5.)

3.3.1 Noudatettavat YVL-ohjeet

Vuonna 2000 tehty perustuslain uudistus aiheutti muutostarpeita ydinenergialakiin ja ydin-energia-asetuksiin, joista aiheutui YVL-ohjeisiin uudistuksia. STUK:n laatimat YVL-ohjeiden uudistus saatiin valmiiksi vuoden 2013 lopulla. Uudet YVL-ohjeet ovat vanho-ja johdonmukaisempia, tiukempia ja parantavat ydinvoimalaitosten turvallisuutta suo-messa. Uudet YVL-ohjeet tulevat automaattisesti voimaan uusiin ydinvoimalaitoksiin. Vanhempiin, käytössä olevien voimalaitosten osalta STUK kertoo, miten uusittua tai uutta ohjetta tullaan noudattamaan kuultuaan ensin asianomaisia. (Plit 2013; STUK 2014; Koutaniemi 2009.)

Uudet YVL-ohjeet koostuvat viidestä ohjeryhmästä A, B, C, D ja E, jotka käsittelevät ydinvoimalan eri osa-alueita. Esimerkiksi ryhmän A ohjeet liittyvät ydinvoimalaitoksen turvallisuuden hallintaan, ryhmän B ohjeet puolestaan ydinvoimalan ja sen järjestelmien suunnitteluun ja ryhmän E ohjeet käsittelevät ydinvoimalaitoksen rakenteita ja laitteita. Kelpoitusprosessissa noudatetaan uusista YVL-ohjeista erityisesti YVL E.7 -ohjetta, mutta myös YVL B.1, YVL B.2, YVL A.8 sekä YVL A.7 -ohjeita. YVL E.7 -ohjeessa asetetaan yleiset vaatimukset sähkö- ja automaatiolaitteiden sekä kaapeleiden vaatimusmäärittelylle, valinnalle, hankinnalle ja laadunhallinnalle. Lisäksi ohjeessa asetetaan ohjeet sähkö- ja automaatiojärjestelmien kelpoistukselle sekä ohjelmistopohjaisten turvallisuusluokiteltujen laitteiden ohjelmiston kelpoistukselle. (YVL E.7 2013; STUK 2014.)

Ydinvoimalan turvallisuusluokkien määritelmät on YVL B.2 -ohjeessa, jossa esitellään perusteet turvallisuusluokkien 1, 2, 3, EYT järjestelmille ja järjestelmän laitteistolle sekä kuvaa soveltumisperusteet. EYT-luokasta voidaan eriyttää vielä EYT/STUK, johon kuuluvat laitteet ja järjestelmät, jotka ovat olleet vanhoissa YVL-ohjeissa turvallisuusluokassa 4. Näitä ovat esimerkiksi paloturvallisuusjärjestelmät ja -laitteet. Lisäksi ohjeessa määritellään maanjäristysluokat, joihin ydinvoimalan järjestelmät, rakenteet ja laitteet on myös luokiteltu turvallisuusluokkien lisäksi. YVL B.1 -ohjeessa puolestaan keskitytään turvallisuussuunnitteluun. Ohjeessa esitetään perusvaatimukset, joita sitten yksityiskohtaistetaan ja täydennetään YVL E.7 -ohjeessa. (YVL B.1 2013; YVL B.2 2013)

Ydinvoimaloiden todennäköisyyspohjaiseen riskianalyysiin ja riskien hallintaan liittyvät määräykset esitetään YVL-ohjeessa A.7. Ohjeessa esitetään yleiset vaatimukset PRA-analyysiin ja sen dokumentointiin. Ohjetta sovelletaan edellä esitellyssä YVL B.1 -ohjeessa riskianalyysien määrittelyssä ja laatimisessa. YVL A.7 -ohjeen lisäksi YVL A -sarjasta myös ohje A.8 tulee huomioida kelpoistusprosessissa. YVL A.8 -ohje asettaa vaatimukset ikääntymisen hallintaan. YVL A.8 -ohjetta sovelletaan muun muassa YVL B.1 -ohjeessa sekä YVL E -sarjan ohjeissa, jotka koskevat ydinvoimalaitoksen rakennetta ja laitteita. Esimerkiksi YVL E.7 -ohjeessa on kokonainen kappale, joka käsittelee ikääntymisen hallintaa. Tuon kappaleen kohdissa viitataankin ohjeeseen YVL A.8. (YVL A.7 2013; YVL B.1 2013;YVL A.8 2013.)

STUK:n laatimat uudet YVL-ohjeet tulevat automaattisesti voimaan suunniteltaville ydinvoimaloille, kuten OL4. Ohjeet eivät ole vielä käytössä Olkiluodon käyvissä ydinvoimalaitoksissa, sillä käynnissä on kuulemiskierros, jossa tarkastellaan, täyttääkö TVO YVL-ohjeissa asetetut vaatimukset ja määräykset. Kuulemiskierros kestää noin vuoden, jonka jälkeen STUK tekee päätöksen, miltä osin uudet YVL-ohjeet tulevat voimaan

3.3.2 Noudatettavat standardit

International Elecrotechnical Commission (IEC) on julkaissut joukon ydinvoimalaitosten turvallisuutta käsitteleviä standardeja, joita hyödynnetään kelpoistusprosessissa. Tässä kappaleessa esitellään yleisimmät kelpoistusrosessissa noudatettavat standardit sekä alueet, joihin ne asettavat määrityksiä ja vaatimuksia.

Standardi tarkoittaa normia, joka on standardointijärjestön määrittämä. Virallisia standardeja laativat viralliset standardointijärjestöt joita IEC:n lisäksi ovat *International Organization for Standardization* (ISO), *Institute of Electrical And Electronics Engineering* (IEEE) ja suomalainen Suomen Standardisoimisliitto ry (SFS). Järjestöjen laatimia standardeja voidaan hyödyntää monella tekniikan alalla, myös kelpoistusprosessissa. Ne asettavat vaatimuksia niin itse kelpoistusprosessin kelpoistusmenetelmille kuin kelpoistettavalle järjestelmälle ja sen ohjelmistolle sekä laitteistolle, jotta prosessi suunnittelusta käyttöön toteutuisi laadukkaasti. Kuitenkaan mikään standardi ei yksin riitä kattamaan koko prosessia, vaan useat standardit täydentävät toisiaan.

Standardi IEC 60780 (1998) esittelee ydinvoimaloiden sähkölaitteiden yleisen kelpoistusprosessin ja kelpoistusmenetelmät, joita käytetään kelpoistuksessa. Se asettaa vaatimukset menetelmien toteuttamiseen sekä tarkemmat määritykset kelpoistunanalyysien tekemiseen. Standardissa käsitellään myös kelpoistukseen ja saatuihin tuloksiin liittyvää dokumentointia. (IEC 60780 1998; Yli-Nikkilä 2012: 24; Halminen 2001: 24.)

Standardi IEC 61226 (2009) esittelee luokittelumenettelyn etenemisen ja määrittelee ydinvoimaloiden turvallisuustoimintoja suorittaville automaatiojärjestelmille ja -laitteille luokittelun kategorioihin. Luokittelu puolestaan asettaa vaatimukset järjestelemien ja laitteiden suunnittelulle. Standardi esittää turvallisuuskategoriat A, B ja C sekä luokittelemattoman esittäen samalla niiden rajat. Määritellyt kategoriat vastaavat YVL B.2:ssa määritettyjä turvallisuusluokkia 2, 3 ja EYT STUK. Turvallisuusluokkien ja kategorioiden vastaavuus on esitetty taulukossa 2, joka on sivulla 38. (IEC 61226 2009; Yli-Nikkilä 2012: 24.)

Standardi IEC 60880 (2006) on vuonna 1986 julkaistun IEC 60880 standardin ja vuonna 2000 julkaistun IEC 60880-2 standardin yhdistelmä. Se käsittelee ydinvoimalan ohjelmistopohjaisten järjestelmien ohjelmistoa ja määrittää vaatimuksia ohjelmiston kehityksen vaiheisiin. Se asettaa määritelmiä jokaiseen vaiheeseen suunnittelusta testaukseen sekä kelpuutukseen, joka on osa kelpoistusta, kuten kappaleen 3.8 kuvassa 13 (sivulla 50) havainnollistetaan. Erityisesti standardin taulukossa E.4.2, joka on esitetty liitteessä 2, käsitellään tarkasti testausmetodeja, joiden avulla ohjelmistot pyritään osoittamaan luotettaviksi ja toimiviksi riippumatta ohjelmiston kehitystavasta tai testausmenetelmästä. Lisäksi standardissa asetetaan vaateita myös ohjelmistonkehitystyökaluille. Sen tähtäimenä on auttaa kehittämään mahdollisimman laadukas ohjelmisto. Standardi kuitenkin käsittelee turvallisuus kategorian A järjestelmän ohjelmistoja. Siksi Standardi IEC 62138 (2004) täydentää sitä, sillä se esittelee vastaavat asiat kuin IEC 60880, mutta turvallisuus kategorioiden B ja C järjestelmille. Näiden standardien myötä saadaan koottua vaatimukset ohjelmiston kehittämiseen ja kelpoistukseen. (IEC 60880 2006; IEC 62138 2004; Yli-Nikkilä 2012: 24; Halminen 2001: 24.)

Esiteltyjen standardien lisäksi kelpoistusprosessissa tulisi noudattaa standardia IEC 61513 (2011), joka asettaa yleiset vaatimukset ydinvoimaloiden turvallisuusjärjestelmil-

le, jotka voivat koostua analogisista laitteista, ohjelmistopohjaisista laitteista tai näiden yhdistelmistä. Standardissa korostetaan ydinvoimalaitosten turvallisuustavoitteita, jotka ovat edellytyksenä tuotteen kattavan arkkitehtuurin suunnittelussa. Standardin liitteessä esitetään myös sen yhtäläisyys standardin IEC 61508 kanssa. (IEC 61513 2011; Yli-Nikkilä 2012: 24; Halminen 2001: 24.)

Standardi IEC 61508 (2010) koostuu seitsemästä osasta. Se esittää tarkat vaatimukset kaikille tekniikoille toiminnallisesta turvallisuudesta. Esimerkiksi standardin osassa 3 määritetään ohjelmistoa koskeva vaatimukset. Lisäksi standardissa esitetään vaara- ja riskianalyysien arviointimenetelmän, jonka tulosten perusteella saadaan määritettyä turvallisuuden neljä eheyden tasoa (TET tai *Safety Integrity Level,* SIL), jotka ovat esitettynä taulukossa 1. (IEC 61508-1 2010; IEC 61508-2; IEC 61508-3; Yli-Nikkilä 2012: 22.)

Taulukko 1. Vikojen todennäköisyys. (Pepperl+Fuchs 2007: 14.)

Turvallisuuden eheyden taso (TET/SIL)	**Harvojen vaateiden toimintatapa** **(Keskimääräinen epäonnistumisen todennäköisyys suunnitellun toiminnon toteuttamisessa vaadittaessa)**	**Tiheiden vaateiden tai jatkuvan toiminnan käyttötapa** **(Vaarallisen vikaantumisen toden-näköisyys tuntia kohti)**
4	$\geq 10^{-5} \ldots < 10^{-4}$	$\geq 10^{-9} \ldots < 10^{-8}$
3	$\geq 10^{-4} \ldots < 10^{-3}$	$\geq 10^{-8} \ldots < 10^{-7}$
2	$\geq 10^{-3} \ldots < 10^{-2}$	$\geq 10^{-7} \ldots < 10^{-6}$
1	$\geq 10^{-2} \ldots < 10^{-1}$	$\geq 10^{-6} \ldots < 10^{-5}$

SIL-luokkien vastaavuutta turvallisuusluokkiin ei ole esitetty standardeissa, mutta SIL-luokat 3, 2 ja 1 voidaan karkeasti arvioida vastaamaan standardissa IEC 61226 määriteltyjä luokkia A, B ja C. Turvallisuusluokkien, -kategorioiden ja SIL-luokkien vastaavuudet on esitetty taulukossa 2.

Taulukko 2. Turvallisuusluokkien ja turvallisuuden eheyden tasojen vastaavuus. (YVL B.2 2013: 5; STUK 2010: Wahlström 2011; YVL 2.1 2000: 5, vanhentunut.)

Turvallisuusluokka	Turvallisuus kategoria	Turvallisuuden eheyden taso
2 (+3 onnettomuus-insturmentit)	A	3
3	B	2
EYT/STUK	C	1
EYT		

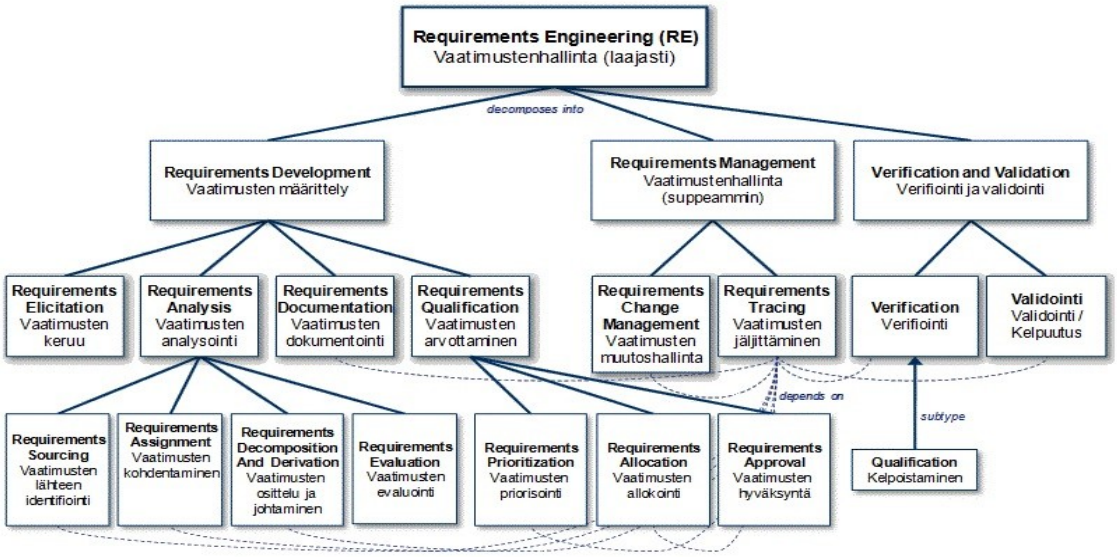
Kelpoisuksessa on huomioitava myös standardi IEC 60987. Standardi käsittelee laitteistoja, joihin ohjelmisto asennetaan. Se määrittää vaatimukset uuden laitteiston kehityksen sekä valmiiden ohjelmistopohjaisten laitteiden, kuten COTS (*Component Off the Shelf*) -laitteistojen arvioinnin. Erityisen laitteistoläheiset laiteohjelmat (*firmware*), tulee myös arvioida IEC 60987 -standardin mukaisesti. Muissa ohjelmistotapauksissa on noudatettava edellä esiteltyjä standardeja IEC 60880 ja IEC 62138. (IEC 60987 2013; Halminen 2001: 24.)

3.4 Vaatimustenhallinta ja vaatimusmäärittely

Vaatimustenhallinta (*Requirement Engineering,* RE) mielletään eräänlaiseksi kattoprosessiksi, joka sisältää vaatimusten hallintaan liittyviä toimintoja ja tehtäviä. Esimerkiksi konfiguraationhallinta, versionhallinta ja muutostenhallinta ovat vaatimustenhallinnan toimintoja, joista kerrotaan enemmän kappaleessa 3.5. Vaatimustenhallinta voidaan jakaa aliprosesseihin, kuten vaatimusmäärittelyyn (*Requirement Development*), suppeampaan vaatimustenhallintaan (*Requirement Management*) sekä verifiointiin (*verification*) ja validointiin (*validation*) seuraavan sivun kuvan 9 mukaisesti. (Kallio 2008: 22; Viitasalo 2014; Wiegers 2000.)

Vaatimusten validoinnin avulla tarkastetaan, että kootut vaatimukset ovat johdonmukaisia ja tarkkoja. Verifioinnilla puolestaan todennetaan vaatimusten toteutuminen. Vali-

dointi ja verifiointi toteutetaan yleensä prosessin loppuvaiheessa. Vaatimusmäärittelystä kerrotaan tarkemmin kappaleessa 3.4.1. (Lintula 2004: 13–14; Wiegers 2000.)



Kuva 9. Vaatimustenhallinnan aliprosessit. (Muokattu lähteestä Viitasalo 2014).

Vaatimustenhallinta on suunnitteluperusteiden hallintaa, joka jakaantuu kehittävän tuotteen elinkaaren jokaiseen vaiheeseen. Sen tehtävän on ylläpitää vaatimusmäärittelyyn koottuja vaatimuksia, jotka muuttuvat ja kehittyvät prosessin edetessä. Kallio (2008: 22) muistuttaa työssään, että ohjelmistoilla vaatimukset voivat muuttua käyttöönoton jälkeen, jolloin vaatimusten muuttamisesta tulee kallis prosessi. Siksi virheelliset ja vanhentuneet vaatimukset olisi hyvä havaita mahdollisimman aikaisessa vaiheessa, jolloin virheellinen vaatimus saadaan korjattua taloudellisemmin. (SoftQA 2009; Kallio 2008: 22; Ludens 2011.)

Jotta vaatimuksia ja niiden riippuvuuksia voidaan pitää helposti ajan tasalla, vaatimustenhallintaan on kehitetty apuvälineeksi vaatimustenhallintatyökaluja. Nämä kuitenkin jakavat mielipiteitä. Muun muassa Ruhe, Eberlein & Pfahl (2002) kehuvat vaatimusten-hallintatyökalujen auttavan tuotteen laadun kehittämisessä, kun taas Heindl & Biffl (2005) esittävät, etteivät ne takaa hyvää tulosta esimerkiksi vaatimusten jäljitettävyy-dessä. (Kallio 2008: 22–23, 35; Ludens 2011; Ruhe, Eberlein & Pfahl 2002: 159; Heindl & Biffl 2005: 60, 68.)

Kallio (2008: 35–36) huomauttaa työssään, etteivät vaatimustenhallintatyökalut ole riippuvaisia kehityskohteestaan, joten ne eivät kykene tarjoamaan sille riittävää tukea. Hänen mukaansa riittävän tuen puute heikentää muun muassa vaatimusanalyysiä. Tilanne on kuitenkin vähitellen korjautumassa, sillä työkaluja on kehitetty antamaan kehityskohdekohtaista tukea. Nämä työkalut eivät ole vielä yleistyneet teollisuudessa, koska kohdealueiden mallintaminen on haastavaa riittävän tarkalla tasolla. Lisäksi tuotteiden nopean kehittymisen myötä mallien ajan tasalla pitäminen on vaikeaa. (Kallio 2008: 35–36; Ruhe ym. 2005: 159.)

Vaatimusten hallinta ei ole kuitenkaan pelkästään dokumenttien hallintaa. Vaatimusten ylläpitämisen lisäksi vaatimustenhallinta on ihmisten välistä viestintää ja pyrkimystä päästä yhteisymmärrykseen kehitettävästä tuotteesta. Kommunikoinnissa apuna käytetään alusta alkaen vaatimusmäärittelyä. (SofQA 2009.)

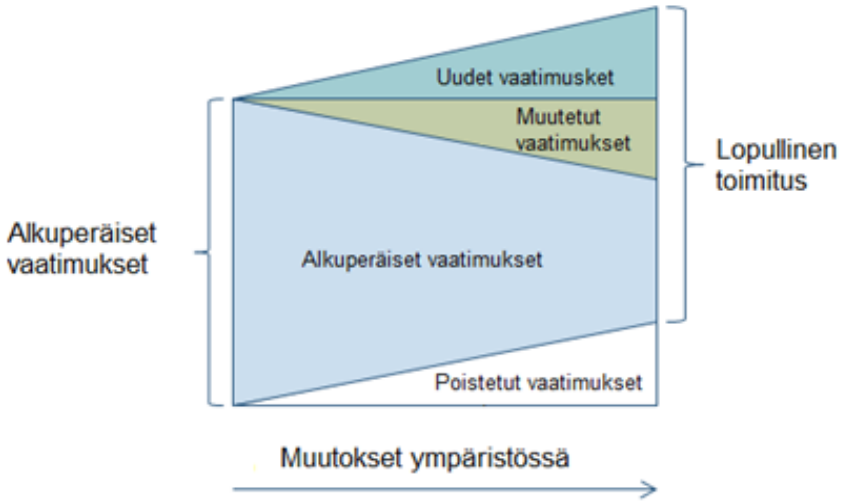
Kiviluoto (2013: 33) kuvaa työssään vaatimusmäärittelyn olevan prosessi, jossa tunnistetaan sidosryhmät ja tärkeimmät tarpeet. Vaatimusmäärittelyn avulla luodaan perusta suunnittelulle ja hankinnalle, joten se tulee laatia prosessin alusta alkaen huolella ja oikein. Vaatimusten kerääminen dokumenttiin on vaatimusmäärittelyssä kaikkein kriittisin työvaihe, sillä vaatimusmäärittelystä on käytävä ilmi järjestelmän, sen ohjelmiston ja laitteiden tärkeimmät toiminnot, vaatimukset, rajoitteet sekä standardit. Jotta haluttuun lopputulokseen päästäisiin, esitetään vaatimusmäärittelyssä, miten järjestelmän ja laitteiden toiminnallisuus saavutetaan. Tämän perusteella vaatimusmäärittelyä voidaan kuvata prosessin navigaatiokartaksi. (Kaskela 2005; Kiviluoto 2013: 33; Sininen meteoriitti 2014; Ruuska 2012: 10; Stinson 2012; Wiegers 2000; Halminen 2001: 31–32.)

Jotta vaatimusmäärittelyn laadinta voidaan aloittaa, ratkaistava toiminnallinen ongelma tulee ymmärtää. On siis selvitettävä ohjelmistopohjaisen järjestelmän ja sen laitteiston käyttötarkoitus ja käyttöolosuhteet. Lisäksi ydinvoimalaan tulevan järjestelmän vaatimusmäärittelyssä on huomioitava ydinvoimalalle ominaiset työolosuhteet, laitospaikkaa koskevat vaatimukset sekä luotettavuusvaatimukset. Myös rajapinnat muihin voimalaitoksen järjestelmiin on määriteltävä sekä huomioitava kelpoistettavan järjestelmän turvallisuusluokan asettamat vaatimukset muiden sitä koskevien rajoitusten, tavoitteiden ja standardien asettamien vaatimusten lisäksi. Laadittavasta vaatimusmärittelystä on käy-

tävä ilmi myös noudatettavat viranomaisen asettamat ohjeet. Näiden pohjalta on ohjelmistopohjaiselle järjestelmälle ja sen laitteistolle asetettava toiminnalliset ja ei-toiminnalliset vaatimukset. Kun kaikki vaatimukset on koottu, ne tulee analysoida. Analysoinnin avulla tarkastetaan ovatko kaikki vaatimukset jäljitettävissä, ovatko ne perusteltuja ja puuttuuko jokin järjestelmän, sen ohjelmiston tai laitteen toiminnan kannalta olennainen vaatimus. Tämän jälkeen vaatimusmäärittely dokumentoidaan ja lopuksi se katselmoidaan, eli vaatimusmäärittelyn tarkastetaan olevan dokumentoitu oikein. (Ruuska 2012: 11–12; Stinson 2012; YVL E.7 2013: 8; Halminen 2001: 31–32.)

Navigaatiokartan lisäksi vaatimusmäärittely voidaan kuvailla projektin osapuolten väliseksi kommunikaatiovälineeksi. Sen avulla kaikki asetetut tavoitteet ja rajaukset ovat selvillä projektiin osallistuvien eri organisaatioiden välillä. Tämän takia vaatimusmäärittelyn laadinnassa on panostettava paitsi täsmällisyyteen, mutta myös selkeyteen ja yksiselitteisyyteen, jotta epäselvyyksiltä, väärinymmärryksiltä ja virheiltä vältyttäisiin. Lisäksi vaatimusmäärittelyn on oltava muokattavissa, koska vaatimukset muuttuvat ja kehittyvät useista eri syistä prosessin edetessä. Esimerkiksi tarpeet muuttuvat, jolloin tulee uusia vaatimuksia ja osa jää tarpeettomiksi kuten kuvassa 10 havainnollistetaan. Muutetut vaatimukset on lisättävä vaatimustenmäärittelydokumenttiin, jonka on todettu olevan hyvä apuväline prosessin riskien hallinnassa. Lisäksi se antaa hyvän pohjan järjestelmän suunnittelusta toteutukseen, sillä jokaiselle vaiheelle tärkeät rajoitteet ja noudatettavat vaatimukset sekä ohjeet on esitettynä vaatimusmäärittelyssä. (YVL E.7 2013: 8; Kiviluoto 2013: 33; Sofokus 2014; Kallio 2008: 23; Halminen 2001: 31–32.)

Vaatimusmäärittely on tärkeä myös järjestelmän, sen laitteiden ja ohjelmien turvallisuuden kannalta. Jotta turvallisuus pystyttäisiin takaamaan jokaisessa prosessin vaiheessa, on vaatimusmäärittely laadittava oikein ja huolella sekä pidettävä ajan tasalla. Siinä tulee esittää kelpoistettavaa järjestelmää, laitetta tai ohjelmaa koskevat turvallisuusvaatimukset, joissa on ilmettävä myös turvallisuusluokitus ja sen asettamat vaatimukset. Näiden, niin kuin muidenkin vaatimusmäärittelyssä esitettyjen vaatimusten ja rajoitteiden, on oltava jäljitettävissä. (YVL E.7 2013: 8; Kiviluoto 2013: 48; Halminen 2001: 31–32.)



Kuva 10. Vaatimusten kehittyminen prosessin edetessä. (Muokattu lähteestä Viitasalo 2014.)

Vaatimusmäärittelyn hyvin jäljitettävistä vaatimuksista on hyötyä erityisesti, kun suunnitellaan järjestelmän laitteistoon muutoksia tai etsitään markkinoilta poistuneelle komponentille korvaavaa tuotetta. (Halminen 2001: 32.)

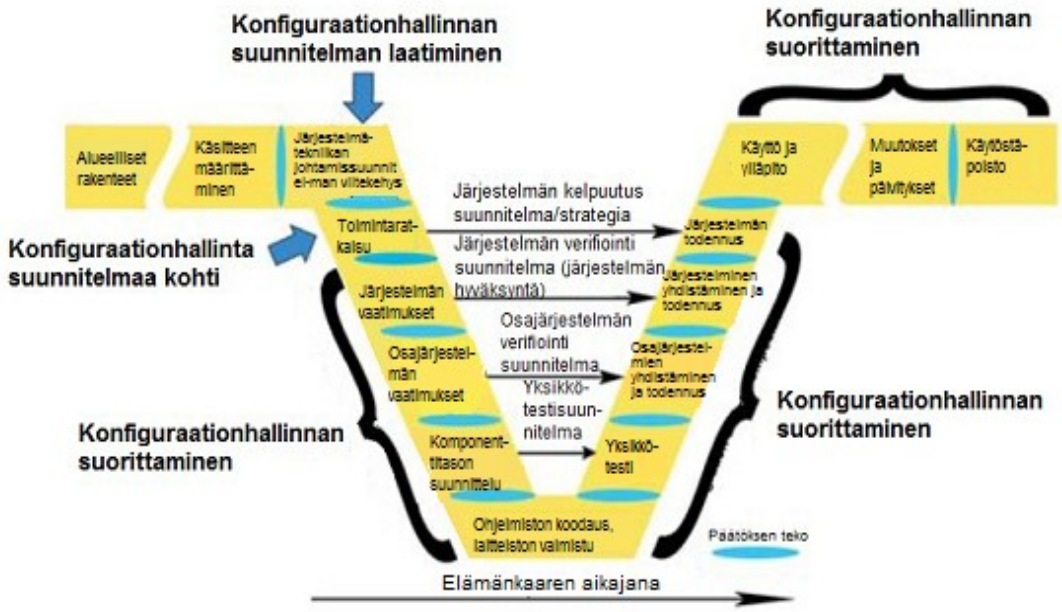
3.5 Konfiguraationhallinta

Konfiguraatio tarkoittaa ominaisuuksia tai kokonaisuutta, joka muodostuu fyysisistä komponenteista. Se tarkoittaa myös versiota puhuttaessa ohjelmistotuotteista ja dokumenteista. Jos jokin järjestelmän ominaisuus tai asetettu vaatimus muuttuu, muuttuu samalla sen konfiguraatio. Tätä varten on olemassa konfiguraationhallinta (*configuration management*, CM), jonka tehtävänä on hallita konfiguraatioissa tapahtuvia muutoksia eri osa-alueiden muodostavien toimintojen avulla. Konfiguraation osa-alueet ovat identifiointi (*identificaton*), versionhallinta (*version control*), muutostenhallinta (*change control*), tilatiedon ylläpito (*status reporting*) sekä konfiguraation tarkastus (*configuration check*). Versionhallinnasta ja muutostenhallinnasta kerrotaan enemmän kappaleissa 3.4.1 ja 3.4.2. (Ranta 2008: 5; Aho 2009: 14; Ren, Xing, Quan & Zhao 2010: 118; IEC 61508-3 2010: 13–14.)

Konfiguraationhallinnalle ei kuitenkaan löydy täysin yksiselitteistä määritelmää, sillä asiantuntijat ja standardit esittävät sille omia, toisistaan hieman poikkeavia määritelmiä. Esimerkiksi Tichyn (2008: 1) mukaan konfiguraationhallinnalla pyritään hallitsemaan monimutkaisien systeemien kehitystä. Iivosen työssä (2011: 9–10) puolestaan esitetään muun muassa standardin ISO 10007:n näkemys, jonka mukaan konfiguraationhallinta sisältää tekniset ja organisatoriset toimenpiteet tuotteen konfiguraation ja informaation tunnistamiseksi, ohjaamiseksi, valvomiseksi ja auditoimiseksi. Aho (2009: 15) puolestaan esittelee työssään sandardin ANSI/EIA-649-A 2004 määritelmän, jonka mukaan konfiguraationhallinta on prosessi, jonka tehtävänä on varmistaa, että tuotteen ominaisuudet vastaavat sen vaatimuksia ja konfiguraation informaatiota koko elinkaaren ajan. (Seppänen 2000: 1; Iivonen 2011: 9–10; Tichy 2008: 1; IEC 61508-3 2010: 13–14; Aho 2009: 15.)

Määritelmissä on samoja elementtejä eri sanoin. Niiden avulla saa hyvän kokonaiskuvan konfiguraation tehtävästä ja merkityksestä prosessissa. Sen lisäksi, että konfiguraationhallinta määritetään prosessiksi, se on jonkin muun prosessin, kuten kelpoistusprosessin tärkeä tukitoiminto. Se on mukana tuotteen jokaisessa elinkaaren vaiheessa kuvassa 11 esitetyn esimerkin mukaisesti. Kuvan esimerkki soveltuu paitsi kelpoistusprosessiin, mutta myös mihin tahansa tuotteen suunnittelu- ja testausprosessiin. (Seppänen 2000: 1; Iivonen 2011: 9-10; Tichy 2008: 1; IEC 61508-3 2010: 13–14; Aho 2009: 44.)

Konfiguraationhallinta on iso kokonaisuus, joka muodostuu alalajeista, jotka myös koostuvat viidestä osa-alueesta. Alalajit ovat muun muassa ohjelmiston konfiguraationhallinta (*software configuration management,* SCM) ja laitteiston konfiguraationhallinta (*harware configuration management,* HCM). Näiden erottamisessa toisistaan on epäselvyyksiä. Ohjelmiston konfiguraationhallinta on monimutkaisten ohjelmistojen kehityksen ja elinkaarenhallintaa, joka sulautuu jokaiseen ohjelmistokehityksen vaiheeseen. Laitteiston konfiguraationhallinnassa puolestaan keskitytään laitteiden kehityksen ja elinkaaren hallintaan. (Tichy 2008: 1; Farah 2013; Niemelä 2006: 1.)



Kuva 11. Esimerkki konfiguraationhallinta ohjelmistopohjaisen järjestelmän kehitysprosessissa. (Muokattu lähteestä California Division 2014.)

Jotta suuria kokonaisuuksia, kuten kelpoistusprosessia, olisi helpompi hallita konfiguraationhallinnalla, jaetaan järjestelmä yksittäin tunnistettaviin, riittävän pieniin kokonaisuuksiin. Näistä kokonaisuuksista käytetään nimitystä konfiguraatioyksikkö (*configuration item*, CI). Ne voivat olla osajärjestelmiä, komponentteja, laitteita tai ohjelmia. Konfiguraatioyksiköitä käytetään paitsi helpottamassa suurien kokonaisuuksien hallintaa, mutta myös mittaamaan edistymistä ja laatua alkuperäisen suunnitelman ja lopullisen tuotteen välillä. (Iivonen 2011: 11; Aho 2009: 15; YVL B.1 2013: 7.)

3.5.1 Versionhallinta

Versionhallinta (*version control* tai *revision control*) on dokumenttien, ohjelmistojen ja tietokoneelle tallennettujen tiedostojen muutosten hallintaa koko tuotteen elinkaaren ajan. Sitä pidetään välttämättömänä toimintona ohjelmistotuotannossa niin isoissa kuin pienissäkin projekteissa. Menetelmän kehittäminen on lähtöisin tarpeesta palata aikaisempiin versioihin kehityksen tai suunnittelun jumiuduttua, tai halutessa paikantaa virheitä ja ongelmia edellisistä versioista. Lisäksi haluttiin projektin jokaisen jäsenen ole-

van ajan tasalla viimeisimmästä julkaistusta versiosta sekä helpottaa projektin sisäistä kommunikointia ja yhteistyötä. Perinteisesti versionhallintaa käytetään ohjelmistoprojekteissa, jossa se hallitsee paitsi dokumentaatioita, mutta myös konfiguraatiotiedostoja sekä lähdekoodia. (Kettunen 2009: 13; Git 2014; Yeates 2013; Aho 2009: 21; Majuri 2006: 8–14.)

Halminen (2001: 34–35) korostaa ydinvoimalaitoksien versionhallinnan roolin tärkeyttä laitteiden ja niiden varaosien valinnassa, sillä varaosaksi kelpuutetaan ainoastaan kelpoistettu versio vastaavasta tuotteesta. Jotta samaa tuotetta pystyttäisiin tilaamaan varaosiksi, on pystyttävä selvittämään laitteiden ja ohjelmistojen versiot. Uusien versioiden myötä laitteen ja ohjelmiston testaukseen voi tulla muutoksi, joiden takia onkin tärkeää, että toimittajan versionhallinta on ajan tasalla. (Halminen 2001: 35–37.)

Versionhallinnan avulla voidaan myös tallentaa muutokset tiedostoon tai tiedostoihin, jotta myöhemmin voitaisiin palata tarkastelemaan haluttua versiota. Jotta edellisten versioiden tarkastelu olisi mahdollista, versionhallinnassa käytetään versionhallintajärjestelmiä (*Version Control Systems*, VCS). Ne ovat erillisiä ohjelmistoja ja niiden avulla tiedoston tai koko projektin voi palauttaa edelliseen tilaan. Lisäksi sen avulla voidaan tarkastella, millaisia muutoksia esimerkiksi edelliseen versioon on tehnyt, kuka on viimeksi tehnyt muokkauksia, millaisia ongelmia on havaittu ja mikä on ongelmien mahdollinen aiheuttaja sekä kuka ongelman on esitellyt. Tällä tavoin tehdyt muutokset ovat jäljitettävissä ja tehdyille ratkaisuille löytyy perustelut. (Kettunen 2009: 13–20; Yeates 2013; Git 2014; Lenkkeri 2013.)

3.5.2 Muutostenhallinta

Muutostenhallinta (*change control*) on häilyvä käsite. Useimmiten sillä tarkoitetaan prosessissa tapahtuvien muutosten seuraamista, ennakointia, tunnistamista, arviointia ja hallintaa läpi prosessin. Jokainen tehtävä muutos täytyy määritellä, harkita ja hyväksyä ennen sen toteuttamista. Tällä tavalla pyritään välttämään tarpeettomat muutokset, jotka veisivät vain aikaa, rahaa ja työvoimaa. Muutostenhallinnan avulla mahdollistetaan on-

nistunut prosessi sekä varma ja laadukas ohjelmistokehitys. (Rouse 2011; Haughey 2011; Majuri 2006: 9.)

Muutostenhallinta on välttämättömyys prosessista ja sen koosta huolimatta. Se ei ole osa vain yhtä prosessia, vaan myös kaikkia siihen liittyviä prosesseja. Sitä käytetään muun muassa prosessin konfiguraationhallinnan, vaatimustenhallinnan lisäksi projektinhallinnassa. Sen avulla taataan prosessin ja järjestelmän jatkuva kehitys, kun tärkeitä muutoksia tehdään esimerkiksi vaatimuksiin tai järjestelmän tai ohjelmiston suunnitteluun ja kehitykseen. Tehtävät muutokset tulee dokumentoida, jotta niitä pystytään seuramaan sekä jäljittämään. (Haughey 2011; Carman 2013.)

3.6 Laatusuunnitelma

Laatusuunnitelman avulla taataan paitsi koko kelpoitusprosessin, mutta myös kelpoistettavan tuotteen laatu. Suunnitelmassa tulee olla kuvattuna yksityiskohtaisesti laatuvaatimukset ja laadunvarmistamista varten käytettävät menetelmät. Tällä tavoin pyritään välttämään virheitä ja riskejä. Suunnitelmassa on kuitenkin esitettävä kriittisten tilanteiden varalle, millä tavoin ne tunnistetaan ja ehkäistään. Laatusuunnitelman avulla varmistetaan prosessin onnistuminen. (YVL E.7 2013: 11–12; YVL B.1 213: 7−8.)

Laatusuunnitelma tulee laatia paitsi koko projektille, mutta myös projektissa suunniteltaville ja määriteltäville turvallisuuskriittisille järjestelmille ja järjestelmä ohjelmistolle sekä laitteille. Se on projektikohtainen sekä järjestelmä-, laite- ja ohjelmistokohtainen dokumentti, josta on käytävä ilmi kaikki vaiheet ja noudatettavat standardit ja ohjeet. Vaikka kehitettävälle tuotteelle on laadittava oma laatusuunnitelma, on se kuvattava yksityiskohtaisesti koko prosessin kattavassa laatusuunnitelmassa. Laatusuunnitelman laatimisessa voidaan hyödyntää asetettuja ohjeita ja standardeja, kuten standardia ISO 10005. (YVL A.3 2013: 13.)

Laatusuunnitelmasta on selvittävä jokaisessa prosessin vaiheessa tehtävät toiminnot. Lisäksi dokumentissa on kuvattava jokaisen vaiheen jälkeen tehtävät katselmoinnit, hyväksymiskriteerit sekä sovellettavat päätöksentekomenettelyt ja vastuut. Laatusuunni-

telmassa on kerrottava asiakirjat ja tallenteet, jotka laaditaan jokaisen vaiheen jälkeen. Siitä on myös käytävä ilmi prosessiin osallistuvat organisaatiot ja mahdolliset riippumattomat tarkastajat sekä niiden rajapinnat sekä tehtävät. Suunnitelmasta tulee selvitä myös, millä menetelmillä alihankkijoiden valvonta tullaan prosessissa toteuttamaan. (YVL B.1 2013: 7−8; YVL E.7: 11–12.)

Laatusuunnitelman tehtävänä on selkeyttää prosessia ja tuoda siihen järjestelmällisyyttä sekä pitää prosessin laatu jokaisessa vaiheessa vaaditulla tasolla. Dokumenttia päivitetään prosessin edetessä, jotta se pysyisi ajan tasalla. Laatusuunnitelman avulla pystytään selvittämään syntyvien dokumenttien oikeellisuus, sillä suunnitelmassa on oltava esitettynä, miten oikeellisuus voidaan osoittaa. (YVL B.1 2013: 7−8; YVL E.7 2013: 11−12.)

3.7 Dokumentointi

Dokumentointi on asiakirjojen hallintaa sekä seurannan apuväline. Sen avulla pyritään kuvaamaan järjestelmien, laitteiden ja ohjelmistojen rakennetta ja toimintoja prosessin jokaisessa suunnittelu- ja toteutusvaiheessa. Tossavainen (2007: 13) korostaa työssään dokumentoinnin merkitystä, kun halutaan ymmärtää monimutkaisia kokonaisuuksia esimerkiksi ohjelmiston tai ohjelmakoodin rakennetta. (IEC 61508-1 2010: 13; Tossavainen 2007:13.)

Dokumentoinnissa on pyrittävä hyvään tarkkuuteen ja yksiselitteisyyteen, sillä se on apuna muutosten huomioimisessa ja dokumenttien ajan tasalla pitämisessä läpi koko prosessin. Se on tärkeä osa järjestelmän ja sen ohjelmiston ja laitteiden elinkaarta. Dokumentointi on myös tärkeä osa, kun yritetään paikantaa suunnittelussa ja toteutuksessa tehtyjä virheitä. Ilman dokumentteja se olisi melkein mahdotonta. Siksi onkin tärkeää, että dokumentit ovat identifioituja ja dokumentinhallinnan alaisena. Näin varmistetaan, että tarkastelussa on oikea dokumentti ja siitä viimeisin versio. (Tossavainen 2007: 13–15; IEC 61508-1 2010: 13–14.)

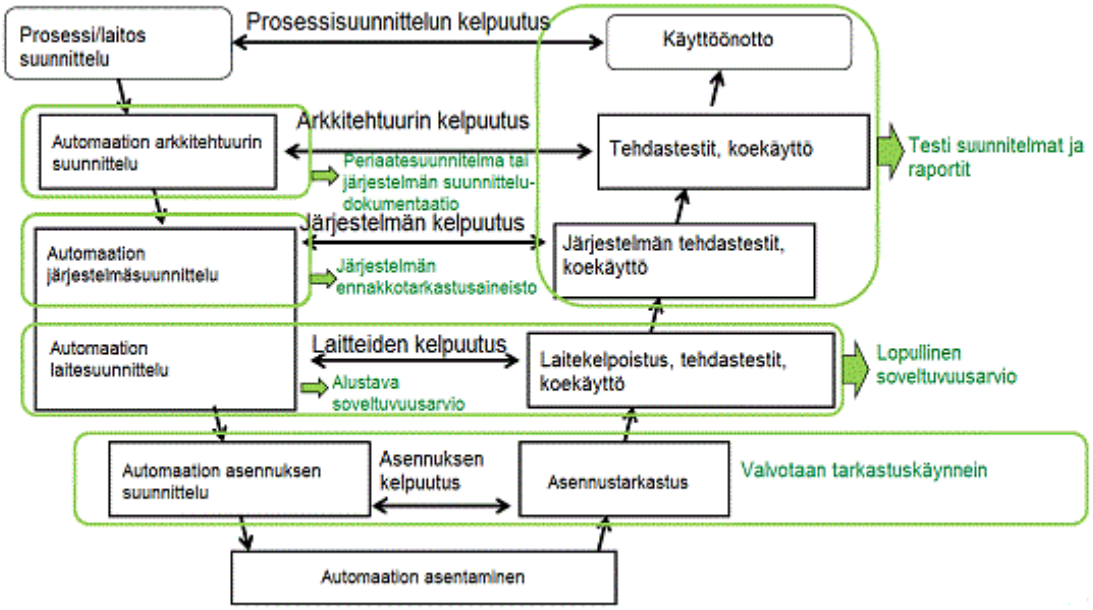
Jokainen dokumentti on pystyttävä tarkistamaan oikeanlaiseksi sekä arvostelemaan ja toteamaan hyväksytyksi. Tämä on tärkeää, sillä dokumenttien avulla tulee kelpoistuk-

sessa pystyä osoittamaan turvallisuuskriittisten järjestelmien sekä niiden laitteiden täyttävän asetetut vaatimukset. Samalla pystytään selvittämään niiden sopivan suunniteltuun käyttötarkoitukseen ja käyttöympäristöön. Kuvassa 12 näkyy paitsi esimerkki kelpoistuksen etenemisestä, mutta myös esimerkki viranomaiselle laitettavista dokumenteista kelpositusprosessin aikana.

3.8 Kelpoistusproseduuri

Kelpoistuksessa tarkastellaan tuotteen elinkaaren vaiheiden laatua, jota arvioimalla osoitetaan tuotteen luotettavuus jokaisessa prosessin vaiheessa. Samalla osoitetaan, että ohjelmistopohjainen laite toteuttaa asetetut vaatimukset myös ohjelmiston osalta. Lisäksi ohjelmoitavan järjestelmän kelpoistuksen on sisällettävä niin perusjärjestelmä kuin sovelluskin. Ohjelmiston kelpoistus on kuitenkin erittäin haastavaa, sillä ohjelmiston täydellinen testaaminen on mahdotonta. Kaikkia vikoja ei pystytä välttämättä havaitsemaan testaamalla, testitapauksia on useita ja viat voivat ilmetä erilaisilla tavoilla, joita ei välttämättä ole osattu odottaa. Tämän takia tuotteen laadukkaalla suunnittelulla ja valmistuksella on tärkeä rooli kelpoistuksessa testauksen rinnalla. (YVL E.7 2013: 18; Kasurinen 2013: 19–20.)

Kelpoistusprosessi koostuu useista prosessivaiheista, kuten määrittelystä, suunnittelusta ja testauksesta. Kelpoistusprosessissa nämä eri vaiheet kelpuutetaan kuvassa 12 esitetyn esimerkkimallin mukaisesti tehtävien tarkastusten ja testien avulla prosessin edetessä. Kelpoistusprosessi käynnistyy tarpeesta, jolla tarkoitetaan vastaavan tuotteen löytämistä uudesta tekniikasta vanhan tuotteen valmistuksen loputtua, uusien ominaisuuksien lisäämistä tai hajonneen osan korvaamista ehjällä. Tekniikan kehittyessä samanlaista laitetta voi olla haastava löytää, jolloin toimittaja ehdottaa vastaavasta laitteesta sopivaa, uudempaa versiota korvaajaksi. (STUK YVL E.7 2013: 30–34; Wahlström 2013; Halminen 2001: 26.)



Kuva 12. Esimerkki automaatiojärjestelmän kelpoistusprosessin etenemisestä. (Muokattu lähteestä Wahlström 2013: 14.)

Kelpoistusprosessi etenee samalla tavalla kuin muutkin suunnitteluprosessit. Etenemiseen kuitenkin vaikuttaa kelpoistettavan tuotteen turvallisuusluokka. Ennen kaikkea kelpoistusprosessin onnistuminen on kiinni alusta asti oikein laaditusta vaatimusmäärittelystä. Vaatimusmäärittelyn tulee olla riittävän yksityiskohtainen, ennen kuin tuote voidaan valita tilattavaksi. Vaatimusten selvittäminen aloitetaan kartoittamalla korvattavan tuotteen vaatimukset sekä selvittämällä, onko tuotteelle tullut uusia vaatimuksia. Vaatimusmäärittelystä on selvittävä projekti-, järjestelmä- ja laitekohtaiset vaatimukset. Lisäksi on huomioitava voimalaitoksen yleiset turvallisuusvaatimukset sekä selvitettävä tarvittavista standardeista tulevat vaatimukset, sekä viranomaisvaatimukset joita on noudatettava. Tämän jälkeen voidaan koota vaatimusmäärittely. (YVL E.7 2013: 30.)

Vaatimusmäärittelyä päivitetään kelpoistusprosessin edetessä. Niiden on oltava riittävän yksityiskohtaiset siirryttäessä seuraavaan vaiheeseen, jota vasten todennukset tulee tehdä. Vaatimusmäärittelyjen lisäksi selvitetään alussa myös muut järjestelmää koskevat taustatiedot, joiden pohjalta vaatimusmäärittelyjen kanssa pystytään selvittämään järjestelmän rakennetta, toimintoja sekä toteutusperiaatteita koskevat alustavat määritykset.

Kerättyjen taustietojen ja alustavien suunnitelmatietojen perusteella laaditaan periaatesuunnitelma, joka välitetään viranomaiselle hyväksyttäväksi. Dokumentissa tulee olla YVL E.7 -ohjeen mukaiset tiedot mukana. (YVL E.7 2013: 30.)

Suunniteltava järjestelmä on pystyttävä arvioimaan soveltuvaksi sille tarkoitettuun käyttökohteeseen ja -ympäristöön. Lisäksi on kyettävä arvioimaan järjestelmän ja sen laitteiston laatu, jonka pohjalta pystytään toteamaan järjestelmän, sen laitteiden ja ohjelmiston suunnittelun olevan tarkoituksen mukaista. Ohjelmistopohjaisten järjestelmien sekä järjestelmän laitteiden arvioinneissa hyödynnetään saatavilla olevia dokumentteja, ja ne on toteutettava yhdenmukaisesti standardin IEC 60880 asettamien vaatimusten kanssa. Arvioinnit suoritetaan järjestelmän suunnittelussa, jossa suunnitellaan myös järjestelemän laitteiden ja ohjelmiston tarkempaa rakennetta. Tuloksena tästä vaiheesta on ennakkotarkastusaineisto (ETA) sekä alustava soveltuvuusarvio, jotka lähetetään viranomaiselle YVL E.7 -ohjeen mukaisesti. (IEC 60880 2006: 117; YVL E.7 2013: 30–34.)

Suunnitteluvaiheiden lopuksi on toteutusvaihe, jossa tuote valmistetaan. Luvanhaltija valvoo tuotteen valmistusta, integrointia ja tehdastestejä. Säteilyturvakeskus valvoo valmistusta ja tehdastestejä luvanhaltijan kanssa. Lisäksi valvontaan voi osallistua tarvittaessa kolmas osapuoli. Valvonta toteutetaan tarkastuskäynneillä, joihin toimittaja välittää hyvissä ajoin kutsun luvanhaltijalle, joka välittää kutsun viranomaiselle. Tehdastestien jälkeen järjestelmän laitteet toimitetaan voimalaitokselle ja ne asennetaan paikoilleen oikeaan käyttöympäristöön. Varsinainen kelpoistus suoritetaan asennuksen jälkeen. Ennen sitä on kuitenkin suoritettava asennustarkastus sekä toiminnalliset testit ja koestus. Näiden avulla testataan laitteiden oikeellisuus. Koekäytössä, joka suoritetaan koestuksen ja toiminnallisten testien jälkeen, testataan koko järjestelmän toimivuutta oikeassa käyttöympäristössään. (YVL E.7 2013: 33–34.)

Liitteessä 3 on esitetty standardin IEC 60880 kaavio kelpoistuksesta.

4 KELPOISTUSPROSESSIMALLIN KEHITTÄMINEN

Kelpoistusprosessimallin avulla esitetään kelpoistusprosessiin kuuluvat vaiheet sekä vaiheiden sisältö. Sen tehtävänä on auttaa hahmottamaan roolijakoa muun muassa TVO:n sisäisessä toiminnassa sekä TVO:n, viranomaisen ja toimittajan välillä. Prosessimallin avulla selviää, missä järjestyksessä tehtävät tulisi tehdä, sekä mitkä tekijät vaikuttavat toisiinsa. Kelpoistusprosessimallissa myös annetaan esimerkkejä muun muassa siitä, mitä viranomaisaineistot sisältävät sekä, missä vaiheessa prosessia ne tulisi lähettää viranomaiselle hyväksyttäväksi.

Kelpoistusprosessimallin kehittäminen lähti liikkeelle tarpeesta luoda riittävän yksityiskohtainen prosessimalli, josta olisi apua prosessin vaiheiden seuraamisessa ja dokumentteja laatiessa. Prosessimallin luominen aloitettiin käsitteen ”kelpoistus” selvittämisestä ja ymmärtämisestä, mitä kelpoistusprosessiin kuuluu. Tässä auttoivat kelpoistusta käsittelevät standardit ja erityisesti YVL-ohjeista YVL E.7 -ohje. Lisäksi keskustelu eri henkilöiden kanssa avarsi näkemystä, miten kelpoistusprosessin tulisi edetä, ja mitä vaiheita siihen pitäisi sisältyä. Myös Wahlstömin tekemistä esityksistä (Wahlström 2013; Wahlström 2011) oli apua kokonaisuuden hahmottamisessa.

Yhtenä vaatimuksena kelpoistusprosessimallin kehittämisessä oli saada se yhtenäiseksi muiden TVO:n prosessimallien kanssa. Tässä auttoi TVO:lle kehitetty uusi muutostyöprosessimalli. Esimerkiksi kelpoistusprosessimallin vaiheet nimettiin vastaaviksi muutostyöprosessimallin kanssa. Myös piirustusohjelma QPR, jolla prosessimalli luotiin, helpotti samankaltaisuuden luomisessa ja prosessimallin tekemisessä. Lisäksi piirustusohjelman avulla pystytään liittämään linkki TVO:n dokumentteihin ja ohjeisiin, joita voidaan käyttää esimerkiksi mallipohjina viranomaisaineistoja laadittaessa.

Kelpoistusmallia kehittäessä aloitettiin yhteistyö Softability Group Oy:n kanssa, sillä huomattiin, että ohjelmistoille tarvittiin tarkemmat ohjeet kelpoistukseen sekä oma ITP (*Inspection ad Testing Plan*) -suunnitelman mallipohja. Softability Group Oy:n laatima ohje sisältää ohjeita ja tarkastuslistoja kelpoistusprosessimallin eri prosesseihin ja osatehtäviin pyrkimyksenä taata laadukas ohjelmiston suunnittelu ja toteutus. Ohjeessa keskitytään erityisesti kelpoistusprosessissa suoritettavaan toimittajan arviointiin ja au-

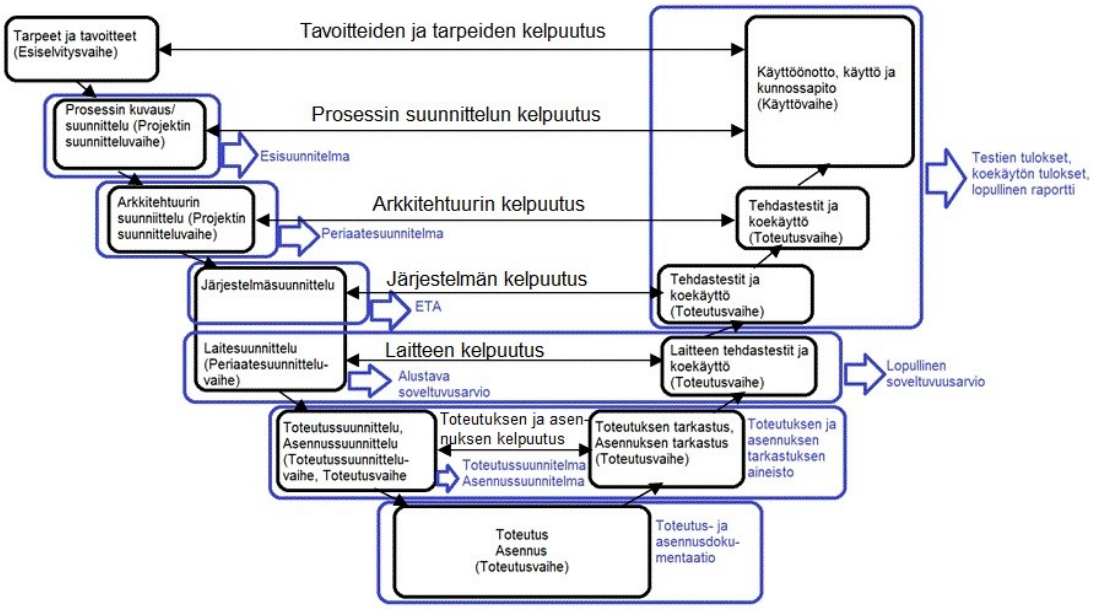
ditointiin sekä ohjelmiston vastaanottoon. Lisäksi ohjeissa keskitytään myös ITP-suunnitelman valvomiseen. Ohjelmiston kelpoistusohjeiden on tarkoitus valmistua syksyn 2014 aikana. Ohje tullaan liittämään kelpoistusmalliin oikeisiin kohtiin ohjeistukseksi. Tähän mennessä ohjeet ovat kutakuinkin valmiina, mutta ITP-suunnitelman mallipohjaa hiotaan vielä. Ohjeiden lisäksi on pohdittu, miten kehitteillä ollutta Nuclear SPICE -mallia voitaisiin hyödyntää kelpoistusprosessimallissa. Nuclear SPICE on turvallisuuskriittisten järjestelmien ja ohjelmistojen prosessien kyvykkyyden ja ydinvoimastandardien mukaisuuden arviointimalli. Toistaiseksi tämän osalta ei ole tehty mitään konkreettista kehitettyyn kelpoistusprosessimalliin.

Haasteellista kelpoistusprosessimallin kehittämisessä teki tavoite saada prosessimallista mahdollisimman selkeä, johdonmukainen ja helposti ymmärrettävä, koska prosessimallin eri vaiheet sisälsivät useita osioita ja aliprosesseja. Lisäksi oli vaikeaa hahmottaa, mitä kaikkea eri vaiheet sisälsivät, mitä näistä tulisi avata enemmän, ja mitä suunnitelmia ja dokumentteja eri vaiheissa laaditaan. Suurena apuna tässä oli YVL E.7 -ohjeen liitetiedosto kaaviokuvat sekä saadut neuvot. Kelpoistusprosessimallin kehittämisessä haastavaa oli myös tuoda eri tekniikan alat näkyviin tekemättä kokonaisuudesta epäselvää. Erityisesti ohjelmoitavuuden korostaminen prosessimallissa osoittautui haastavaksi. Apua ongelmaan tuli asiantuntijoilta, standardeista, kirjoista sekä artikkeleista, joiden avulla tietämys lisääntyi ja näkemys asiasta kehittyi.

Tässä kappaleessa esitellään kehitetty kelpoisusprosessimalli ja sen vaiheet, muttei liian yksityiskohtaisesti. Tavoitteena on antaa kuva, mitä eri vaiheissa tuotetaan, ja mikä näiden vaiheiden rooli on kelpoitusprosessissa.

4.1 Valmis kelpoistuprosessimalli

Aloitettaessa muodostamaan kelpoistusrosessimallia oli pohdittava, mitä prosessimalliesitystapaa käytettäisiin. Vuokaavion tapainen ratkaisu, joka etenisi virtaustyyppisesti, oli luontevin vaihtoehto, sillä myös muut TVO:n prosessimallit etenevät kutakuinkin tällä tavalla. Joissakin on käytetty myös vesiputousmallia.



Kuva 13. Pelkistetty kelpoistusprosessimalli. (Perustuu kehitettyyn kelpoistusprosessimalliin liitteenä 4 sekä lähteisiin Wahlström 2013: 14 ja Österholm 2005.)

Tätä kappaletta varten prosessimalli kuitenkin päätettiin yksinkertaistaa yllä olevassa kuvassa 13 esitettyyn v-mallin muotoon. Prosessimallin viemisessä v-mallin muotoon hyödynnettiin Wahlströmin esitystä sekä Österholmin laatimaa v-mallia. Itse valmis malli on nähtävissä liitteenä 4.

Kelpoistusprosessimalli koostuu yhteensä kuudesta vaiheesta, jotka on nimetty kuvan 13 laatikoissa sulkeisiin. Kelpoistusprosessimallin vaiheet ovat esiselvitysvaihe, projektin suunnitteluvaihe, perussuunnitteluvaihe, toteutussuunnitteluvaihe, toteutusvaihe ja käyttövaihe. Vaiheiden tehtävä on täydentää toisiaan ja niiden syötteenä onkin edellisessä vaiheessa tehty päätös. Lisäksi jokaisen vaiheen on täytettävä edellisessä vaiheessa laaditut vaatimukset. (Wahlström 2013: 12–14; IEC 61508-3: 17.)

4.1.1 Esiselvitysvaihe

Kuten kuvasta 14 voidaan havaita, selvitetään esiselvitysvaiheessa prosessin tavoitteet, tarpeet, laajuus sekä vaatimukset, joita tulee muun muassa voimalaitokselta käyttökoh-

teesta sekä muista järjestelmistä. Lisäksi on selvitettävä noudatettavat standardit ja YVL-ohjeet. Jos kelpoistettavassa järjestelmässä on ohjelmistoa, se tulee huomioida noudatettavissa standardeissa. Esiselvitysvaiheessa otetaan kantaa myös riskeihin, hankkeen kannattavuuteen, kustannuksiin, aikatauluun sekä hieman prosessinlaajuuteen, johon vaikuttaa muun muassa tuotteen turvallisuusluokka. Toisin sanoen esiselvitysvaiheessa laadittu esiselvitys on pohja koko prosessille. Esiselvitys on laadittava huolella, sillä huonosti toteutettu esiselvitys voi edesauttaa prosessin hankaloitumista sekä hidastumista. (Kalanen 2012.)

Kelpoistusprosessin esiselvitysmallissa kartoitetaan suunnitteluperusteet, laaditaan vaatimusmäärittelyn runko sekä laaditaan alustava tietoturvasuunnitelma, joka noudattaa TVO:n ohjeistusta. Lisäksi esiselvitysvaiheessa selvitetään prosessille eri ratkaisumallit ja toimittajaehdokkaat. Esiselvitystä laadittaessa on muistettava, että sen on oltava linjassa organisaation, tässä tapauksessa TVO:n, strategian ja tavoitteiden kanssa. (Kalanen 2012.)

Esiselvitykselle on tehtävä riittävän laaja tarkastuskierros ennen sen esittelyä jatkosta päättävälle taholle. Päätöksen tekevä taho päättää siirtymisestä seuraavaan prosessin vaiheeseen (projektin suunnitteluvaihe), projektipäälliköstä sekä projektin ohjausryhmästä.

4.1.2 Projektin suunnitteluvaihe

Projektin suunnitteluvaihe koostuu kehitetyssä kelpoistusprosessimallissa esisuunnittelusta, johon sisältyy alustavan projekti- ja laatusuunnitelman sekä esisuunnitelman laatiminen. Edellisellä sivulla esitetyn kuvan 13 mukaisesti tässä suunnitteluvaiheessa pyritään kuvaamaan prosessi ja sen eteneminen sekä suunnittelemaan kelpoistettava järjestelmä sen arkkitehtuuritasolla. Tästä on selvittävä muun muassa järjestelmän alijärjestelmät, toimintoja sekä toimintojen toteutusperiaatteet vähintään karkeasti esitettynä. Arkkitehtuuritason suunnitelmasta on käytävä ilmi, jos järjestelmässä on ohjelmistoa. Projektin suunnitteluvaihe on toteutettava esiselvitysvaiheen tavoin huolella, jotta hankaloitumis- ja hidastumisriski pienenisi. (MITRE 2014a; MITRE 2014b.)

Projektin suunnitteluvaiheessa laadittavan esisuunnitelman on oltava riittävän selkeä, jotta sen perusteella voidaan tehdä ja toteuttaa investointipäätös. Esisuunnitelmassa täsmennetään ja päivitetään esiselvityksessä laaditut karkeat suunnitelmat sekä vaatimukset. Lisäksi arvioidaan esiselvitysvaiheessa kartoitetut ratkaisumallit ja valitaan niistä yksi, jonka mukaan prosessi suositellaan toteutettavaksi. (Novox Oy 2014.)

Esisuunnitelman laatimisen rinnalla toteutettavassa alustavassa projekti- ja laatusuunnitelmassa varataan resurssit sekä määritetään laajuus, aikataulu ja kustannusarvio esiselvityksessä selvitettyjen tietojen perusteella. Näihin vaikuttaa myös esisuunnitelmaa laadittaessa tehtävä alustava kelpoistussuunnitelma. Vastaavasti alustava projekti- ja laatusuunnitelma vaikuttaa esisuunnitelman laatimiseen. Laaditulle esiselvitykselle on tehtävä riittävän laaja tarkastuskierros ennen kuin siitä laaditaan esitys investointipäätökseen, jossa tehdään päätös perussuunnitteluvaiheeseen etenemisestä.

Näiden suunnitelmien lisäksi projektin suunnitteluvaiheessa määritetään ja laaditaan alustavat tarjouspyynnöt toimittajaehdokkaille, joille tehdään tarvittaessa arviointi. Arvioinnissa selvitetään, onko toimittaja kykenevä täyttämään vaaditut vaatimukset esimerkiksi laadun suhteen. Toimittajan tekemä tarjous ja toimittajalle tehty arviointi vaikuttavat investointipäätöksen tekoon.

Projektin suunnitteluvaiheen lopuksi laaditaan viranomaisen ohjeiden mukainen periaatesuunnitelma, joka lähetetään viranomaiselle hyväksyttäväksi. Periaatesuunnitelman hyväksyntä vaikuttaa tarjouksen ja arviointituloksen tavoin investointipäätökseen ja perussuunnitteluvaiheeseen etenemiseen.

4.1.3 Perussuunnitteluvaihe

Perussuunnitteluvaiheessa laaditaan kuvan 13 (sivulla 53) mukaisesti järjestelmä- ja laitesuunnitelma. Ne laaditaan perussuunnitteluvaiheeseen kuuluvassa järjestelmän suunnittelussa. Järjestelmäsuunnitelmassa selvitetään mitä laitteistoja ja ohjelmistoja järjestelmä tarvitsee. Laitesuunnitelmassa puolestaan esitetään muu muassa laitteistot, käyttöjärjestelmät ja ohjelmistot. Suunnitelmissa on otettava kantaa myös käyttöönottoon ja huoltoon. Suunnitelmat laaditaan yhdessä toimittajan kanssa, jolle määritellään järjes-

telmä- ja laitteistosuunnitteluaineiston vaatimukset ja rajoitteet. Näistä selviää muun muassa järjestelmän ja sen laitteiston käyttöpaikkakohtaiset vaatimukset. (YVL E.7 2013: 31−32.)

Järjestelmäsuunnitelma ja laitesuunnitelma ovat osa kehitetyn kelpoistusprosessimallin perussuunnitteluvaihetta. Tähän vaiheeseen sisältyy järjestelmän suunnittelun lisäksi auditointi ja arviointi sekä projekti- ja laatusuunnitelman laatiminen. Auditoinnissa ja arvioinnissa selvitetään muun muassa, onko toimittajan laatujärjestelmä vaatimusten mukainen, ja täyttävätkö toimittajan tuotteen valmistukseen liittyvät prosessit asetetut vaatimukset. Auditoinnissa pyritään selvittämään, toteutetaanko tuotteen valmistus laadukkaasti ja vaatimusten mukaisesti. Aina auditointia ei tarvitse tehdä, tällöin toteutetaan arviointi. Arvioinnissa pyritään selvittämään laadullisuus toimittajalta saatujen, tarvittavien dokumenttien avulla. (Laatukeskus 2014.) Projekti- ja laatusuunnitelmassa päivitetään projektin suunnitteluvaiheessa laadittu alustava projekti- ja laatusuunnitelma. Lisäksi tarpeen vaatiessa toimittajan on toimitettava TVO:lle projektisuunnitelma omasta osuudestaan. Toimittajan tulee toimittaa muun aineiston lisäksi TVO:lle testisuunnitelmat hyväksyttäväksi.

Kuten edeltäneissäkin suunnitteluvaiheissa, laaditaan järjestelmän suunnittelusta esitys, joka vaikuttaa päätökseen siirtyä toteutussuunnitteluvaiheeseen. Päätökseen vaikuttavat esityksen lisäksi myös viranomaisen hyväksymät aineistot, jotka laaditaan perussuunnitteluvaiheen loppupuolella. Viranomaisaineistoon kuuluu ennakkotarkastusaineisto ja alustava soveltuvuusarvio. Näiden aineistojen on oltava viranomaisen ohjeiden mukaisia.

4.1.4 Toteutussuunnitteluvaihe

Toteutussuunnitteluvaihe koostuu kelpoistusprosessimallissa sivun 53 kuvan 13 mukaisesti toteutussuunnittelusta. Toteutussuunnittelussa laaditaan järjestelmän tekniikkakohtaiset toteutussuunnitelmat, jotka kuvaavat, miten esimerkiksi laitteistot testataan, asennetaan, otetaan käyttöön ja miten niistä tulee osa järjestelmää. Suunnitelmassa työt vaiheistetaan tarkempiin kokonaisuuksiin. Lisäksi siinä pyritään kuvaamaan laite ja ohjelmisto mahdollisimman yksityiskohtaisesti listaamalla niiden toiminnot, asennusohjeet

sekä arvioimaan aikataulut esimerkiksi testien suorittamiseen. (Oikarinen 2013: 1; Teknologiateollisuus ry 2014; Maryland. Gov 2014: 1.)

Toteutussuunnitteluvaiheessa laaditaan toteutussuunnitelmien lisäksi toteutussuunnittelun aineiston vaatimukset sekä rajoitteet toimittajalle. Näiden avulla toimittaja pystyy päivittämään omat suunnitelmansa ja toimittamaan ne TVO:lle tarkasteltavaksi. Toimittaja päivittää myös laitteistojen ja ohjelmistojen testisuunnitelmansa ja välittää ne TVO:lle. Lisäksi TVO:lla laaditaan alustavat suunnitelmat laitoksella tehtävistä koestuksesta ja koekäytöstä. Toteutussuunnitteluvaiheessa määritellään myös, mitä hankintoja on tehtävä, sekä mitkä vaiheet TVO suorittaa omilla resursseillaan ja sisäisillä palveluillaan. Toteutussuunnittelussa siis pyritään työstämään yksityiskohtaista aineistoa, jonka avulla seuraava vaihe (toteutusvaihe) pystytään toteuttamaan. Jotta päätös toteutusvaiheeseen siirtymisestä voidaan tehdä, on järjestelmän suunnittelusta laadittava esitys.

4.1.5 Toteutus- ja käyttövaihe

Kelpoistusprosessimallissa toteutusvaihe koostuu valmistus- ja tehdastesti osiosta sekä toteutus ja koekäyttö osioista. Näitä vaiheen osioita ei kuitenkaan ole erikseen nimetty sivun 53 kuvassa 13. Käyttövaiheeseen puolestaan sisältyy kuvan 13 mukaisesti käyttöönotto, käyttö ja lopullisten tulosten raportointi viranomaiselle. Jotta käyttövaiheeseen voidaan siirtyä, tarvitaan viranomaiselta hyväksyntä käyttöönottotarkastuksesta, joka suoritetaan toteutusvaiheessa koekäytön lopuksi.

Toteutusvaiheen ensimmäisessä osiossa, valmistus- ja tehdastesteissä suoritetaan toteutuksen aikainen valvonta, johon sisältyy muun muassa ohjelmiston toteutuksen tarkastelu. Tässä osiossa suoritetaan myös tehdastestien ja yhdistelmätestien valvonta, jotta varmistutaan järjestelmän laitteistoineen ja ohjelmistoineen toimivan halutulla tavalla myös vikatilanteissa. Testien tulosten perusteella pystytään päivittämään koestus-, yksikkötoimintakoe- ja koekäyttösuunnitelma. Valmistus- ja tehdastesti -osiossa päivitetään tarvittaessa laaditut asennussuunnitelmat sekä valmistellaan asennus suunnittelemalla tuotteen laitokselle vienti, asennuksen valvonta sekä asennuksen tarkistuslista. Tästä osiosta saadaan loput aineistot lopulliseen soveltuvuusarvioon, joka lähetetään viranomaiselle hyväksyttäväksi. Lisäksi viranomaisaineistoon kuuluvat myös laadittu

koekäyttösuunnitelma aikatauluineen, jolle haetaan myös viranomaisen hyväksyntää. (YVL E.7 2013: 33.)

Valmistus ja tehdastesti -osiosta siirrytään toteutus-osioon, jossa tuote vastaanotetaan TVO:lla. Tuotteelle tehdään vastaanottotarkastus, joka koostuu vastaanoton lisäksi saapumistarkastuksesta ja laatutarkastuksesta. Vastaanottotarkastuksen jälkeen tuote viedään tapauksesta riippuen varastoon tai suoraan asennettavaksi. Asennusta valvotaan asennustyön ajan ja asennukselle suoritetaan asennustarkastus sekä sähköturvallisuustarkastus, joiden jälkeen voidaan siirtyä suorittamaan koestusta ja yksikkötoimintakokeita laadittujen suunnitelmien mukaisesti. (YVL E.7 2013: 33–34.)

Toteutusosiosta siirrytään koekäyttöosioon, jossa järjestelmälle suoritetaan koekäyttö viranomaisen valvonnassa. Ennen koekäyttöä suoritetaan käyttöönottotarkastuksen ensimmäinen osa, jossa todetaan järjestelmän koekäyttövalmius. Koekäytössä järjestelmää ajetaan tietynaikaa sen oikeassa käyttöympäristössä ja käyttöpaikassa. Koekäytöstä saatu tulosraportti välitetään viranomaiselle hyväksyttäväksi. Koekäytön jälkeen suoritetaan toinen osa käyttöönottotarkastuksesta, jossa laaditaan pöytäkirja. Tämän jälkeen viranomainen suorittaa harkinnanvaraisesti vielä järjestelmän käyttöönottotarkastuksen, jonka lopputuloksena järjestelmälle voidaan myöntää käyttöönottolupa. (YVL E.7 2013: 34.).

5 KELPOISTUSPROSESSIMALLIN TOIMIVUUDEN OSOITTAMINEN

Kelpoistusprosessimallin kehityksessä on sovellettu konstruktiivista tutkimusmenetelmää. Kehitetyn konstruktion, kelpoistusprosessimallin toimivuuden osoittaminen toteutetaan kehityksen aikaisten katselmointien ja haastattelujen lisäksi prosessimallin valmistuttua kolmella case-tarkastelulla. Tarkastelujen laitteet ja järjestelmä on jo kelpoistettu poistuvien YVL-ohjeiden mukaisiksi. Poistuvilla ja uusilla YVL-ohjeilla, joiden mukaan malli on kehitetty, ei ole suuria eroavaisuuksia, joten kelpoistettujen tuotteiden kelpoistusprosessi ja kehitetty kelpoistusprosessimalli ovat keskenään vertailukelpoisia.

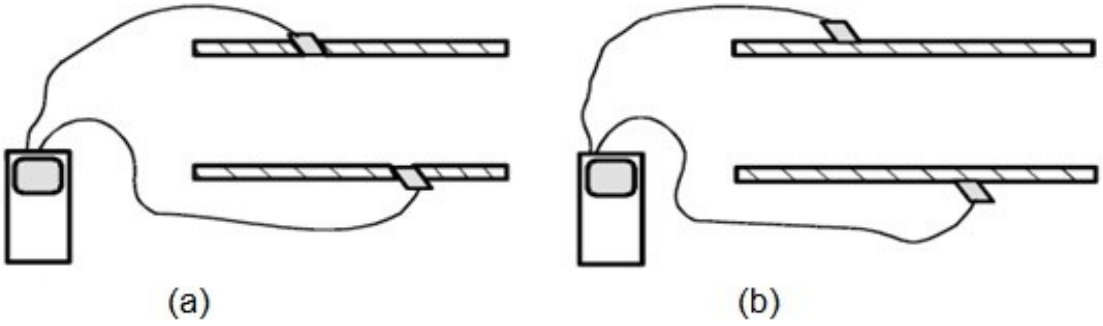
Tapaustarkasteluissa verrataan tehdyn kelpoistusprosessin etenemistä kehitettyyn kelpois-tusprosessimalliin muun muassa laadittujen viranomaisaineistojen ja haastatteluiden avulla. Tällä tavoin pyritään selvittämään, soveltuuko kehitetty kelpoistusprosessimalli tarkastelukohteena olevan tuotteen kelpoistusprosessin toteuttamiseen. Jokaisessa tarkastelussa mukana on henkilö, joka tuntee kyseisen tapauksen tuotteen suunnittelu- ja kelpoistusprosessin. Haastattelemalla tarkasteluihin osallistuvia henkilöitä pyritään selvittämään kehitetyn prosessimallin hyödyllisyys ja mahdolliset korjaustarpeet, joiden avulla prosessimallia voitaisiin kehittää lisää siten, että tulevat käyttäjät hyötyisivät siitä mahdollisimman paljon.

Tässä osiossa esitellään vertailukohteet sekä niiden toimintaperiaate. Lisäksi käsitellään tarkastelusta saatuja tuloksia ja niiden pohjalta tehtäviä päätelmiä. Lopuksi yhteenvedossa pohditaan, miten mallia voisi kehittää, ja voiko kaikkiin haasteisiin vaikuttaa. Ultraäänivirtausmittarin tarkasteluun osallistui Pasi Björklöf, suojareleen tarkasteluun Kimmo Kopra ja päähöyryputken säteilynmittausjärjestelmän tarkasteluun puolestaan Juha Halminen.

5.1 Tapaus 1: Ultraäänivirtausmittari.

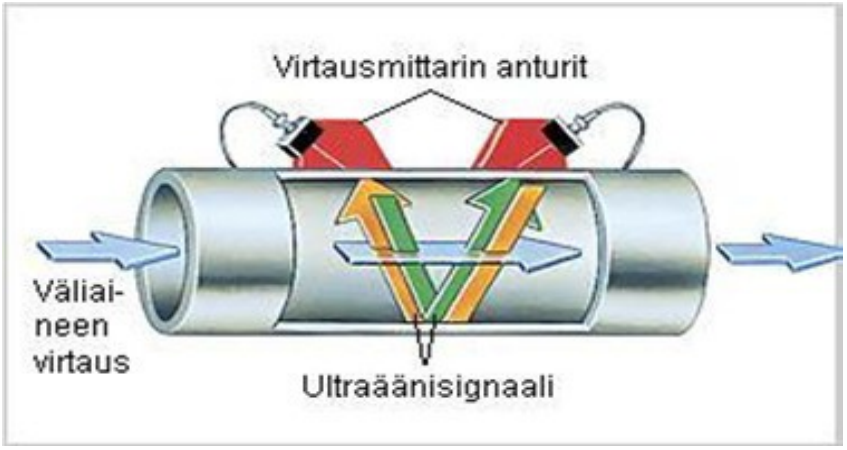
Ultraäänivirtausmittareiden toiminta perustuu ultraääneen, jonka avulla saadaan mitattua virtausputken nesteen virtaus. Ultraäänimittareita on kahdentyyppisiä, joista perinteiset vaativat valmiin asennuspaikan toisin kuin "*clamp-on*" tekniikalla toimivat, jotka asennetaan

putken päälle. Kuvassa 14 voidaan havaita perinteisen ultraäänivirtausmittarin ja clamp-on ultraäänivirtausmittarin asentamisen eroavaisuus. (Asikainen 2000: 16; Mård 2012: 8.)



Kuva 14. Ultraäänivirtausmittareiden asennustavat; perinteinen (a) ja clamp-on (b). (Asikainen 2000: 16.)

Molemmat mittarityypit tarvitsevat toimiakseen anturiparin, joista toinen lähettää signaalin myötävirtaan ja toinen vastavirtaan. Anturit vastaanottavat toistensa lähettämät signaalit. Signaalien vastaanottoaikojen erosta pystytään laskemaan nesteen virtaama ja virtauksen suunta. Kuvassa 15 on esitetty clamp-on tekniikalla toimivan ultraäänimittarin mittausperiaate. (Björklöf 2012; Mård 2012: 8.)



Kuva 15. Clamp-on tekniikkaan perustuvan ultraäänivirtausmittarin mittausperiaate. (Mård 2012: 8.)

Kelpoistusprosessimallin toimivuuden tarkastelussa käytettävä ultraäänivirtausmittari on ohjelmistopohjainen, clamp-on tekniikkaan perustuva virtausmittari. Laite koostuu lähettimestä ja lähettimeen yhdistetyistä ultraääniantureista. Ultraäänivirtausmittari kuuluu turvallisuusluokkaan 3. (Björklöf 2012.)

Tehdyssä tarkastelussa havaittiin, että kehitetty kelpoistusprosessimalli oli liian yksityiskohtainen siihen nähden, mitä tarkasteltavan laitteen prosessi olisi vaatinut. Esimerkiksi ultraäänivirtausmittarille oli laadittu viranomaisaineistosta vain soveltuvuusarvio, kun taas prosessimalliin on merkitty YVL E.7 -ohjeessa mainitut, viranomaiselle laadittavat aineistot. Tosin viranomaisaineisto oli sisältänyt kaiken vaadittavan materiaalin, kuten vaatimukset, laitteen kuvauksen, laitteen ohjelmiston arvioinin, tiedot käyttökokemuksista sekä toimittajasta. Eron voi selittää sillä, että vastaavaa laitetta oli ollut jo laitoksella EYT-luokituksella, mikä oli hieman helpottanut ultraäänivirtausmittarin kelpoistusta turvallisuusluokkaan 3 muun muassa esiselvityksen ja muun aineiston suhteen.

Tarkastelussa selvisi, että ultraäänivirtausmittarille tehty kelpoistusprosessi pitkittyi toimittajan kanssa tehtävän sopimuksen myötä. Lisäksi laitteiden testeihin oli kulunut arveltua enemmän aikaa. Näistä huolimatta prosessi oli kuitenkin edennyt kutakuinkin johdonmukaisesti. Tarkastelussa havaittiinkin, että prosessimalli ja aikaisemmin tehty kelpoistusprosessi etenivät samalla tavalla ja niissä oli samoja elementtejä, vaikka osin eri nimillä (esimerkiksi alustava ja lopullinen soveltuvuusarvio verrattuna soveltuvuusarvio) (YVL E.7 2013: 22). Tarkastelun lopputuloksena voidaan tiivistää kehitetyn kelpoistusprosessimallin sopivan tähän tapaukseen soveltuvin osin.

Vaikka prosessimalli todettiin toimivaksi, sen kuitenkin arveltiin sopivan paremmin turvallisuusluokan 2 laitteille ja järjestelmille yksityiskohtaisuutensa puolesta. Kelpoistusprosessimallista voi kuitenkin olla hyötyä esimerkiksi kelpoistusprosessin etenemisen suurpiirteiseen seuraamiseen ja dokumenttimallien tarkasteluun, joita liitetään prosessimallin laatikoihin malliksi ja avuksi. Prosessimalliin voisi kuitenkin suunnitella polun, joka osoittaisi kevyempien prosessien etenemisen. Näiden turvallisuuluokka on pääsääntöisesti EYT, mutta tapauksesta riippuen myös turvallisuusluokan 3 laitteet. Polun avulla kelpoistusprosessimallista saataisiin soveltuvampi myös turvallisuusluokan 3 ja EYT-luokiteltujen laitteiden kelpoitusprosesseille.

5.2 Tapaus 2: Suojarele

Suojareleellä tarkoitetaan laitetta, jonka tehtävänä on suojata sähkönjakeluverkkoa sekä lisätä sen käyttöturvallisuutta. Sen tehtävänä on kytkeä vikatilanteessa kohde pois järjestelmästä ja huolehtia vikatilanteesta toipumisesta. Tällä tavoin se suojaa laitteita ja järjestelmiä vaurioilta. (ABB 2005)

Tarkasteltava suojarele on mikroprosessoripohjainen laite, jota käytetään Olkiluodon voimalaitoksilla pienjännitekojeiston tuloyksikössä syöttävän kiskosillan ja kojeiston sähköisenä suojana. Lisäksi sitä käytetään laitosyksiköissä kaapeleiden, moottoreiden ja alakeskusten sähköisessä suojauksessa. Tarkasteltavana olevaa suojarelettä voidaan käyttää laitoksilla turvallisuusluokissa 2, 3 ja EYT, riippuen sen käyttökohteesta ja -ympäristöstä. Suojareleet asennetaan laitokselle joko kojeistoihin mittauskenttien tai laitosyksiköiden oviin. (Kopra 2011.)

Suojareleet olivat osa isompaa TVO:n projektia, johon kuului myös muita komponentteja sekä toisen valmistajan suojareleitä. Tarkasteltavat suojareleet olivat kelpoistettu turvallisuusluokkaan 2, mutta ainoastaan yhdessä järjestelmässä ne toimivat turvallisuusluokassa 3. Tarkastelussa ei kuitenkaan keskitytty muihin komponentteihin tai laajempaan kokonaisuuteen, vaan ainoastaan suojareleeseen.

Tarkastelussa selvisi, että suojareleille tehty kelpoistusprosessi vastasi kehitettyä kelpoistusprosessimallia etenemiseltään. Viranomaisaineistoon kuuluivat mallissa esitetyt viranomaisaineistot. Ainoana erona oli, ettei suojareleille ollut laadittu alustavaa ja lopullista soveltuvuusarviota vaan soveltuvuusarvio. Lisäksi tarkastellessa viranomaisen kanssa tehtyä kirjeenvaihtoa ilmeni, että viranomaisaineistot sisälsivät tarvittavat aineistot, mutta niihin tehtiin joitakin korjauksia viranomaisen kehotteesta. Tämä ei kuitenkaan hidastanut prosessin etenemistä.

Tarkastelun yhteydessä tehdystä haastattelusta sekä kirjeenvaihdosta ja dokumenteista kävi selville, ettei suojarele vastannut täysin vaadittua IEC 60880 -standardia. Tästä olisi pitänyt heti prosessin alussa tehdä poikkeamien merkittävyyden analyysi, joka tehtiin vasta prosessin loppuvaiheilla. Suojareleiden diverssin selvittäminen muiden projektin

releiden kanssa kulutti aikaa, jota käytettiin myös syvälliseen tietoturvaselvitykseen. Näiden voidaan sanoa hieman mutkistaneen prosessia, muttei kuitenkaan niin, että siitä olisi aiheutunut kriittistä vaikutusta etenemiseen. Haastattelussa selvisi myös, ettei toimittajan kanssa ollut ollut ongelmia.

Vertailun lopuksi todettiin kehitetyn kelpoistusprosessimallin olevan toimiva ja hyödyllinen. Sen avulla pystyy näkemään, mitä on tehtävä prosessin vaiheissa, ja missä järjestyksessä pitäisi edetä. Lisäksi sen todettiin auttavan esimerkiksi projektin hoidossa. Tarkastelussa havaittiin myös samoja asioita kuin tapaus 1:ssä. Prosessimallin arveltiin soveltuvan parhaiten isoille prosesseille ja järjestelmille. Lisäksi yksinkertaisempiin prosesseihin voi mallista poimia apua. Kuitenkin polku, joka osoittaisi kevyemmän prosessin etenemisen, voisi helpottaa kelpoistusprosessimallin soveltumista yksinkertaisemmille prosesseille.

5.3 Tapaus 3: Päähöyryputken säteilynmittausjärjestelmä

Päähöyryputken säteilymittausjärjestelmä on ydinvoimalaitoksen keskeinen onnettomuusinstrumentti. Sen tehtävänä on valvoa primääripiirin päähöyryputken kuljettaman prosessihöyryn aktiivisuutta ja käynnistää tarvittaessa voimalaitoksen reaktorin suojaustoimet. Järjestelmän turvallisuustoimintoja ovat reaktorin sammuttaminen pikasululla ja voimalaitoksen suojarakennuksen eristäminen. Havaitusta viasta järjestelmä lähettää hälytyksen suojaus- ja hälytysjärjestelmiin sekä voimalaitoksen valvomoon releiden avulla. Tärkeytensä puolesta järjestelmä kuuluu turvallisuusluokkaan 2. (Laukkanen 2013.)

Järjestelmälle tehty kelpoistusprosessi eteni aivan kuin kehitetyssä kelpoistusprosessimallissa myös viranomaisaineiston osalta. Tämän johdosta kelpoistuprosessimalli päätettiin tarkastella vaiheittain mahdollisia poikkeamia ja kehitysideoita silmällä pitäen. Merkittäviä puutoksia prosessimallissa ei havaittu. Ainoastaan TVO:n tarkastuslaitoksen roolia voisi tuoda esille sekä esiselvitysvaiheeseen lisätä järjestelmän vaatimusten vaikutuksen määrittämisen muihin voimalaitoksen järjestelmiin ja päinvastoin. Lisäksi

mallissa tulisi tuoda hieman paremmin vielä esille eri tekniikoiden alueet, joita järjestelmät sisältävät.

Tarkastelun yhteydessä tehdystä haastattelusta selvisi, ettei tehty kelpoistusprosessi ollut edennyt täysin ilman ongelmia. Vaikka vaatimusmäärittelyt oli laadittu alusta alkaen kunnolla, analysoitu ja tarkastettu useamman kerran prosessin edetessä, ei säteilynmittauslaite kuitenkaan vastannut täysin vaatimuksia. Tämän seurauksena jouduttiin vaihtamaan laite toiseen, hieman eri toimintaperiaatteella toimivaan vastaavaan laitteeseen. Tämä hidasti prosessia noin vuoden. Mallissa ei pystytä vaikuttamaan tällaisiin yllättäviin hidasteisiin, mutta niitä voidaan yrittää kuitenkin vähentää hyvän ohjeistuksen avulla.

Tarkastelun lopputuloksena todettiin kelpoistusprosessimallin olevan toimiva, tehtävänsä täyttävä ja hyödyllinen. Se antaa selkeät roolijaot ja sen avulla on helpompi ohjeistaa muita prosessin etenemisestä. Lisäksi vastaavasta olisi ollut jo aikaisemmin hyötyä, koska sen avulla näkee helposti koko prosessin laajuuden.

5.4 Tapaus-tarkastelujen yhteenveto

Tehtyjen tarkastelujen perusteella voidaan todeta kehitetyn kelpoistusprosessimallin olevan toimiva ja soveltuva eri tilanteisiin. Tietenkin on huomioitava tapauskohtaiset tekijät, kuten turvallisuusluokka, prosessin laajuus ja vaativuus. Prosessimallin todettiin tarkasteluissa soveltuvan kaikkein parhaiten isoille ja vaativille prosesseille. Jotta prosessimalli sopisi paremmin myös kevyemmille prosesseille, lisättiin malliin niille oma polku. Sen tehtävänä on osoittaa kevyempien prosessien eteneminen ja helpottaa tällä tavoin esimerkiksi yksittäisen laitteen kelpoistamisprosessia. Vaarana tässä uudessa polussa on, että jotain olennaista jätetään tekemättä. Esimerkiksi esiselvitystä ei mallin mukaan tarvitse tehdä kevyillä ja normaaleilla prosesseilla. Jokaiselle tuotteelle tehdään kuitenkin jonkinlainen esiselvitys, vaikkei se sillä nimellä olisikaan. Tässä selvitetään muun muassa vaatimukset ja toimittajaehdokas. Siksi kevyemmissäkin prosesseissa on tärkeää muistaa, että prosessimalli näyttää vain ihanteellisen etenemisen. Tämän takia

jokaisessa tapauksessa on punnittava tarpeet ja vaatimukset, joiden mukaan kelpoistusprosessi toteutetaan.

Kelpoistusprosessimallissa ei kuitenkaan pystytä ennakoimaan prosessia hidastavia tekijöitä, koska ne ovat suurimmaksi osaksi tapauskohtaisia. Prosessimallin avulla kuitenkin voidaan yrittää vähentää näitä esimerkiksi hyvällä ohjeistuksella ja vaiheiden sisällön kuvauksella. Kelpoistusprosessimallille ollaankin kirjoittamassa ohjeita, jotka tukevat sitä.

Lopullisen prosessimallin ylin taso on liitteessä 4. Tässä on huomioitu tarkasteluista saadut kehitysehdotukset. Koska dokumentti oli kooltaan iso, jouduttiin se jakamaan kahteen osaan.

6 YHTEENVETO

Ydinvoimaa on jo vuosikymmenten ajan käytetty energian tuotannossa. Sinä aikana tekniikka on kehittynyt huimasti ja muun muassa automaatiolaitteissa hyödynnetään enenevissä määrin ohjelmoitavaa elektroniikkaa. Samanaikaisesti vanhentuville voimalaitosten laitteille on yhä haastavampaa löytää sopivia varaosia, sillä vanhaa tekniikkaa sisältäviä komponentteja ei kannata enää valmistaa. Perinteisesti laitteiden ja järjestelmien luotettavuus on osoitettu kelpoistuksen avulla, mutta ohjelmistojen kelpoistus on haastavaa muun muassa testitapausten suuren määrän takia. Lisäksi ohjelmistopohjaisten laitteiden ohjelmistojen luotettavuuden ja täydellisen virheettömyyden osoittaminen on vaikeaa, ellei lähes mahdotonta. Siksi ohjelmistojen laadukkuus ja vaatimusten täyttäminen osoitetaan laadukkaalla suunnittelu- ja kehitystyöllä. Vaikka luotettavuuden osoittamista varten on kehitetty erilaisia menetelmiä, työkaluja ja standardeja, eivät ne kuitenkaan kata kaikkia mahdollisia tapauksia. Muun muassa standardit on kehitetty lähinnä uusia ohjelmistoja silmällä pitäen sekä antamaan vaatimuksia esimerkiksi ohjelmiston suunnitteluun.

Tässä diplomityössä tavoitteena oli luoda kelpoistusprosessimalli Teollisuuden Voima Oyj:lle. Prosessimallin kehityksessä oli huomioitava erityisesti uudistuneet YVL-ohjeet sekä yhtiön sisäiset ohjeet ja uudet prosessimallit. Uudistuneiden YVL-ohjeiden lisäksi työssä keskityttiin standardien asettamiin määräyksiin, jotka koskivat kelpoistusta, vaatimuksia sekä järjestelmää, sen laitetta ja ohjelmistoa, sekä miten ne voitaisiin huomioida kehitetyssä prosessimallissa.

Kelpoistusmallin kehittämistä varten selvitettiin voimalaitosten toimintaperiaate, miten turvallisuus taataan, sekä mikä kelpoistuksen rooli ydinturvallisuudessa on. Ydinvoimalaitoksissa noudatetaan turvallisuuskriittistä ajattelua, jossa voimalaitosten turvallisuuteen keskitytään jo suunnitteluvaiheessa. Lisäksi selvitettiin, miten ja millaisilla järjestelmillä ydinturvallisuus pyritään takaamaan voimalaitoksen käytön aikana ja mahdollisen onnettomuuden sattuessa. Esimerkiksi reaktorisydämen hätäjäähdytysjärjestelmillä, säätösauvoilla ja boorijärjestelmällä varmistetaan onnettomuustilanteen sattuessa reaktorin sammuttaminen ja estetään tai lievennetään seurauksia.

Kelpoistuksella varmistetaan järjestelmän laitteiston ja ohjelmiston täyttävän asetetut vaatimukset sekä toimivat halutulla tavalla. Kelpoistus on kuitenkin vain pieni osa koko kelpoistuprosessista, joka alkaa vaatimusten määrittämisestä ja päättyy käyttöön. Jotta prosessi onnistuisi laadukkaasti, on laadittava muun muassa kelpoistussuunnitelma sekä selvitettävä käytettävät kelpoistusmenetelmät. Myös voimalaitokselta tulevien vaatimusten lisäksi on selvitettävä noudatettavat standardit ja YVL-ohjeet. Suunnitelmat ja dokumentit on pidettävä koko prosessin ajan päivitettynä esimerkiksi konfiguraation- ja vaatimustenhallinnan avulla. Vaikka kelpoistusprosessi on itsessään laaja kokonaisuus, on se osa muita prosesseja, kuten lisensiointi tai muutostenhallintaprosessi. Tämä oli huomioitava kehitettävässä kelpoistusprosessimallissa viranomaisen ohjeistuksen lisäksi tekemällä siitä yhtenäinen muiden TVO:n prosessimallien kanssa.

Kelpoistusprosessimallia kehitettäessä näkemysten ja kokemusten kerääminen eri henkilöiltä oli tärkeässä roolissa. Tällä tavoin saatiin selvitettyä esimerkiksi vastuualueet sekä kelpoistuprosessi eri vaiheet yksityiskohtineen. Kehitetyn kelpoistusmallin toimivuus osoitettiin kolmella tarkastelulla, joissa kehitettyä mallia verrattiin toteutettuihin kelpoistusprosesseihin. Kelpoistusprosessimalli todettiin tarkasteluissa toimivaksi sekä täyttävän sille asetetut vaatimukset. Sen avulla kelpoistusprosessin vaiheiden seuranta havaittiin helpoksi sekä sen todettiin olevan hyödyllinen. Prosessimallista käy ilmi roolijaot ja vastuualueet niin TVO:n, viranomaisen ja toimittajan välillä kuin TVO:n sisäisessä toiminnassa. Lisäksi kelpoistusprosessimallin avulla pystytään ohjeistamaan prosessiin osallistuvia sen etenemisestä, sillä prosessimallista näkee, mitä eri vaiheissa kuuluu tehdä, ja missä järjestyksessä on edettävä.

Tehtyjen tarkastelujen yhteydessä löytyi myös kehitysideoita prosessimallille. Tarkastelujen yhteydessä prosessimallin todettiin sopivan vaativille järjestelmille, jotka kuuluvat turvallisuusluokkaan 2. Jotta prosessimallista saataisiin myös sopivampi muun muassa yksittäisille laitteille, oli EYT-luokitteluille ja turvallisuusluokan 3 laitteille lisättävä oma polku kelpoistusprosessimalliin. Tämä osoittaisi vaiheet, jotka kevyemmissä kelpoistusprosesseissa on suoritettava. Kuitenkin jokaiselle tuotteelle on muistettava ottaa huomioon tapauskohtiaset vaatimukset ja muutokset, jotka voivat vaikuttaa kelpoistusprosessin etenemiseen. Lisäksi tarkastuslaitoksen roolia oli tuotava esille kelpoistuspro-

sessissa sekä järjestelmän eri tekniikanaloja tuli korostaa hieman enemmän esimerkiksi kelpoistuprosessimallin perussuunnittelu- ja toteutussuunnitteluvaiheessa.

Kelpoistusprosessimallia kehitettäessä laadittiin yhteityössä Softability Group Oy:n kanssa ohjeet ohjelmiston kelpoistukseen. Ohjeiden avulla pyritään helpottamaan ohjelmiston suunnittelun ja toteutuksen laadun varmistusta muun muassa tarkistuslistojen avulla. Ohjeen myötä heräsi ajatus hyödyntää kehitteillä ollutta Nuclear SPICE -mallia kelpositusprosessimallissa. Mitään konkreettista ei ole vielä tehty, mutta tästä aiheesta voisi löytyä lisää tutkittavaa. Esimerkiksi selvittää, miten kelpoistusprosessimalli voisi hyötyä Nuclear SPICE -mallista.

Kelpoistusprosessimallia kehittäessä heräsi myös muita kehitysideoita tarkasteluissa tehtyjen havaintojen lisäksi. Esimerkiksi kelpoistusprsessimalliin voitaisiin lisätä myös mekaanisten komponenttien osuus. Lisäksi vaatimusmäärittelystä ja -hallinnasta voisi tehdä lisäselvitystä esimerkiksi tavoitteena laatia tarkat ja kunnolliset ohjeet tai kehittää prosessimalli, sillä oikein laadittu vaatimusmäärittely on erittäin tärkeässä roolissa kelpoistusprosessissa. Näiden lisäksi keskustelua voisi käydä myös prosessiin osallistuvien henkilöiden rooleista ja vastuualueista ja tarpeen tullen näiden uudistamisesta, sillä vastuualueiden, erityisesti TVO:n sisäisten vastuualueiden, määrittäminen oli yksi haastavista tehtävistä kelpoistusprosessimallin kehityksessä.

Koska standardeilla on viranomaismääräysten lisäksi tärkeä rooli tuotteen kehityksessä ja kelpoistuksessa, niiden tulisi olla verrattavissa viranomaisen asettamiin vaatimuksiin tai täydentämässä niitä. Esimerkiksi turvallisuuden eheyden tasot tulisi voida kytkeä viranomaisten asettamiin vaatimuksiin ja tällä tavoin mahdollisesti yhtenäistämään esimerkiksi turvallisuusluokitusta YVL-ohjeiden ja standardien välillä.

Nyt kun kelpoistusprosessimalli on todettu soveltuvan tehtäväänsä, sitä voidaan alkaa käyttää. Käytön aikana voitaisiin pohtia prosessimallin kehitystä ja parantelua, sillä varsinaisessa käytössä voidaan havaita myös joitakin korjauskohtia. Näitä tulisi listata ylös ja pohtia mitkä ovat kriittisiä ja mitkä eivät. Korjauskohtia tulisi verrata viranomaisen ohjeistukseen, sillä ne vaikuttavat kelpoistusprosessimallin etenemiseen ja muotoutumiseen.

LÄHDELUETTELO

ABB Oy (2005). *Mikä on sähkönjakeluautomaatio?* [online]. [Siteerattu 16.7.2014]. Saatavana: <URL:http://www02.abb.com/global/fiabb/fiabb254.nsf/0/3f6330cc75bafdf5c12570a0003c02c1/$file/FISUB2209_2005.ppt>.

Aho, J. (2006). *Arvonmääritysmallin kehittäminen sijoittajan näkökulmasta: case F-Secure.* Lappeenrannan teknillinen yliopisto. Tuotantotalouden osasto. Diplomityö. 128 s.

Aho, M. (2009). *Konfiguraationhallinta automaatiojärjestelmäprojekteissa.* Tampereen teknillinen yliopisto. Automaatiotekniikan koulutusohjelma. Diplomityö. 79s.

Ahonen, E. (2011). *Vikasietoisuuden tutkiminen todennäköisyysperusteisen riskianalyysin avulla.* Lappeenrannan teknillinen yliopisto. Energiatekniikan koulutusohjelma. Diplomityö. 81 s.

Alanko, T. (2010). *Kansainvälisten yritysten satakunnassa toimivien tytäryhtiöiden taloudellinen menestys vuosina 2005-2008 sekä niiden alueelliseen sitoutumiseen vaikuttavat kriittiset tekijät.* Turun kauppakorkeakoulu, Porin yksikkö. Liiketaloustiede. Pro gradu -tutkielma. 111 s.

Apthorpe, R. (2001). A Probabilistic Approach to Estimating Computer System Reliability. *15th System Administration Conference LISA.* San Diego, USA. 2.12.-7.12.2001.

Björklöf, P. (2012). *Soveltuvuusarvio ultraäänivirtausmittari DF868.* Olkidoc 142862. Luottamuksellinen.

Blinnikka, S. (2002). *Asiakas- ja kiinteitokannattavuus kiinteitöhoitopalveluissa - case YIT Rapido Kiinteistöpalvelut Oy*. Jyväskylän yliopisto. Taloustieteiden tiedekunta. Pro Gradu -tutkielma. 91 s.

California Division (2014). *Configuration Management.* [online]. [Siteerattu 17.6.2014]. Saatavana: <URL:http://www.fhwa.dot.gov/cadiv/segb/views/document/sections/section3/3_9_6.cfm>.

Canadian Nuclear Safety Commission (2006). *Regulatory Guide G-306. Safety Accident Management for Nuclear Reactors.* Ottawa, Kanada: Canadian Nuclear Safety Commission. 9s. ISBN 0-662-43248-7.

Carman, C. (2013). *4 Stepst to Effective Change Control.* [online]. [Siteerattu 4.7.2014]. Saatavana: <URL:http://news.dice.com/2013/05/08/why-change-control-isnt-for-sissies/>.

Eskelinen, T. (2010). *Asiakaslähtöisten palveluiden kehittäminen paloilmoitinliikkeelle.* Tampereen ammattikorkeakoulu. Yrittäjyyden ja liiketoimintaosaamisen koulutusohjelma. Opinnäytetyö. 91 s.

Eurasto, T., Hyvärinen, J., Järvinen, M-L.,Standberg, J. & Sjöblom, K-L. (2004). Ydinvoimalaitostekniikan perusteita. Teoksessa *Ydinturvallisuus,* 26-87. Toimittaja Sandberg, J. Hämeenlinna: Karisto Oy.

European Nuclear Society (2014). *Nuclear Power Plants, World Wide.* [online]. [Siteerattu 25.7.2014]. Saatavana: <URL:http://www.euronuclear.org/info/encyclopedia/n/nuclear-power-plant-world-wide.htm>.

Farah, J. (2013). *Waht Is the Real Difference between Software Configuration Management and Hardware Configuration Management.* [online]. [Siteerattu 1.5.2014]. Saavana: <URL:http://www.cmcrossroads.com/article/what-real-difference-between-software-configuration-management-and-hardware-configuration?page=0%2C0>.

Finlex (2014). *Ydinenergialaki.* [online]. [Siteerattu 16.7.2014]. Saatavana: <URL:http://www.finlex.fi/fi/laki/ajantasa/1987/19870990#a29.12.1994-1420>.

Git (2014). *Getting Started-About Version Control.* [online]. [Siteerattu 4.5.2014]. Saatavana: <URL:http://git-scm.com/book/en/Getting-Started-About-Version-Control>.

Halminen, J. (2001). *Ohjelmoitavien laitteiden kelpoistaminen ydinvoimalaitoksen turvallisuusjärjestelmiin*. Tampereen teknillinen korkeakoulu. Tietotekniikan osasto. Diplomityö. 55 s.

Halminen, J. & Nevalainen, R. (2007). Qualification of Safety-Critical Systems in TVO Nuclear Power Plants. Teoksessa *Software Process: Improvement and Practie,*559-567. John Wiley & Sons, Ltd. ISSN 1099-1670

Harju, H. (2000). *Ohjelmiston luotettavuuden kvalitatiivinen arviointi.* 1. painos. Espoo: Otamedia Oy. 111s. ISBN 951-38-5767-0.

Haughey, D. (2011). *What is Change Control?* [online]. [Siteeattu 4.7.2014]. Saatavana: <URL:http://www.projectsmart.co.uk/what-is-change-control.php>.

Havuajo, J. (2012). *PWR PACTEL -koelaitteiston ylätilan mallinnusvaihtoehtojen tarkastelu APROS-ohjelmistolla.* Lappeenrannan teknillinen yliopisto. Energiatekniikan koulutusohjelma. Diplomityö. 82 s.

Heikkilä, J. (2007). *Ydinvoimalaitoksen putkistojen riskitietoinen tarkastusohjelma.* Tampereen teknillinen yliopisto. Konetekniikan koulutusohjelma. Diplomityö. 53 s.

Heindl, M. & Biffl, S. (2005). A Case Study on Value-based Requirements Tracing. *Proceedings of the 10th European Software Engineering Conference held jointlyeith 13th ACM SIGSOFT International Symposium on Foundations of Software Engineering.* Lissabon, Portugali 5.9.-9.9.2005. 60-69. ISBN 1-59593-014-0.

Henriksson, A. (2012). *Loviisa 1 ja 2 tuottavat pian enistä enemmän?* [online]. [Siteerattu 25.7.2014]. Saatavana: <URL:http://www.loviisansanomat.net/lue.php?id=5361>.

Honkanen, H. (2013). *Ydinvoimatekniikka.* [online]. [Siteerattu 14.7.2014]. Saatavana: <URL:http://gallia.kajak.fi/opmateriaalit/yleinen/honHar/ma/>. Oppimateriaali.

Hölttä, J. (2012). *Requirement Specification for Station Blackout Gas Turbine Generator in a Nucleat Power Plant*. Tampereen teknillinen yliopisto. Ympäristö- ja energiatekniikan koulutusohjelma. Diplomityö. 63 s.

IAEA (2014). *The "Atoms for Peace" Agency.* [online]. [Siteerattu 1.3.2014]. Saatavana: <URL:http://www.iaea.org/About/about-iaea.html>.

IAEA. (2010). *Information Technology for Nuclear Power Plant Configuration Management.* Viini, Itävalta: International Atomic Energy Agency. 103 s. IAEA-Tecdoc-1651. ISBN 978-92-0-106310-6

IEC 60780 (1998). *Nucleat Power Plants - Electrical Equipment of the Safety System - Qualification.* 2. painos. Sveitsi,Geneve: International Electrotechnical Commission. 59 s. ISBN 2-8318-4534-3

IEC 60880 (2006). *Nuclear Power Plants - Instrumentation and Control Important to Safety - Software Aspects for Computer-Based Systems Performing Category A Functions.* 2. painos. Sveitsi, Geneve: International Electrotechnical Commission. 217 s. ISBN 2-8318-8636-8.

IEC 60987 (2013). *Nuclear Power Plants - Instrumentation and Control Important to Safety - Hardware Design Requirements for Computer-Based Systems.* 2.1 painos.

IEC 61226 (2009). *Nuclear Power Plants - Instrumentation and Control Important to Safety - Classification of Instrumentation and Control Functions.* 3. painos. Sveitsi, Geneve: International Electrotechnical Commission. 68 s. ISBN 2-8318-1052-1

IEC 61508-1 (2010). *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related System - Part 1: General Requirements.* 2. painos. Sveitsi,

Geneve: International Electrotechnical Commission. 132 s. ISBN 978-2-88910-524-3.

IEC 61508-2 (2010). *Functionla Safety of Electrical/Electronical/Programmable Electronic Safety-rated Systems - Part 2: Requirements for Electrical/Electronic/Programmable Electronic Safety Related Systems.* 2. painos. Sveitsi, Geneve: International Electrotechnical Commission. 187 s. ISBN 978-88910-525-0.

IEC 61508-3 (2010). *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related System - Part 3: Software Requirements.* 2. painos. Sveitsi, Geneve: International Electrotechnical Commission. 236 s. ISBN 978-2-88910-526-7.

IEC 61513 (2011). *Nuclear Power Plants - Instrumentationa and Control Important to Safety - General Requirements for Systems.* 2. painos. Sveitsi, Geneve: International Electrotechnical Commission. 210 s.

IEC 62138 (2004). *Nuclear Power Plants - Instrumentation and Control Important for Safety - Software Aspects for Computer-Based Systems Performing Category B or C Functions.* 1. painos. Sveitsi, Geneve: International Electrotechnical Commission. 104 s. ISBN 2-8318-7335-5.

ICRP (2014). *About ICRP.* [online]. [Siteerattu 10.3.2014]. Saatavana: <URL:http://www.icrp.org/>.

Iivonen, J. (2011). *Konfiguraation hallintasuunnitelma Millog Oy:lle.* Lappeenrannan teknillinen yliopisto. Tuotantotalouden osasto. Diplomityö. 57 s.

Isolankila, A., Järvinen, M-L., Keskinen, R., Niemelä, I., Ojanen, M., Rantala, R., Sandberg, J., Tiippana, P., Valtonen, K., Virolainen, R & Åstrand K. (2004). Ydinturvallisuuden varmistaminen. Teoksessa *Ydinturvallisuus,* 90-142. Toimittaja Sandberg, J. Hämeenlinna: Karisto Oy.

Kalanen, S. (2012). *Esiselvitys luo pohjan onnistuneelle projektille*. [online]. [Siteerattu 9.8.2014]. Saatavana: <URL:http://tietotyomaa.meteoriitti.com/2012/04/23/esiselvitys-auttaa-onnistumaan/>.

Kallio, J. (2008). *Vaatimustenhallinta ja sen kehittaminen ohjelmiston elinkaaren näkökulmasta.* Jyväskylan yliopisto. Tietojenkäsittelytieteen laitos. Pro gradu -tutkielma. 131 s.

Karjunen, T., Suksi, S. & Tossavainen, K. (2004). Kokemukset onnettomuuksista ja poikkeuksellisista tapahtumista ydinlaitoksissa. Teoksessa *Ydinturvallisuus,* 208-266s. Toimittaja Sandberg, J. Hämeenlinna: Karisto Oy.

Kaskela, L. (2005). *Tietotekniikkahankinnat*. [online]. [Siteerattu 27.5.2014]. Saatavana: <URL:http://www.tieke.fi/pages/viewpage.action?pageId=3441242>.

Kasurinen, J. P. (2013). *Ohjelmistotestauksen käsikirja*. 1. painos. Jyväskylä: Docendo. 236 s. ISBN 978-952-5912-99-9.

Kessler, G. (2012). *Sustainable and Safe Nuclear Fission Energy. Technology and Safety of Fast and Thermal Nuclear Reactors.* Berliini, Heidelberg: Springer-Verlag. 464 s. ISBN 978-3-642-11990-3

Kettunen, T. (2009). *Versionhallintajärjestelmä eEDUn Moodle-tarpeisiin.* Tampereen ammattikorkeakoulu. Tietojenkäsittelyn koulutusohjelma. Opinnäytetyö. 42 s.

Kiviluoto, P. (2013). *Vaatimusmäärittelu ja vaatimusten priorisointi ohjemistoprojekteissa.* Seinäjoen ammattikorkeakolu. Teknologiaosaamisen johtamisen koulutusohjelma. Opinnäytetyö. 78 s.

Kopra, K. (2011). *OL1 ja OL2, soveltuvuusarvio - suojareleet.* Olkidoc 133639, luottamuksellinen.

Korpelainen, L. (2000). *Sähkövoimatekniikan ympäristöopus. 2.1. Ydinvoima.* [online]. [Siteerattu 26.2.2014]. Saatavana: <URL: http://www.leenakorpinen.fi/node/194>. Opetusmateriaali.

Korpelainen, L. Silvennoinen, S., Havunen, I. & Kaartinen, S. (1998). *Sähkövoimatekniikkaopus. 2. Sähkön kulutus ja tuotanto*. [online]. [Siteerattu 15.8.2014]. Saatavana: <URL:http://www.leenakorpinen.fi/node/158>. Opetusmateriaali.

Koskiniemi, T. (2005). *Ydinvoimalaitoksen varalla olevien turvallisuusjärjestelmien määräaikaistestauksien riittävyys ja kattavuus.* Lappeenrannan yliopisto. Energiatekniikan osasto. Diplomityö. 78 s.

Kotiluoto, P. (2002). *Lataussuunnittelu.* Teknillinen korkeakoulu. Teknillisen fysiikan koulutusohjelma. Seminaarityö. 13 s.

Koutaniemi, P., Reponen, H., Salminen, P., Sandberg, J. & Varjoranta, T. (2004). Ydinenergialainsäädäntö ja -hallinto. Teoksessa *Ydinturvallisuus,* 354-382. Toimittaja Sandberg, J. Hämeenlinna: Karisto Oy.

Koutaniemi, P. (2009). *STUK-YVL-ohjeuudistus ja WERNA-hankkeet.* [online]. [Siteerattu 11.6.2014]. Saatavana: <URL:http://www.ats-fns.fi/index.php?option=com_joomdoc&task=cat_view&gid=65&Itemid=&lang=fi>.

Laatukeskus (2014). *Auditointi.* [online]. [Siteerattu 12.8.2014]. Saatavana: <URL: http://www.laatukeskus.fi/palvelut-asiantuntijapalvelut/auditointi>.

Laukkanen, J. (2013). *55 1- OL1/OL2 - Päähöyryputken säteilyynmittausjärjestelmä - lopullinen turvallisuusseloste.* Olkidoc 106266. Luottamuksellinen.

Lauronen, P. (2003). *Järjestelmä yksityisen sähköpostiviestinnän turvaamiseksi työelämässä.* Teknillinen korkeakoulu. Tietotekniikan osasto. Diplomityö. 81s.

Lenkkeri, J. (2013). *Versionhallinta teoriassa.* [online]. [Siteerattu 16.7.2014]. Saatavana: <URL: ://www.sugif.fi/arkisto2013/CVS_esitys.pptx>.

Lintula, H. (2004). *Vaatimusten validointi ja verifiointi.* Kuopion yliopisto. Tietojenkäsittelytieteen laitos. Pro Gradu -tutkielma. 95 s.

Lukka, K. (2001). *Konstruktiivinen tutkimusote.* [online]. [Siteerattu 18.6.2014]. Saatavana:<URL:http://www.metodix.com/fi/sisallys/01_menetelmat/02_ metodiartikkelit/lukka_const_research_app/kooste>.

Majuri, J-P. (2006). *Versionhallinta ohjelmistotuotannossa. Toteutus UNES Oy:ssä.* Tampereen ammattikorkeakoulu. Tietojenkäsittelyn koulutusohjelma. Opinnäytetyö. 44 s.

Maryland.Gov (2014). *Implementation plan.* 7 s. Mallipohjadokumentti.

Metsävaino, M. (2013). *Sosiaalinen toimintakyky - käsiteanalyyttinen tutkimus.* Itä-Suomen yliopisto. Yhteiskuntatieteiden laitos. Pro Gradu -tutkielma. 117 s.

MITRE (2014a). *System Architecture*. [online]. [Siteerattu 12.8.2014]. Saatavana: <URL:http://www.mitre.org/publications/systems-engineering-guide/se-lifecycle-building-blocks/system-architecture>.

MITRE (2014b). *Architectural Frameworks, Models and Views.* [online]. [Siteerattu 12.8.2014]. Saatavana: <URL:http://www.mitre.org/publications/systems-engineering-guide/se-lifecycle-building-blocks/system-architecture/architectural-frameworks-models-and-views>.

NASA (2014). *The NASA Risk Management Page.* [online]. [Siteerattu 30.6.2014]. Saatavana: <URL:http://www.hq.nasa.gov/office/codeq/risk/>.

NEA (2002). *Probabilistic safety assessment: an analytical tool for assessing nuclear safety.* [online]. [Siteerattu 30.6.2014]. Saatavana: <URL:https://www.oecd-nea.org/brief/brief-08.html>.

Novox Oy (2014). *Tekninen esisuunnittelu ja investoinnin valmistelu*. [online]. [Siteerattu 11.8.2014]. Saatavana: <URL: http://www.novox.fi/fi/palvelut/palvelut-9>.

Oikarinen, T. (2013). *Kuntatieto-ohjelman johtoryhmän linjaukset.* 3 s. Valtionvarainministeriön linjausaineistoa.

Pepperl+Fuchs (2007). *Safety Integrity Level Manual.* 40 s. Internetti dokumentti.

Plit, H. (2013). *STUK asetti uudet ydinvoimalaitosten turvallisuusvaatimukset.* [online]. [Siteerattu 31.5.2014]. Saatavana: <URL:http://www.tem.fi/ajankohtaista/uutiset/stuk_asetti_uudet_ydinlaitosten_turvallisuusvaatimukset.112752.news>.

Posiva (2014). *Loppusijoitus.* [online]. [Siteerattu 14.7.2014]. Saatavana: <URL:http://www.posiva.fi/loppusijoitus>.

Rohweder, L. & Virtanen, A. (2008). *Kohti kestävää kehitystä. Pedagoginen lähestymistapa.* Yliopistopaino, Helsinki. ISBN 978-952-485-477-1. Opetusministeriön julkaisu.

Rouse, M. (2011). *Change Control.* [online]. [Siteerattu 21.5.2014]. Saatavana: <URL:http://searchdisasterrecovery.techtarget.com/definition/change-control>.

Ruhe, G., Eberlein, A. & Pfahl, D. (2005). Quantitative WinWin - A New Method for Decision Support in Requirements Negotiation. *Proceeding of the 14th International Conference on Software Engineering and Knowledge Engineering.* Ischia, Italia. 15.7.-19.7.2002. 159-166. ISBN 1-58113-556-4.

Ruuska, T. (2012). *Vaatimusmäärittelyt ketterässä ohjelmistokehityksessä.* Jyväskylän yliopisto. Tietojenkäsittelytieteiden laitos. Pro-gradu tutkielma . 78 s.

SFS (2014a). *Mitä standardointi on?* [online]. [Siteerattu 1.6.2014]. Saatavana: <URL:http://www.sfs.fi/standardien_laadinta/mita_standardisointi_on>.

SFS (2014b). *Usein kysyttyä – Onko standardeja pakko noudattaa?* [online]. [Siteerattu 1.6.2014]. Saatavana: <URL:http://www.sfs.fi/usein_kysyttya# Miltkaikiltaerialoita-standardejaon>.

Seppänen, V. (2000). *Konfiguraationhallinta.* Helsingin yliopisto. Tietojenkäsittelytieteen laitos. Seminaarityö. 9 s.

Sininen meteoriitti (2014). *Vaatimusmäärittely.*[online]. [Siteerattu 27.5.2014]. Saatavana: <URL:https://www.meteoriitti.com/Mita-teemme/Palvelut/Strateginen-suunnittelu/Vaatimusmaarittely/>.

Sistonen, J. (2012). *Ydinvoimalaitoksen rakentamisen aikainen viranomaistoiminta ja -vaatimukset.* Lappeenrannan teknillinen yliopisto. Energiatekniikan koulutusohjelma. Diplomityö. 126 s.

Sofokus (2014). *Tekninen vaatimusmäärittely.* [online]. [Siteerattu 24.4.2014]. Saatavana: <URL: http://www.sofokus.com/tekninen-vaatimusmaarittely>.

Stinson, M. (2012). *Reguirements Engineering Today.* [online]. [Siteerattu 25.4.2014]. Saatavana: <URL: http://www.rtcmagazine.com/articles/view/102675>.

STUK (2007). *Säteilysuojelun periaatteet.* [online]. [Siteerattu 30.6.2014]. Saatavana: <URL:http://www.stuk.fi/proinfo/vaatimukset_kaytolle/fi_FI/sateilysuojelun_periaatteet/>.

STUK (2013a). *Kiehutusvesireaktori.* [online]. [Siteerattu 28.2.2014]. Saatavana: <URL:http://www.stuk.fi/ydinturvallisuus/miten-ydinvoimalaitos-toimii/ydinvoimalaitostyypit/kiehutusvesireaktori/>.

STUK (2013b). *Painevesireaktori.* [online]. [Siteerattu 28.2.2014]. Saatavana: <URL:http://www.stuk.fi/ydinturvallisuus/miten-ydinvoimalaitos-toimii/ ydinvoimalaitostyypit/fi_FI/painevesireaktori/>.

STUK (2013c). [online]. [Siteerattu 4.3.2014]. Saatavana: <URL:http://www.stuk.fi/ ydinturvallisuus/ydinvoimalaitosten-toiminta/periaatteet/fi_FI/syvyys/>.

STUK (2013d). *Turvallisuutta puolustetaan syvyyssuunnassa.* [online]. [Siteerattu 15.3.2014]. Saatavana: <URL:http://www.stuk.fi/ydinturvallisuus/ ydinvoimalaitosten-toiminta/periaatteet/fi_FI/syvyys/_print/>.

STUK (2013e). *Ydinvoimalaitostyypit*. [online]. [Siteerattu 12.9.2014]. Saatavana: <URL:http://www.stuk.fi/ydinturvallisuus/miten-ydinvoimalaitos-toimii/ ydinvoimalaitostyypit/fi_FI/tyypit/>.

STUK (2014). *YVL-ohjeet.* [online]. [Siteerattu 31.5.2014]. Saatavana: <URL:http://www.stuk.fi/julkaisut_maaraykset/viranomaisohjeet/fi_FI/yvl/>.

STUK (2010). *HSE:n luokitus "yhdistettynä STUK:n vaatimuksiin"*. Turvallisuusluokitus luonnos. Luottamuksellinen. 5 s.

Teknologiateollisuus (2014). *Toteutus*. [online]. [Siteerattu 13.8.2014]. Saatavana: <URL: http://teknologiateollisuus.fi/fi/palvelut/toteutus.html>.

Tossavainen, J. (2007). *Tietojärjestelmän dokumentointi - Case: StoraEnso Oyj Heinolan Flutintehdas*. Lahden ammattikorkeakoulu. Liiketalouden koulutusohjelma. Opinnäytetyö. 78 s.

TVO (2014a). *Toimintakulttuuri.* [online]. [Siteerattu 24.2.2014]. Saatavana: <URL: http://www.tvo.fi/Toimintakulttuuri>.

TVO (2014b). *Ydinturvallisuus*. [online]. [Siteerattu 10.6.2014]. Saatavana: <URL: http://www.tvo.fi/Ydinturvallisuus2>.

TVO (2014c). *Reaktorityypit.* [online]. [Siteerattu 12.7.2014]. Saatavana: <URL:http://www.tvo.fi/Reaktorityypit>.

TVO (2014d). *Yhtiötietoja.* [online]. [Siteerattu 14.7.2014]. Saatavana: <URL:http://www.tvo.fi/Yhtiötietoja>.

TVO (2014e). *OL1 ja OL2.* [online]. [Siteerattu 25.7.2014]. Saavana: <URL:http://www.tvo.fi/OL1%20ja%20OL2

TVO (2014f). *Ydinvoimalaitos.* [online]. [Siteerattu 14.8.2014]. Saatavana: <URL:http://tvo.fi/Ydinvoimalaitos>.

TVO (2013a). *OL1&OL2. Ydinvoimalayksiköt*. Rauma: Laine Direct Oyj. 58s. Esite.

TVO (2013b). *TVO:n Toimintaohje*. [online]. [Siteerattu 24.2.2014]. Saatavana: <URL:http://www.tvo.fi/page-2249 >.

TVO (2009). *Perustietoa Olkiluoto 3:sta. Toimitaperiaate, käyttö, turvallisuus*. Eura: Eura Print. 27s. Esite.

TVO (2008). *Ydinvoimalaitosyksikkö Olkiluoto 3.* Eura: Eura Print. 61s.

TVONS (2014). *TVONS - Ydinvoimaosaamisen edelläkävijä.* [online]. [Siteerattu 14.7.2014]. Saatavana: <URL:http://www.tvons.fi/tvons_info>.

Työ- ja elinkeinoministeriö (2010). *Kansallinen ydinvoimalaitosten turvallisuustutkimus 2011-2014. Uuden tutkimusohjelman SAFIR2014 runkosuunnitelma.* Helsinki: Edita Publishing Oy/Ab/Ltd. 103s. ISBN 978-952-227-420-5. Työ- ja elinkeinoministeriön julkaisuja. Energia ja ilmasto. 49/2010

Urunga, G. S., Sözbir, M. F. & Özyildirim A. (2013). Qualification of Microwave Hybrid Production Line for Space. *6th International Conferense on Recent Advances in*

Space Technology (RATS). Istanbul. 12.6.-14.6.2013. 747-745. ISBN 978-1-4673-6395-2.

Yeates, S. (2013). *What Is Version Control? Why Is It Important For Due Diligence?* [online]. [Siteerattu 4.5.2014]. Saatavana: <URL:http://oss-watch.ac.uk/resources/versioncontrol>.

Yli-Nikkilä, L. (2012). *Turvallisuusluokan 3 ydinpolttoaineen käsittelyjärjestelmän sähkö- ja automaatio-osuuksien kelpoistus*. Satakunnan ammattikorkeakoulu. Sähkötekniikan koulutusohjelma. Opinnäytetyö. 51 s.

YVL 2.1 (2000). *Ydinvoimalaitosten järjestelmien, rakenteiden ja laitteiden turvallisuusluokitus*. Helsinki. ISBN 951-712-406-6. Kumottu 1.12.2013.

YVL A.7 (2013). *Ydinvoimalaitoksen todennäköisyysperusteinen riskianalyysi ja riskien hallinta.* Helsinki. ISBN 978-952-478-923-3

YVL A.8 (2013). *Ydinvoimalaitoksen ikääntymisen hallinta.* Helsinki. ISBN 978-952-309-021-7.

YVL B.1 (2013). *Ydinvoimalaitoksen turvallisuussuunnitelma*. Helsinki. ISBN 978-952-478-854-0.

YVL B.2 (2013). *Ydinlaitosten järjestelmien, rakenteiden ja laitteiden luokittelu*. Helsinki. ISBN 978-952-478-857-1.

YVL E.7 (2013). *Ydinvoimalaitoksen sähkö- ja automaatiolaitteet.* Helsinki. ISBN 978-952-478-953-0.

Valtonen, K. (2011). *Fukushiman ja Japanin tapahtuminen vaikutus ydinturvallisuusäädöksiin*. [online]. [Siteerattu 30.6.2014]. Saatavana: <URL:http://www.ats-fns.fi/index.php?option=com_joomdoc&task=doc_download&gid=361&Itemid=>.

Vatenfall (2014). *Ydinvoiman historia.* [online]. [Siteerattu 13.7.2014]. Saatavana: <URL:http://corporate.vattenfall.fi/tietoa-energiasta/sahkon-jalammontuotanto/tietoa-ydinvoimasta/ydinvoiman-historia/>.

Viitasalo, M. (2014). *Reaktori automaation suunnittelu perusteet.* TVO:n koulutusmateriaali.

VTT (2003). *Turvallisuus prosessien suunnittelussa ja käyttöönotossa.* 23 s Luentomateriaali.

Wahlström, K. (2011). *Laitteiden ja järjestelmien kelpoistaminen ydinvoimarakentamisessa.* [online]. [Siteerattu 22.4.2014]. Saatavana: <URL:http://www. lahtimechatronics.fi/filebank/1865-02_Kim_Wahstrom_esity_Lahti_%5BYhteensopivuustila%5D.pdf.>

Wahlström, K. (2013). *Inspection of I&C Eguipment E.7.* Esitelmämateriaali.

Wang, W., Azarian, M. H. & Pecht, M. (2008). Qualification for Product development. *International Conference on Electronic Packaging Technology & High Density Packaging.* Shanghai, Kiina. 28.7.-31.7.2008. 1-12. ISBN 978-1-4244-2740-6.

Wester, B. F. (2008). *Buy Vs. Build Software Applications: The Eternal Dilemma.* [online]. [Siteerattu 21.7.2014]. Saatavana: <URL:http://www.baselinemag.com/c/a/Application-Development/Buy-vs-Build-Software-Applications-The-Eternal-Dilemma/>.

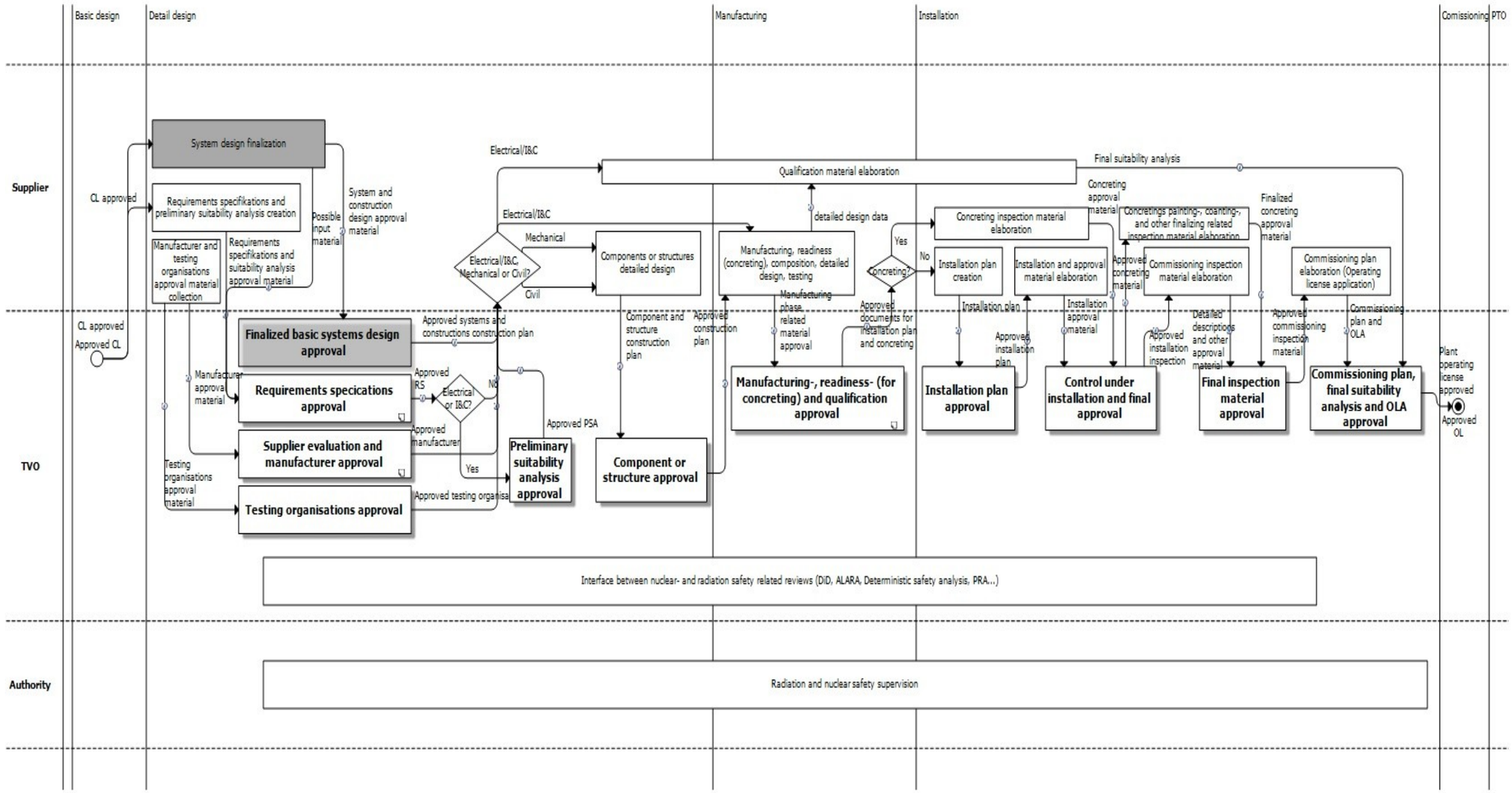
Wiegers, K. E. (2000). *When Telepathy Won't Do: Requirements Engineering Key Practices.* [online]. [Siteerattu 16.7.2014]. Saatavana: <URL:http://www.processimpact.com/ articles/telepathy.html>.

World Nuclear Association (2010). *RBML Reactors.* [online]. [Siteerattu 12.7.2014]. Saatavana: <URL:http://www.world-nuclear.org/info/Nuclear-Fuel-Cycle/Power-Reactors/Appendices/RBMK-Reactors/>.

Österhom, S. (2005). *Vaatimusmäärittely*. [online]. [Siteerattu 1.8.2014]. Saatavana: <URL:http://www05.turku.fi/ah/amk/2005/1027010l/1256433.htm>. Luentomateriaali.

LIITTEET

Liite 1. Mikael Eklöfin kehittämä lisensointiprosessimalli.



Liite 2. Testimetodit standardista IEC 60880. (Muokattu lähteestä IEC 60880 2013: 185–189.)

Yleiset				
No	Testi	Havaitut virheet	Suoritetaan	Huomautukset
1	Tapaukset jotka edustavat ohjelman käyttäytymistä yleensä, sen laskentaa ja ajoitusta.	Kaikki, muttei takuita tyhjentävyydestä.	Aina	Oletetaan, että järjestelmä toimii oikein, jos tapaukset suoritetaan asianmukaisesti.
2	Kaikki yksilöllisesti ja selkeästi yksilöidyt vaatimukset.	Unohdetut toiminnot täysin havaittu.	Pääasiassa aina, jos tarvittavat toiminnot on määritelty yksityiskohtaisesti	Voi olla kattava testi, jos toiminnot pidetään täysin erillään. Ei kerro paljon ajoitus ongelmista.
3	Kaikki syötemuuttujat ääriasennoissa (törmäys testi).	Ajoitusvirheet, mutta ei takuuta. Ylivirtaus, alivirtaus.	Aina	
4	Kaikkien ulkoisten laitteiden toiminta	Laite- ja ohjelmistorajapinnan suunnitteluvirheet.	Aina	
5	Staattiset tapaukset ja dynaamiset polut, jotka edustavat teknisen prosessin käyttäytymistä.	Kaikki, mutta ilman takuuta.	Aina	Erittäin arvokas, jos tekninen simulaattori on käytössä.
6	Oikean toiminnan osoittaminen ottamalla ja poistamalla käytöstä jokainen ylimääräinen alijärjestelmä/ulkoinen laite (jotkut yhdistelmät tulisi myös testata tarvittaessa)	Laiterajapinnan käsittelyvirheet.	Aina	Järjestelmän robustisuuden varmistaminen.

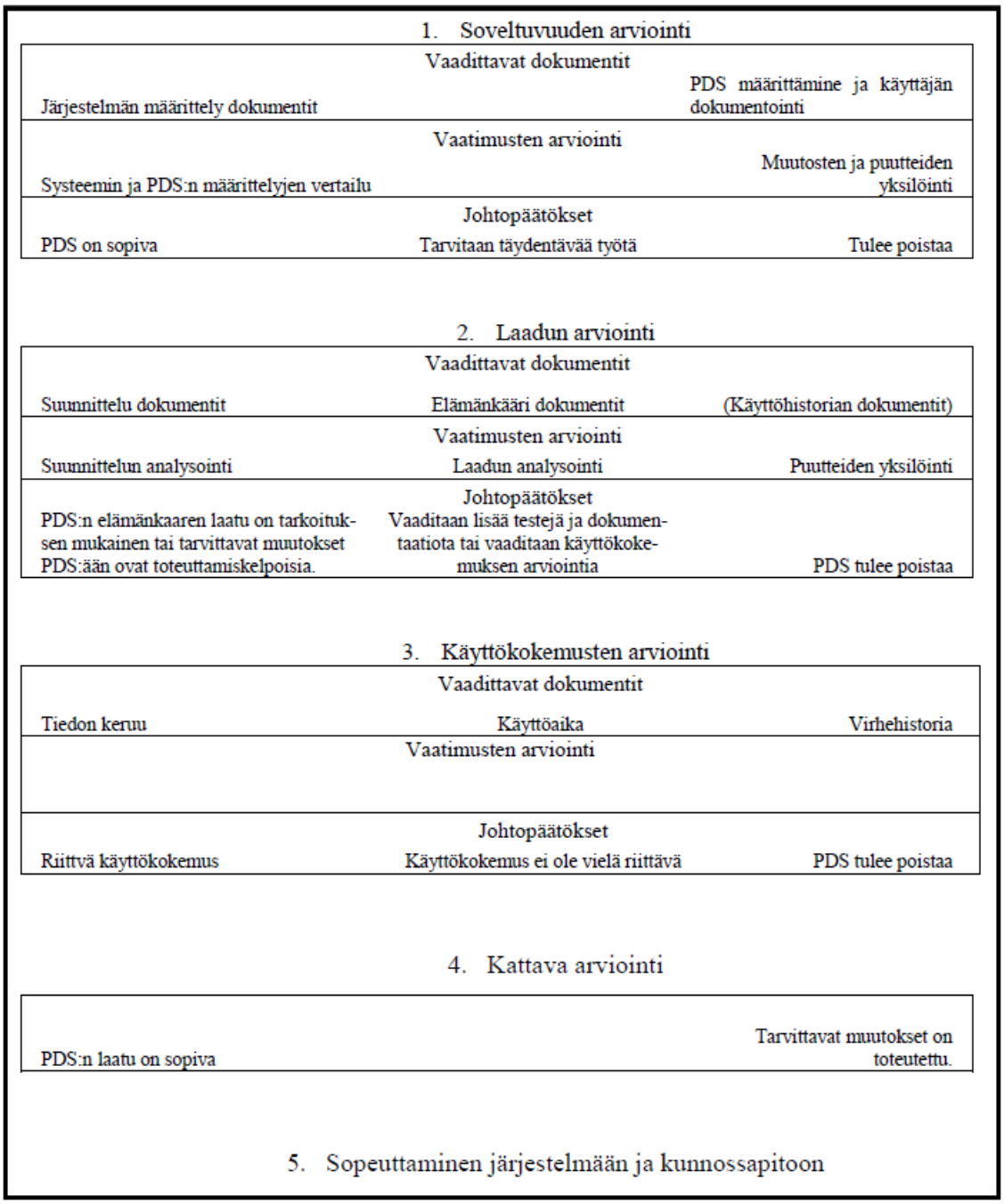
Polun testaus				
No	Testi	Havaitut virheet	Suoritetaan	Huomautukset
7	Jokainen lause toteutetaan vähintään kerran.	Koodia ei voida käyttää	Aina	
8	Kaikkien haarat suoritetaan vähintään kerran.	Virheitä suorituspolussa, ei takuita täydellisyydestä.	Aina	Sisältää 5; voi olla tyhjentävä, jos ei silmukoita ei ajoitus ongelmia. Puhtaasti kombinatorinen ongelma yhdistetään ohjelmarakenteeseen.
9	Jokaista predikaattitermiä käytetään jokaisessa haarassa.	Virheitä suorituspolussa ja tiedonsiirrossa.	Jos testien 8 ja 12 yhdistelmä ei ole sovellettavissa.	Sisältää 8; sisällytetty yhdistelmiin 9 ja 14.
10	Jokainen silmukka suoritetaan pienimmällä, suurimmalla ja vähintään yhdellä väli toistojen numerolla.	Virheitä silmukan hallinnassa ja taulukkodatan käsittelyssä.	Aina, jos ohjelma sisältää silmukoita.	Ei koske ”ikuisen silmukan” rakenteita.
11	Jokainen polku suoritetaan vähintään kerran.	Virheellinen suorituspolku.	Varmista, ettei suunnittelu ja ohjelmointivallinnat eivät tee tarkastuksesta liian hankalaa.	Saavutettavissa vain moduuleille. Sisältää 8, huomaa, että kaikki uudet silmukoiden suoritukset edellyttävät vähintään uutta polkua.

Datan liikkumistesti				
No	Testi	Havaitut virheet	Suoritetaan	Huomautukset
12	Jokainen tehtävä suoritetaan jokaiselle muistipaikalle vähintään kerran.	Virheitä tietovirrassa, muttei takuuta.	Käytettäessä taulukoita	
13	Kaikki viittaukset suoritetaan jokaiselle muistipaikalle vähintään kerran.	Virheitä tietovirrassa, tyhjentävä erikoistapauksissa.	Käytettäessä taulukoita	Sisältää 12 useimmissa tapauksissa. Vain järkevä yhdistettäessä 12 kanssa.
14	Kaikki yhteydet syötteestä lopputulokseen suoritetaan vähintään kerran kukin.	Kaikki tietovirta virheet	Aina yksilöllisille osioille	Vain mahdollinen moduuleille, sovelletaan 7, 8, tai 11.

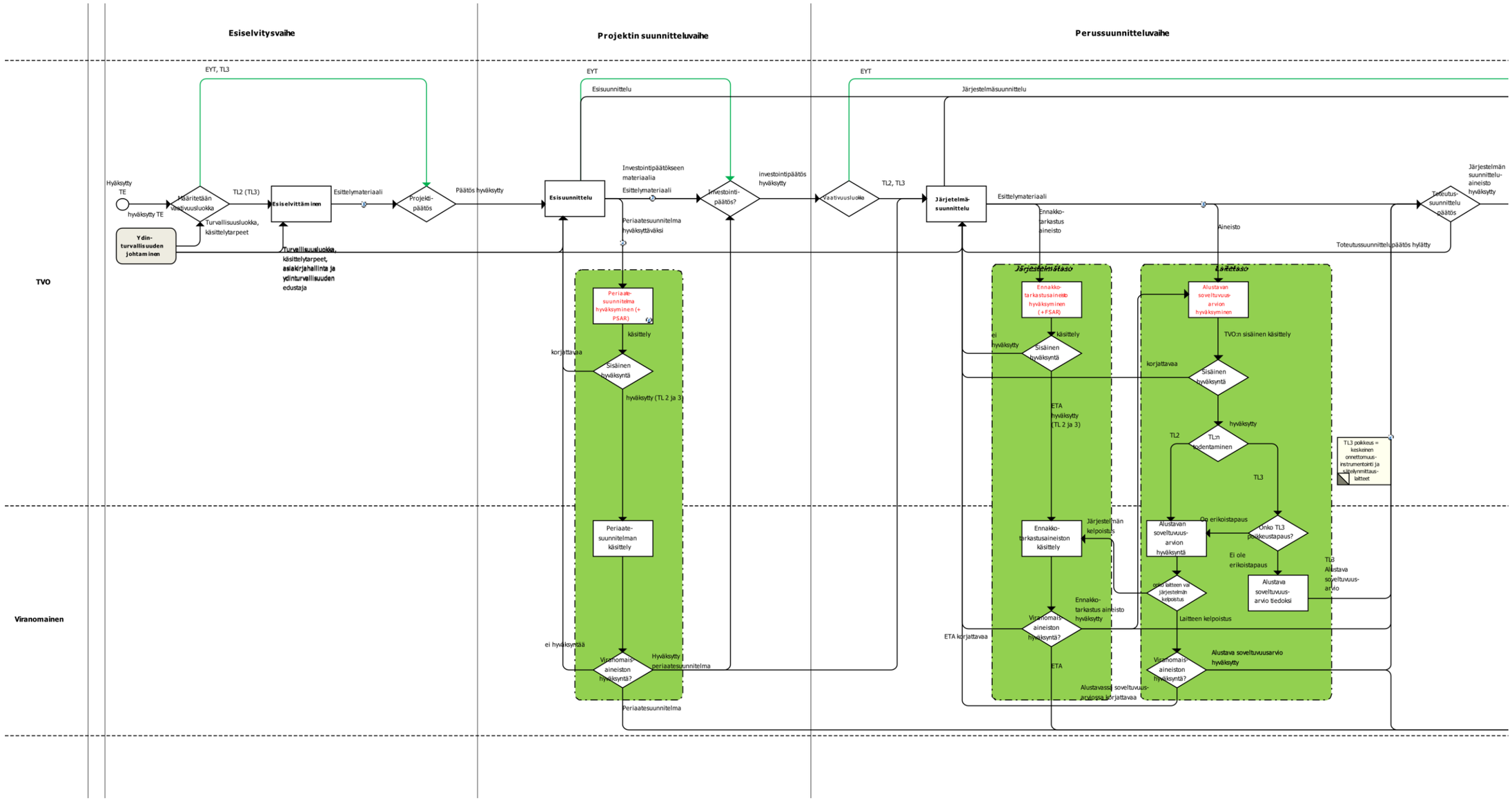
Ajoitustestaus				
No	Testi	Havaitut virheet	Suoritetaan	Huomautukset
15	Kaikkien aikarajoitusten tarkastus.	Ajoitus virheet, laskenta-aika liian pitkä	Aina	
16	Suurin mahdollinen keskeytysten sarja.	Järjestysvirheet.	Jos numero ei ole liian suuri	
17	Keskeytettyjen sekvenssien kaikki merkittävät sarjat.	Järjestysvirheet.	Aina	

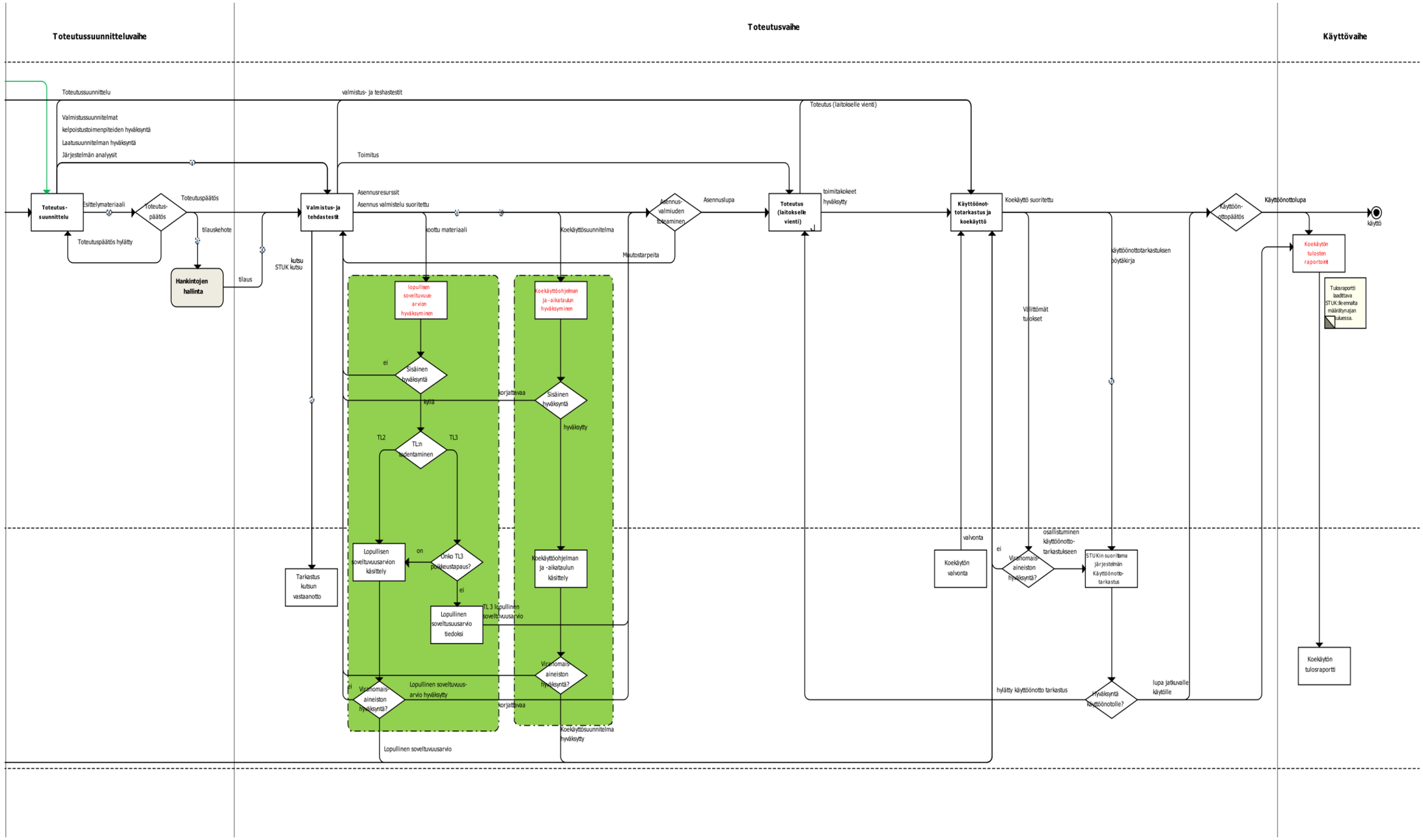
Sekalaista				
No	Testi	Havaitut virheet	Suoritetaan	Huomautukset
18	Tarkastetaan tiedonsyötön rajojen oikeellisuus.	Arvoavaruuden virheellinen jako.	Jos käytetään analogista syötettä.	Syötteiden lukumäärät ja tyypit löydetään analyyseillä.
19	Tarkastetaan aritmeettisten laskelmien riittävä tarkkuus kaikissa kriittisissä paikoissa.	Numeeriset virheet, virheet algoritmissa, pyöristysvirheet.	Jos tietokoneen sanan (word) pituus on lyhyt (short); monimutkainen aritmeettinen käyttö.	
20	Vain ohjelmille; moduuli-rajapinojen ja moduuli-vuorovaikutusten testi.	Virheellinen datan siirto moduulien välillä.	Aina	Testiapu tervetullut.
21	Jokainen moduuli kutsutaan vähintään kerran.	Virheellinen suorituspolku ja virheellinen tietovirta moduulien välillä, ei takuuta.	Aina	
22	Jokainen kutsu moduuliin suoritetaan vähinään kerran.		Aina	
23	Toiminta korkeilla kuormilla.	Järjestelmän ajoitus- ja vastaanottovirheet.	Aina	Varmistetaan systeemin robustisuus.

Liite 3. Kaavio standardissa IEC 60880 esitetystä kelpoistuksesta. (Muokattu lähteestä IEC 60880 2006: 117.)



Liite 4. Kelpoistusprosessimalli.




Toteutussuunnitteluvaihe
Toteutusvaihe
Käyttövaihe
Toteutussuunnittelu
Valmistussuunnitelmat
kelpoistustoimenpiteiden hyväksyntä
Laatusuunnitelman hyväksyntä
Järjestelmän analyysit
valmistus- ja teshastestit
Toimitus
Toteutus (laitokselle vienti)
Toteutus-suunnittelu
Esittelymateriaali
Toteutus-päätös
Toteutuspäätös
Toteutuspäätös hylätty
tilauskehote
Hankintojen hallinta
tilaus
kutsu
STUK kutsu
Valmistus- ja tehdastestit
Asennusresurssit
Asennus valmistelu suoritettu
koottu materiaali
Koekäyttösuunnitelma
Muutostarpeita
Asennus-valmiuden toteaminen
Asennuslupa
Toteutus (laitokselle vienti)
toimitakokeet hyväksytty
Käyttöönot-totarkastus ja koekäyttö
Koekäyttö suoritettu
Välittömät tulokset
käyttöönottotarkastuksen pöytäkirja
Käyttöön-ottopäätös
Käyttöönottolupa
käyttö
Koekäytön tulosten raportointi
Tulosraportti laadittava STUK:lle ennalta määrätynajan kuluessa.
lopullisen soveltuvuus-arvion hyväksyminen
ei
Sisäinen hyväksyntä
korjattavaa
kyllä
TL2
TL3
TL:n identaminen
Lopullisen soveltuvuusarvion käsittely
on
Onko TL3 poikkeustapaus?
ei
Lopullinen soveltusuusarvio tiedoksi
TL 3 lopullinen soveltuvuusarvio
Tarkastus kutsun vastaanotto
Koekäyttöohjelman ja -aikataulun hyväksyminen
Sisäinen hyväksyntä
hyväksytty
Koekäyttöohjelman ja -aikataulun käsittely
Viranomais-aineiston hyväksyntä?
ei
Viranomais-aineiston hyväksyntä?
Lopullinen soveltuvuus-arvio hyväksytty
korjattavaa
Koekäyttösuunnitelma hyväksytty
Lopullinen soveltuvuusarvio
valvonta
Koekäytön valvonta
ei
Viranomais-aineiston hyväksyntä?
osallistuminen käyttöönotto-tarkastukseen
STUK:in suorittama järjestelmän Käyttöönotto-tarkastus
hylätty käyttöönotto tarkastus
Hyväksyntä käyttöönotolle?
lupa jatkuvalle käytölle
Koekäytön tulosraportti