Aalto-yliopisto MS-E2177 Operaatiotutkimuksen projektityöseminaari

DYNAAMISIIN TAPAHTUMAPUIHIN PERUSTUVA TODENNÄKÖISYYSPOHJAINEN RISKIANALYYSI YDINVOIMALAMALLILLE

Projektisuunnitelma 8.3.2016

Lauri Nyman 219707
Sakke Rantala 84408M

AALTO-YLIOPISTON PERUSTIETEIDEN KORKEAKOULU, RISKPILOT AB JA TEKNOLOGIAN TUTKIMUSKESKUS VTT OY
Espoo, Finland

Sisällysluettelo

1. Projektin yleisesittely

Ydinvoimalaonnettomuuden seurauksia voivat olla vakavimmillaan kuolemantapaukset sekä laajat ympäristövahingot tai vähintään tuotannolliset haitat. Jotta onnettomuuden riski saadaan mahdollisimman pieneksi, ydinvoimalaympäristön riskien arviointi ja niiden hallinta erilaisin turvajärjestelyin on tärkeä osa ydinvoimalan suunnittelua, rakentamista sekä itse ydivoimalan sähköntuotantoprosessia.

Riskianalyysin tavoitteena on tukea päätöksentekoa eri vaiheissa siten, että vältettäisiin vahingon syntyminen, estettäisiin syntyneen vahingon laajeneminen sekä minimoitaisiin lopulliset vaikutukset. Vakavissa ongelmatilanteissa tapahtumien kulku ei ole yksikäsitteinen eikä deterministinen. Mahdollisia skenaarioita voidaan mallintaa esimerkiksi tapahtumapuu- ja vikapuumenetelmillä, jossa fysikaalisesti perusteltuihin tapahtumiin tai vikaantumisiin liittyy jokin todennäköisyysjakauma sekä vaikutus.

Tässä projektissa sovellamme todennäköisyyspohjaista riskiarviointimenetelmää (PRA[1], Probabilistic Risk Assessment) ydinvoimalan demomalliin. Työn konkreettisena tavoitteena on saada aiemmin käytössä ollut ydinvoimalamalli DOS-maailmasta Windows 7/8/10-maailmaan. Käytännössä vanhan järjestelmän olemassa oleva ohjelmakoodi tuodaan uuteen ohjelmaan. Tuonnin onnistuminen verifioidaan vertailemalla vanhan järjestelmän tunnettuja tuloksia saatuihin uusiin tuloksiin.

Projektin on tilannut yhteistyössä Teknologian tutkimuskeskus VTT Oy (VTT) sekä Riskpilot AB (Riskpilot). VTT:n tehtävänä on tehdä riippumatonta tutkimusta ja tuottaa teknologisia ratkaisuja julkiselle, yksityiselle ja kolmannelle sektorille. VTT ei tavoittele taloudellista voittoa vaan toimii pääosin konsultointiyrityksenä ja johtavana tutkijaorganisaationa. Suuruudeltaan VTT on Pohjois-Euroopan suurin soveltavaa tutkimusta tekevä organisaatio. Riskpilot on kansainvälinen konsultointiyritys, joka tarjoaa yrityksille tukea monimutkaisten teknisten systeemien turvallisuusanalyyseissä sekä projektien hallinnassa.

2. Riskianalyysin hyödyt

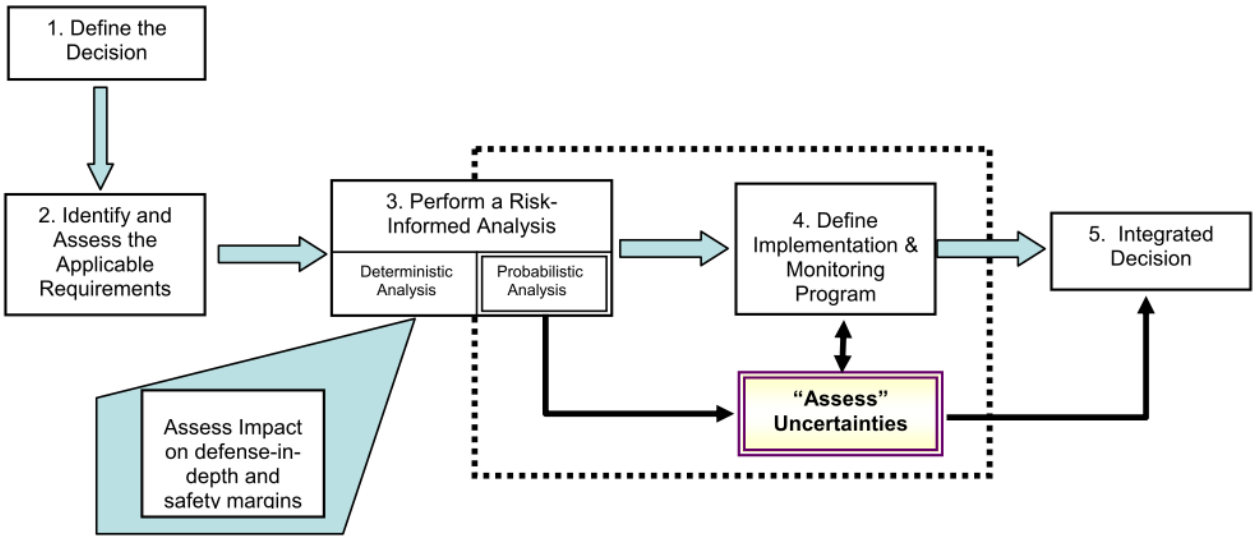
Riskianalyysin tavoitteena on tukea päätöksentekoa, jotta mahdolliset riskit ja niihin liittyvät vaikutukset osataan ottaa huomioon eri vaiheissa. NRC (s. 13, 2009) kuvaa riskitietoisen päätöksenteon vaiheet (kuva 1) ja luettelee esimerkkejä mahdollisista päätöksistä ydinvoimalakontekstissa:

- ydinvoimalan rakenteellinen suunnittelu ja operointi (materiaalit ja tuotantojärjestelmä)
- ydinvoimalan tekniset rajoitteet operoinnille (maksimituotanto tai tuotannon muutos)

[1] Usein myös termillä PSA (Probabilistic Safety Assessment, todennäköisyyspohjainen turvallisuusarviointi) viitataan samaan asiaan.

- huoltojaksojen tiheys (kuinka kauan voi olla huoltamatta)
- turvallisuusjärjestelmien yhtäaikainen huolto ja poiskytkentä
- turvallisuussuunnitelmien riittävyys onnettomuuksissa sekä henkilöstön, omaisuuden että ympäristön kannalta

Kuvassa 1 on korostettu epävarmuuksien huomiointi päätöksentekoprosessissa. Epävarmuudet voidaan jakaa kahteen luokkaan: *aleatorisiin* ja *episteemisiin*. Esimerkiksi nopanheiton tulokseen liittyy epävarmuus, koska silmäluku voi olla mikä tahansa väliltä 1 - 6. Tähän ei kuitenkaan liity episteemistä epävarmuutta, koska kaikki mahdolliset tulokset tunnetaan ja niille voidaan määrittää todennäköisyysjakauma. Nopanheittoon liittyvä epävarmuus on luonteeltaan aleatorista. Päätöksentekotilanteissa esiintyy yleisesti kuitenkin runsaasti niin sanottuja episteemisiä epävarmuuksia. Ydinvoimalakontekstin päätöksentekoprosessiin liittyen NRC (2009) esittää kolme esimerkkiä episteemisistä epävarmuuksista: parametrien epävarmuus, mallin epävarmuus sekä epävarmuus täydellisyydestä. Parametrien epävarmuus tarkoittaa sitä, että esimerkiksi inhimillisen tai tahallisen henkilövirheen todennäköisyysjakaumaa ei tunneta luotettavasti. Silti useiden komponenttien vikaantumisen todennäköisyys voidaan tuntea varsin hyvin – esimerkiksi diesel-generaattoreiden käynnistymistodennäköisyys on tilastollisesti tunnettu. Mallin epävarmuus syntyy, koska vasteita tapahtumille voidaan mallintaa useilla tavoilla ja keskenään yhtä hyvien mallien tulokset voivat olla erilaisia. Epävarmuus täydellisyydestä on sitä, että mallin laajuus ei kata välttämättä ongelman todellista laajuutta. Siksi jokin oleellinen alkutapahtuma saattaa jäädä kokonaan huomioimatta. Koska ydinvoimaonnettomuuden vaikutukset voivat olla suuria, pienenkin todennäköisyyden tapaukset täytyy huomioida.



Kuva 1: Riskitietoisen päätöksenteon vaiheet. Kuvan lähde: NRC (2009).

Työssä käytettävän ohjelman (ks. luku 3.2 FinPSA-ohjelma) ratkaisut perustuvat Monte Carlo-simulointiin. Menetelmä saattaa jättää jonkin todennäköisyysjakauman ”ohuen hännän” eli pienen todennäköisyyden tapahtuman huomiotta. Siksi pienillä määrillä simulaatioita ulostulona saatavien todennäköisyysjakaumien muoto saattaa poiketa toivotusta. Tämä luonteeltaan

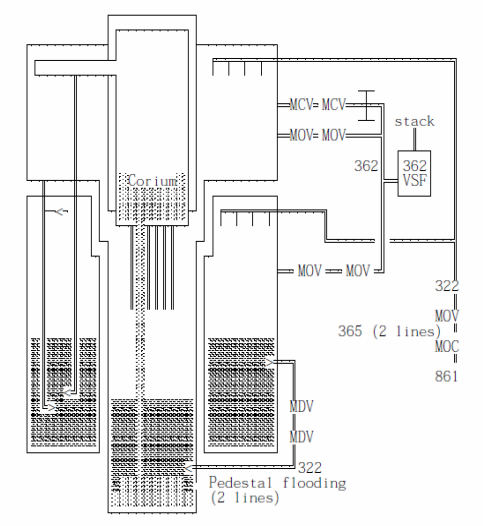
episteeminen epävarmuus on ratkaisumenetelmän epävarmuutta, jota tosin minimoidaan suurella määrällä simulaatioita sekä hyvillä satunnaisluvuilla. Projektiryhmän käytössä olevassa ohjelman demoversiossa simulaatioiden määrä on hyvin rajattu eikä mainittua epävarmuutta voida sulkea pois. Siksi tämän projektin puitteissa tehtävä mallin verifiointiin liittyy epäonnistumisen riski eikä todennäköisyysjakaumien validointi voi olla kovin luotettavaa.

3. Ydinturvallisuusanalyysi PRA-menettelyllä

3.1 Ydinvoimalaitos ja sen vikaantuminen

Ydinvoimalaitoksissa on useita peräkkäisiä ja rinnakkaisia turvamekanismeja (kuva 2), joiden tehtävänä on estää yksittäisen vikatilanteen aiheuttama onnettomuus. Esimerkiksi reaktorin jäähdytysjärjestelmille varavirtaa tuottavia generaattoreita on useita, jolloin järjestelmä kestää yhden vikaantumisen ilman vahinkoa. Voimalaitoksen ja sen turvajärjestelmien jokaisen komponentin erilaisille vikatilanteille voidaan määrittää todennäköisyydet. Nämä todennäköisyydet voivat myös olla ehdollisia ja riippua muista toteutuneista vikatilanteista. Tästä syntyy mallin dynaamisuus. Siksi dynaaminen todennäköisyyspohjainen riskiarviointi on luonteva lähestymistapa ydinvoimalaympäristössä. Kun yksittäisten vikatapahtumien todennäköisyydet ovat tiedossa, voidaan muodostaa niin sanottu tapahtumapuumalli, joka on esitelty tarkemmin luvussa 3.3 FinPSA:n metodit.

Ydinonnettomuus on seurausta useiden vikaantumisten muodostamasta ei-toivotusta tapahtumaketjusta, jollaisen todennäköisyys nykyaikaisissa voimalaitoksissa on häviävän pieni. Esimerkiksi vuoden 2011 Fukushiman ydinonnettomuuden tapauksessa Japanin rannikolle iskenyt tsunami aiheutti erilaisia vikaantumisia muun muassa reaktorien eri jäähdytysjärjestelmissä, mikä lopulta johti hallitsemattomaan onnettomuuteen (IAEA, 2011). Fukushimassa onnettomuuden aiheuttu mitoitusperiaatteiden riittämättömyys.



Kuva 2: Esimerkkikaavio ydinvoimalaitoksen onnettomuudenhallintajärjestelmästä. Kuvan lähde: Okkonen (1996).

3.2 FinPSA-ohjelma

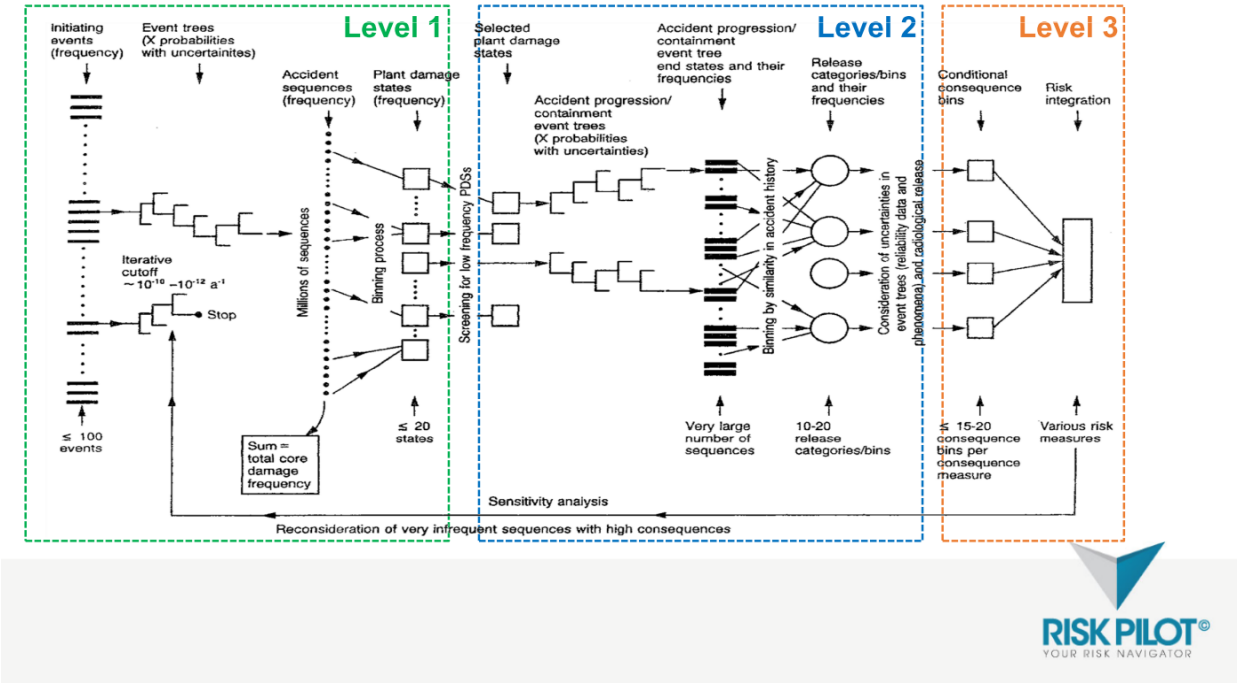
Vuosina 1988–2012 Säteilyturvakeskuksessa (STUK) kehitettiin PRA-menetelmään perustuvaa ohjelmistoa ydinturvallisuuden analysointiin DOS-käyttöjärjestelmässä. Ohjelmiston kehitys on siirtynyt vuonna 2012 STUK:lta VTT:lle. VTT:llä vanha DOS-ympäristössä ajettava ohjelma on siirretty nyt nykyaikaisiin graafisiin käyttöjärjestelmiin (Windows 7/8/10). Ohjelma perustuu tapahtumapuilla esitettäviin tapahtumaketjuihin ja vikapuihin. Vikaantumiset jaetaan kolmeen tasoon (graafisesti kuvassa 3):

1. Ydinreaktorin reaktorivaurioon johtavan tapahtumaketjun todennäköisyyspohjainen analyysi (erilaiset tapahtumaketjut ja niiden todennäköisyydet).

2. Vaiheen 1 reaktorivaurion vaikutukset ympäristöön pääseviin päästöihin (muun muassa cesium). Alkutapahtumilla todennäköisyysjakauma, muita jakaumia paljon: hyödynnetään Monte Carlo -simulaatiota.

3. Radioaktiivisten aineiden leviäminen ympäristöön (otetaan huomioon jakaumat tuulen suunnasta ja vauhdista sekä muita tekijöitä).

Okkonen (1996) kuvaa FinPSA:n perusteet kattavasti ja tarjoaa DOS-maailmassa käytetyt tapahtumasolmujen ohjelmakoodit. Lisäksi projektiryhmän käytössä on FinPSA:n manuaalit tasoille 1 ja 2.

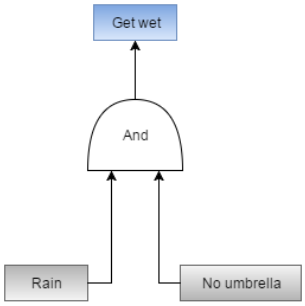


Kuva 3: PRA-menetelmän kolme tasoa. Kuvan lähde: Risk Pilot AB:n esitysmateriaali, esitetty 15.1.2016.

3.3 FinPSA:n metodit

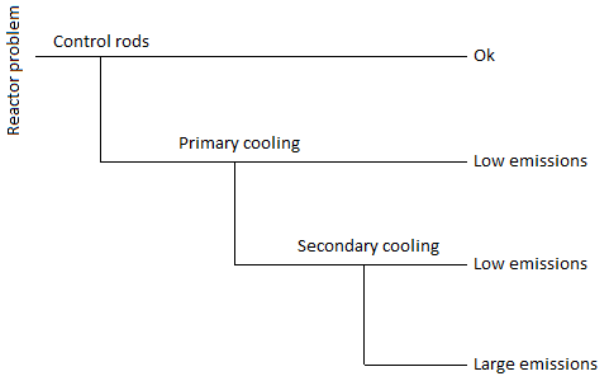
Tässä kappaleessa käsitellään FinPSA-ohjelman hyödyntämät tekniset menetelmät. Ne ovat tapahtuma- ja vikapuut sekä niihin liittyvät minimikatkosjoukot. Lopuksi arvioidaan menetelmien luotettavuutta ja toimivuutta. PSA:lla tarkoitetaan riskien tarkastelua tapahtumien todennäköisyys- ja frekvenssipohjaisella analyysillä. Tapahtumaketjuja mallinnetaan usein tapahtuma- ja vikapuilla.

Yleisesti on olemassa monimutkaisia syy-seuraus-suhteita, jotka on hyvä saada muotoiltua matemaattiseksi rakenteeksi analyysiä varten. Eräs tällainen rakenne on *vikapuu*, jossa toisistaan riippuvat tapahtumat yhdistetään logiikkaporteilla (and-, or- ja muut portit). Kuvan 4 vikapuu kuvaa tilannetta, jossa tarkastellaan henkilön kastumista sateen ja sateenvarjon käytön seurauksena. Esimerkissä henkilön kastumiseen vaaditaan satamisen lisäksi (AND) sateenvarjon puuttuminen.



Kuva 4: Esimerkki vikapuurakenteesta: sateen ja sateenvarjon vaikutus henkilön kastumiseen.

Tapahtumapuulla tarkoitetaan rakennetta, jossa jokaiseen tapahtumaan liittyy sen totuusarvo. Jokainen yksittäinen tapahtuma tuo tapahtumapuuhun uuden haaran. Yksinkertaistetun ydinvoimalaonnettomuuden tapahtumapuu esitetään kuvassa 5. Tapahtumapuussa on kuvattu reaktoriongelmista aiheutuvat vauriot riippuen säätösauvojen, pääjäähdytysjärjestelmän ja varajäähdytyksen toiminnasta. Kaikkien pettäminen yhdessä aiheuttaa vakavan onnettomuuden. Puussa ei pääjäähdytysjärjestelmän toimiessa tarkastella enää, toimiiko varajäähdytysjärjestelmä, koska varajäähdytyksen toiminta ei tällöin vaikuta enää systeemin toimintaan.



Kuva 5: Yksinkertaistettu ydinvoimalan tapahtumapuu.

Yksinkertaisissa tilanteissa voidaan määrittää kaikki mahdolliset vikapuiden ja tapahtumapuiden tapahtumakombinaatiot ja niiden todennäköisyydet. Kun järjestelmä sisältää paljon komponentteja, kaikkien tapahtumakombinaatioiden määrittäminen muuttuu laskennallisesti erittäin haastavaksi, tai käytännössä mahdottomaksi. Tätä varten huipputapahtumien (lopputapahtumien) todennäköisyyksien approksimointiin voidaan käyttää hyväksi niin sanottuja *minimikatkosjoukkoja*.

Katkosjoukolla tarkoitetaan sellaista joukkoa tapahtumia (ydinvoimalan tilanteessa vikaantuneita komponetteja), jotka aiheuttavat ei-toivottuja seurauksia (esimerkiksi päästöt ympäristöön). *Minimikatkosjoukolla* tarkoitetaan sellaista katkosjoukkoa, jossa minkä tahansa osan korjaaminen johtaa järjestelmän toimivuuteen. Nämä ovat oleellisia ydinvoimalan riskianalyysin kannalta, koska usein ydinvoimalassa tapahtuu juuri täsmälleen vaadittava määrä vikaantumisia eikä yhtään enempää. Minimikatkosjoukkojen löytäminen ja käsittely algoritmisesti on paljon helpompaa kuin kaikkien mahdollisten kombinaatioiden tutkiminen.

Varsinkin ydinvoimaloissa todennäköisyydet ovat niin pieniä, että on verraten epätodennäköistä, että vikaantumisia olisi yhtään enempää kuin vikaantumiseen vaadittu määrä. (jos komponentit pidetään ehjinä yleisesti). Tällaiset mahdollisuudet tulevat minimijatkosjoukkojen laskumenetelmässä huomioitua hiukan yläkanttiin. Tämä ei haittaa, koska todennäköisyydet ja riskit on hyvä huomioida riskianalyysin kannalta konservatiivisesti eli yläkanttiin. Ei-toivottujen tapahtumien todennäköisyyksien arviointi yläkanttiin takaa, että minimikatkosjoukkoja hyödyntävä menetelmä ei arvioi riskejä ainakaan alakanttiin. [Koutras et al. 2003] On kuitenkin muita asioita, joissa riskien alakanttiin arvioinnin mahdollisuutta on hyvä tarkastella: esimerkiksi Monte Carlo -menetelmä.

4 Projektin järjestäytyminen

Projektin loppuraportin kieli on englanti. Projektisuunnitelma tehdään suomeksi ja esitykset pidetään suomen kielellä.

4.1 Projektiryhmä

Projektiryhmä jakautuu kolmeen osaan. Opiskelijajäsenet suorittavat annetun tehtävän, projektin asettajat opastavat ja tukevat tehtävän suorittamisessa ja projektin valvoja valvoo projektia yleisellä tasolla ja tukee tarpeen mukaan.

Nimi	**Rooli projektissa**	**Organisaatio**
Lauri Nyman	Projektipäällikkö (opiskelija)	Aalto-yliopisto
Sakke Rantala	Projektityöntekijä (opiskelija)	Aalto-yliopisto
Jan-Erik Holmberg	Asiantuntija (Projektin asettaja)	Riskpilot
Tero Tyrväinen	Asiantuntija, FinPSA (Projektin asettaja)	VTT
Ahti Salo	Projektin valvoja	Aalto-yliopisto

4.2 Projektin ositus

Projekti jakautuu seuraaviin työvaiheisiin:

1. **Ydinvoimalaympäristön riskienhallinnan ja PSA:n metodiikan kuvaaminen**
   - Miksi riskienhallintaa tarvitaan ydinvoimalaympäristössä **(Sakke)**
   - Ydinvoimalaympäristön kvalitatiivinen ja kvantitatiivinen kuvaaminen **(Lauri & Sakke)**
   - FinPSA:n perusperiaatteet (tekniset metodit) ja sovelluskohteet, ydinturvallisuusanalyysi **(Lauri)**
   - Kirjallisuuden tutkiminen: PSA ja ydinvoimalan turvallisuusanalyysi **(Lauri & Sakke)**

2. **Demomallin tuominen FinPSA ohjelmaan**
   - Vanhojen ohjelmakoodien siirtäminen uuteen ohjelmaan moduuleittain (DOS -> Windows 7/8/10) **(Lauri & Sakke, ohjelmakoodi jaetaan mahdollisuuksien mukaan paloittain)**
   - Saada moduulit ja funktiot yhdessä toimivaksi kokonaisuudeksi **(Lauri & Sakke , pyritään rakentamaaan ja testaamaan osissa mahdollisuuksien mukaan)**

3. **Väliraportti**
   - Ohjelmakoodin siirtämisen tarkempi kuvaaminen (työvaiheet ja projektin aikainen projektin suunnittelu käytännössä) ja kohdatut haasteet.
   - Etenemissuunnitelma

4. **Ohjelman toiminnan verifiointi**
    - Toimivan ohjelman luominen **(Lauri & Sakke)**
    - Tulosten verifiointi **(Lauri & Sakke, mahdollisten virheiden tarkastelu voidaan osittaa)**

5. **Työn viimeistely ja loppuraportti**
    - Mallin validointi ja parannusehdotukset **(Jos mahdollista ja jää aikaa)**
    - Viimeistely ja yhdistely kokonaisuudeksi **(Lauri & Sakke, pääkontribuutio omissa osa-alueissa)**
    - Loppuraportti **(Lauri & Sakke)**

4.3 Projektin aikataulu

Projektin etenemissuunnitelmaa kuvataan kaaviossa 1. Tähän mennessä projektiryhmä on kokoontunut kaksi kertaa ja saanut koulutusta liittyen projektin käytäntöihin: mitä halutaan tehtävän ja miten se toteutetaan. Lisäksi olemme saaneet koulutusta projektiin liittyvään teoriaan. VTT:llä on myös ohjeistettu FinPSA-ohjelman käytössä. Projektiryhmän on myös pyydettäessä mahdollista saada lisäkoulutusta ja apua ylläoleviin osa-alueisiin. Ohjelman validointi ja parannusehdotusten määrittäminen ovat mukana optiona, koska demomallissa ohjelman toiminnallisuutta rajoitetaan huomattavasti.

Taulukko 1 Projektin aikataulusuunnitelma

Tilanne 23.2.	*Vaihe / Viikko*	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
100 %	Projekti alkaa	■																
80 %	PRA ja FinPSA-koulutus		■			■												
100 %	Projektisuunnitelma 24.2.			■	■	■	■	■										
10 %	FinPSA mallin importaus								■	■	■	■						
0 %	Väliraportti pe 1.4. (viikko 13)										■	■	■					
0 %	FinPSA-mallin verifiointi											■	■	■	■			
0 %	Mallin validointi + parannus													■	■	■	■	
0 %	Loppuraportti pe 6.5. (viikko 18)															■	■	■

4.4 Projektin riskit, niihin liittyvät seuraukset ja korjaustoimenpiteet

Riski	Mahdollisuus	Haitat	Korjaustoimenpiteet
Henkilön sairastuminen	Suuri	Työn viivästyminen (matala)	Tehtävien allokointi muille/muuta
Henkilön luopuminen projektista	(Toteutunut)	Työmäärän kasvaminen tai projektin epäonnistuminen	Tavoitteiden uudelleenmäärittely siten, että projekti saadaan oleellisin osin maaliin.
FinPSA:n tekniset ongelmat	Keskisuuri	Huonot lopputulokset (keskisuuri)	Viesti VTT:lle ohjelman kehittäjille.
FinPSA:n demoversion tekniset rajoitteet	Keskisuuri	Verifiointi epäonnistuu (keskisuuri)	Riski ei ole hallittavissa.
Laajan ohjelmiston tuottaminen ilman versionhallintajärjestelmää	Suuri	Ohjelmakoodi ei toimi (suuri)	Riski voidaan välttää näin pienessä ryhmässä selkeällä tehtäväjaolla sekä selkeillä päivityskäytännöillä.

Lähdeviitteet

[IAEA], Fukushima Nuclear Accident Update Log, 2011 (2. Kesäkuuta 2011)
https://www.iaea.org/newscenter/news/fukushima-nuclear-accident-update-log-49

Koutras, M. V., S. Tsitmidelis, and V. Zissimopoulos. "Evaluation of reliability bounds by set covering models." *Statistics & probability letters* 61.2 (2003): 163-175.

[NRC, 2009] U.S. Nuclear Regulatory Commission, *Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making*, NUREG-1855, vol. 1, March 2009.

Okkonen, Timo. *Development of a Parametric Containment Event Tree Model for a Severe PWR Accident*. Finnish Centre for Radiation and Nuclear Safety, 1996.

VTT, FinPSA Level 1 Manual, 201X

VTT, FinPSA Level 2 Manual, 2016