STUK-TR 9 / HUHTIKUU 2010

TR

Todennäköisyyspohjainen riskien seuranta ydinvoimalaitosten valvonnassa

Diplomityö

Janne Laitonen

Säteilyturvakeskus
Strålsäkerhetscentralen
Radiation and Nuclear Safety Authority

STUK

STUK-TR 9 / HUHTIKUU 2010

Todennäköisyyspohjainen riskien seuranta ydinvoimalaitosten valvonnassa

Diplomityö

Janne Laitonen

Aalto-yliopisto, Teknillinen korkeakoulu
Informaatio- ja luonnontieteiden tiedekunta

Valvoja prof. Ahti Salo

Ohjaaja DI Reino Virolainen

STUK • **SÄTEILYTURVAKESKUS**
STRÅLSÄKERHETSCENTRALEN
RADIATION AND NUCLEAR SAFETY AUTHORITY

Osoite/Address • Laippatie 4, 00880 Helsinki
Postiosoite / Postal address • PL / P.O.Box 14, FIN-00881 Helsinki, FINLAND
Puh./Tel. (09) 759 881, +358 9 759 881 • Fax (09) 759 88 500, +358 9 759 88 500 • www.stuk.fi

STUKin raporttisarjoissa esitetyt johtopäätokset ovat tekijöiden johtopäätöksiä, eivätkä ne välttämättä edusta Säteilyturvakeskuksen virallista kantaa.

ISBN 978-952-478-533-4 (nid) Yliopistopaino, Helsinki 2010
ISBN 978-952-478-534-1 (pdf)
ISSN 1796-7171

Aalto-yliopisto
Teknillinen korkeakoulu
Informaatio- ja luonnontieteiden tiedekunta

Janne Laitonen

Todennäköisyyspohjainen riskien seuranta ydinvoimalaitosten valvonnassa

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi diplomi-insinöörin tutkintoa varten teknillisen fysiikan ja matematiikan tutkinto-ohjelmassa.

Helsingissä, 5.3.2010

Valvoja:	Professori Ahti Salo
Ohjaaja:	Diplomi-insinööri Reino Virolainen

Aalto-yliopisto
Teknillinen korkeakoulu
Informaatio- ja luonnontieteiden tiedekunta

DIPLOMITYÖN TIIVISTELMÄ

Tekijä:	Janne Laitonen
Työn nimi:	Todennäköisyyspohjainen riskien seuranta ydinvoimalaitosten valvonnassa
Päivämäärä:	5.3.2010 **Sivuja:** viii+66
Tutkinto-ohjelma:	Teknillisen fysiikan ja matematiikan tutkinto-ohjelma
Pääaine:	Systeemi- ja operaatiotutkimus
Sivuaine:	Kognitiivinen teknologia
Opetusyksikkö:	Mat-2 Sovellettu matematiikka
Työn valvoja:	Prof. Ahti Salo
Työn ohjaaja:	DI Reino Virolainen

Tämä työ tarkastelee ydinvoimalaitosten todennäköisyyspohjaista riskien seurantaa. Suomessa ydinvoimaloiden turvallisuutta valvova viranomainen on Säteilyturvakeskus, jolle voimayhtiöt raportoivat käyttötapahtumistaan. Aluksi työssä esitellään ydinturvallisuuden ja todennäköisyyspohjaisen riskien arvioinnin (PRA) keskeisimpiä käsitteitä, joiden ymmärtäminen on riskien seurannan kannalta välttämätöntä. Työssä keskitytään tason 1 PRA-malleihin.

Riskien seurannassa arvioidaan PRA-perustaisesti sattuneiden käyttötapahtumien aiheuttamaa ehdollisen sydänvauriotodennäköisyyden kasvua. Seurannan tavoitteena on luokitella tapahtumat niiden vakavuuden perusteella, seurata tapahtumien toistuvuutta laitoksen elinkaaren aikana ja tapahtumia analysoimalla oppia aikaisemmista virheistä ja puutteista. Työssä käsitellään riskien seurannan teoreettisia perusteita ja ongelmia, jotka liittyvät ehdollisen todennäköisyyden jälkikäteislaskentaan: Ehdollinen onnettomuustodennäköisyys määritetään tilanteelle, jonka tiedetään olleen ”läheltä piti” -tilanne. Tämä ongelma ratkaistaan erottamalla riskien seurannassa alkutapahtumat ja laiteviat laskennallisesti omiin luokkiinsa. Vuoden 2009 aikana Suomen ydinvoimaloissa ei sattunut ainoatakaan alkutapahtumaa. Laitevikojen osalta merkittävimmät tapahtumat olivat Loviisan laitosyksiköissä ilmenneet toistuvat ilmastointiviat ja Olkiluodon laitosyksiköissä tapahtuneet dieselgeneraattoreiden viat.

Riskien seuranta on Säteilyturvakeskuksessa keskittynyt riskin mukaan luokiteltujen tapahtumien vuosittaiseen tilastointiin. Näiden tapahtumien lukumäärät vaihtelevat vuodesta toiseen, sillä käyttötapahtumien voi olettaa noudattavan satunnaisprosessia. Tästä syystä vikojen lukumäärästä on ollut vaikea tehdä luotettavia päätelmiä tilanteen poikkeuksellisuudesta. Huomio on kiinnittynyt absoluuttisiin arvoihin ja satunnaisvaihtelun merkitystä ei ole arvioitu. Kehitetty menetelmä simuloi uusiutumisprosessin avulla vikatapahtumia, joiden riskimerkitys arvioidaan PRA-mallin rakennefunktion avulla. Näin vikaantumisten lukumäärälle saadaan epävarmuusjakauma tukemaan päätöksentekoa. Esimerkkinä käytetään Olkiluodon laitosyksiköiden vikatapahtumia. Tulokset viittaavat odotetusti käytetyn PRA-mallin parametrien konservatiivisuuteen.

Avainsanat: riskien seuranta, riskianalyysi, PRA, ydinvoimalaitos

Aalto University
School of Science and Technology
Faculty of Information and Natural Sciences

ABSTRACT OF
MASTER'S THESIS

Author:	Janne Laitonen
Title:	Risk Follow-up in Regulatory Control of Nuclear Safety
Date:	5 March 2010 **Pages:** viii+66
Degree programme:	Degree Programme in Engineering Physics and Mathematics
Major subject:	Systems and Operations Research
Minor subject:	Cognitive Technology
Chair:	Mat-2 Applied Mathematics
Supervisor:	Prof. Ahti Salo
Intructor:	Reino Virolainen, M.Sc.

This thesis examines risk follow-up in the framework of regulatory control of nuclear safety. In Finland, the power companies are obliged to report all operational events to the Radiation and Nuclear Safety Authority (STUK). First, the essential concepts of nuclear safety and probabilistic risk assessment (PRA) are introduced, for they build the foundation of risk follow-up. The thesis concentrates on level 1 PRA-models.

In risk follow-up, the incremental conditional core damage probability of operational events is evaluated based on a plant specific PRA-model. The objective of this PRA-based event analysis is to classify the events based on their risk significance, follow the recurrence of the events during the life cycle of the nuclear power plant, and offer lessons learned for future improvements. The theoretical concepts and methodological problems of risk follow-up are introduced, one issue being retrospective probability assessment. This means that the probability of an accident is evaluated given the fact that no accident ever occurred. This problem is handled by separating the operational information into two modes. The first concerns initiating events and the second component failures. In 2009, no initiating events occurred at Finnish nuclear power plants. The most risk significant events at Loviisa site were recurrent failures in ventilation and at Olkiluoto site diesel generator failures.

At STUK, risk follow-up is focused on the yearly risk-based classification of operational events. The number of these events varies every year depending on the assumed stochastic properties of the events. Therefore, it has been difficult to make reliable inferences on the abnormality of the yearly result. Attention has been paid to the absolute number of events, and the significance of the stochastic process has not been evaluated. The method introduced in this thesis simulates component failures through a stochastic process, and the risk significance is assessed based on a PRA-model. This way, an uncertainty distribution for the number of failures is obtained to help the inference and decision-making. As an example, events at Olkiluoto site are utilized. The results indicate that the parameters of the PRA-model are conservative, as expected.

Keywords: risk follow-up, precursor study, risk analysis, PRA, nuclear power plant

Alkusanat

Tämä diplomityö on tehty Säteilyturvakeskuksen Ydinvoimalaitosten valvonta -osaston Riskianalyysit-toimistossa.

Haluan kiittää toimiston päällikköä DI Reino Virolaista mahdollisuudesta diplomityön tekoon sekä asiantuntevasta ohjauksesta työn eri vaiheissa. Kiitokset kuuluvat myös työn valvojalle professori Ahti Salolle, jonka tarkkaavaiset kommentit ja nopea reagointi edesauttoivat työn valmistumista. Lisäksi haluan kiittää Säteilyturvakeskuksen henkilökuntaa työhön liittyvistä ja liittymättömistä keskusteluhetkistä.

Lopuksi kiitän vanhempiani, jotka ansaitsevat suuret kiitokset tuesta opintojeni aikana, sekä veljiäni ja ystäviäni, jotka auttoivat pääsemään irti arjen pyörteistä.

Helsingissä, 5.3.2010

Janne Laitonen

Sisältö

Lyhenteet ja merkinnät

CCDP	Ehdollinen sydänvauriotodennäköisyys
ΔCCDP	Ehdollisen sydänvauriotodennäköisyyden kasvu
CCF	Yhteisvika
HRA	Inhimillisen luotettavuuden arviointi
PRA	Todennäköisyyspohjainen riskien arviointi
PSA	Todennäköisyyspohjainen turvallisuuden arviointi
b_i	Tapahtumapuun i. haara
E	Perustapahtuma
F	Epäonnistuminen
H_j	Tapahtumapuun haarautumiskohtaan j ulottuva historia
H_t	Riskien seurannassa käytetty hetkeen t ulottuva tapahtumahistoria
H_t^*	Hetkeen t ulottuva tunnettu, täydellinen tapahtumahistoria
H_t^1	Alkutapahtumat huomioiva tapahtumahistoria
H_t^2	Laiteviat huomioiva tapahtumahistoria
IE	Alkutapahtuma
M	Minimikatkosjoukko
S	Onnistuminen
T	Vikapuun huipputapahtuma
X	Tapahtuma
y	Onnettomuuden sisältävä tapahtumaketjujen aliavaruus
a	Käytettävyys
a_{ave}	Aikakeskiarvoistettu käytettävyys
C	Seuraus, satunnaismuuttuja
c	Seuraus
g	Järjestelmän logiikkaa kuvaava rakennefunktio
N	Vikojen lukumäärä, satunnaismuuttuja
n	Vikojen lukumäärä

Q	PRA-mallin sisältämät parametrit
q	Testauksesta aiheutuvan vian todennäköisyys
q_0	Tositarvekäynnistyksen epäonnistumisen todennäköisyys
R	Riski
r	Luotettavuus
s	Menneisyydessä oleva ajanhetki, $s < t$
T	Aika, satunnaismuuttuja
t	Aika
t_f	Keskimääräinen vikaantumisaika
t_r	Keskimääräinen korjausaika
t_t	Koestuksen (testaus) kesto
t_0	Tositarvetilanteen kesto
u	Epäkäytettävyys
u_{ave}	Aikakeskiarvoistettu epäkäytettävyys
β	Yhteisvikataajuuden ja kokonaisvikataajuuden suhde
λ	Vian tai onnettomuuden taajuus
λ_{I}	Yksittäisen komponentin vikataajuus
λ_{CCF}	Yhteisvikataajuus
$\lambda_s(\mathrm{y}\|\mathrm{H}_t)$	Onnettomuuden taajuus menneisyydessä ajanhetkellä s ($s < t$) historialle H_t ehdollistettuna
λ_0	Tositarvetilanteen aikainen vikataajuus
μ	Korjausintensiteetti eli korjautuvuus
τ	Tarkastelu- tai testausväli

Luku 1

Johdanto

Ydinenergian hyödyntämisen yhteydessä syntyy suuria määriä radioaktiivisia aineita. Ydinvoimalaitosonnettomuuksiin liittyvät riskit ympäristölle aiheutuvatkin lähes täysin reaktoriin kertyvistä radioaktiivisista fissiotuotteista, joiden lähettämä säteily voi aiheuttaa vahinkoa elolliselle ympäristölle ja rajoituksia maan käytölle. Tämän takia radioaktiivisten aineiden pääsy ympäristöön on estettävä luotettavasti. Ydinenergian hyödyntämisen edellytyksenä on sen käytön turvallisuus, joka on pidettävä niin korkealla tasolla kuin käytännöllisin toimenpitein on mahdollista.

Turvallisuuden varmistamiseksi ydinenergian käyttö on luvanvaraista ja tarkoin valvottua. Suomessa ydinlaitoksen rakentaminen edellyttää sijaintikunnan, valtioneuvoston ja eduskunnan hyväksyntää. Lisäksi rakentamisen ja käytön edellytyksenä on, että turvallisuusviranomaiset ovat varmistuneet laitoksen turvallisuudesta. Käytön aikana turvallisuuden kehittämiseksi on tehtävä ne toimenpiteet, joita voidaan pitää perusteltuina ottaen huomioon käyttökokemukset ja turvallisuustutkimukset sekä tieteen ja tekniikan kehittyminen.

Ydinenergian rauhanomainen käyttö aloitettiin 1950-luvulla. Tällä hetkellä maailmassa on 436 teollisessa käytössä olevaa ydinreaktoria [1] ja vuoden 2010 alkuun mennessä ydinvoimalaitoksilta oli kertynyt kokemuksia lähes 15000 vuoden ajalta [2]. Suomessa on tällä hetkellä käytössä viisi ydinreaktoria, joista ensimmäinen rakennettiin tutkimusreaktoriksi Otaniemeen vuonna 1962 [3]. Neljä muuta, joista kaksi omistaa Fortum Loviisassa ja toiset kaksi Teollisuuden Voima Olkiluodossa, ovat kaupallisessa käytössä. Viides kaupallinen ydinvoimalaitos on rakenteilla Olkiluotoon (Olkiluoto 3), jossa sähköntuotannon arvioidaan alkavan vuonna 2012.

Lisäydinvoiman rakentamisesta Suomeen käydään tällä hetkellä keskustelua, sillä Fennovoima, Fortum ja Teollisuuden Voima jättivät vuonna 2009 lupahakemuksensa uuden ydinvoimalaitoksen rakentamiselle. Hallitus esittänee kantansa vuoden 2010 keväällä, jonka jälkeen eduskunta äänestää lupien myöntämisestä.

1.1 Työn tavoite

Säteilyturvakeskus vastaa ydinenergian käytön turvallisuusvalvonnasta Suomessa. Yksi osa käytönvalvontaa on käyttötapahtumien seuranta ja niiden riskimerkityksen arviointi. Riskimittana seurannassa käytetään tapahtumaan liittyvää sydänvauriotodennäköisyyden (conditional core damage probability, CCDP) kasvua. Tapahtumat jaotellaan riskin mukaan kolmeen kategoriaan ja tarkoituksena on seurata kuhunkin kategoriaan liittyvien tapahtumien vuosittaista lukumäärää.

Tässä seurannassa on kaksi ongelmaa, joita tässä työssä pyritään ratkaisemaan. Ensimmäinen liittyy laskentamenetelmien määrittelyyn. Riskin jälkikäteislaskennassa menneet tapahtumat tunnetaan, joten onnettomuustodennäköisyys tälle historialle ehdollistettuna on triviaalisti 0, jos onnettomuutta ei sattunut. Tällöin tapahtumien seuranta ja järjestäminen niiden vakavuuden perusteella ei ole mahdollista. Intuitiivisesti on kuitenkin selvää, että jotkut tapahtumat ovat vakavampia ja lähempänä onnettomuustilannetta kuin toiset eli jonkinlaisen laskentasäännön määritteleminen voisi olla mielekästä. Tavoitteena on käytännöllisten laskentasääntöjen määrittely, jotta menneille tapahtumille voidaan laskea riskimerkitys siitä huolimatta, että onnettomuusriski ei tapahtumassa toteutunutkaan.

Toinen ongelma liittyy tapahtumien lukumäärän seurantaan. Laitoksella tapahtuvia laitevikoja ja alkutapahtumia on mielekästä pitää satunnaisilmiöinä, joten näiden tapahtumien lukumäärä vaihtelee vuodesta toiseen jonkin odotettavissa olevan arvon ympärillä. Tavoitteena on tutkia tätä prosessia ja pyrkiä arvioimaan tapahtumien odotettavissa olevaa lukumäärää ja vaihtelua eri riskikategorioissa, jolloin voidaan vastata kysymykseen, onko tehty havainto vain satunnaisvaihtelun aiheuttamaa vai voidaanko esimerkiksi tulkita voimayhtiön turvallisuuskulttuurin heikentyneen. Sivutuloksena saadaan karkea arvio käytetyn riskimallin parametrien oikeellisuudesta ja havaitaan mahdollisia virheitä. Tarvittavat tiedot käyttötapahtumista kerätään voimayhtiöiden käyttötapahtumaraporteista.

1.2 Työn rakenne

Aluksi työssä esitellään käytetyt menetelmät yleisemmin suurempina kokonaisuuksina ja tämän jälkeen tarkastelua syvennetään asteittain. Luvussa 2 käydään läpi ydinturvallisuuden keskeisiä perusteita sekä deterministisen periaatteiden että riskitietoisen lähestymistavan kannalta ja esitellään lyhyesti todennäköisyyspohjaisen riskianalyysin sovelluksia ydinvoimalaitosten turvallisuuden parantamisessa. Seuraavassa luvussa todennäköisyyspohjaista riskianalyysia käsitellään tarkemmin ja määritellään riskin käsite. Lisäksi tässä luvussa esitellään viranomaisvaatimuksia ja joitain riskianalyysin erityispiirteitä ydinvoimasovellusten kannalta.

Luvussa 4 esitellään todennäköisyyspohjaisen riskien arvioinnin laskentamenetelmiä lähtien systeemiä kuvaavasta rakennefunktiosta sekä tapahtuma- ja vikapuista. Tämän jälkeen syvennytään yksittäisten laitteiden ja komponenttien mallinnukseen luotettavuustekniikan avulla. Luvussa 5 käsitellään todennäköisyyspohjaisen riskien jälkikäteislaskennan erityispiirteitä ja oletuksia, jonka jälkeen esitellään käytännön keino riskien jälkikäteislaskennalle ja tapahtumien yleisyyden arvioimiselle. Laskentatuloksia verrataan pääasiassa Olkiluodon laitosyksiköiden käyttötapahtumiin. Luku 6 on varattu yhteeenvedolle ja johtopäätöksille.

Luku 2

Ydinturvallisuusperiaatteet ja riskitietoisuus

Ydinvoimalaitosten turvallisuuden kannalta on keskeistä ottaa huomioon odotettavissa olevat käyttöhäiriöt ja oletetut onnettomuudet laitoksen suunnittelussa. Tarkastelun kohteena ovat sekä sisäiset tapahtumat, kuten laiteviat, laitosprosessien häiriöt ja käyttöhenkilökunnan virheet, että ulkoiset tekijät, joita ovat mm. tulipalot, tulvat, maanjäristykset, poikkeukselliset sää- ja ympäristöolosuhteet sekä lentokoneiden törmäykset.[3]

Vaadittujen turvallisuusmääräysten täyttäminen on osoitettava tarvittaessa kokeellisin ja laskennallisin menetelmin. Tähän käytetyt turvallisuusanalyysit voi jakaa karkeasti kahteen osaan: deterministisiin onnettomuusanalyyseihin ja todennäköisyyspohjaiseen riskien arviointiin.[4]

2.1 Deterministiset turvallisuusperiaatteet

Deterministisillä onnettomuusanalyyseillä selvitetään tapahtumien eteneminen onnettomuustilanteessa ja perustellaan sitä, kuinka hyvin laitoksen tekniset ratkaisut täyttävät määritellyt turvallisuusvaatimukset. Analyysin avulla voidaan esimerkiksi arvioida jäähdyteveden tarvetta putkikatkon sattuessa ja mitoittaa tarvittavat turvallisuusjärjestelmät, kuten tarvittavien hätäpumppujen määrä.[4]

Turvallisuussuunnittelun lähtökohdaksi valitaan pahimpia mielekkäästi kuviteltavissa olevia tapahtumia ja olosuhteita, joiden aiheuttamat rasitukset ja kuormitukset arvioidaan laskennallisten ja kokeellisten menetelmien avulla. Rakenteet ja järjestelmät mitoitetaan niin, että tapahtumien seuraukset pysyvät vaatimusten sallimissa rajoissa turvallisuusjärjestelmien toimiessa minimikapasiteetillaan. Laitteiden vikaantumisen mahdollisuus otetaan analyyseissa huomioon tavallisesti siten, että alkutapahtuman lisäksi kuhunkin turvallisuusjärjestelmään oletetaan samanaikaisesti yksi tai useampi mahdollisimman haitallinen vika ja muilta osin järjestelmien oletetaan toimivan suunnitellusti, jolloin lähestymistapa on lähtökohdiltaan deterministinen.[3]

Deterministiset turvallisuusperiaatteet sisältävät syvyyssuuntaisen turvallisuusajattelun käsitteen, josta voidaan johtaa myös muita turvallisuusjärjestelmien suunnitteluperiaatteita.

2.1.1 Syvyyssuuntainen turvallisuusajattelu

Syvyyssuuntaisella turvallisuusajattelulla (defence in depth) tarkoitetaan suunnittelufilosofiaa, jolla taataan kolmen olennaisen turvallisuustehtävän – reaktiivisuuden hallinnan, polttoaineen jäähdyttämisen ja radioaktiivisen materiaalin eristyksen – toiminta. Se on yksi tärkeimpiä ja perustavanlaatuisia ydinturvallisuuden periaatteita, jossa asetetaan useita peräkkäisiä, toisiaan varmentavia suojatoimia kompensoimaan mahdollisista inhimillisistä virheistä ja järjestelmä- tai laitevioista johtuvaa puutteellista onnettomuustilanteen hallintaa. Näin turvallisuustavoitteet saavutetaan, vaikka yksi suojauksen taso epäonnistuisi tai vaikka sattuisi hyvin poikkeuksellisten vikojen yhdistelmä. Erityistä huomiota on kiinnitettävä tapahtumiin, jotka voivat rikkoa monia järjestelmiä ja läpäistä useita suojauksen tasoja. Näitä tapahtumia ovat esimerkiksi tulipalot, tulvat ja maanjäristykset. Turvallisuuden varmistamisessa voidaan erottaa ennaltaehkäisevä, suojaava ja lieventävä taso.[3, 5]

Ennaltaehkäisevän tason tarkoituksena on estää kaikki poikkeamat laitoksen normaalista käyttötilasta. Tämän takia laitteiden suunnittelussa, valmistuksessa, asennuksessa ja huollossa sekä käytössä sovelletaan korkeita laatuvaatimuksia ja riittäviä turvallisuusmarginaaleja. Suunnittelussa pyritään luontaisesti vakaisiin, epänormaaleja olosuhteita korjaaviin ratkaisuihin. Jotta voimalaitosta käytettäisiin mahdollisimman turvallisesti, kiinnitetään huomiota laadunvarmistukseen sekä erityisesti organisaation toimintaan, menettelytapoihin, koulutukseen ja ohjeistoon.[2, 6]

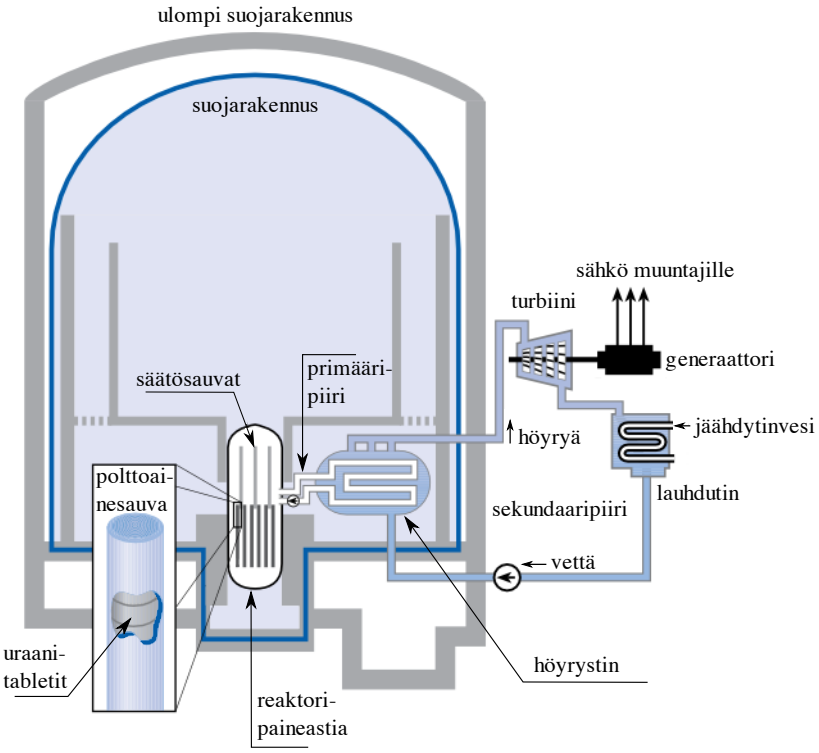
Ennaltaehkäisevien toimien epäonnistuessa suojaavan tason järjestelmien tehtävänä on havaita häiriöt ja estää niiden kehittyminen vakaviksi onnettomuuksiksi. Näillä järjestelmillä varmistetaan reaktorin sammutus, reaktorisydämen jäähdytys sekä jälkilämmön poisto ja siten taataan polttoaineen suojakuoren eheys.[2]

Lieventävää tasoa tarvitaan, jos onnettomuuden etenemistä ei saada pysäytettyä ensimmäisen tai toisen tason toimista huolimatta. Onnettomuuden sattuessa on mahdollista lieventää sen seurauksia ja ympäristövaikutuksia. Tällöin tärkeintä on varmistaa suojarakennuksen säilyminen ehjänä ja suojarakennukseen liittyvien järjestelmien toiminta.[2, 6] Vaikka vakavan onnettomuuden mahdollisuus on oikein toimivalla laitoksella hyvin pieni, siihen varaudutaan erilaisilla onnettomuuden hallintamenetelmillä sekä valmius- ja pelastusjärjestelyillä. Näitä voidaan pitää syvyyssuuntaisen turvallisuusajattelun neljäntenä ja viidentenä tasona.[3, 7]

Eräs syvyyssuuntaisen turvallisuusajattelun tärkeä sovellus on radioaktiivisen materiaalin eristäminen ympäristöstä peräkkäisillä esteillä, joita ovat polttoaine ja sen suojakuori, ydinreaktorin jäähdytyspiiri (primääripiiri) ja suojarakennus [8]. Tämä rakenne on nähtävissä kuvassa 2.1. Ensimmäisenä esteenä on keraaminen ydinpolttoaine itsessään. Normaalikäytön aikana se sisältää suurimman osan fissiotuotteista kiinteässä olomuodossa. Ydinreaktiossa vapautuu kuitenkin pieni määrä kaasua, joka tihkuu ulos polttoainemateriaalista. Nämä kaasut jäävät kuitenkin kaasutiiviin zirkoniumista valmistetun polttoainesauvan sisään. Toinen este on jäähdytyspiirin seinämä, joka pitää sisällään jäähdytysvedessä olevat radioaktiiviset aineet. Kolmantena esteenä on jäähdytyspiiriä ympäröivä paineenkestävä ja kaasutiivis suojarakennus, jonka tehtävänä on pitää sisällään jäähdytyspiirin vaurioituessa vapautuva radioaktiivisia aineita sisältävä höyry ja vesi. Viimeisenä esteenä on suojarakennusta ympäröivä reaktorirakennus tai ulompi suojarakennus, jonka tarkoituksena on myös suojata reaktorirakennusta ulkoisilta uhkatekijöiltä, mukaanlukien lentokoneen törmäys.[2]

2.1.2 Turvallisuusjärjestelmien suunnitteluperiaatteet

Turvajärjestelmien suunnittelussa on ensisijaisesti käytettävä hyväksi luontaisia turvallisuusominaisuuksia. Reaktori suunnitellaan siten, että luontaiset takaisinkytkennät pyrkivät estämään reaktorin tehon hallitsemattoman kasvun. Tämä perustuu siihen, että tehon kasvu johtaa reaktorin lämpötilan nousuun, mikä puolestaan vaikuttaa tehoa pienentävästi. Jos luontaisia turvallisuusominaisuuksia ei voida



Kuva 2.1: Havainnollistus painevesityyppisen reaktorin rakenteesta ja syvyyssuuntaisen puolustuksen toteutuksesta. Muokattu lähteestä [3].

käyttää hyväksi, laitteiden ja järjestelmien on ensisijaisesti toimittava ilman ulkoista käyttövoimaa. Vaihtoehtoisesti, menetettäessä ulkoinen käyttövoima järjestelmien on asetuttava turvallisuuden kannalta edulliseen tilaan. Tätä suunnitteluperustetta kutsutaan turvallisen tilan periaatteeksi.[2, 8] Esimerkiksi sijoitettaessa säätösauvat reaktorin yläpuolelle niitä pidetään ylhäällä sähkömoottoreiden avulla. Jos moottoreiden sähkönsyöttö katkeaa, säätösauvat tippuvat painovoiman seurauksena ja aiheuttavat reaktorin pikasulun.

Turvallisuustoimintoja toteuttavien järjestelmien on kyettävä toteuttamaan tehtävänsä, vaikka mikä tahansa laite järjestelmässä olisi toimintakyvytön. Tämän vaatimuksen toteutuminen varmistetaan rinnakkaisperiaatteella (myös redundanssiperiaate), jolloin turvajärjestelmä koostuu useista toisiaan korvaavista rinnakkaisista ja identtisistä osajärjestelmistä. Suomessa ohjeistukset edellyttävät, että turvallisuustoimintojen on toteuduttava, vaikka mikä tahansa järjestelmän yksittäinen laite olisi toimintakyvytön ja vaikka mikä tahansa turvallisuustoimintoon vaikuttava laite olisi samanaikaisesti poissa käytöstä korjauksen tai huollon vuoksi [8]. Käytännössä

tämä tarkoittaa, että järjestelmässä edellytetään vähintään kolmea rinnakkaista laitetta, joista yksi riittää tehtävän suorittamiseen. Tällaista rinnakkaisjärjestelmää kutsutaan $3 \times 100\%$ järjestelmäksi. Vaihtoehtoisesti järjestelmä voi koostua neljästä rinnakkaisesta laitteesta, joista kahden on toimittava. Tällöin kyseessä on $4 \times 50\%$ järjestelmä.

Rinnakkaisperiaatteen käyttö ei kuitenkaan sulje pois mahdollisuutta, että järjestelmän kaikki laitteet vikaantuisivat esimerkiksi tulipalon tai tulvan vuoksi. Tästä syystä toisiaan varmistavat turvallisuusjärjestelmät sekä niiden rinnakkaiset laitteet on erotettava toisistaan. Tämän erotteluperiaatteen mukaisesti laitteet sijoitetaan eri tiloihin tai riittävän etäälle toisistaan. Fyysisen erottelun lisäksi käytetään toiminnallista erottelua, jolla estetään eri järjestelmien väliset vuorovaikutukset.[2, 8]

Rinnakkaisperiaatteella saavutettavaa luotettavuutta rajoittaa yhteisvikojen mahdollisuus. Tämän vuoksi tärkeimpien turvallisuustoimintojen varmistamisessa käytetään eri toimintaperiaatteisiin perustuvia laitteita eli erilaisuusperiaatetta (myös diversiteettiperiaate), jolloin sama toiminto voidaan toteuttaa eri menetelmiin perustuvilla laitteilla. Esimerkiksi reaktori voidaan sammuttaa säätösauvojen avulla tai pumppaamalla booriliuosta reaktoriin.[2, 8]

Onnettomuustilanteiden varalta järjestelmät automatisoidaan siten, että ne turvallisuustoiminnot, joita tarvitaan 30 minuutin sisällä onnettomuuden alusta, käynnistyvät automaattisesti. Automatisoinnin tarkoituksena on varmistaa, että valvomohenkilökunnalle jää riittävästi harkinta-aikaa oikeiden jatkotoimenpiteiden aloitukseen. Henkilökunta voi ryhtyä toimenpiteisiin aiemminkin mutta automatisoituja toimenpiteitä ei voida pysäyttää, ellei tilanne ole palannut normaaliksi.[2]

2.2 Riskitietoisuus turvallisuuden varmentamisessa

Perinteisen deterministisen lähestymistavan rinnalla voimalaitosten lupakäsittelyssä, valvonnassa ja turvallisuuden varmentamisessa käytetään todennäköisyyspohjaista tarkastelua. Tässä kappaleessa esitellään lyhyesti todennäköisyyksiin pohjautuvaa riskianalyysia ydinvoimasovellusten kautta ja aihe käsitellään seuraavissa luvuissa perusteellisemmin.

Jo rakentamisluvan myöntämisen edellytyksenä on, että voimayhtiö tekee alustavan todennäköisyyspohjaisen riskianalyysin, jonka avulla voidaan arvioida laitok-

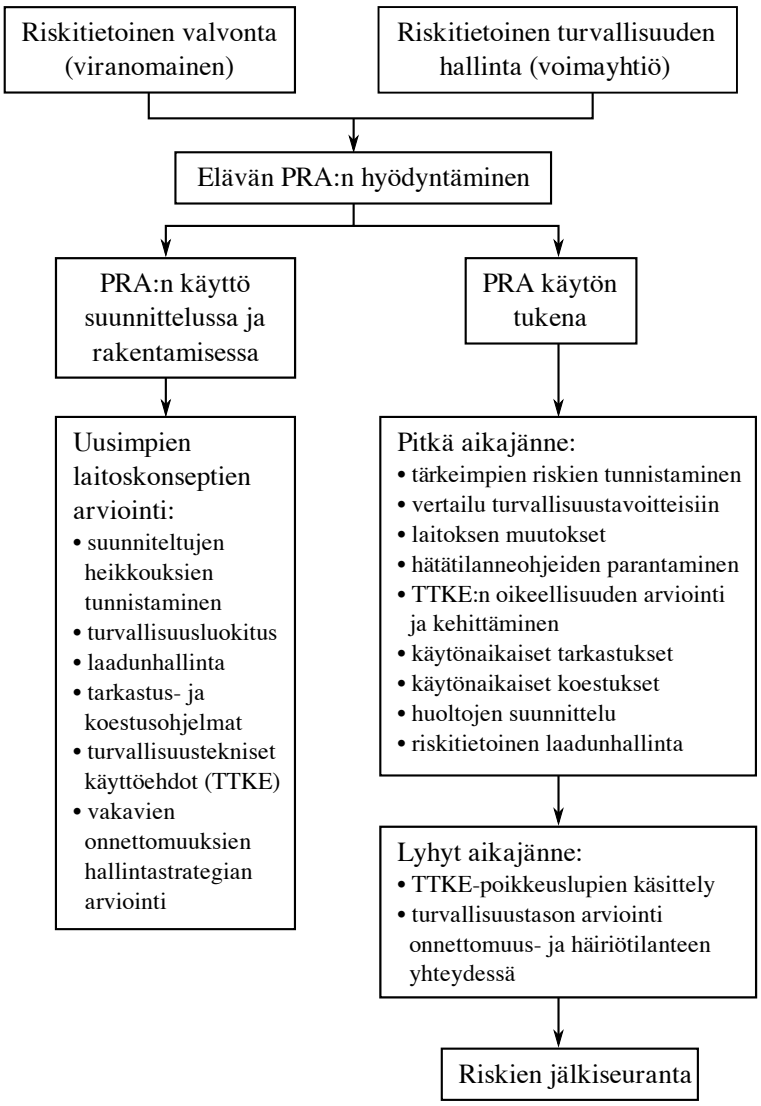
sen turvallisuutta ja mahdollisesti havaitaan järjestelmien välisiä kytkentöjä, vuorovaikutuksia ja vikojen aiheuttajia. Käyttölupaa hakiessa riskianalyysia tarkennetaan ja laajennetaan. Tarkoituksena on varmentaa suunnitteluvaiheessa tehdyt johtopäätökset laitoksen turvallisuudesta ja luoda perusta todennäköisyyspohjaiselle riskien hallinnalle laitoksen käytön aikana.[3]

2.2.1 Riskianalyysin hyödyntäminen laitoksen käytön aikana

Riskianalyysin tuloksia käytetään ydinvoimalaitosten turvallisuutta koskevien päätösten tukena eli päätökset ovat riskitietoisia (risk informed). Todennäköisyyspohjaiset menetelmät täydentävät perinteistä valvontamenettelyä monimutkaisten turvallisuusongelmien arvioinnissa. Systemaattiset, laitoskokonaisuutta arvioivat todennäköisyysmenetelmät soveltuvat erityisesti järjestelmien välisten riippuvuuksien, vuorovaikutusten ja yhteisten vianaiheuttajien käsittelyyn. Todennäköisyyspohjaisesta riskien arvioinnista (PRA) onkin kehitetty työväline – elävä PRA (Living PRA) – jonka avulla voidaan käsitellä pitkän ja lyhyen tähtäimen tai jopa päivittäisiä turvallisuuskysymyksiä. Elävä PRA pidetään jatkuvasti ajantasaisena, jotta se vastaa laitoksen käyttökokemuksia ja rakennetta. Riskitietoista turvallisuusvalvontaa (risk informed regulation/safety management) koskevat sovelluskohteet on esitetty tiivistetysti kuvassa 2.2.[3]

Riskitietoiseen valvontaan ja tarkastustoimintaan sekä niiden sovelluksiin kuuluvat mm. riskitietoinen putkistojen tarkastaminen (risk informed in-service inspection, RI-ISI), laitteiden koestaminen (risk informed in-service testing, RI-IST), turvallisuustekniset käyttöehdot (risk informed technical specifications, RI-TechSpecs) ja laitostapahtumien riskitietoinen jälkiarviointi (Risk Follow-Up).[3]

Putkistojen tarkastusohjelmassa (RI-ISI) kohteiden tarkastus tasapainotetaan niiden riskimerkityksen perusteella. Analyysin avulla tunnistetaan kohteet, joissa putkimurtuma vaikuttaa eniten kyseisen järjestelmän toimintaan. Tulosten perusteella poistetaan vähemmän tärkeitä tarkastuskohteita ja lisätään uusia etenkin niissä kohdissa, joiden vauriot lisäävät riskiä eniten. Turvallisuusjärjestelmien ja niiden tukijärjestelmien käytettävyyttä parannetaan määrittämällä järjestelmien testausvälit ja testaustavat riskiin perustuvien mittojen avulla (RI-IST). Erilaisten laitevikojen ja vanhenemisilmiöiden tunnistamiseksi tehtävien testauksien tehokkuuden arviointi tehdään myös riskipohjaisesti.[3] Riskitietoista laitostapahtumien jälkiarviointia eli riskien seurantaa (Risk Follow-Up) käsitellään luvussa 5.



Kuva 2.2: Riskitietoisen turvallisuusvalvonnan ja elävän PRA:n sovelluskohteet. Muokattu lähteestä [3].

Yleisesti ottaen valvonta ja tarkastustoiminta on tarkoituksenmukaista kohdistaa riskien kannalta olennaisimpiin kohteisiin ja käyttää niihin työmäärä, joka on tasapainossa riskimerkityksen kanssa. Järjestelmien riskimerkitystä voidaan arvioida todennäköisyyspohjaisen riskianalyysin avulla, jota käsitellään seuraavissa luvuissa.

Luku 3

Todennäköisyyspohjainen riskianalyysi

Todennäköisyyspohjaisessa riskianalyysissa tarkastellaan turvallisuustoimintoja suorittavien laitteiden ja järjestelmien sekä esimerkiksi ihmisen toimintojen luotettavuutta tilastollisin ja todennäköisyyspohjaisin menetelmin, joilla täydennetään perinteistä determinististä turvallisuusajattelua. Menetelmän avulla voidaan löytää tärkeimmät riskitekijät ja sitä voidaan käyttää apuna järjestelmien suunnittelussa sekä kehityksessä.[3]

Riskianalyysin termistö ei ole kovin yhtenäistä ja usein riskianalyysilla tarkoitetaan enemmänkin riskien arviointia. Usein todennäköisyyspohjaisten riskianalyysien (Probabilistic Risk Analysis, PRA) sijaan puhutaan myös todennäköisyyspohjaisista turvallisuusanalyyseistä (Probabilistic Safety Analysis, PSA), jolla tarkoitetaan samaa asiaa. Lisäksi lyhentenne PRA (tai PSA) viittaa usein pelkästään todennäköisyyspohjaiseen riskien arviointiin (Assessment). Tässä työssä käytettäessä lyhennettä PRA viitataan juuri todennäköisyyspohjaiseen riskien arviointiin, johon tässä työssä keskitytään etenkin ydinvoimasovellusten avulla.

3.1 Riskin määrittely

Riski mielletään usein mahdollisen epämieluisan seurauksen mittana. Riskiin kuuluu siis tappion mahdollisuus jossain tapahtumaketjussa. On syytä huomata, että

epävarmuus itsessään ei aiheuta riskiä; vasta epätoivottu seuraus aikaansaa riskin. Vaikka intuitiivisesti riskin käsite lienee kaikille selvä, niin siitä huolimatta sillä on monenlaisia määritelmiä, joista osa on kappaleen aloituslauseen mukaisia kansanomaisia esityksiä ja toiset joko kvalitatiivisia tai kvantitatiivisia määritelmiä. Riskin käsitteeseen liittyy läheisesti kuitenkin kolme jo mainittua tekijää: riski on määritellyn *tapahtuman mahdollinen epämieluisa seuraus*.

Kvantitatiivisessa riskin määrittelyssä seuraukset ja epävarmuus on kyettävä ilmaisemaan lukuarvoina. Riskiin liittyvää epävarmuutta kuvataan usein tapahtuman taajuudella tai todennäköisyydellä. Seurauksien mittana voidaan käyttää esimerkiksi taloudellista menetystä, ihmishenkiä tai haitallisia terveysvaikutuksia. Taajuuden λ_i (tai todennäköisyyden p_i) ja seurauksen c_i tulon avulla voidaan suoraviivaisesti määritellä tapahtumasarjaan liittyvä (insinööri) riskimitta lineaarisena piste-estimaattina:

$$R_i = c_i \lambda_i, \quad i = 1, 2, ..., n \tag{3.1}$$

Riski on siis tapahtuman taajuuden (tai todennäköisyyden) ja seurauksen tulo.[9, 10] Tarkasteltaessa useita tapahtumaketjuja kokonaisriski voidaan (joissain tapauksissa) laskea summaamalla kunkin tapahtumaketjun riskit eli laskemalla riskin odotusarvo [10]:

$$R = \sum_{i=1}^{n} c_i \lambda_i. \tag{3.2}$$

Vaikka riskimitan määrittely eteni suoraviivaisesti, riskin arviointi voi olla hyvin työlästä sen vaatimien parametrien vuoksi. Esimerkiksi tapahtumien taajuuksien tai todennäköisyyksien määrittäminen voi olla huomattavan hankalaa. Toisinaan ne voidaan estimoida tilastoista mutta esimerkiksi ydinvoimasovelluksissa käsitellään toisinaan äärimmäisen harvinaisia ilmiöitä, jolloin parametrien estimointi datasta on mahdotonta. Myös seurausten arviointi ja yhteismitallistaminen sisältää ongelmia: Jokin tapahtuma voi johtaa taloudellisiin tappioihin, toinen kuolemiin ja kolmas mahdollisesti syöpään. Jos näiden tapahtumien riskejä haluaa vertailla kvantitatiivisesti, myös seurausten tulisi olla vertailukelpoisia.

Myös itse riskimitan määritelmää, yhtälöä (3.1), voidaan kritisoida siitä, että siinä oletetaan riskineutraali asenne. Hyvin harvinaiset ja seurauksiltaan suuret ilmiöt ovat siis samanarvoisia kuin kohtuullisen yleiset pienen mittakaavan tapahtumat. Yleisesti ottaen yhteiskunta on riskejä karttava eli yksittäisen suuren onnettomuuden riskiä pidetään suurempana kuin usean pienen, vaikka keskiarvoinen vaikutus

yhteiskuntaan olisikin sama. Itse asiassa, yhteiskunta vaikuttaa ennemmin hyväksyvän usein tapahtuvia pieniä onnettomuuksia kuin harvinaisia ja suuria, vaikka suurten onnettomuuksien yhteiskunnallinen vaikutus olisi jopa pienempi. Esimerkki tällaisesta tilanteesta on auto-onnettomuuksien hyväksyttävyys verrattuna lentokoneonnettomuuksiin. Tämä saattaa johtua suurten onnettomuuksien saamasta mediahuomiosta ja siitä, että ihmisen on vaikea käsitellä pieniä todennäköisyyksiä. Jos siis suuria onnettomuuksia tapahtuu, ne ovat mahdollisia ja niiden pieni tapahtumistodennäköisyys jätetään huomioimatta. Riskin hyväksyttävyyteen vaikuttaa myös vapaaehtoisuus, sillä ihmiset voivat hyväksyä yhteiskunnallisesti ajatellen suuriakin riskejä vapaaehtoisesti esimerkiksi joissain urheilumuodoissa.[9]

Vaikka yhtälön (3.2) tapaista osariskien summaamista käytetään usein, sitä on useimmiten syytä välttää [10]. Vaikka seuraukset voitaisiin yhteismitallistaa, osariskien summaus antaa usein väärän tai jopa täysin virheellisen kuvan tilanteesta. Esimerkiksi osakkeita hajauttamalla pyritään juuri riskin pienentämiseen; toisen arvon laskiessa toisen nousee, jolloin kokonaisriski on pienempi kuin ostaessa vain samaa osaketta. Erilaisten osakkeiden sisältämien osariskien summa johtaa siis täysin väärään lopputulokseen, sillä skalaarein laskettaessa summassa ei huomioida osariskien välistä korrelaatiota. Lisäksi, jos seuraukset ovat suuruudeltaan hyvin eri luokkaa, yhtälö (3.2) voi antaa seurauksen odotusarvosta harhaanjohtavan tai informatiivisesti riittämättömän kuvan, sillä odotusarvo on herkkä poikkeaville havainnoille ja kadottaa jakauman multimodaalisuuden. Tämä on tärkeä havainto riskianalyysin kannalta, jolle on tyypillistä, että tavanomaisten tilanteiden lisäksi on kiinnitettävä erityistä huomiota harvinaisiin ja vaikutuksiltaan suuriin tapahtumiin – erittäin epätodennäköisen vaikutukseen.

Monessa tilanteessa onkin informatiivisempaa määritellä riskiprofiili tai -käyrä. Oletetaan, että seuraus on satunnaismuuttuja C, joka noudattaa jakaumaa $f(c)$. Diskreetissä tapauksessa $\lambda_i = f(c_i)$ ja jatkuvassa tapauksessa $\lambda_i = \int_{c_i} f(c)dc$. Riski voidaan siis mieltää pistepareina tai jakaumana

$$R = \{(c_i, \lambda_i) \,|\, i = 1, 2, ..., n\}. \tag{3.3}$$

Kritisoitaessa aiemmin yhtälöä (3.2) sivuutettiin se tosiasia, että toisinaan jakauman käyttö esimerkiksi päätöksenteon tukena on hankalaa ja jakauman sijasta on pakko käyttää jakaumaa kuvaavia tunnuslukuja, kuten yhtälön (3.2) mukaista odotusarvoa eli tässä mielessä riskin odotusarvon laskeminen jakaumasta on perusteltua.

Jatkossa seuraus oletetaan jatkuvaksi muuttujaksi mutta vastaava menettely onnistuu myös diskreetille tapaukselle. On syytä huomata, että jakauma $f(c)$ ei välttämättä toteuta todennäköisyystiheysfunktion ehtoja, vaikka yhtäläisyys on suuri. Syy tähän on, että usein kiinnostuksen kohteena on jonkin onnettomuuden aiheuttamat seuraukset, jolloin jakauman integraali vastaa kyseisen onnettomuuden kokonaistaajuutta, joka usein poikkeaa arvosta 1. Luonnollisesti taajuuden tilalla voidaan tarkoituksen mukaan käytää myös todennäköisyyttä mutta tällöinkin kaikkien seurausten yhteenlasku harvoin tuottaa varmaa tapahtumaa – paitsi, jos jakaumaan sisällytetään tapaus, että onnettomuutta ei satu.

Tiheysfunktion avulla voidaan laskea kertymäfunktio

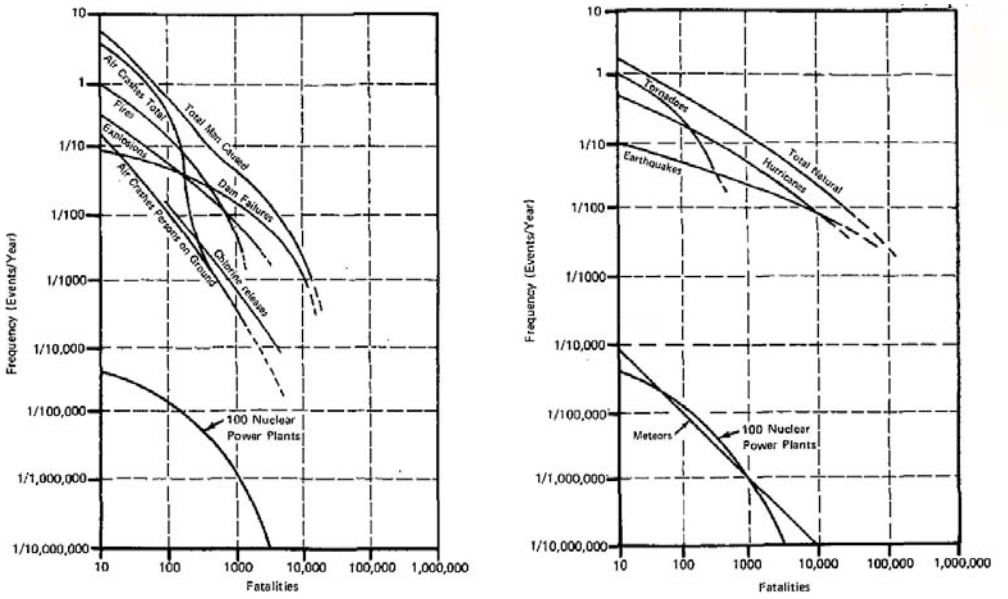
$$F(c) = \int_0^c f(c')dc', \tag{3.4}$$

joka siis ilmaisee taajuuden tapahtumalle, jonka seuraus on alle tarkasteltavan rajan c. Tyypillisesti tästä lasketaan kertymäfunktion komplementti (complementary cumulative distribution function) eli tapahtumataajuus, jolla ylitetään tarkasteltava seuraus: $\bar{F}(c) = \int_c^\infty f(s)ds$. Tätä käyrää nimitetään joissain yhteyksissä myös Farmerin käyräksi [10]. Kuvassa 3.1 on esitetty muutama tällainen käyrä.

Vaikka edellä on käsitelty riskimitan määrittämiseen liittyviä ongelmia, on syytä huomauttaa, että todennäköisyyspohjaisen riskien arvioinnin päätavoite ei aina ole riskin numeerinen arvo. Sen sijaan, tavoitteena on tutkia systeemin suunnitteluperusteita ja löytää toiminnallisia heikkouksia, sekä optimoida resursseja, joita käytetään parantamaan systeemin rakennetta ja toimintaa.[10]

3.2 Riskianalyysin historiakatsaus

Todennäköisyyksiin perustuva riskien arviointi kehittyi tilastotieteen soveltamisesta teknisten järjestelmien suunnitteluun. 1900-luvun puolivälissä tilastotieteen ja todennäköisyyslaskennan matemaattiset menetelmät olivat saavuttaneet hyväksynnän luotettavuustekniikan ja rakenteiden mekaniikan aloilla. Tuolloin pääpaino oli elektroniikka-alan sotilaallisissa sovelluksissa.[11] Vaikka luotettavuustekniikka muodostaa tärkeän osan todennäköisyyspohjaisesta riskianalyysistä, täytyy korostaa, ettei se ole kvantitatiivista riskien arviointia, sillä siitä puuttuu vikojen seurausten arvioiminen [12].



(a) Ihmisen aiheuttamien riskien profiileja.

(b) Luonnollisista tapahtumista aiheutuvien riskien profiileja.

Kuva 3.1: Esimerkki riskikäyristä. Molemmissa kuvissa on verrattu ydinvoiman aiheuttamia riskejä muihin tapahtumiin. Kuvat lähteestä [9].

Riskianalyysin historiaa voi jäljittää pitkällekin menneisyyteen mutta tässä yhteydessä rajoitutaan lähihistorian merkittävimpiin tapahtumiin, jotka ovat vaikuttaneet riskianalyysin kehitykseen ja hyväksymiseen. Monet menetelmät yleensä saavat alkunsa käytännön tarpeesta, eikä riskianalyysi valitettavasti ole tässä poikkeus: Vuonna 1957 Isossa-Britanniassa Windscalen ydinvoimalassa sattunut vakava tulipalo osoitti, ettei absoluuttista turvallisuutta voitu saavuttaa; riskejä täytyi pystyä kvantifioimaan, mikä johti todennäköisyyspohjaisen riskien arvioinnin aloittamiseen [12]. Toinen riskianalyysia vauhdittava tapahtuma sattui USA:ssa kymmennen vuotta myöhemmin, kun NASA:n Apollo-ohjelman testissä sattunut tulipalo johti kolmen astronautin kuolemaan. Vaikka todennäköisyyksiin perustuva riskianalyysi on saanut vauhtia mainituista onnettomuuksista, modernin PRA:n katsotaan alkaneen vuonna 1975 sen ensimmäisellä kattavalla sovelluksella – Reactor Safety Study -tutkimuksella.[11, 12, 13]

Reactor Safety Study [9] (tunnetaan myös nimellä Wash-1400) oli ensimmäinen kattava raportti, jossa arvioitiin ydinvoimalaitoksen onnettomuustodennäköisyyksiä ja -seurauksia. Vaikka kyseistä raporttia pidetään nykyään PRA:n virstanpylväänä, näin ei ollut sen valmistuessa. Tutkimus sai osakseen paljon julkisuutta sekä hy-

vin kriittisen vastaanoton ja lopulta tammikuussa 1979 tutkimuksen julkaisija, Yhdysvaltain ydinviranomainen (United States Nuclear Regulatory Commission, U.S. NRC), päätti vetäytyä tulosten tukemisesta. Tosin kolme kuukautta myöhemmin asenteet muuttuivat täysin. Maaliskuussa 1979 Three Mile Islandin ydinonnettomuudessa voimalan toisen yksikön ydin suli osittain. Jälkikäteen paljastui, että onnettomuusketju oli ennustettu Wash-1400 -tutkimuksessa. Tämä antoi uuden alun PRA-menetelmien käytölle.[11, 13, 14] Muita onnettomuuksia, jotka ovat osaltaan vaikuttaneet PRA:n käyttöön, ovat olleet esimerkiksi Challenger- ja Columbia-avaruussukkuloiden tuhoutumiset vuosina 1986 ja 2003, kemianteollisuuden onnettomuudet (mm. Seveson onnettomuus Italiassa 1976 ja vuonna 1984 Intiassa sattunut Bhopalin katastrofi, jossa arviolta puoli miljoonaa ihmistä altistui tuholaismyrkkypäästölle aiheuttaen vain muutamassa päivässä noin 10000 ihmisen kuoleman [15, 16]), sekä tietenkin vuonna 1986 tapahtunut Tšernobylin katastrofaalinen ydinonnettomuus.

Vuosituhannen vaihteessa ja sen jälkeen, ydinvoimasovelluksissa huomiota on kiinnitetty etenkin riskitietoisiin ohjeisiin ja säännöstöihin, joissa riskitietoa käytetään determinististen säännöstöjen lisänä ja tukena. Nykyajan turvallisuussäännöstöt ovat yhdistelmä syvyyssuuntaisen puolustuksen suunnitteluperustaisia vaatimuksia täydennettynä riskitiedolla. Ydinvoimalaitosten säännöstöjen kehityksestä voidaan ottaa opiksi siinä, että syvyyssuuntainen puolustus ei yksinään riitä takaamaan turvallisuutta, kuten TMI:n ydinonnettomuus osoitti. Siksi tarvitaan muita turvallisuuden ja riskien arviointitekniikoita, kuten PRA:ta, täydentämään deterministisiä turvallisuusmenettelyjä.[14]

Suomessa todennäköisyyksiin pohjautuva riskianalyysi sai vauhtia akateemikko Pekka Jauhon perustettua Valtion teknillisessä tutkimuskeskuksessa luotettavuuden ja riskien tutkimukseen keskittyvän erityisyksikön. Vaikuttimena ryhmän perustamiseen lienevät olleen päätökset Suomeen rakennettavista ydinvoimalaitoksista sekä Jauhon tausta vakuutusmatemaatikkona. Nykyään PRA on vakiintunutta tekniikkaa, jota harjoitetaan erityisesti ydinvoimalaitosriskien hallitsemiseksi voimayhtiöissä ja Säteilyturvakeskuksessa sekä Valtion teknillisessä tutkimuskeskuksessa. Prosessiteollisuus on ottanut riskiarviot käyttöön etenkin kemianteollisuudessa.[1]

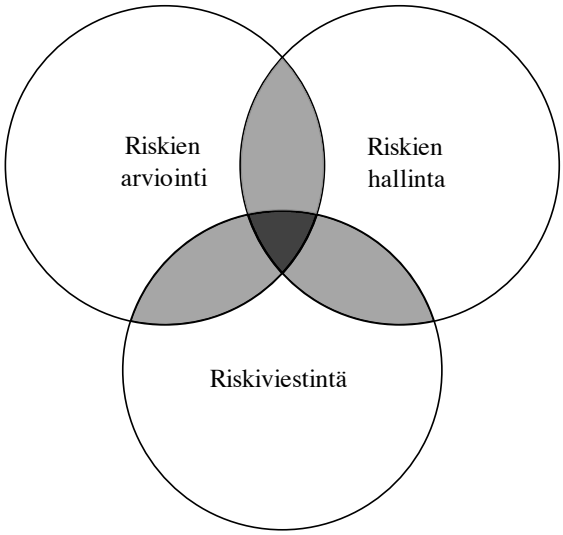
[1] Lähteenä keskustelu Reino Virolaisen kanssa.

3.3 Riskianalyysin käyttö ja rakenne

Yleisesti riskianalyysi voidaan käsittää prosessina, jolla määritetään, hallitaan ja tiedotetaan erilaisten tapahtumaketjujen riskeistä ja turvallisuustoimien mahdollisista heikkouksista. Analyysin etuina on, että se osoittaa järjestelmien heikkouksia sekä tuo arviot ja laskelmat kaikkien nähtäville. Tällöin järjestelmäparannuksin ja analyysin tulosten avulla on mahdollista osoittaa riskien pienentyneen ja turvallisuuskulttuurin olevan korkea, jolloin yleinen luottamus riskejä sisältävään menettelyyn, esimerkiksi ydinvoiman käyttöön, kasvaa. Menetelmän käytöllä on hyötyä niin taloudelliselta kuin inhimilliseltä tai eettiseltä kannalta: Riskien tiedostaminen ja niihin varautuminen pienentävät syntyneitä kustannuksia ja mahdollisia muita tappioita, esimerkiksi kuolemia tai haitallisia ympäristöpäästöjä (mm. kemialliset tai radioaktiiviset päästöt). Riskianalyysia voidaan käyttää myös esimerkiksi viranomaisvalvonnassa todentamaan, että vaaditut turvallisuusmääräykset toteutuvat tarkasteltavassa kohteessa.

Riskianalyysi koostuu kolmesta limittäisestä ja vuorovaikuttavasta osasta: riskien arvioinnista, riskien hallinnasta ja riskiviestinnästä (kts. kuvaa 3.2). Riskien arviointiin kuluu karkeasti tapahtumaketjujen määritys sekä epämieluisten seurausten suuruuden sekä todennäköisyyden arviointi tai estimointi. Riskien hallinta taas keskittyy arvioitujen riskien estämiseen tai tappioiden minimoitiin, jolloin keskitytään vaihtoehtojen valintaan ottaen huomioon esimerkiksi riskin suuruus, taloudelliset ja teknologiset rajoitteet, tai poliittiset kysymykset. Riskiviestinnällä välitetään tietoa riskien arvionnin ja hallinnan tuloksista päättäjien, analyytikoiden ja asianomaisten välillä.[10]

Riskianalyysi voidaan jaotella käytettyjen menetelmien perusteella kvantitatiiviseen ja kvalitatiiviseen analyysiin, tai näiden yhdistelmään. Kvantitatiivisessa analyysissa käytetään hyväksi saatavilla olevaa dataa, josta voidaan laskennallisesti estimoida tarvittavat todennäköisyydet, tapahtumien taajuudet ja seurausten aiheuttamat kustannukset. Kyseessä on siis todennäköisyyspohjainen analyysi. Kvalitatiivisessa analyysissä todennäköisyydet sekä seuraukset arvioidaan sanallisesti ja niistä muodostetaan riskimatriisi päätöksenteon tueksi. Tällainen analyysi on huomattavasti helpompi toteuttaa kuin kvantitatiivinen, jonka toteutus on usein kallista, aikaa vievää ja monimutkaista. Toisaalta, kvalitatiivinen analyysi voi olla äärimmäisen subjektiivista. Kolmas vaihtoehto on käyttää edellä mainittujen menetelmien yhdistelmää, jolloin esimerkiksi päätökset ja viranomaisvaatimukset voidaan perustaa



Kuva 3.2: Riskianalyysin perusosat. Kuva suomennettu lähteestä [10].

yhdistämällä kvantitatiivisten riskiarvioiden, deterministististen onnettomuusanalyysien sekä enemmän tai vähemmän subjektiivisten asiantuntija-arvioiden tulokset. Tällaista menettelyä kutsutaan riskitietoiseksi päätöksenteoksi.[10]

3.4 PRA ydinvoimasovelluksissa

Ydinvoimasovellusten PRA:ssa tunnistetaan sellaiset tapahtumayhdistelmät, jotka johtavat vakavaan reaktorionnettomuuteen eli reaktorisydämen vaurioitumiseen. PRA:lla arvioidaan jokaisen tapahtumaketjun yleisyys (todennäköisyys tai taajuus) ja näiden tapahtumien seurausvaikutukset. Tavoitteena on yhdistää olennaiset tiedot laitoksen suunnittelusta, käytöstä, käyttöhistoriasta, laitteiden ja ihmisen toimenpiteiden luotettavuudesta, sydämen vaurioitumisen fysikaalisesta kehittymisestä sekä radioaktiivisten aineiden käyttäytymisestä ja ympäristövaikutuksista. Menetelmät perustuvat sekä loogisiin että fysikaalisiin malleihin. Loogiset mallit kuvaavat vikojen vaikutusta laitosjärjestelmissä ja tapahtumayhdistelmiä, jotka voivat johtaa sydänvaurioon. Fysikaalisilla malleilla puolestaan kuvataan onnettomuuden etenemistä sekä onnettomuuden seurauksia. PRA:n menestyksellinen soveltaminen edellyttää, että käytettävissä oleva malli on laadukas ja että se kuvaa koko laitoksen kattavasti. Riskianalyysien rajoitukset ja luontaiset epävarmuustekijät tulee huomioida sovellettaessa tuloksia riskitietoiseen päätöksentekoon.[3]

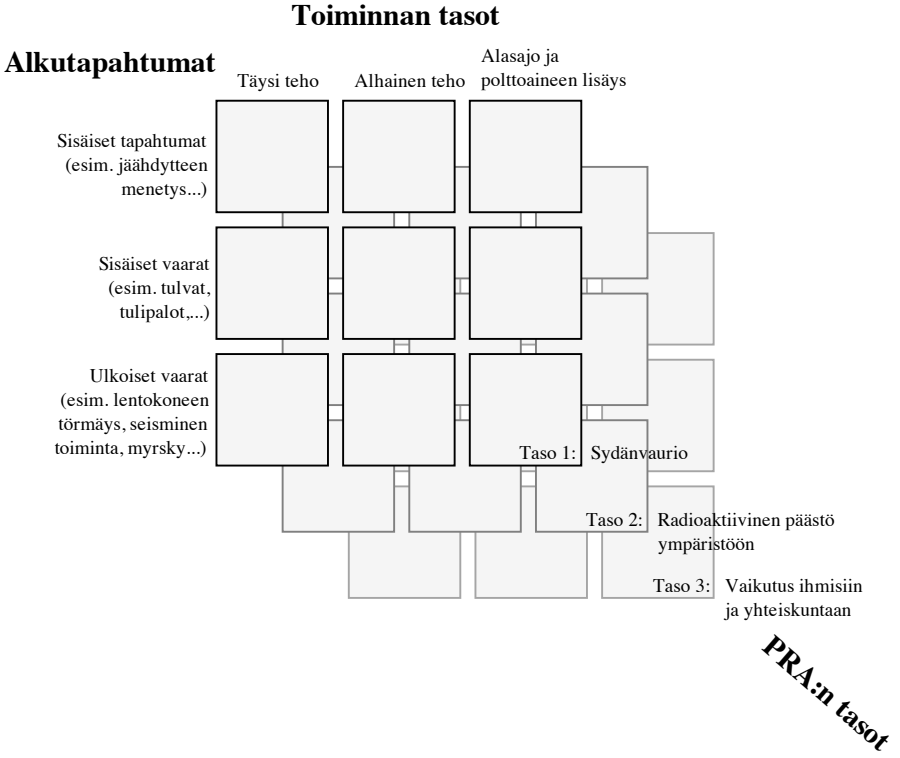
Fysikaaliset mallit sisältävät erityisesti tiedollista epävarmuutta liittyen mm. sydänvaurion kehittymiseen ja sulan sydämen käyttäytymiseen. Epävarmuuksia on myös fissiotuotteiden kulkeutumisessa reaktoripaineastiasta suojarakennukseen sekä suojarakennuksen tiiveyttä uhkaavissa äkillisissä ilmiöissä. Tästä syystä radioaktiivisten päästöjen seurausten arviointiin liittyy huomattavia epävarmuuksia, mihin vaikuttavat myös ulkoiset satunnaistekijät kuten tuulen suunta ja voimakkuus, sade tai evakuointitoimien tehokkuus. Erilaisiin ulkoisiin alkutapahtumiin ja vaaroihin liittyvien onnettomuustodennäköisyyksien epävarmuustekijät ovat myös suuria. Esimerkiksi maanjäristysten, tulvien ja lentokonetörmäysten analyysi tarvitsee lisätutkimusta tiedollisen epävarmuuden selvittämiseksi. Lisäksi organisaatiota ja sen toimivuutta arvioidaan PRA:ssa pääasiassa vain ihmisen toimintoihin liittyvien virheiden näkökulmasta, jolloin organisaation toimintakyvyn mittausta turvallisuuden kannalta on arvioitava muilla menetelmillä.[3]

3.4.1 PRA:n eri tasot ja niiden viranomaisvaatimukset

Ydinvoimasovelluksissa PRA jaetaan kolmeen tasoon seurausten mukaan. Tasolla 1 määritetään reaktorisydämen vaurioitumiseen johtavat onnettomuusketjut alkutapahtumasta lähtien ja arvioidaan niiden todennäköisyydet. Analyysin lopputuloksena saadaan myös tietoa turvajärjestelyiden suorituskyvystä ja tehokkuudesta. PRA:n tasolla 2 tutkitaan vakavia onnettomuuksia arvioimalla suojarakennuksesta vuotavien radioaktiivisten aineiden päästön määrää, todennäköisyyttä ja ajoittumista. Taso 2 eroaa tasosta 1 myös mallinnus- ja laskentarutiinien osalta. Kolmannella, ja viimeisellä, tasolla arvioidaan radioaktiivisen päästön kulkeutumista voimalaitoksen ulkopuolella ja siitä aiheutuvaa riskiä ihmisille, ympäristölle ja omaisuudelle.[17, 18]

Eri tasot voidaan edelleen jakaa omiin osiinsa erilaisten alkutapahtumien ja voimalaitoksen toimintatilan mukaan. PRA:lla on siis useita tavoitteita, jotka osaltaan määräytyvät sen tason, toimintatilan ja tarkasteltavan alkutapahtuman mukaan. Tätä jakoa eri osiin ja tasoihin on havainnollistettu kuvassa 3.3.

Suomessa PRA:n käyttö on lainsäädännöllinen edellytys ydinvoimaloiden suunnitteluvaiheesta lähtien. Voimayhtiöillä on velvollisuus pitää PRA-mallinsa ajantasaisena koko voimalaitoksen elinkaaren ajan. Laitoskohtaiset suunnitteluvaiheen PRA:t tasoilta 1 ja 2 ovat vaatimuksena rakennusluvan saamiselle ja täydellisten versioiden tulee olla valmiit käyttöluvan saamiseksi. Voimalaitosten PRA:t tarkastetaan



Kuva 3.3: Todennäköisyyspohjaisen riskianalyysin tavoitteet ja ulottuvuudet. Kuva suomennettu lähteestä [19].

ja hyväksytään Säteilyturvakeskuksessa. Voimayhtiöiden on arvioitava sisäisten alkutapahtumien, ulkoisen sähköverkon menetyksen, tulipalojen, tulvien, poikkeuksellisten sääolosuhteiden ja maanjäristysten vaikutus laitoksen turvallisuuteen sekä täyden tehon vaiheessa että alhaisella teholla ja seisokin aikana. Jokaisessa lupahakemusvaiheessa PRA:n avulla on osoitettava, että seuraavat vaatimukset toteutuvat [18]:

- Sydänvauriotaajuuden odotusarvo on alle 10^{-5} / vuosi.
- Suuren päästön (yli 100 TBq Cesium-137 -isotooppia) taajuus on odotusarvoltaan alle 5×10^{-7} / vuosi.

Vaatimuksista ensimmäinen koskee tasoa 1, jolla seurauksen mittana on sydänvaurion syntyminen. Tällöin riskin mitta on sydänvaurion taajuus tai todennäköisyys. Toinen viranomaisvaatimus koskee tasoa 2, jolla seurauksen suuruus mitataan päästön osuutena ympäristöön. Se on siis jatkuva muuttuja välillä [0,1] ja riski ilmoitetaan

usein riskiprofiilin avulla eli päästön osuuden ja sen taajuuden avulla (vertaa kuviin 3.1). Tason 3 PRA:ta ei voimayhtiöiltä edellytetä.

3.4.2 Ydinvoimalaitoksen onnettomuusriski

Ydinvoimalaitoksen onnettomuusriskiä mitataan ydinpolttoaineen vakavaan vaurioitumiseen johtavan onnettomuuden todennäköisyydellä vuotta kohti eli sydänvauriotaajuudella. Kuvassa 3.4 on esitetty PRA-malleilla laskettu sydänvauriotaajuuden kehitys Loviisan ja Olkiluodon laitoksissa. Tavoitteena on, että ydinvoimalaitosta käytetään ja ylläpidetään niin, että onnettomuusriski pienee tai pysyy ennallaan. On syytä muistaa, että tuloksiin vaikuttavat sekä voimalaitoksen että laskentamallin kehittyminen. Vaaratekijöiden poistamiseksi tehdyt laitoksen tai toimintatapojen muutokset pienentävät sydänvauriotaajuutta. Kasvu voi johtua mallin laajentamisesta uusiin tapahtumaryhmiin tai uusien vaaratekijöiden tunnistamisesta. Lisäksi PRA-mallin ja sen parametrien tarkentaminen voi johtaa riskiarvioiden muutoksiin kumpaankin suuntaan.[6]

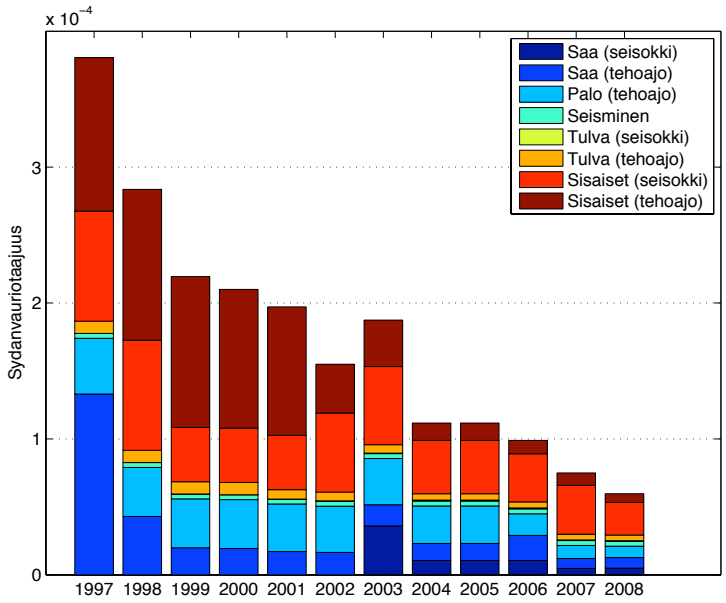
Kuvassa 3.4(a) on esitetty Loviisan yhden laitosyksikön laskennallinen sydänvauriotaajuus, joka on koko ajan pienentynyt. Riskianalyysin laajennusten yhteydessä havaittuja uusia riskitekijöitä onkin poistettu tehokkaasti. Vuoden 2003 sydänvauriotaajuuden kasvu johtui analyysin laajentamisesta kattamaan poikkeuksellisen ankarat sääolosuhteet ja merellä tapahtuvat öljyonnettomuudet polttoaineenvaihtoseisokin aikana. Seuraavana vuonna riski pieneni mm. tarkemman analyysin tuloksena. Vuonna 2007 Loviisassa valmistui uusi merivesilinja, jonka avulla sammutetun laitoksen jäähdytykseen tarvittava merivesi voidaan ottaa vaihtoehtoisesti poistokanavasta. Tämä pienensi riskiä tilanteissa, joissa levä, suppojää tai öljypäästö vaarantavat meriveden saannin tavanomaista reittiä. Loviisan laitoksilla tärkeimmät onnettomuusriskin aiheuttajat ovat seisokin aikaiset sisäiset tapahtumat (mm. raskaan taakan pudotus ja reaktorin säätöön käytettävän boorin äkillisen laimentumisen aiheuttama tehopiikki), tulipalot, korkea meriveden pinta tehokäytön aikana ja öljyonnettomuus polttoaineenvaihtoseisokin aikana.[6]

Olkiluodon voimalaitoksissa laskennallinen sydänvauriotaajuus (kuva 3.4(b)) on kasvanut vuosina 1998-2001 johtuen PRA-mallin laajennuksista uusiin tapahtumaryhmiin. Tämän jälkeen onnettomuusriski on pienentynyt lievästi laitoksella toteutettujen pienehköjen muutostöiden ansiosta. Tärkeimmät onnettomuusriskin aiheuttajat ovat tehokäytön aikaiset sisäiset tapahtumat (käyttöhäiriöön johtavat laiteviat ja

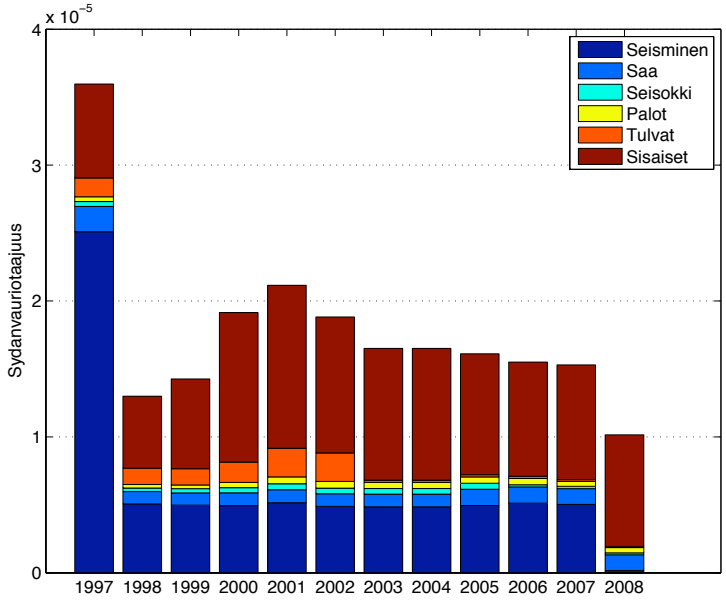
putkimurtumat) sekä Suomessa mahdollisiksi arvioitujen maanjäristysten seurauksena esiintyvät releiden toimintahäiriöt.[6]

Kuten kuvasta 3.4 havaitaan, uusi viranomaisvaatimus sydänvauriotaajuuden yläarajalle (10^{-5}/vuosi) on melko tiukka, sillä kummankaan paikkakunnan voimalaitokset eivät tätä ehtoa toteuta. Vaatimus tosin koskee uusia voimalaitoksia ja Olkiluoto 3:n tulee toteuttaa tämä ehto. Lisäksi, nykyisellä tekniikalla ei ole erityisen vaikea päästä mainittuun tason 1 vaatimukseen mutta tason 2 vaatimus on jo erittäin tiukka ja vaatii todella hyvää suunnittelua ja laadunvalvontaa[2].

[2]Lähteenä keskustelu Reino Virolaisen kanssa.



(a) Loviisan laitosyksiköiden sydänvauriotaajuuden kehittyminen.



(b) Olkiluodon laitosyksiköiden sydänvauriotaajuuden kehittyminen.

Kuva 3.4: Laskennallisesti määritetty sydänvauriotaajuuden muuttuminen eri laitosyksiköille. Ajoittainen kasvu voi johtua esim. uusien vaaratekijöiden tunnistamisesta ja mallintamisesta. Laitosmuutoksilla saadaan parannettua turvallisuutta ja pienennettyä onnettomuusriskiä. Huomaa, että kuvissa on eri asteikot.

Luku 4

PRA:n laskentamenetelmät

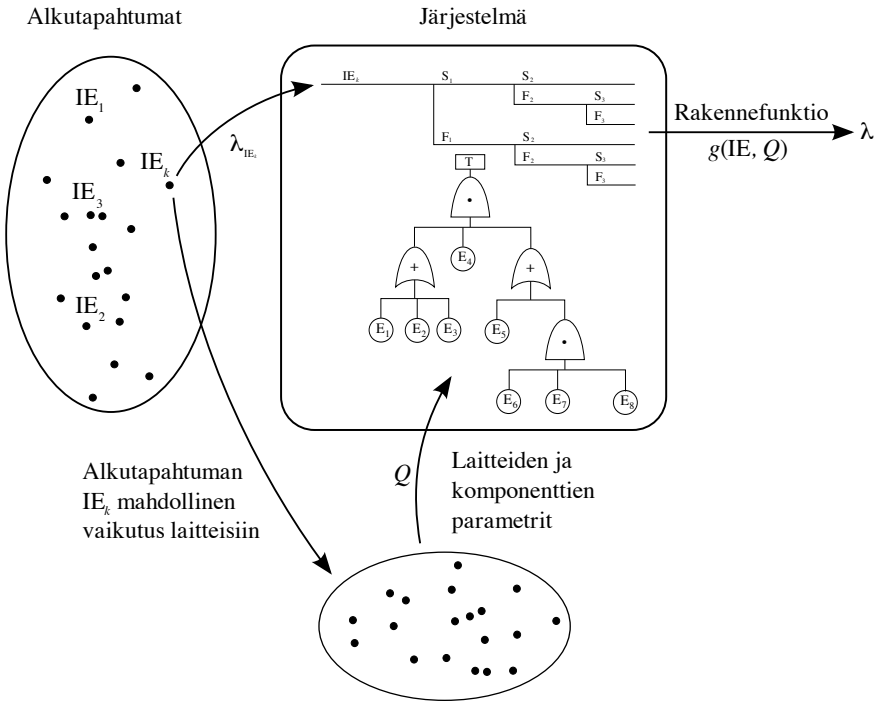
Harvinaisten tapahtumien todennäköisyyksien arviointi voidaan joskus toteuttaa pilkkomalla tapahtumaketju osiin, joiden todennäköisyydet tiedetään. Yksinkertainen esimerkki tästä on kruunan saaminen peräkkäin jokaisella heitolla viidenkymmenen heiton sarjassa. Kokemuksesta tiedetään, että reilulle kolikolle todennäköisyys saada kruuna yhdellä heitolla on 0.5, jolloin viidenkymmenen heiton sarjalle todennäköisyys on 0.5^{50}. Tälle hyvin harvinaiselle tapahtumalle voitiin siis laskea todennäköisyys, vaikka tapahtumaa tuskin koskaan on havaittu. Tähän ideaan perustuvat tässä luvussa esiteltävät vika- ja tapahtumapuu-tekniikat, jolloin hyvin harvinaisten tapahtumien todennäköisyyksiä voidaan arvioida lähtemällä liikkeelle todennäköisemmistä tapahtumista.[9]

Seuraavassa tarkastellaan erityisesti PRA:n tasoa 1, jolloin kiinnostuksen kohteena on onnettomuusketjujen taajuuksien arviointi eli tässä sovelluksessa sydänvauriotaajuus. Esitetty riskien arviointimenettely sopii etenkin teknisten järjestelmien analysointiin, jolloin tutkittavan järjestelmän looginen rakenne on tiedossa ja sitä voi pitää tapahtumien ajan staattisena järjestelmänä.

4.1 Järjestelmän rakennefunktio

Mallinnetaan teknisen järjestelmän, esimerkiksi ydinvoimalan, turvallisuustoimintoja rakennefunktion g avulla. Turvallisuustoimilla estetään jonkin alkutapahtuman IE_k kehittyminen onnettomuudeksi. Moninkertaisten turvallisuusjärjestelmien toi-

minta on riippuvainen useista erilaisista laitteista ja komponenteista, joilla on erilaisia toimintaa kuvaavia parametreja kuten luotettavuus, käytettävyys tai tieto siitä, että laite on epäkunnossa. Merkitään koko järjestelmän sisältämiä parametreja Q:lla. Rakennefunktion avulla voidaan määrittää onnettomuuden, tässä tapauksessa sydänvaurion, taajuus: $\lambda = g(\mathrm{IE}, Q)$. Kuvassa 4.1 on esitetty kaavio mainitusta menettelystä.



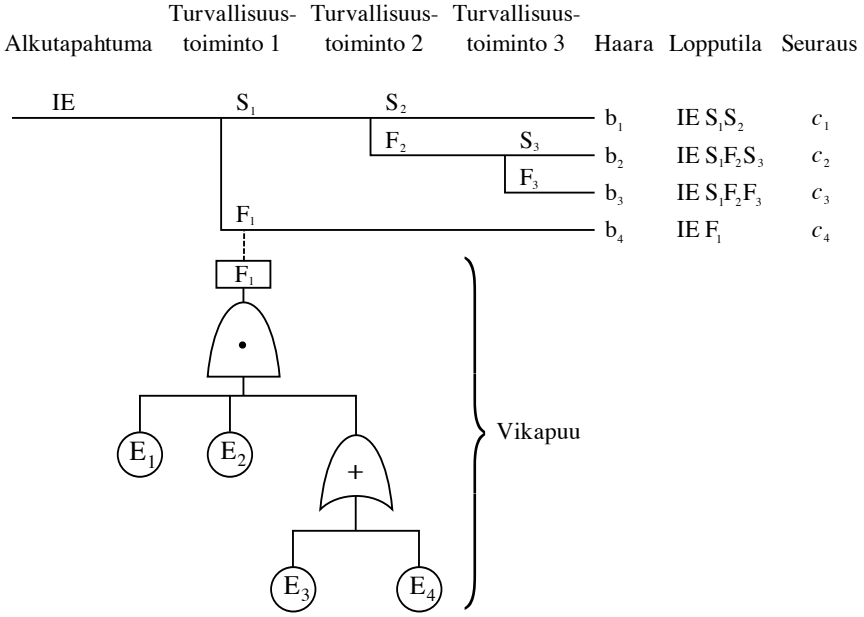
Kuva 4.1: Kaaviokuva järjestelmään vaikuttavista tekijöistä ja rakennefunktion yhteydestä sydänvauriotaajuuteen λ.

Järjestelmän toimintaa voidaan kuvata graafisesti tapahtuma- ja vikapuiden avulla ja rakennefunktio voidaan muodostaa näistä Boolen algebran avulla.

4.2 Tapahtumapuut

Tapahtumapuu on tapahtumaketjujen graafinen esitys ja sen avulla voidaan arvioida alkutapahtuman aiheuttamia seurauksia. Tapahtumapuu alkaa alkutapahtumasta (yksittäinen tapahtuma, joka ilman onnistuneita turvallisuustoimenpiteitä johtaa epätoivottuihin seurauksiin), jonka etenemistä estävät turvallisuustoimet mallinne-

taan tapahtumapuuhun haarautumiskohtina, yleensä aika- tai riippuvuusjärjestyksessä. Haarautumistodennäköisyydet eli turvallisuusjärjestelmän toiminnan tai toimimattomuuden todennäköisyydet voidaan arvioida esimerkiksi vikapuuanalyysin avulla.[20] Esimerkki tapahtumapuusta on esitetty kuvassa 4.2, joka havainnollistaa myös, kuinka tapahtuma- ja vikapuut voivat liittyä toisiinsa.



Kuva 4.2: Tapahtumapuun ja vikapuun välinen yhteys.

Kuhunkin tapahtumapuun haarautumiskohtaan j liittyvä todennäköisyys, eli kyseisen toiminnon onnistumisen tai epäonnistumisen todennäköisyys, on ehdollinen sen hetkiselle historialle H_j, johon kuuluu esimerkiksi alkutapahtuma ja mahdollisesti aiempien turvallisuustoimintojen epäonnistuminen. Haarautumiskohdan jälkeinen todennäköisyys voidaan laskea ehdollisen todennäköisyyden avulla: $P(\mathrm{X}_j \cap \mathrm{H}_j) = P(\mathrm{X}_j|\mathrm{H}_j)P(\mathrm{H}_j)$, missä X_j:llä merkitään haarautumiskohdassa olevan tapahtuman, esimerkiksi turvallisuustoiminnon, epäonnistumista F_j tai sen kompementtitapausta eli onnistumista S_j. Lopullinen, seuraukseen c_i johtava todennäköisyys saadaan peräkkäisten haarautumiskohtien todennäköisyyksien tulona:

$$P(c_i|\mathrm{IE}) = \prod_{j \in \mathrm{b}_i} P(\mathrm{X}_j|\mathrm{H}_j), \tag{4.1}$$

missä b_i:llä merkitään alkutapahtumasta IE seuraukseen c_i ulottuvaa tapahtumapuun haaraa, joita on n kappaletta. Seuraus c_i on siis diskreetti muuttuja tai jatkuva

muuttuja, joka on jaettu luokkiin. Kunkin haaran b_i seuraus c_i toteutuu taajuudella:

$$\lambda(c_i|\mathrm{IE}) = \lambda_{\mathrm{IE}} P(c_i|\mathrm{IE}), \tag{4.2}$$

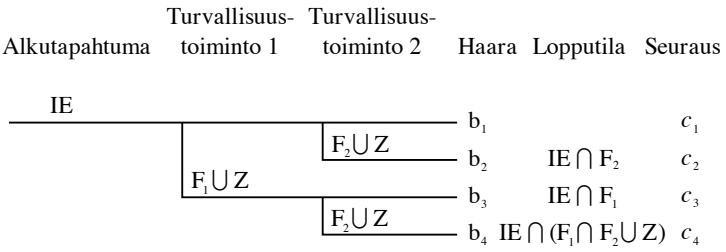
missä λ_{IE} on alkutapahtuman IE taajuus. Tarkasteltaessa useita alkutapahtumia IE_k kokonaistaajuus lasketaan yhdistämällä eri tapahtumapuut:

$$\lambda_i = \lambda(c_i) = \sum_k \lambda_{\mathrm{IE}_k} P(c_i|\mathrm{IE}_k) \tag{4.3}$$

Näin kaikkiin alkutapahtumiin liittyvä riski on saatu laskettua pistepareina $R = \{(c_i, \lambda_i) \,|\, i = 1, 2, ..., n\}$.

Pienissä järjestelmissä tapahtumapuu voidaan ratkaista arvioimalla tai määrittämällä kunkin haarautumiskohdan todennäköisyydet ja laskemalla koko haaran todennäköisyys näiden tulona. Laajoissa järjestelmissä tapahtumapuut ovat erittäin suuria, jolloin laskettavien haarojen lukumäärä on hyvin suuri. Lisäksi turvallisuustoiminnoilla voi tällöin olla voimakkaita riippuvuussuhteita, esimerkiksi eri järjestelmien laitteet voivat vikaantua jostain yhteisestä syystä, jolloin yhtälön (4.1) käyttö ei käytännössä onnistu. Tällöin tapahtumapuu ratkaistaan yhdistämällä kunkin haaran sisältämien vikaantumiskohtien F_j vikapuut JA-portilla yhdeksi suureksi vikapuuksi. Eri alkutapahtumiin liittyvät tapahtumapuut yhdistetään TAI-porteilla isommaksi kokonaisuudeksi ja näin muodostettu puu ratkaistaan Boolen algebraan erikoistuneilla algoritmeilla. Haarautumiskohtien onnistumiset huomioidaan poistamalla vikapuun ratkaisusta loogiset mahdottomuudet. Lisäksi jos useampi haara halutaan liittää toisiinsa (esimerkiksi useat haarat johtavat samaan seuraukseen), näiden haarojen ratkaisut yhdistetään ja minimoidaan. Havainnollistava esimerkki tästä on esitetty kuvassa 4.3. Vikapuita ja niiden ratkaisemista käsitellään seuraavassa kappaleessa.

Tapahtumapuiden avulla voidaan arvioida tapahtumaketjuihin liittyviä riskejä mutta tässä yhteydessä riskin toinen kvantitatiivinen osa eli seuraus jäi varsin vähälle huomiolle. Vaikka todellisuudessa kuhunkin haaraan liittyvän seurauksen arviointi voi olla hankala prosessi, tässä työssä sen arviointiin ei syvennytä, sillä keskittymiskohteena on pääasiassa tason 1 PRA, jossa seuraus ilmaistaan suoraviivaisesti sydänvauriona. Tasolla 2 arvioidaan myös seurauksia mutta tälläkin tasolla riskikäyrää (katso luku 3.1 ja kuva 3.1) varten lasketaan eri päästöryhmiä, joita on noin 20 [17].

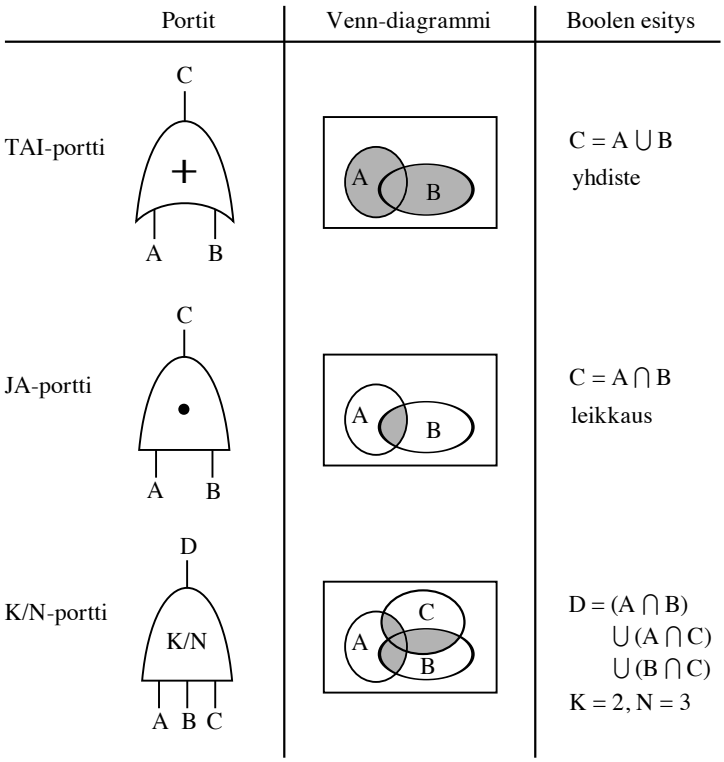


Kuva 4.3: Havainnollistus tapahtumapuun ratkaisemisesta ottaen huomioon loogiset mahdottomuudet. Turvallisuustoiminto 1 epäonnistuu tapahtuman F_1 tai Z sattuessa, turvallisuustoiminto 2 vastaavasti. Z voi edustaa esimerkiksi vikaantumista yhteisestä syystä tai yhteistä tukijärjestelmää. Haarasta b_2 on poistettu tapahtuma Z, sillä se on looginen mahdottomuus: haara sisältää turvallisuustoiminnon 1 onnistumisen, mikä edellyttää, että tapahtumaa Z ei tapahdu. Vastaavasta syystä Z on poistettu haarasta b_3. Mikäli seurauksia halutaan yhdistää esimerkiksi kokonaisriskin arvioimiseksi, vastaavien haarojen ratkaisut yhdistetään ja minimoidaan. Yhdistettäessä haarat b_2, b_3 ja b_4 ratkaisu olisi $IE \cap (F_1 \cup F_2 \cup Z)$ eli tapahtuma $F_1 \cap F_2$ poistettaisiin. Tämän jälkeen voidaan arvioida näiden haarojen sisältämä kokonaisriski.

4.3 Vikapuut

Vikapuu on järjestelmän (esimerkiksi jokin turvallisuusjärjestelmä) vikatilan looginen malli, Boolen algebran graafinen esitys, jossa järjestelmän vikatila esitetään komponenttien vikatilojen loogisena funktiona eli järjestelmän rakennefunktiona.[20]

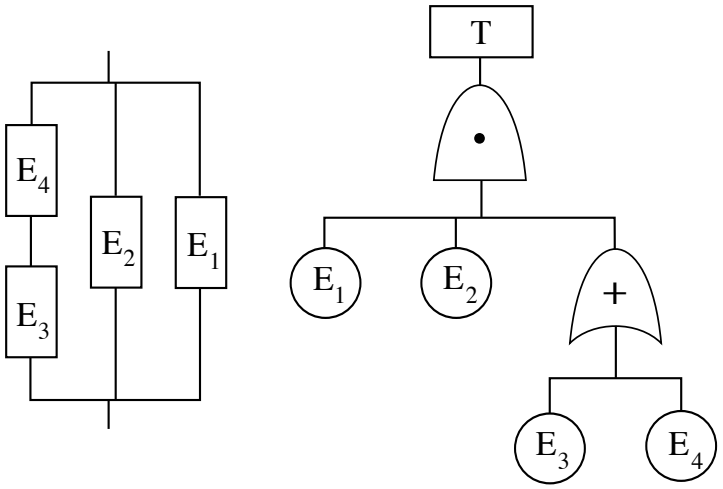
Vikapuun rakentaminen aloitetaan hankkimalla, tai laatimalla, järjestelmän toimintaa kuvaavat aineistot ja PI-kaaviot. Seuraavaksi on määriteltävä järjestelmän tehtävä ja epäonnistumiskriteeri, jonka jälkeen voidaan aloittaa varsinaisen vikapuun rakentaminen päättelemällä, miten ja miksi järjestelmän toiminta voi epäonnistua. Järjestelmän vikaa edustavaa ylintä vikapuun ulostuloa kutsutaan huipputapahtumaksi, josta edetään järjestelmällisesti kohti huipputapahtumaan johtavia syitä eli päätellään, mitkä yksittäiset tapahtumat voivat aiheuttaa tutkittavan järjestelmän vikaantumisen. Tapahtumat liitetään toisiinsa loogisin portein, joilla on yhteys Boolen algebraan. Vikapuun rakentamista jatketaan niin monta tasoa alaspäin kuin tarvitaan halutun tarkkuuden saavuttamiseksi. Vikapuu loppuu perustapahtumatasolle, jossa erilaiset tapahtumat on esitetty puun lehtinä. Kuvassa 4.4 on esitetty yleisimmät vikapuun portit ja niiden yhteydet Boolen algebraan.[20, 21]



Kuva 4.4: Vikapuuanalyysissä yleisimmin käytetyt portit ja niiden yhteydet Boolen algebraan.

Yleensä vikapuu laaditaan ensin komponenttitasolle siten, että kutakin komponenttia vastaa yksi perustapahtuma. Yksittäisellä komponentilla voi kuitenkin olla useita vikaantumistapoja ja useita epäkäytettävyyden syitä, esimerkiksi kriittiset laiteviat, jotka estävät heti laitteen toiminnan; viat, jotka eivät välittömästi estä laitteen toimintaa mutta vaativat korjausta; tai määräaikaistoimenpiteiden aiheuttama epäkäytettävyys. Näille määritellään silloin erilliset perustapahtumat ja komponentti korvataan TAI-portilla, jonka sisäänmenoina ovat mainitut erilliset perustapahtumat. Myös yhteisvikojen mallinnus voidaan sisällyttää vikapuuanalyysin mallintamalla ne omina lehtinään.[20] Lopputuloksena voidaan saada esimerkiksi kuvan 4.5(b) mukainen vikapuu.

Vikapuu ratkaistaan approksimoimalla vikapuun (eli tutkittavan järjestelmän) rakennefunktiota minimikatkosjoukkojen yhdisteenä (kvalitatiivinen ratkaiseminen), jonka jälkeen huipputapahtuman todennäköisyys voidaan laskea (kvantitatiivinen ratkaiseminen). Katkosjoukko on sellaisten perustapahtumien yhdistelmä, joiden seurauksena järjestelmä ei toimi. Minimikatkosjoukko on minimaalinen katkosjouk-



(a) Lohkokaavio. (b) Vikapuu.

Kuva 4.5: Esimerkki osajärjestelmän lohkokaaviosta ja sitä vastaavasta vikapuusta. Minimikatkosjoukot ovat $\mathrm{E}_1 \cap \mathrm{E}_2 \cap \mathrm{E}_3$ sekä $\mathrm{E}_1 \cap \mathrm{E}_2 \cap \mathrm{E}_4$.

ko eli jos yksikin minimikatkosjoukon komponenteista toimii, niin kyseinen minimikatkosjoukko ei aiheuta huipputapahtumaa. Perustapahtumat yhdistetään Boolen algebran avulla ja lopputuloksena saadaan huipputapahtuma T perustapahtumien $\mathrm{E}_1, ..., \mathrm{E}_n$ funktiona (rakennefunktion approksimaatio)

$$\mathrm{T} = \mathrm{T}(\mathrm{E}_1, ..., \mathrm{E}_n) \approx \bigcup_{i=1}^{k} \mathrm{M}_i, \tag{4.4}$$

missä k on minimikatkosjoukkojen lukumäärä ja jokainen termi M_i on leikkaus joistakin perustapahtumista

$$\mathrm{M}_i = \bigcap_{j \in \mathrm{e}_i} \mathrm{E}_j, \tag{4.5}$$

e_i on niiden perustapahtumien joukko, jotka kuuluvat minimikatkosjoukkoon M_i. Suurissa järjestelmissä minimikatkosjoukkojen laskenta voidaan joutua katkaisemaan, jolloin säilytetään vain tiettyä, valittua kertalukua lyhyemmät minimikatkosjoukot [20]. Katkaisuehtona voi käyttää myös todennäköisyysrajaa, jolloin minimikatkosjoukkojen laskenta katkaistaan, kun katkaisurajaa todennäköisemmät minimikatkosjoukot on laskettu. Minimikatkosjoukkojen laskenta Boolen algebralla on laskennallisesti hyvin raskas operaatio. Tähän soveltuvia ohjelmia ovat mm. Säteilyturvakeskuksessa kehitetty FinPSA ja Ruotsissa kehitetty RiskSpectrum.

Huipputapahtuman todennäköisyys $P(\mathrm{T})$ on yleisesti

$$P(\mathrm{T}) \approx S_1 - S_2 + S_3 - ... + (-1)^{k-1} S_k, \quad \text{missä} \tag{4.6}$$

$$S_1 = P(\mathrm{M}_1) + P(\mathrm{M}_2) + ... + P(\mathrm{M}_k), \tag{4.7}$$

$$S_2 = P(\mathrm{M}_1 \cap \mathrm{M}_2) + ... + P(\mathrm{M}_{k-1} \cap \mathrm{M}_k), \tag{4.8}$$

$$\vdots$$

$$S_k = P(\mathrm{M}_1 \cap \mathrm{M}_2 \cap ... \cap \mathrm{M}_k). \tag{4.9}$$

Useimmiten $P(\mathrm{T}) \approx S_1$ on riittävän tarkka arvo, jolloin tehtävä palautuu minimikatkosjoukkojen todennäköisyyksien määrittämiseen. Kun perustapahtumat ovat toisistaan riippumattomia, yhtälön (4.5) minimikatkosjoukon todennäköisyys voidaan ilmaista perustapahtumien todennäköisyyksien (esim. komponentin vikaantumisen todennäköisyys) tulona

$$P(\mathrm{M}_i) = \prod_{j \in \mathrm{e}_i} P(\mathrm{E}_j). \tag{4.10}$$

Perustapahtumat tulee määritellä toisistaan riippumattomiksi; eri syyt aiheuttavat eri perustapahtumat.[20] Jos esimerkiksi kuvan 4.5 tapauksessa $P(\mathrm{E}_1) = 0.1$, $P(\mathrm{E}_2) = 0.2$, $P(\mathrm{E}_3) = 0.15$ ja $P(\mathrm{E}_4) = 0.3$, saadaan $S_1 = 0.003 + 0.006 = 9 \times 10^{-3}$ ja $S_2 = 0.003 \times 0.006 = 1.8 \times 10^{-5}$, jolloin $P(\mathrm{T}) = 8.982 \times 10^{-3}$. Approksimaation $P(\mathrm{T}) \approx S_1$ lisäksi $P(\mathrm{T})$:lle pätee tarkempi yläraja:

$$P(\mathrm{T}) \leq 1 - \prod_{i=1}^{k} \big(1 - P(\mathrm{M}_i)\big) \leq S_1. \tag{4.11}$$

Kuvan 4.5 esimerkin tapauksessa saadaan $P(\mathrm{T}) = 8.982 \times 10^{-3}$.

Vikapuuanalyysin tuloksena saadaan huipputapahtuman todennäköisyys ja lisäksi tietoa järjestelmän rakenteesta sekä sen heikkouksista minimikatkosjoukkojen avulla. Minimikatkosjoukoilla voidaan myös tarkastella syvyyssuuntaisen puolustuksen toteutumista turvallisuuden kannalta [21]. Mitä lyhyempi minimikatkosjoukko on, sitä luotettavampia sen sisältämien komponenttien tulee olla. Vikapuuanalyysin avulla voidaan kuitenkin arvioida vain tutkittavan järjestelmän luotettavuutta, ei huipputapahtuman aiheuttamia seurauksia.

Järjestelmän rakennefunktion ja erilaisiin seurauksiin johtavien tapahtumaketjujen todennäköisyyksien arviointi onnistuu kuvatulla tapahtuma- ja vikapuuanalyysillä.

Tämä kuitenkin vaatii arviot alkutapahtumataajuuksille ja perustapahtumien todennäköisyyksille, mikä tarkoittaa, että on tutkittava komponenttien toimintaa ja vikaantumista luotettavuustekniikan avulla.

4.4 Vikaantumisen ja korjaamisen mallinnus

Yksi keskeisimmistä käyttövarmuuden mitoista on luotettavuus, joka määritellään todennäköisyytenä, että laite suorittaa sille asetetut vaatimukset tietyn aikaa määrättyjen olosuhteiden vallitessa. Käsite on erityisen keskeinen tilanteissa, joissa laitetta ei voida korjata.

Tutkitaan aluksi kertaluonteista tapahtumaa, jossa lähtötilasta siirrytään kertaluonteisesti toiseen tilaan. Nämä kaksi tilaa ovat "kunnossa" sekä "epäkunnossa" ja kiinnostuksen kohteesta riippuu kumpi valitaan lähtötilaksi. Jos lähtötilaksi valitaan "kunnossa" tutkitaan vikaantumista, kun taas päinvastaisessa tilanteessa tarkastelun kohteena on korjaus. Olkoon lähtötilassa kulutettu aika jatkuva satunnaismuuttuja T, jonka tiheysfunktio on $f(t)$. Kertymäfunktio $F(t)$ kuvaa silloin todennäköisyyttä, että lähtötilasta siirrytään (eli komponentti vikaantuu tai vastaavasti korjataan) ajanjakson $[0, t]$ aikana: $F(t) = P(T \leq t)$.

Kertymäfunktion oikeanpuoleisella häntäfunktiolla $\bar{F}(t) = 1 - F(t) = P(T > t)$ on etenkin vikaantumista tarkasteltaessa hyvin tärkeä tulkinta: $\bar{F}(t)$ kuvaa laitteen luotettavuutta eli todennäköisyyttä, että laite ei vikaannu välillä $[0, t]$. Tällöin merkitään $r(t) = P(T > t)$[1]. Kertymäfunktiolle asetettavat matemaattiset vaatimukset $F(0) = 0$ ja $\lim_{t\to\infty} F(t) = 1$ on luontevaa hyväksyä myös luotettavuuden kannalta: Ensimmäinen tarkoittaa, että laite on täysin toimintakuntoinen alkuhetkellä ja toinen, että kaikki laitteet vikaantuvat äärellisessä ajassa.[20] Vikaantumisajan todennäköisyystiheysfunktio on $F(t)$:n derivaatta: $f(t) = dF(t)/dt = -d\bar{F}(t)/dt$.

Merkitään funktiolla $\lambda(t)$ siirtymisintensiteettiä lähtötilasta lopputilaan. Tällöin $\lambda(t)dt$ on ehdollinen todennäköisyys, että siirrytään tilasta toiseen hetkellä $(t, t+dt]$:

[1]Tyypillisesti luotettavuus merkitään isolla R:llä mutta tässä yhteydessä tästä käytännöstä poiketaan, sillä R on haluttu varata yksinomaan riskin symboliksi.

$$\lambda(t)dt = P(t < T \leq t + dt | T > t) = \frac{P(t < T \leq t + dt)}{P(T > t)} \tag{4.12}$$

$$= \frac{\bar{F}(t) - \bar{F}(t + dt)}{\bar{F}(t)} = -\frac{d\bar{F}(t)}{\bar{F}(t)}. \tag{4.13}$$

Tästä differentiaaliyhtälöstä, olettaen $\bar{F}(0) = 1$, saadaan

$$\bar{F}(t) = e^{-\Lambda(t)}, \quad \text{missä} \quad \Lambda(t) = \int_0^t \lambda(s)ds. \tag{4.14}$$

Tuloksesta seuraa, että $f(t) = \lambda(t)e^{-\Lambda(t)} = \lambda(t)\bar{F}(t)$. Havaitaan, että mikä tahansa esitellyistä funktioista, $f(t)$, $F(t)$, $\bar{F}(t)$, $\lambda(t)$ tai $\Lambda(t)$, määrittelee jäljelle jäävät funktiot.

Laitteen vikaantumista tarkasteltaessa satunnaismuuttujaa T kutsutaan vikaantumisajaksi (tai eliniäksi) ja tavanomaisesti mielenkiinto kohdistuu vikaantumisajan odotusarvoon t_f eli keskimääräiseen vikaantumisaikaan (Mean Time To Failure):

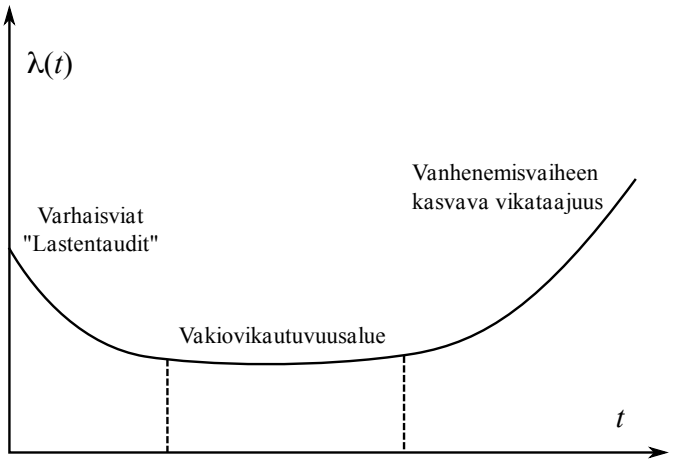
$$t_f = \int_0^\infty tf(t)dt = \int_0^\infty tdF(t) = -\int_0^\infty tdr(t). \tag{4.15}$$

Osittaisintegroinnilla ja oletuksella, että $\lim_{t\to\infty} t\,r(t) = 0$ (yleensä näin on) saadaan

$$t_f = \int_0^\infty r(t)dt. \tag{4.16}$$

Myös todennäköisyyksille voidaan antaa konkreettiset tulkinnat: Kertymäfunktio $F(t)$ kuvaa laitteen epäluotettavuutta, jonka vastakohta on jo mainittu luotettavuus $r(t)$, josta joissain yhteyksissä käytetään myös termiä eloonjäämisfunktio. Lisäksi $\lambda(t)dt$ kuvaa todennäköisyyttä, että vikaantuminen tapahtuu hetkellä $(t, t + dt]$ ehdolla, että vikaantumista ei ole vielä tapahtunut. Funktiota $\lambda(t)$ kutsutaan vikataajuudeksi tai vikautuvuudeksi. Sillä voi olla "kylpyammekäyrän" muoto, joka on esitetty kuvassa 4.6. Ensimmäinen osa vähenevällä vikataajuudella esittää sisäänajovaihetta (burn-in) eli alkuvaiheen "lastentauteja". Vakiovikataajuuden ajanjakso on laitteen normaali käyttöalue. Kolmannen vaiheen nouseva vikataajuus johtuu laitteen kulumisesta tai ikääntymisestä (wear-out). Aikaisten vikojen määrää pyritään vähentämään sisäänajovaiheella ja tarkoituksena on vaihtaa laite ennen ikääntymisvaihetta.[20] On huomattava, että sisäänajotestauksella ei voida parantaa yksittäisen laitteen luotettavuutta. Kyse ei siis ole yksittäisen laitteen laadun

parantamisesta. Ennemmin kyse on koko tuotepopulaation luotettavuuden parantamisesta, sillä testauksella voidaan karsia joukosta huonot yksilöt, jolloin lopputuloksena on luotettavampi ja tasalaatuisempi tuotejoukko.



Kuva 4.6: Kylpyammekäyrä koostuu kolmesta osasta. Ensimmäinen osa kuvaa alkuvaiheen "lastentauteja", jolloin vikataajuus vähenee ajan funktiona. Tämän jälkeen seuraa vakiotaajuuden alue, jota seuraa kasvavan vikautuvuuden vanhenemisvaihe.

Vikaantumisten aikariippuvuuden mallintamiseen käytetään tyypillisesti Weibull-jakaumaa: $f(t) = \alpha\lambda^\alpha t^{\alpha-1} e^{(-\lambda t)^\alpha}$. Tällöin vikautuvuus on muotoa $h(t) = \alpha\lambda^\alpha t^{\alpha-1}$ ja luotettavuus $r(t) = e^{-(\lambda t)^\alpha}$. Vähenevälle vikataajuudelle $\alpha < 1$ ja kasvavalle $\alpha > 1$. Vakiovikataajuuden alueella $\alpha = 1$, jolloin vikautuvuus on vakio λ. Tällöin luotettavuusfunktio saa muodon $r(t) = e^{-\lambda t}$ ja vikaantumisaika T on eksponentiaalisesti jakautunut: $f(t) = \lambda e^{-\lambda t}$. Keskimääräinen elinikä on silloin $t_f = 1/\lambda$ ja varianssi $\sigma_f^2 = 1/\lambda^2$. Eksponenttijakauma on muistiton, jolloin vikaantumisen todennäköisyys tietyllä ajanjaksolla on sama alkamisajankohdasta riippumatta eli komponentti ei kulu.

Tarkasteltaessa vialla olevan laitteen korjausta tilanne on analoginen vikautuvuuden kanssa mutta vastaaville termeille ei ole aivan yhtä konkreettista tulkintaa tai termistöä. Tosin vikautuvuuden vastineena käytetään termiä korjautuvuus [20]. Lisäksi korjautuvuuden sijasta on mielekkäämpää muodostaa erilaisia korjausmalleja käyttäen korjausajalle erilaisia todennäköisyysjakaumia. Ensimmäinen vaihtoehto on luonnollisesti kiinteä korjausaika t_0, jolloin $t_r = t_0$ ja varianssi $\sigma_r^2 = 0$ tai tästä jalostettu tasajakautuneen korjausajan malli. Luonnollisempaa olisi kuitenkin käyttää mallia, jossa korjausintensiteetti eli korjautuvuus on vakio μ, jolloin tilanne johtaa vakiovikautuvuutta vastaavaan tilanteeseen: $t_r = 1/\mu$ ja $\sigma_r^2 = 1/\mu^2$. Vielä realisti-

sempi malli olisi vakiokorjautuvuuden malli minimikorjausajalla eli korjaus kestää vähintään minimiajan θ, jonka jälkeen korjausaika on vakiokorjautuvuuden mallin mukaisesti eksponentiaalisesti jakautunut. Tällöin $t_r = \theta + 1/\mu$ ja $\sigma_r^2 = 1/\mu$.[20]

4.5 Vikojen ja korjausten vuorotteluprosessi

Edellinen kappale käsitteli komponentin vikaantumista tai korjaamista yksittäisenä, kertaluonteisena tapahtumana. Todellisuudessa vioittunut laite voidaan joko vaihtaa uuteen tai korjata. Lisäksi laitteita tyypillisesti huolletaan niiden käyttövarmuuden parantamiseksi ja testataan, jotta havaittaisiin mahdollisia piileviä vikoja. Laiteviat voidaankin luokitella välittömästi havaittaviin vikoihin ja piileviin vikoihin, jotka paljastuvat vasta huollon, testauksen tai tarvetilanteen yhteydessä. Viat voidaan edelleen luokitella kriittisiin ja ei-kriittisiin vikoihin. Kriittiset viat aiheuttavat laitteen toimimattomuuden välittömästi sen satuttua, kun taas ei-kriittiset viat voidaan korjata myöhemmin sopivana ajankohtana. Tätä jaottelua on havainnollistettu kuvassa 4.7.

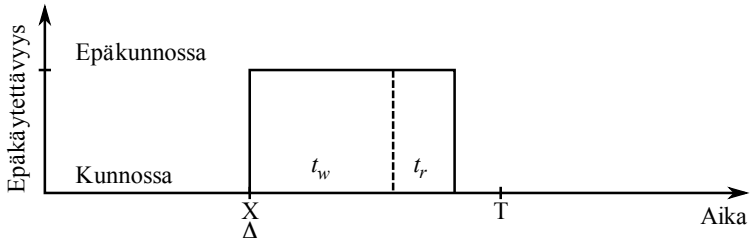
Vikaantumisten ja korjausten vuorotteluprosessissa käyttövarmuutta mitataan luotettavuden sijasta käytettävyydellä. Hetkellinen käytettävyys $a(t)$ määritellään todennäköisyytenä, että laite on toimintakunnossa hetkellä t riippumatta siitä, onko vikoja tai korjauksia ollut ennen hetkeä t. Jos laitetta ei voi korjata, luotettavuus ja käytettävyys ovat samat $r(t) = a(t)$ ja vastaavasti epäluotettavuus on yhtä suuri kuin epäkäytettävyys $u(t)$. Muita käytettävyyssuureita ovat asymptoottinen käytettävyys

$$a(\infty) = \lim_{t \to \infty} a(t) \tag{4.17}$$

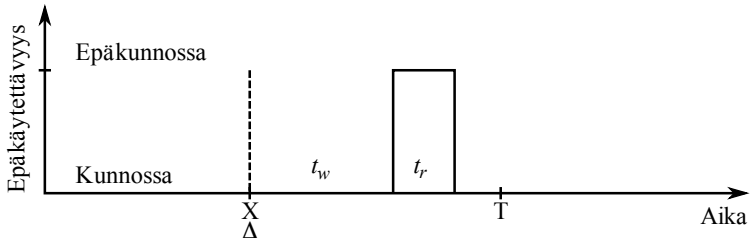
sekä tarkasteluvälille τ aikakeskiarvoistettu käytettävyys

$$a_{ave} = \frac{1}{\tau} \int_0^\tau a(t)dt. \tag{4.18}$$

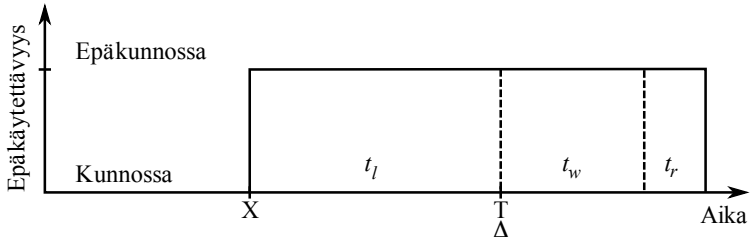
Vastaavat määritelmät pätevät myös epäkäytettävyydelle [10, 20, 23, 24], joka on riskianalyysin kannalta usein käytettävyyttä kiinnostavampi suure. Lisäksi, keskiarvoistettua epäkäytettävyyttä tarkempaan tulokseen käytännön riskianalyyseissa harvoin päästään.



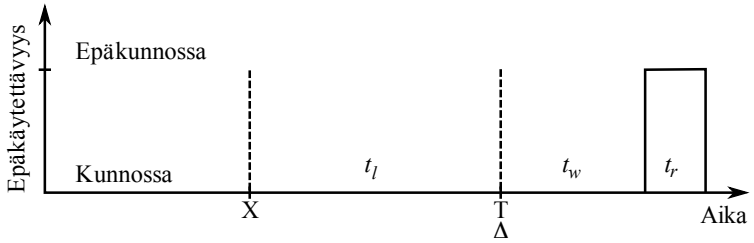
(a) Havaittavat kriittiset viat.



(b) Havaittavat ei-kriittiset viat.



(c) Piilevät kriittiset viat.



(d) Piilevät ei-kriittiset viat.

Kuva 4.7: Epäkäytettävyys eri vikatyypeille. t_l merkitsee vian piilevyysaikaa, t_w korjauksen odottamisaikaa ja t_r aktiivista korjausaikaa. Vikaantumishetki on merkitty X:llä, vian havaitsemishetki Δ:lla ja testausajankohta T:llä. Selvästi pisin epäkäytettävyysjakso on piilevillä kriittisillä vioilla. Kuvat tehty lähteen [22] kuvien avulla.

Seuraavassa käsitellään aluksi vikaantumisten ja korjausten kannalta keskeinen Poisson-prosessi, jonka jälkeen tutkitaan välittömästi havaittavien vikojen prosessia yksinkertaisen Markov-mallin avulla. Lopuksi käsitellään piilevien vikojen mallinnusta.

4.5.1 Poisson-prosessi

Tarkastellaan vikaantumisia pisteprosessina, jossa korjausajat ovat lyhyitä (nollakesto) ja vikaantuminen tapahtuu vakiotaajuudella λ. Korjaus palauttaa laitteen välittömästi uuden veroiseksi ja täysin toimintakykyiseksi. Tällä prosessilla voidaan mallintaa yksittäisen, välittömästi korjattavan tai vaihdettavan laitteen vikaantumista tai vaihtoehtoisesti tarkastella identtisten laitteiden populaatiota, jossa populaation koko pysyy vakiona.[10]

Vikaantumisten välillä laitetta voidaan luotettavuusmielessä käsitellä korjaamattomana, jolloin vakiovikautuvuudella λ yksittäiset vikaantumisajat ovat toisistaan riippumattomia ja noudattavat eksponenttijakaumaa $T_i \sim \exp(\lambda)$. Tällöin hetkeen t mennessä sattuneiden vikaantumisten lukumäärä

$$N(t) = \max\{n \mid \sum_{i=1}^{n} T_i \leq t\} \tag{4.19}$$

noudattelee Poisson-jakaumaa: $N(t) \sim \text{Poisson}(\lambda t)$ [25], jolloin

$$P(N(t) = n) = e^{-\lambda t}\frac{(\lambda t)^n}{n!}. \tag{4.20}$$

Poisson-jakauman odotusarvo on $E(N(t)) = \lambda t$ ja varianssi $Var(N(t)) = \lambda t$.

Poisson-prosessilla on sovellusten kannalta tärkeä superpositioperiaate. Jos kukin $N_i(t)$ on riippumaton ja Poisson$(\lambda_i t)$-jakautunut, niin osaprosessien summa on myös Poisson-jakautunut: $\sum_{i=1}^{k} N_i(t) \sim \text{Poisson}(\sum_{i=1}^{k} \lambda_i t)$ [25]. Superpositioperiaatteella voidaan laskea vakiotaajuudella vikaantuvan populaation odotettavissa olevien vikojen lukumäärä $E(N(t)) = \sum_{i=0}^{k} \lambda_i t$, kun yksittäisen laitteen vikataajuus on λ_i. Jos kyseessä on homogeeninen populaatio, esimerkiksi redundanttinen järjestelmä, vikataajuudet ovat samoja koko populaation yli: $\lambda_i = \lambda$, $\forall i$. Tällöin saadaan

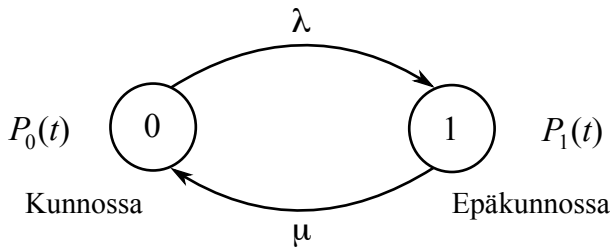
$$n = k\lambda t \quad \Leftrightarrow \quad \lambda = \frac{n}{kt}. \tag{4.21}$$

Laitteen odotusarvoinen vikataajuus voidaan siis estimoida hyvin yksinkertaisella kaavalla, jossa havaittujen vikojen lukumäärä n jaetaan laitteiden lukumäärällä k ja tarkasteluajalla t eli laitetunneilla.

Superpositioperiaatteen lisäksi Poisson-prosessille pätee myös ohennusperiaate: Alkuperäinen Poisson-prosessi voidaan pilkkoa useaan osaan, joista jokainen on myös Poisson-prosessi. Kyseessä on siis superpositioperiaatteelle käänteinen ominaisuus. [25]

4.5.2 Markov-prosessi

Edellä käsitelty Poisson-prosessi sisälsi oletuksen, että epäkunnossa olevan laitteen palauttaminen toimintakuntoiseksi kestää mitättömän lyhyen ajan (nollakesto). Tässä luvussa tarkastellaan yleisempää mallia, jossa vikaantuminen ja korjaus seuraavat toisiaan vakiotaajuudella λ ja μ, vastaavasti. Molemmat siirtymät ovat siis analogisia ja tätä yksittäistä siirtymää käsiteltiin aiemmin luvussa 4.4. Laitteen vikaantumisten ja korjausten vuorottelua voidaan esittää Markov-diagrammilla, joka on esitetty kuvassa 4.8. Laitteella on siis kaksi tilaa "kunnossa" ja "epäkunnossa" tai vastaavasti tilat 0 ja 1.



Kuva 4.8: Markov-diagrammi vikaantumisen ja korjaantumisen vuorottelusta. Vikaantuminen tapahtuu vakiotaajuudella λ ja laite korjataan vakiotaajuudella μ.

Merkitään $P_0(t) = a(t)$ (hetkellinen käytettävyys) eli todennäköisyys, että laite on toimintakunnossa hetkellä t, joka siis tarkoittaa todennäköisyyttä olla tilassa 0 hetkellä t. Vastaavasti $P_1(t) = u(t)$ epäkäytettävyydelle. Koska muita tiloja ei ole $P_0(t) + P_1(t) = 1$, $\forall\, t$. Oletetaan, että tila hetkestä t eteenpäin riippuu vain tilasta hetkellä t, eikä tapahtumista ennen sitä (Markov-oletus) [25]. Tarkastellaan niin lyhyttä hetkeä $[t, t + dt]$, että siinä voi tapahtua korkeintaan yksi tilasiirto. Oltaessa hetkellä t tilassa 0 siinä pysytään todennäköisyydellä $1-\lambda dt$ ja siirrytään tilaan 1 todennäköisyydellä λdt, tilalle 1 menettely on täysin vastaava. Kun otetaan huomioon

tilassa olemisen todennäköisyydet $P_0(t)$ ja $P_1(t)$, voidaan kirjoittaa muutosyhtälöt

$$P_0(t+dt) = P_0(t)(1-\lambda dt) + P_1(t)\mu dt \tag{4.22}$$
$$P_1(t+dt) = P_0(t)\lambda dt + P_1(t)(1-\mu dt). \tag{4.23}$$

Ryhmittelemällä saadaan kirjoitettua differentiaaliyhtälöt

$$\dot{P}_0(t) = -\lambda P_0(t) + \mu P_1(t) \tag{4.24}$$
$$\dot{P}_1(t) = \lambda P_0(t) - \mu P_1(t). \tag{4.25}$$

Sijoittamalla $P_0(t) = 1 - P_1(t)$ yhtälöön (4.25) saadaan $P_1(t) = \lambda/(\lambda+\mu) + Ce^{-(\lambda+\mu)t}$, missä vakio C määräytyy alkuehdosta $P_1(0) = \lambda/(\lambda+\mu) + C$.

Alkutilanteelle on kolme vaihtoehtoa: tiedetään, että laite on aluksi kunnossa ($P_1(0) = 0$) tai epäkunnossa ($P_1(0) = 1$), tai alkutilaa ei tiedetä varmasti, jolloin $P_1(0) = p$ eli laite on aluksi epäkunnossa todennäköisyydellä p. Ensimmäisessä tapauksessa alkutilana on 0 eli

$$u_0(t) = \frac{\lambda}{\lambda+\mu}\left(1 - e^{-(\lambda+\mu)t}\right) \tag{4.26}$$
$$a_0(t) = \frac{\mu}{\lambda+\mu} + \frac{\lambda}{\lambda+\mu}e^{-(\lambda+\mu)t}. \tag{4.27}$$

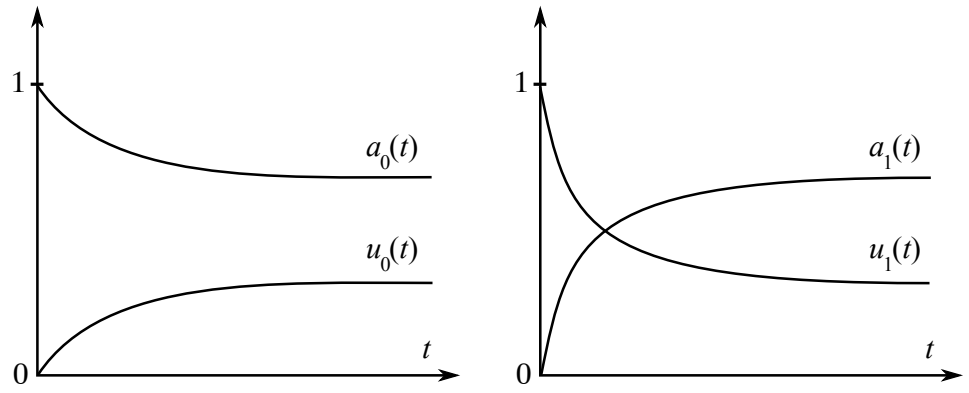
Toisessa tapauksessa alkutilana on 1, jolloin

$$u_1(t) = \frac{\lambda}{\lambda+\mu} + \frac{\mu}{\lambda+\mu}e^{-(\lambda+\mu)t} \tag{4.28}$$
$$a_1(t) = \frac{\mu}{\lambda+\mu} + \left(1 - e^{-(\lambda+\mu)t}\right). \tag{4.29}$$

Yleisellä ehdolla $P_1(0) = p$ saadaan

$$u(t) = p\,u_1(t) + (1-p)u_0(t) \tag{4.30}$$
$$a(t) = (1-p)a_1(t) + p\,a_0(t). \tag{4.31}$$

Kuvassa 4.9 on havainnollistettu käytettävyyden ja epäkäytettävyyden kehittymistä ajan funktiona. Kuvat havainnollistavat, miten $a(t)$ ja $u(t)$ saavuttavat kohtuullisen nopeasti asymptoottisen raja-arvon. Käytettävyydellä ja luotettavuudella on siis selvä ero. Käytettävyys saavuttaa vakioarvon, kun taas luotettavuus pienenee eksponentiaalisesti kohti nollaa.[20]



(a) Alkuoletus: laite on aluksi kunnossa. (b) Alkuoletus: laite on aluksi epäkunnossa.

Kuva 4.9: Markov-mallin käytettävyyden $a(t)$ ja epäkäytettävyyden $u(t)$ kehittyminen ajan funktiona eri alkuoletuksilla.

Yhtälöistä (4.30) ja (4.31) voidaan laskea raja-arvot eli asymptoottinen rajaepäkäytettävyys ja -käytettävyys:

$$\lim_{t\to\infty} u(t) = \frac{\lambda}{\lambda+\mu} \quad \text{ja} \quad \lim_{t\to\infty} a(t) = \frac{\mu}{\lambda+\mu}. \tag{4.32}$$

Luvussa 4.4 käsiteltiin vakiotaajuudella tapahtuvaa vikaantumista sekä korjausta ja todettiin, että keskimääräinen vikaantumisaika $t_f = 1/\lambda$ ja korjaantumisaika $t_r = 1/\mu$. Sijoittamalla nämä edellisiin yhtälöihin saadaan

$$\lim_{t\to\infty} u(t) \approx \frac{t_r}{t_f+t_r} \quad \text{ja} \quad \lim_{t\to\infty} a(t) \approx \frac{t_f}{t_f+t_r}. \tag{4.33}$$

Käytettävyys ja epäkäytettävyys voidaan siis arvioida t_f:n ja t_r:n avulla, joiden estimaattoreina voi käyttää aritmeettista keskiarvoa olettaen, että laitteen käyttö- ja korjausajat ($t_f^{(i)}$ ja $t_r^{(i)}$, $i = 1, ..., N$) tunnetaan. Lisäksi, laitteen ollessa käytössä $u(t) = 0$ ja muulloin (eli kun rikkinäistä laitetta korjataan) $u(t) = 1$, jolloin aikakeskiarvoistettu epäkäytettävyys on

$$u_{ave} = \frac{1}{\tau}\int_0^\tau u(t)dt = \frac{1}{\sum_{i=1}^N \left(t_f^{(i)} + t_r^{(i)}\right)} \sum_{i=1}^N t_r^{(i)} = \frac{t_r}{t_f+t_r} \approx \lim_{t\to\infty} u(t). \tag{4.34}$$

Eli vakiotaajuudella tapahtuvien havaittavien vikaantumisten ja korjausten tapauksessa laitteen aikakeskiarvoistettu epäkäytettävyys on sama kuin Markov-mallin antama asymptoottinen epäkäytettävyys. Yhtälön (4.34) epäkäytettävyys voidaan

myös kirjoittaa vikataajuuden λ avulla muotoon

$$u_{ave} = \frac{t_r}{1/\lambda + t_r} = \frac{\lambda t_r}{1 + \lambda t_r} \approx \lambda t_r, \tag{4.35}$$

sillä usein pätee riittävällä tarkkuudella $1 + \lambda t_r \approx 1$. Tätä muotoa käytetään usein käytännön laskuissa [24], sillä laitteiden vikataajuus ja keskimääräinen korjausaika voidaan estimoida käyttökokemuksista esimerkiksi yhtälön (4.21) avulla. Ydinvoimaloissa käytettyjen laitteiden osalta vikataajuuksia on esitetty mm. teoksessa [22], jossa on käytetty eri voimaloista saatua dataa ja estimointi on toteutettu Bayesilaisen mallinnuksen avulla.

Esitetyistä lausekkeista on havaittavissa, että komponentin epäkäytettävyyttä voi pienentää kahdella tavalla. Kasvattamalla komponentin luotettavuutta eli pienentämällä vikataajuutta tai nopeuttamalla korjaustoimenpiteitä, jolloin korjausaika lyhenee. Tärkeiden järjestelmien onkin oltava luotettavia ja lisäksi niille on usein määrätty suurin sallittu korjausaika esimerkiksi turvallisuusteknisissä käyttöehdoissa.

4.5.3 Varalla olevat laitteet

Edeltävä kappale käsitteli tapausta, jossa laitteet ovat normaalisti käynnissä osana järjestelmää ja niiden viat havaitaan välittömästi joko hälytyksistä tai esimerkiksi tuotannon häiriintymisestä. Korjaukset oletettiin aloitettavan välittömästi vian ilmettyä. Toinen tyypillinen käyttötapa on pitää laitteita varalla, valmiustilassa, ottaen ne käyttöön vasta tarpeen tullen. Tällaisia laitteita tai järjestelmiä ovat esimerkiksi turvallisuus- ja suojajärjestelmät kuten palonsammutus- tai ydinreaktorin hätäjäähdytysjärjestelmä. Näihinkin laitteisiin viat syntyvät satunnaisella hetkellä, mutta niitä ei havaita, koska laitteet ovat normaalin tuotantokäytön aikana varalla (kts. kuvaa 4.7). Tästä syystä varalla olevia laitteita tai järjestelmiä koestetaan määrävälein ja niiden epäkäytettävyys riippuu mm. vikataajuudesta, korjausajasta sekä koestusvälistä. Koestettaessa laite voi olla järjestelmästään poiskytkettynä, jolloin se ei pysty toteuttamaan sille asetettuja tehtäviä mutta toisaalta koestamattomassa laitteessa voi olla piileviä vikoja.

Varalla olevan laitteen epäkäytettävyys esitetään usein kuudella voimalaitoskäytäntöä kuvaavalla termillä:

1. Laitteeseen tulee piilevä vika vakiotaajuudella λ, jolloin sitä voidaan luotettavuusmielessä ajatella korjaamattomaksi testausvälin $[0, \tau)$ aikana eli hetkellinen epäkäytettävyys on $u(t) = F(t) = 1 - e^{-\lambda t}$. Tällöin aikakeskiarvoistettu epäkäytettävyys on

$$u_{ave}^{(1)} = \frac{1}{\tau}\int_0^\tau (1 - e^{-\lambda t})dt = \frac{1}{\tau}\big(\tau + \frac{1}{\lambda}(e^{-\lambda\tau} - 1)\big) \tag{4.36}$$

$$= 1 + \frac{1}{\lambda\tau}\big(- \lambda\tau + \frac{1}{2!}(\lambda\tau)^2 - \frac{1}{3!}(\lambda\tau)^3 + ...\big) \approx \frac{1}{2}\lambda\tau, \tag{4.37}$$

   kun $\lambda\tau \approx 0$, jolloin käytetty approksimaatio Taylorin sarjakehitelmästä on riittävän tarkka käytännön laskuja ajatellen.

2. Testauksen aikana $[\tau, \tau + t_t]$ oletetaan, laite on poiskytkettynä testausajan $t_t << \tau$, jolloin hetkellinen epäkäytettävyys on $u(t) = 1$. Tällä välillä

$$u_{ave}^{(2)} = \frac{1}{\tau}\int_\tau^{\tau+t_t} dt = \frac{t_t}{\tau}. \tag{4.38}$$

3. On mahdollista, että testausvälillä τ laitteeseen tulee piilevä vika, jolloin laitteen epäkäytettävyys testin alkaessa on $u(\tau)$. Vika havaitaan testissä ja korjaustoimenpide aloitetaan välittömästi kestäen keskimäärin ajan $t_r << \tau$. Epäkäytettävyydeksi saadaan

$$u_{ave}^{(3)} = \frac{1}{\tau}\int_{\tau+t_t}^{\tau+t_t+t_r} u(\tau)dt = \frac{1}{\tau}t_r(1 - e^{-\lambda\tau}) \approx \lambda t_r. \tag{4.39}$$

4. Testaus voi myös aiheuttaa laitteeseen vian todennäköisyydellä q, jolloin korjaamiseen kuluu keskimäärin t_r. Tästä aiheutuva epäkäytettävyys on

$$u_{ave}^{(4)} = \frac{1}{\tau}\int_{\tau+t_t}^{\tau+t_t+t_r} q dt = q\frac{t_r}{\tau}. \tag{4.40}$$

5. Samoin kuin testikäynnistys myös tositarvekäynnistys voi aiheuttaa laitteeseen vian. Tästä aiheutuu vakioepäkäytettävyys koko käytön ajaksi $u_{ave}^{(5)} = q_0$. Tyypillisesti asetetaan $q = q_0$ [22].

6. Vaikka tositarvetilanteessa laite käynnistyisi, se voi vikaantua taajuudella λ_0 sinä aikana t_0, jonka sen tulisi toimia ilman korjausta. Mahdollinen vika ei siis jää piileväksi mutta laitetta ei mielletä korjattavaksi. Tästä aiheutuu lisätermi $u^{(6)} = F(t_0) = 1 - e^{-\lambda_0 t_0} \approx \lambda_0 t_0$.

Edellyttäen, että esitellyt kuusi epäkäytettävyyttä ovat pieniä, saadaan kokonaisepäkäytettävyydelle karkea approksimaatio laskemalla ne yhteen:

$$u_{ave} \approx q_0 + \lambda_0 t_0 + \frac{1}{2}\lambda\tau + (q + \lambda\tau)\frac{t_r}{\tau} + \frac{t_t}{\tau}. \tag{4.41}$$

Tästä yhtälöstä on eri teoksissa hieman erilaisia versioita mutta esimerkiksi teoksissa [20, 22] käytetään vastaavaa laskentatapaa. Lisäksi teoksessa [20] on esitetty erilaisia mahdollisia lisätermejä, kuten vasta korjausvaiheessa epäkäytettävyyttä aiheuttavien ei-kriittisten vikojen tai välittömästi havaittavien vikojen huomiointi. Lisäksi koestuksessa ei välttämättä jouduta ottamaan laitetta pois käytöstä, vaan yleensä laite voidaan tarpeen tullen ohjata vakiotodennäköisyydellä koestustilasta käyttötilaan. On kuitenkin muistettava, että ylimääräisten parametrien lisääminen ei välttämättä lisää muuta kuin mallin kompleksisuutta tai subjektiivisuutta, sillä joidenkin parametrien estimointi tai muu arviointi voi olla hyvin hankalaa. Yhtälössä (4.41) on kolme laitteelle ominaista estimoitavaa parametria: q_0, λ_0 ja λ. Muut parametrit määräytyvät laitteen testauksen ja huollon mukaan ja ovat siten tiedossa. Estimaatteja mainituille kolmelle parametrille ydinvoimaloissa käytettyjen laitteiden osalta on kirjattu esimerkiksi teoksessa [22].

Kuten edellä mainittiin, liian pitkä testausväli lisää piilevien vikojen todennäköisyyttä ja toisaalta liian tiheä testaus voi aiheuttaa myös epäkäytettävyyttä, jos laite on testattaessa poiskytkettynä. Yhtälön (4.41) avulla voidaan arvioida optimaalista testausväliä τ_{opt} minimoimalla keskimääräistä epäkäytettävyyttä, mikä johtaa derivaatan nollakohdan määrittämiseen:

$$\frac{d\,u_{ave}}{d\tau}\Big|_{\tau=\tau_{opt}} = \frac{1}{2}\lambda - \frac{t_t + qt_r}{\tau_{opt}^2} = 0, \quad \text{josta} \quad \tau_{opt} = \sqrt{\frac{2(t_t + qt_r)}{\lambda}}. \tag{4.42}$$

Tulos on minimi, sillä u_{ave} on konveksi funktio: $\frac{d^2}{d\tau^2}u_{ave} = 2(t_t + qt_r)/\tau^3 > 0$, kun $\tau > 0$. Käytännössä optimaalisen testausvälin valintaan vaikuttavat monet muut tekijät, esimerkiksi käytettävissä olevat resurssit ja laitteiden kuluminen (vikaantumisintensiteetti oletettiin mallissa vakioksi). Lisäksi on mahdollista, että funktio u_{ave} on verraten laakea, jolloin epävarmuudet huomioiden minimikohta ei ole tarkka, eikä silloin turvallisuuden kannalta erityisen merkittävä.

4.6 Yhteisviat

Yhteisvialla (Common Cause Failure, CCF) tarkoitetaan vähintään kahden laitteen tai järjestelmän vikaantumista lyhyen ajan sisällä yhteisestä syystä. Tällöin vioittumiset eivät tapahdu toisistaan riippumattomalla tavalla. Yhteisvioilla on huomattavan suuri vaikutus järjestelmiin, joilta vaaditaan korkeaa luotettavuutta ja ne ovat yksi riskianalyysin haastavimpia aiheita. Niiden johdosta rinnakkaiset osajärjestelmät eivät voi taata koko järjestelmän ihanteellista luotettavuutta, vaan yhteisvikojen suuri vaikutus päihittää rinnakkaisperiaatteen merkityksen.[20, 26]

Yhteisvikoihin johtavia tunnistettavia tapahtumia ovat mm. tulipalot, tulvat, seisminen toiminta ja muut ympäristön aiheuttamat ilmiöt. Lisäksi, useat komponentit voivat sisältää samoja suunnittelu- tai valmistusvirheitä tai niiden käyttö ja kunnossapito on toistuvasti virheellistä.[20, 26] Laitteiden välillä voi myös olla tunnistamattomia riippuvuuksia (jäännösyhteisviat). Näiden riippuvuuksien mallinnukseen on käytössä erilaisia malleja mm. "Square-Root" -menetelmä [9, 24], β-faktorimalli, α-faktorimalli, MGL-malli (Multiple Greek Letters), BFR-malli (Binomial Failure Rate) [10, 24, 26] tai BPM-malli (Basic Parameter Model) [26].

Paljon käytetty yhteisvikamalli on β-faktorimalli [24, 26]: Tarkastellaan n:stä identtisestä komponentista koostuvaa rinnakkaista järjestelmää, joista jokainen vikaantuu vakiotaajuudella λ. Vikaantumisen oletetaan jakautuvan kahteen osaan, komponenttikohtaisiin riippumattomiin vikoihin (taajuus λ_{I}) ja yhteisvikoihin (taajuus λ_{CCF}). Mallissa oletetaan siis riippuvuuksien symmetrisyys ja että yhteisvika vaikuttaa kaikkiin rinnakkaisen järjestelmän komponentteihin. Kunkin komponentin kokonaisvikataajuus on (superpositioperiaate)

$$\lambda = \lambda_{\mathrm{I}} + \lambda_{\mathrm{CCF}}. \tag{4.43}$$

Yhteisvikaa kuvaava β-tekijä määritellään yhteisvikataajuuden ja kokonaisvikataajuuden suhteena

$$\beta = \frac{\lambda_{\mathrm{CCF}}}{\lambda} = \frac{\lambda_{\mathrm{CCF}}}{\lambda_{\mathrm{I}} + \lambda_{\mathrm{CCF}}}. \tag{4.44}$$

Tyypillisesti β:lle käytetään arvoja välillä $[0.01; 0.1]$ [20]. Yhteisvikataajuudeksi saadaan

$$\lambda_{\mathrm{CCF}} = \frac{\beta}{1-\beta}\lambda_{\mathrm{I}}. \tag{4.45}$$

Rinnakkainen järjestelmä on siis mallinnettu järjestelmänä, jossa rinnakkaisten kom-

ponenttien kanssa on sarjaankytkettynä yhteisvikaa kuvaava ”virtuaalikomponentti”. Kun yhteisvikataajuus on saatu arvioitua edellä kuvatulla tavalla voidaan edelleen arvioida sen aiheuttama epäkäytettävyys tai vaikutus järjestelmän luotettavuuteen. Muita yhteisvikamalleja ei esitellä, sillä niitä ei tulla tässä työssä käyttämään.

4.7 Ihmisen toiminnallinen luotettavuus

Inhimillisen luotettavuuden arviointi (Human Reliability Analysis, HRA) lisääntyi huomattavasti Three Mile Islandin onnettomuuden jälkeen, jolloin opittiin tunnistamaan operaattorin tärkeys onnettomuustilanteen hallinnassa [27]. Inhimillisen toiminnon luotettavuudella tarkoitetaan todennäköisyyttä, että henkilö suorittaa oikein tietyn, edellytetyn toiminnon käytettävissä olevan ajan puitteissa, ja ettei henkilö suorita ylimääräistä haitallista toimintoa. Toiminnoille voidaan nimetä seuraavia virhetyyppejä: puuttuva toiminto, väärä toiminto, haitallinen lisätoiminto, väärä suoritusjärjestys ja väärä ajoitus. Inhimillisten virheiden todennäköisyys tehdään mahdollisimman pieneksi työtilanteen, työvälineiden, testien ja työympäristön huolellisella suunnittelulla. Ohjeiden laatu, työn ja tarkastusten kuittaus sekä koulutus ovat myös avainasemassa.[20]

Inhimillisten virheiden vähentämiseksi ja liian hitaan diagnoosin välttämiseksi ydinvoimalaitosten suunnittelussa käytetään 30 minuutin sääntöä: Kaikki turvallisuustoiminnot, joita tarvitaan nopeammin kuin 30 minuutin kuluessa häiriötilanteesta, automatisoidaan eikä niitä jätetä operaattorin diagnoosin varaan.[2, 20]

HRA-menetelmien käyttö kytkeytyy osaksi PRA:n tapahtuma- ja vikapuuanalyysia: Inhimillinen toiminto kuvataan järjestelmän komponenttina, joka voi epäonnistua tietyllä todennäköisyydellä. Ongelmana kuitenkin on, että ihmisen toiminnan kuvaaminen luotettavuusteknisin keinoin ei suoraan huomioi käyttäytymiseen vaikuttavia tekijöitä. Puutteellisen, ristiriitaisen tai harhaanjohtavan tiedon vaikutuksen huomioiminen toiminnassa on varsin vaikeaa. Lukuarvoja erilaisissa tilanteissa tehtävien virheiden todennäköisyyksille on olemassa mutta ne ovat usein subjektiivisia arvioita. Luotettavia havaintoihin perustuvia arvoja on vain harvoille yksinkertaisille toiminnoille.[20, 27]

Inhimillisen luotettavuuden arviointiin on kehitetty useita erilaisia menetelmiä, esimerkiksi THERP (Technique for Human Error Rate Prediction), HCR (Human

Cognitive Model for PRA Analysis) tai ATHEANA (A Technique for Human Error Analysis) [27]. Uusimpia tutkimuksia ovat olleet esimerkiksi simulaattorin avulla tehty operaattorikoe HAMMLAB:ssa (HAlden huMan-Machine LABoratory), jonka tuloksia on analysoitu kansainvälisesti useassa maassa. Valtion teknillinen tutkimuskeskus on osallisena tässä benchmark-projektissa käyttäen "enhanced Bayesian THERP" -menetelmää tulosten arvioinnissa.

Luku 5

Riskien seuranta

Käyttökokemusten seuranta on aiemmin perustunut deterministiseen lähestymistapaan, jolla on selvitetty tutkittavan tapahtuman perussyitä ja vaikuttavia tekijöitä. Todennäköisyyteen perustuvalla riskien seurannalla pyritään analysoimaan jo tapahtuneita tilanteita niiden riskin kannalta käyttäen hyväksi voimalaitoksen PRA:ta. Erilaisesta lähetymistavasta huolimatta päätavoite on molemmissa tavoissa sama: käyttökokemuksista oppiminen tulevien onnettomuuksien ehkäisemiseksi.

Deterministiseen lähestymistapaan verrattuna PRA:han pohjautuva riskien seuranta tarjoaa tapahtuman riskimerkitykselle kvantitatiivisen mitan ja sopii erityisen hyvin arvioimaan moninkertaisten vikojen tai epäkäytettävyyksien riskimerkitystä sallien melko monimutkaisten tapahtumaketjujen tarkastelun. Se antaa myös lisätietoa syvyyssuuntaisen puolustuksen jäljelle jääneistä turvallisuustoiminnoista ja auttaa määrittämään tarkoituksenmukaisen tason käyttökokemusten seurannalle. Deterministisillä menetelmillä ei myöskään voitaisi tutkia mahdollisia ”entä jos” -tapahtumia yhtä tehokkaasti eikä se mahdollistaisi laitoksen turvallisuuden valvonnan trendianalyysia.[28]

Riskien seurannalla pyritään kvantifioimaan, kuinka kaukana ”läheltä piti” -tilanne oli onnettomuudesta eli millainen marginaali tapahtuman ja mahdollisen onnettomuuden välille jäi. Ongelmaksi muodostuukin tähän tarkoitukseen sopivan mitan määritys. Yleinen tapa on käyttää mittana tapahtuman aiheuttamaa sydänvauriotodennäköisyyden kasvua verrattuna keskimääräiseen, vuotta kohti laskettuun, sydänvauriotodennäköisyyteen. Todennäköisyyspohjainen riskien seuranta onkin yk-

si PRA:n sovellus ja usein puhutaan PRA-perustaisesta tapahtumien arvioinnista.[1]

Tässä luvussa esitellään riskien seurannan teoreettisia perusteita, jonka jälkeen käsitellään riskien seurantaa käytännölliseltä kannalta käyttäen esimerkkinä Olkiluodon käyttötapahtumia.

5.1 Teoreettinen perusta

Riskien seurantaa on käytetty PRA:n sovelluksena kansainvälisesti monissa ydinvoimaloissa jo yli vuosikymmenen ajan [29], vaikka käytetty todennäköisyyden jälkikäteislaskenta sisältää teoreettisia vaikeuksia. Perustavanlaatuisin ongelma on, miten tunnettu tapahtumahistoria sisällytetään ehdollisiin todennäköisyysarvioihin, jotta vältettäisiin triviaali ratkaisu: jos onnettomuutta ei sattunut, sen todennäköisyys tapahtumahistorialle ehdollistettuna on 0. Riskien seurantaa käsitellään teoreettiselta kannalta mm. teoksissa [29, 30, 31, 32], kun taas teoksissa [28, 33] on käytännöllisempi lähestymistapa.

5.1.1 Tapahtumahistorian käsittely

Ensimmäinen vaihe riskien seurantaprosessissa on tarkasteltavan tapahtuman tai tapahtumaketjun hahmottaminen. Tämän vuoksi analysoitava tilanne tulee käydä läpi kokonaisuudessaan ja merkitä kaikki tilanteen kannalta merkitykselliset tapahtumat muistiin aikajärjestyksessä.[33] Määritellään hetkeen t ulottuva tapahtumahistoria H_t pistejoukoksi

$$\mathrm{H}_t = \{(\mathrm{X}_1, t_1), ..., (\mathrm{X}_k, t_k)\}, \tag{5.1}$$

missä t_i on tapahtuman ajanhetki ja X_i vastaavan tapahtuman määrittelevä muuttuja. Esimerkiksi jokaisella alkutapahtumalla tai laitoksen tilaa muuttavalla tapahtumalla on oma X_i:n arvo.[29] Tapahtumat määritellään siis pisteprosessin avulla.

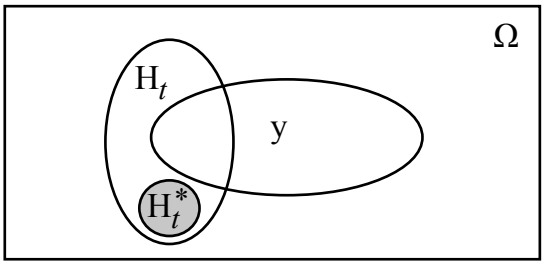
Riskien jälkiseurannassa tarkasteltava ajanhetki s on menneisyydessä ($s < t$) ja laskennassa käytetään tietämystä tapahtumahistoriasta H_t. Merkitään y:llä avaruutta, joka sisältää onnettomuuden sisältävät tapahtumaketjut. Analogiana yhtälölle 4.3,

[1] Todennäköisyyspohjaisesta riskien seurannasta käytetään kansainvälisesti useita erilaisia termejä, mm. risk follow-up, PSA-based event analysis (PSA-EA), probabilistic event analysis, accident sequence precursor (ASP) analysis tai probabilistic operational event analysis, eikä yhtenäistä käytäntöä ole muodostunut.

onnettomuuden taajuus historialle H_t ehdollistettuna on

$$\lambda_s(\mathrm{y}|\mathrm{H}_t) = \sum_k \lambda_{\mathrm{IE}_k}(\mathrm{H}_t) P(\mathrm{y}|\mathrm{H}_t), \quad s < t. \tag{5.2}$$

Jos koko tunnettu tapahtumahistoria H_t^* sisällytetään laskentaan ja jos onnettomuutta ei ole tapahtunut, saadaan triviaalisti $\lambda_s(\mathrm{y}|\mathrm{H}_t^*) = 0$, sillä aliavaruuksien H_t^* ja y leikkaus on tyhjä joukko. Jotta laskennassa päästäisiin käsiksi tapahtuman riskimerkitykseen ja ei-triviaaleihin tuloksiin, historiaa H_t^* on laajennettava siten, että se leikkaa aliavaruuden y kanssa. Tämä tarkoittaa, että laajennettu historia H_t ei sisällä kaikkea täydellisen historian H_t^* sisältämää tietoa, vaan kattaa useampia realisaatioita. Tämä on esitetty kuvassa 5.1.[29]



Kuva 5.1: Tunnetun tapahtumahistorian H_t^* laajentaminen historiaksi H_t, jolloin se leikkaa onnettomuusketjut sisältävän avaruuden y kanssa. Kaikkia mahdollisia tilahistorioita on merkitty Ω:lla.

Ongelmaksi muodostuu H_t^*:n laajennussääntöjen määrittely siten, että jälkikäteislaskennalla olisi jokin mielekäs ja yhdenmukainen tulkinta. Yksi keino on määritellä tapahtuma-avaruus jaettavaksi kahteen osaan: alkutapahtumiin liittyvään osaan H_t^1 ja turvajärjestelmien toimimattomuuteen liittyvään osaan H_t^2, jolloin riskien jälkiseuranta jakautuu näitä vastaaviin osiin. Molemmat määritelmät siis jättävät osan tunnetusta historiasta huomioimatta, mikä aiheuttaa konservatiivisuutta laskentatuloksiin. Lisäksi, eri määritelmillä laskettuja tuloksia ei voida pitää täysin vertailukelpoisina.[29]

5.1.2 Alkutapahtumat huomioiva seuranta

Alkutapahtumat huomioivassa määritelmässä eli tapahtumahistorian ensimmäisessä laajennussäännössä sattunut alkutapahtuma tunnetaan eli se tapahtuu varmasti mutta laitoksen tilasta (erityisesti turvajärjestelmien onnistumisesta) ei ole tietoa.

Onnettomuuden todennäköisyys on tällöin $P(\mathrm{y}|\mathrm{H}_t^1)$. Käytännössä tämän määritelmän mukainen laskenta toteutetaan siten, että laitoskohtaisessa PRA-mallissa sattunutta alkutapahtumaa vastaavan tapahtumapuun avulla lasketaan alkutapahtumalle ehdollinen sydänvauriotaajuus $\lambda_s(\mathrm{y}|\mathrm{H}_t^1)$, jonka jälkeen lasketaan tapahtuman riskimerkitystä kuvaava ehdollinen sydänvauriotodennäköisyys (kts. yhtälöä (5.2))

$$\mathrm{CCDP} = P(\mathrm{y}|\mathrm{H}_t^1) = \frac{\lambda_s(\mathrm{y}|\mathrm{H}_t^1)}{\lambda_{\mathrm{IE}}}. \tag{5.3}$$

5.1.3 Laiteviat huomioiva seuranta

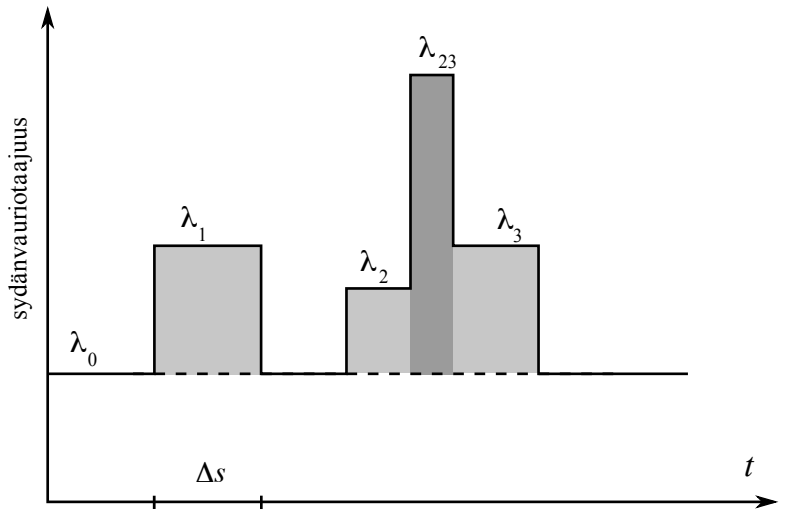
Toisessa tapahtumahistorian laajennussäännössä laitoksen turvajärjestelyjen tila oletetaan tunnetuksi niiden toimimattomuuksien tai operaattorivirheiden osalta ja riski aiheutuu siitä, olisiko tälle välille sattunut alkutapahtuma. Myös osittaiset toimimattomuudet, esimerkiksi tieto järjestelmän osittaisesta suoriutumisesta, otetaan huomioon kohonneen vikatodennäköisyyden avulla mutta laitteiden tai operaattoreiden oikeanlainen toiminta jätetään huomioimatta pitämällä niiden vikatodennäköisyydet nimellisarvoissaan. Tätä menettelyä kutsutaan "failure memory"-lähestymistavaksi.[33] Onnettomuuden todennäköisyys ajanjaksolla $[s, s + \Delta s]$ on (kts. lukua 4.4 ja vertaa esim. yhtälöön (4.14))

$$\mathrm{CCDP} = 1 - e^{-\int_s^{s+\Delta s} \lambda_{s'}(\mathrm{y}|\mathrm{H}_t^2)ds'} \approx \int_s^{s+\Delta s} \lambda_{s'}(\mathrm{y}|\mathrm{H}_t^2)ds'. \tag{5.4}$$

Tämän määritelmän mukainen riskilaskenta toteutetaan siten, että PRA-mallilla lasketaan turvajärjestelmän viallisuudelle ehdollinen (järjestelmä tai järjestelmät asetetaan mallissa vialliseksi ja mahdollisesti kasvatetaan muiden vikatodennäköisyyttä) kohonnut sydänvauriotaajuus $\lambda_1 = \lambda_s(\mathrm{y}|\mathrm{H}_t^2)$. Tämän jälkeen lasketaan sydänvauriotaajuuden kasvu $\Delta\lambda = \lambda_1 - \lambda_0$, missä λ_0 viittaa laitoksen laskettuun sydänvauriotaajuuden perustasoon (esim. kuvassa 3.4 on esitetty Loviisan ja Olkiluodon laitosyksiköiden sydänvauriotaajuuden perustason kehitys). Joissakin organisaatioissa sydänvauriotaajuuden kasvua tosin verrataan sydänvauriotaajuuden keskiarvoon, joka lasketaan laitoskokemusten perusteella [29]. Ehdollinen sydänvauriotodennäköisyyden kasvu ΔCCDP lasketaan sydänvauriotaajuuden kasvun ja sen keston Δs avulla:

$$\Delta\mathrm{CCDP} \approx \int_s^{s+\Delta s} (\lambda_1 - \lambda_0)ds' = \Delta\lambda \cdot \Delta s, \tag{5.5}$$

missä siis oletetaan, että $\Delta\lambda$ on ajan Δs vakio. Päällekkäisten eli yhtä aikaa ilmenevien vikojen tapauksessa tämä ei pidä paikkaansa, jolloin tapahtuma on jaoteltava osiin ja minimikatkosjoukot on laskettava myös päällekäiselle tapahtumalle. Tämä on esitetty kuvassa 5.2. On lisäksi muistettava, että sydänvauriotaajuudet ilmoitetaan vuositasolla. Tapahtuman keston yksikön on siis oltava myös vuosi. Tavanomainen tapa on jakaa tunneissa ilmoitettu kesto 8000 tunnilla, joka vastaa keskimäärin laitoksen tehoajoaikaa vuodessa.



Kuva 5.2: Yksittäisen ja riippumattomien päällekäisten tapahtumien riskimerkityksen laskenta. Harmaa alue kuvaa kyseiselle tapahtumalle ehdollista sydänvauriotodennäköisyyden kasvua. Päällekäisille tapahtumille on laskettava omat minimikatkosjoukot ja sydänvauriotaajuus, joka kuvan tapauksessa on merkitty λ_{23}:lla.

5.2 Tapahtumien luokittelu

Edellä kuvatulla menettelyllä voidaan laskea jokaiselle tapahtumalle sen riskimerkitys. Tyypillisesti tapahtumat jaotellaan kohonneen sydänvauriotodennäköisyyden ΔCCDP mukaan eri kategorioihin, jolloin saadaan laitostapahtumien lukumäärän jakauma ΔCCDP:n funktiona. Melko yleisessä käytössä on tapa, että tapahtuma dokumentoidaan erikseen riskiseurantaan, jos sen aiheuttama $\Delta\text{CCDP} > 10^{-6}$ (mm. GRS Saksassa, U.S. NRC Yhdysvalloissa, EDF Ranskassa, CSN Espanjassa), jonka jälkeen tapahtumat luokitellaan riskimerkityksen mukaan [34].

Tunnetun tapahtumaketjun analysoinnin lisäksi suositellaan ”entä jos” -tilanteiden arviointia, joissa tarkoituksena on lisätä tapahtumaan erilaisia muunnelmia, kuten tiettyjen järjestelmien vikaantumisia, yhteisvikoja, operaattoreiden epäonnistumisia tai erilaisia laitoksen toimintatiloja [28, 33]. Kattava riskin jälkikäteisarviointi ”entä jos” -analyyseineen tehdään usein vain merkittävimmille tapahtumille. Seurantaprosessiin valitut tapaukset arvioidaan aluksi nopeasti käyttäen konservatiivisia oletuksia, jolloin tapaukselle saadaan arvioitua yläraja. Tämän jälkeen laskentaa voidaan halutessa tarkentaa paremman arvion saamiseksi ja tehdä mahdollisia lisäanalyyseja.

Säteilyturvakeskuksessa käyttötapahtumien (esim. tulipalo tai turvallisuusjärjestelmän huolto) seurannassa on käytetty jakoa riskin kannalta merkittävimpiin (ΔCCDP $> 10^{-7}$), merkityksellisiin ($10^{-8} < \Delta$CCDP $< 10^{-7}$) ja muihin (ΔCCDP $< 10^{-8}$) tapahtumiin. Jako on siis huomattavasti tiukempi kuin monissa muissa maissa. Vaikka riskimerkitykseltään korkea tapahtuma on tärkeä käyttökokemuksen kannalta, ei siitä välttämättä seuraa, että matalan onnettomuusriskin tapahtuma olisi vähäpätöinen. Toistuvia ja mahdollisesti organisaation turvallisuuskulttuurin heikkenemistä osoittavia tapahtumia voi täysin oikeutetusti pitää tärkeänä palautteena niiden pienestä riskimerkityksestä huolimatta [33].

Voimayhtiöt ovat velvollisia raportoimaan Säteilyturvakeskukselle laitoksilla sattuneista käyttötapahtumista. Näiden käyttötapahtumaraporttien avulla seurataan mm. esiintyneitä laitevikoja ja niiden kestoa, joiden perusteella riskimerkitys arvioidaan PRA-perustaisesti käyttäen hyväksi yhtälöitä (5.3) ja (5.5). Riskien seuranta vie verraten paljon aikaa ja vaivaa, sillä raporttien määrä on kohtalaisen suuri ja seurannan oikea toteutus vaatii hyvää laitosyksiköiden tuntemusta. Suomessa valvottavien laitosyksiköiden määrä on tosin sen verran pieni, että kaikki käyttötapahtumat käydään läpi. Tyypillisesti Säteilyturvakeskuksessa todennäköisyyspohjainen riskien seuranta tehdään puolivuosittain ja tulokset esitetään vuosiraporteissa. Taulukossa 5.1 on esitetty eri laitosyksiköissä vuonna 2009 sattuneiden käyttötapahtumien lukumäärät eri riskikategorioihin jaoteltuna.

Vuoden 2009 riskien seurannassa havaittiin Loviisan laitosyksiköiden osalta paljon riskimerkitykseltään suuria ilmastointivikoja. Tämä onkin esimerkki riskien seurannan yhdestä tavoitteesta eli toistuvien vikojen havaitsemisesta. Olkiluodon laitosyksiköiden kohdalla riskimerkitykseltään suurimmat tapahtumat aiheutuivat dieselgeneraattoreista. Taulukon 5.1 mukaan Olkiluodon ja Loviisan laitosyksiköillä näyttää olevan eroa sekä riskimerkitykseltään suurten että pienten tapahtumien lukumäärässä. Tämä saattaa johtua Loviisan laitosten rakenteellisesta erosta tai kor-

Taulukko 5.1: Vuonna 2009 sattuneiden laitevioista johtuvien käyttötapahtumien lukumäärät laitosyksiköittäin eri riskikategorioihin luokiteltuna. Alkutapahtumia ei sattunut millään laitosyksiköllä.

Riskikategoria	Olkiluoto 1	Olkiluoto 2	Loviisa 1	Loviisa 2
$\Delta\text{CCDP} > 10^{-7}$	1	3	8	6
$10^{-8} < \Delta\text{CCDP} < 10^{-7}$	10	5	4	11
$\Delta\text{CCDP} < 10^{-8}$	56	42	33	16

jausaikojen pituudesta ja toisaalta pienemmistä vikaantumistaajuuksista. Eri organisaatioilla saattaa myös olla hieman erilaiset raportointi- ja seurantakäytännöt. Säteilyturvakeskus ei edellytä voimayhtiöiltä todennäköisyyspohjaista riskien seurantaa mutta Teollisuuden Voima on aloittanut käyttötapahtumien seurannan ja tilastoinnin. Tämä auttaa viranomaisen tekemää työtä huomattavasti, sillä riskien seurannan kannalta Teollisuuden Voiman toimittamat raportit ovat huomattavasti käyttökelpoisemmassa muodossa kuin Fortumin käyttötapahtumaraportit.

Vaikka taulukon 5.1 mukainen seuranta auttaa ydinturvallisuuden valvonnassa, sen hankaluutena on, että käyttötapahtumien määrä vaihtelee vuosittain, jolloin on vaikea arvioida, oliko jokin vuosi riskimerkitykseltään poikkeuksellinen. Koska laitteiden vikaantumisia on mielekästä pitää satunnaisprosessina, on luonnollista, että tapahtumien lukumäärät vaihtelevat jonkin odotettavissa olevan arvon ympärillä. Tähän asti Säteilyturvakeskuksessa ei ole ollut käytössä tätä huomioivaa menettelyä, jolloin satunnaisvaihtelun merkitystä ei ole arvioitu ja huomio kiinnittyy helposti vikojen absoluuttisiin lukumääriin eikä poikkeamaan odotusarvosta.

5.3 Vikatapahtumien lukumäärien simulointi luokittain

Säteilyturvakeskuksessa tehdään riskien seurantaa sekä Loviisan että Olkiluodon laitosyksiköiden osalta mutta tässä yhteydessä käsitellään ainoastaan Olkiluodon laitosyksiköitä. Tämä johtuu siitä, että Teollisuuden Voima käyttää PRA-ohjelmanaan Säteilyturvakeskuksen suosimaa FinPSA:ta, jolloin simulaation käytännön toteutus on yksinkertaisempaa.

Vuodessa tapahtuvien vikojen lukumäärän odotusarvon ja satunnaisvaihtelun selvittämiseksi vikatapahtumia mallinnetaan uusiutumisprosessin avulla käyttäen Ol-

kiluodon PRA-mallin parametreja. Yksittäisen vian aiheuttaman riskin lisäys voidaan tämän jälkeen arvioida järjestelmän rakennefunktion ja riskien seurannan teorian avulla. Uusiutumisprosessia simuloimalla ja PRA-mallin rakennefunktiota hyväksi käyttämällä voidaan siis määrittää kunkin riskikategorian vertailutaso ja satunnaisuudesta aiheutuva vaihtelu. Koska simulaatiomalli perustuu PRA-mallin parametreihin eikä havaintoaineistoon sovittamiseen, saadaan myös viitteitä käytettyjen parametrien oikeellisuudesta suhteessa havaintoihin.

Simulaatiossa keskitytään laitevikojen tarkasteluun, jolloin riskien seurantaan liittyvät laskut toteutetaan tämän oletuksen mukaisesti. Havaittujen laitevikojen prosessia voisi tutkia myös esimerkiksi aikasarja-analyysin keinoin mutta tätä lähestymistapaa rajoittaa datan soveltuvuus: Todennäköisyyksiin pohjautuvaa riskien seurantaa on käytetty vasta runsas kymmenen vuotta ja lisäksi merkittävimmät viat ovat harvinaisia eli havaintoja on vähän. Tässä työssä tarkoituksena on myös arvioida PRA-mallin parametrien oikeellisuutta vertaamalla simulointituloksia havaintoihin. Tämä ei olisi mahdollista esimerkiksi aikasarja-analyysiä käyttäen, jossa parametrit estimoidaan havainnoista.

5.3.1 Simulointimallin ja parametrien käsittely

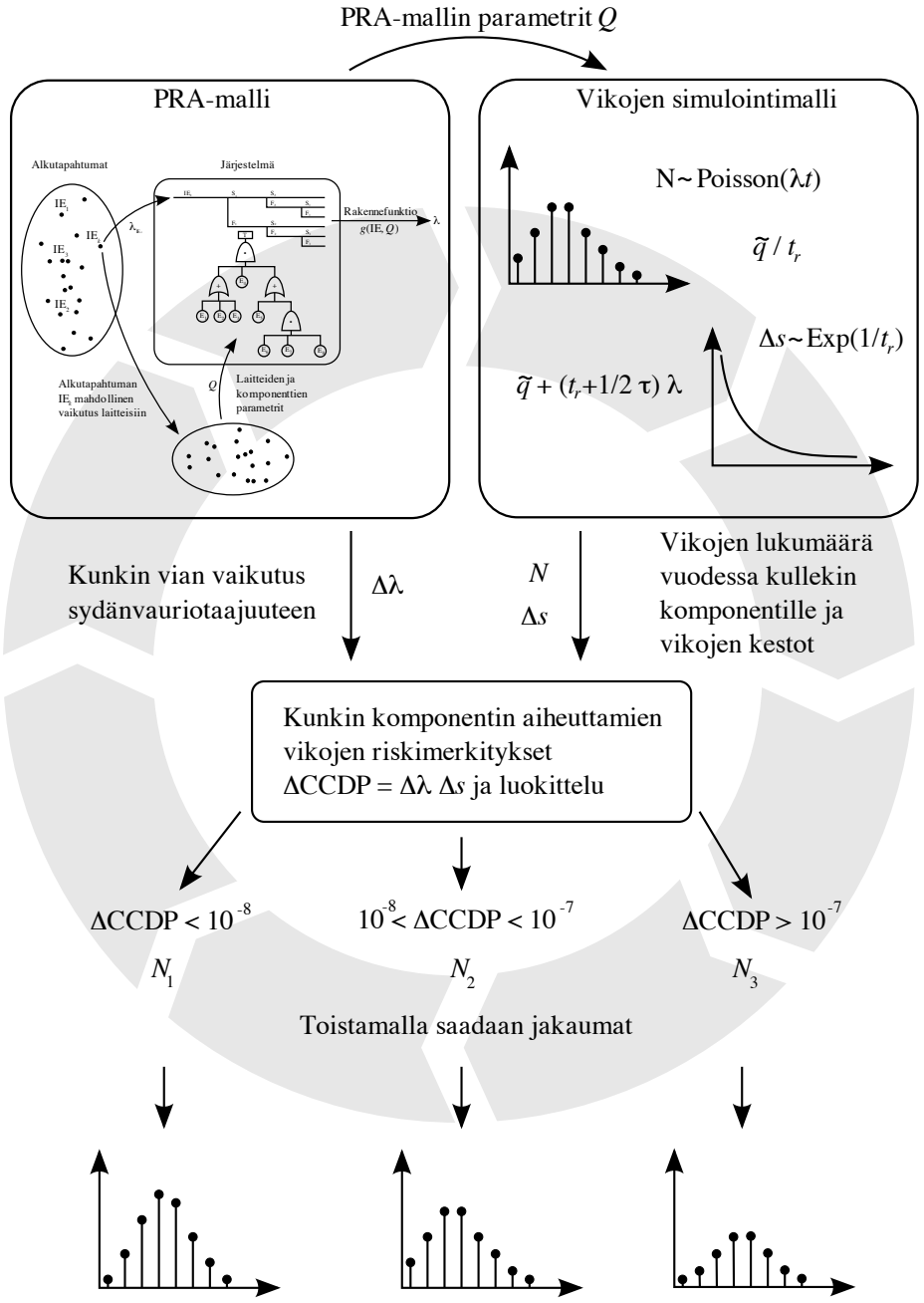
Komponenttien vikaantumisten simulointiin otetaan mukaan 437 erilaista vikatapahtumaa, jotka on määritelty Olkiluodon PRA-mallissa. Tapahtumat sisältävät mm. venttiilien juuttumisia, pumppujen tai dieselgeneraattoreiden sammumisia ja käynnistymättömyyksiä sekä yhteisvikoja. Tutkittavat laitteet ovat joko monitoroituja, jolloin niiden viat havaitaan välittömästi, tai varalla olevia, jolloin viat pysyvät piilevinä tarkastushetkeen tai tositarvetilanteeseen asti.

Vikaprosessien oletetaan tapahtuvan vakiotaajuudella ja korjaukset oletetaan lyhyiksi verrattuna toiminta-aikaan, jolloin vuoden aikana sattuvien vikojen lukumäärät voidaan arpoa komponenteittain Poisson-jakauman avulla. Tästä seuraa, ettei simulaatiossa huomioida riippumattomia päällekäisiä vikoja. Simulaation käyttötarkoitus huomioiden tämä ei aiheuta suurta eroa todellisuuteen, sillä suurin osa laitevioista on ei-kriittisiä, jolloin ennen korjauksen aloittamista voidaan varmistaa, että muita laitteita ei korjata samanaikaisesti. Mutta luonnollisesti yksinkertaistus jättää huomioimatta erilaiset tapahtumien yhdistelmät, joilla voi olla suuri riskimerkitys niiden harvinaisuudesta huolimatta. PRA-mallissa määritellyt yhteisviat otetaan simulaatiossa huomioon ja ne mallinnetaan omina tapahtuminaan.

Korjauksen kesto arvotaan eksponenttijakaumasta, sillä komponentin korjaaminen oletetaan myös vakiotaajuudella tapahtuvaksi. Piilevien kriittisten vikojen kestoon lisätään vian piilevyydestä aiheutuva osa, joka oletetaan tasajakautuneeksi testivälille. Vikojen kesto Δs arvotaan, jotta voitaisiin laskea yhtälön (5.5) mukainen riskimitta jokaiselle vikatapahtumalle. Arvotut kestot skaalataan tunneista tehoajovuotta vastaavaksi suureeksi jakamalla ne 8000 tunnilla. Sydänvauriotaajuuden kasvu $\Delta\lambda$ lasketaan FinPSA-ohjelmalla käyttäen Olkiluodon PRA-mallia, muuten simulointi toteutetaan Matlab-ohjelmistolla. Yhtä vuotta vastaavan simulaatiokierroksen vikatapahtumat luokitellaan eri riskikategorioihin ja simulaatiokierroksia lisäämällä saadaan määrättyä kunkin kategorian jakaumat. Simulaation rakennetta on havainnollistettu kuvassa 5.3.

Tarvittavat parametrit saadaan Olkiluodon PRA-mallista ja pääosin niiden arvoja voidaan käyttää hyväksi suoraan. Varalla olevan laitteen keskimääräinen epäkäytettävyys on yhtälössä (4.41) esitettyä muotoa, jossa piilevien kriittisten vikojen vaikutusta kuvaa osa $(t_r+\frac{1}{2}\tau)\lambda$. Parametri λ on varaoloaikana sattuvien kriittisten vikojen taajuus, t_r vikojen keskimääräinen korjausaika ja τ testivälin pituus. PRA-mallin "residuaaliepäkäytettävyys" $\tilde{q}$ sisältää yhtälössä (4.41) määritellyt muut epäkäytettävyydet, poislukien tositarvetilanteen epäkäytettävyys, joka jätetään huomioimatta. Mainitut parametrit tunnetaan ja $\tilde{q}$:n avulla varalla olevan laitteen ei-kriittisten vikojen taajuus arvioidaan yhtälön (4.35) avulla. Samaa yhtälöä käyttäen arvioidaan vikataajuus monitoroiduille laitteille (keskimääräinen epäkäytettävyys ja keskimääräinen korjausaika tunnetaan), joille oletetaan vain yksi vikatyyppi, koska havaittavien kriittisten ja ei-kriittisten vikojen erotteluun tarvittavia parametreja ei ole. Eroa näiden vikatyyppien välillä voidaan kuitenkin pitää pienenä, sillä tyypillisesti ydinturvallisuutta vähäisestikin heikentäviin vikoihin reagoidaan nopeasti, jolloin kuvassa 4.7 esitetty korjauksen odotusaika jää lyhyeksi. Kaikille komponenteille korjausajat arvottiin eksponenttijakaumasta parametrilla $1/t_r$.

Käytettävissä olevien parametrien suhteen dieselgeneraattorit ja komponenttien yhteisviat aiheuttavat poikkeuksen, sillä niille on PRA-mallissa määritelty ainoastaan kokonaisepäkäytettävyys. Tämän vuoksi Olkiluodon dieselgeneraattoreiden viat selvitettiin vuoden 2006 alusta vuoden 2009 kesään. Näistä vioista noin 10 % arvioitiin piileviksi vioiksi. Ei-kriittisten vikojen taajuus arvioitiin epäkäytettävyyden ja keskimääräisen korjausajan avulla aivan kuten muillekin laitteille ja tämän taajuuden avulla määrättiin piilevien vikojen taajuus. Yhteisvikojen osalta oletetaan, että varalla olevien laitteiden yhteisvikaprosessille termi $t_r + \frac{1}{2}\tau$ on sama kuin yksittäiselle



Kuva 5.3: Simulaatiossa käytetään hyväksi PRA-mallin parametreja. Komponenttivikoja ja niiden kestoja simuloidaan satunnaisprosessin avulla. Tämän jälkeen lasketaan kunkin tapahtuman riskimerkitys käyttäen hyväksi PRA-mallilla laskettua sydänvauriotaajuuden kasvua. Näin saadaan kullekin riskikategorialle simuloitua yksi mahdollinen tulos. Toistamalla tätä prosessia saadaan muodostettua jakaumat.

laitteelle. Perustelu oletukselle on, että järjestelmävika saadaan korjattua, kun yksikin vioittuneista laitteista on korjattu mutta toisaalta ei voida sanoa, mikä on yhteisvian testiväli, joten se oletetaan samaksi. Vastaavasti oletetaan, että monitoroitujen laitteiden yhteisvian keskimääräinen korjausaika on sama kuin yksittäiselle laitteelle. Tästä karkeasta oletuksesta seuraa $u = u_{ave} - \tilde{q} \propto \lambda$, jolloin yhteisvikataajuudelle saadaan β-faktorimallia (4.45) muistuttava yhtälö

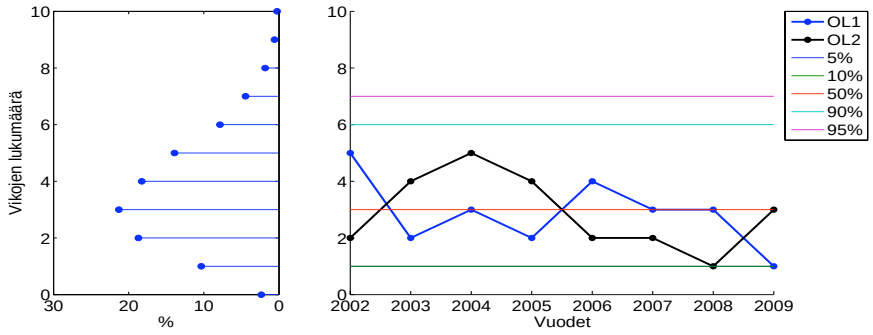
$$\lambda_{\mathrm{CCF}} \approx \frac{u_{\mathrm{CCF}}}{u}\lambda_{\mathrm{I}}. \tag{5.6}$$

5.3.2 Simulaation tulokset ja vertailu riskien seurannan tuloksiin

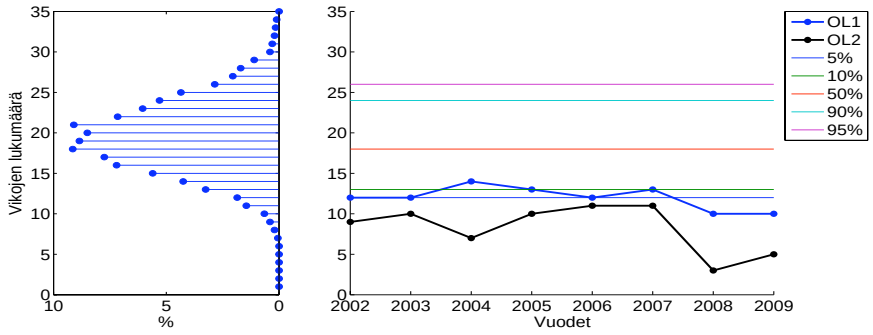
Kuvassa 5.4 on esitetty simulaation tuottamat jakaumat 2000 kierroksen jälkeen sekä Olkiluodon riskien seurannan havainnot eri riskikategorioihin luokiteltuna. Tarkennettakoon, että havainnoilla tarkoitetaan tässä yhteydessä todellista laitoksen vikaraporttiin merkittyä laitostapahtumaa, jonka riskimerkitys on määritetty laskennallisesti PRA-mallin avulla. Simulaatiotuloksilla taas tarkoitetaan edellisessä kappaleessa kuvatun mallinnuksen tuloksia.

Kuvissa on vyöhykkeillä esitetty jakaumasta lasketut fraktiilit, jotka rajaavat ilmoitetun osuuden simulaatiotuloksista alapuolelleen. Koska vikojen lukumäärä on diskreetti muuttuja, fraktiilirajat eivät ole täsmällisiä mutta niistä saa kuitenkin hyvän vertailukohdan havainnoille. Kuvista on nähtävissä, että simulaation mukaan vikoja olisi odotettavissa enemmän kuin mitä havainnot osoittavat. Tämän voi olettaa johtuvan PRA-mallin parametrien konservatiivisuudesta, jolloin niihin perustuva simulaatio tuottaa liioittelevan tuloksen suhteessa todellisuuteen.

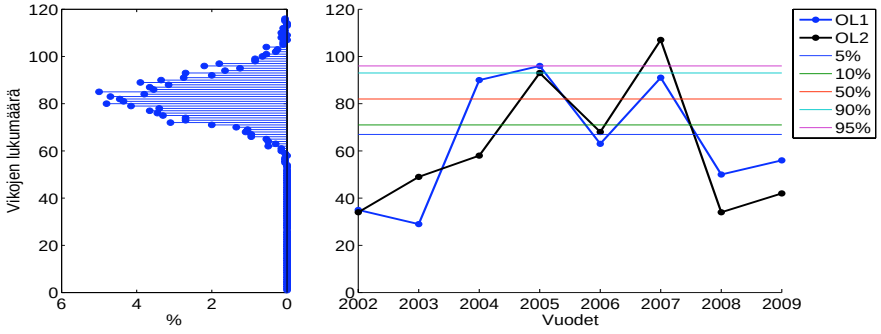
Tutkittava ajanjakso on melko lyhyt vikojen vaihtelun arvioimiseen havaintojen perusteella mutta simulaatio osoittaa, että satunnaisuudesta johtuen vuosittainen vaihtelu voi olla suurta. Tämän vuoksi havaintojen vuosittaisesta vaihtelusta ei pidä tehdä liian nopeita johtopäätöksiä. Parametrien tarkentaminen ja konservatiivisuuden vähentäminen parantaisi esitetyn menetelmän käyttöä riskien seurannan ja päätöksenteon tukena, sillä tällöin havainnon poikkeavuudesta voisi antaa luotettavamman arvion. Tämän vuoksi riskien seurannassa tulisi jatkossa tilastoida yksittäisten komponenttien viat, jolloin vikataajuuksia voitaisiin seurata ja päivittää aineiston kasvaessa. Nyt Säteilyturvakeskuksen tekemä todennäköisyyspohjainen riskien seuranta on käytännössä tiivistynyt taulukon 5.1 mukaisiin tuloksiin, jolloin tarkempi seuranta ja jäljitettävyys kadotetaan.



(a) Riskin kannalta merkittävimmät tapahtumat (ΔCCDP$> 10^{-7}$). Havainnot pysyvät mediaanin ympäristössä eikä erityisen poikkeavia havaintoja ole.



(b) Riskin kannalta merkitykselliset tapahtumat ($10^{-8} < \Delta$CCDP$< 10^{-7}$). Parametrien konservatiivisuus näkyy selvästi, sillä havaittuja vikoja on huomattavasti simulaation ennustamaa määrää vähemmän.

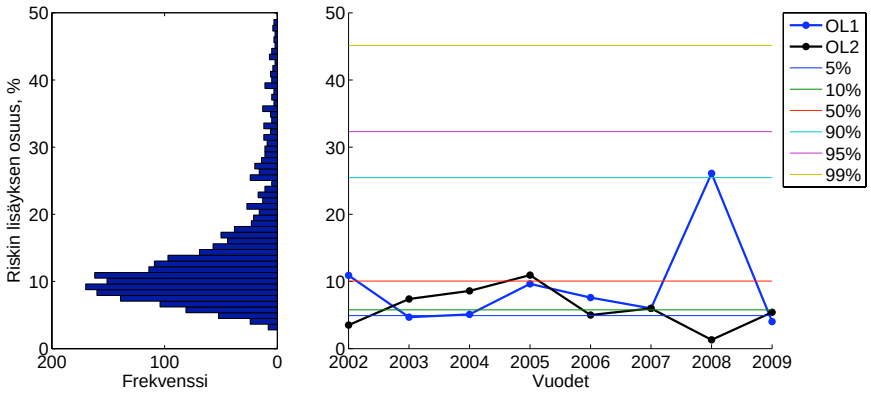


(c) Muut tapahtumat (ΔCCDP$< 10^{-8}$). Havaintojen vaihtelu on erittäin suurta ja eri laitosten välillä on havaittavissa korrelaatio (korrelaatiokerroin 0.79). Näin pienet riskinlisäykset johtuvat lyhyistä huoltotoimenpiteistä, jolloin korrelaatio on odotettua, sillä laitoksilla on sama huolto-organisaatio. Tällöin voi myös epäillä, että havainnot eivät täysin noudata satunnaisprosessia.

Kuva 5.4: Vasemmassa kuvassa simuloinnilla (kierroksia 2000) tuotettu jakauma. Oikeassa kuvassa jakauman avulla saadut fraktiilit, jotka rajaavat ilmoitetun osuuden simulaatiotuloksista alapuolelleen, sekä toteutuneet havainnot.

Vaikka simulaation tuottamat jakaumat eivät täysin vastaa havaintoja, eri kategorioiden suhteelliset osuudet ovat hyvin samansuuntaisia: Simuloitujen jakaumien mediaaneista laskettuna vikoja sattuu vuoden aikana eri kategorioissa noin 3, 17 ja 81 eli yhteensä 101 kappaletta, jolloin suhteelliset osuudet ovat vastaavasti 3 %, 17 % ja 80 %. Olkiluoto 1:lle havaintojen keskiarvoista lasketut osuudet ovat vastaavasti 4 %, 17 % ja 79 % ja Olkiluoto 2:lle 4 %, 12 % ja 84 %.

Esitetyn menetelmän avulla voidaan huomata eri riskiluokkien kohdalla poikkeavat havainnot mutta tämä ei anna käsitystä vuoden aikana sattuneesta kokonaisriskistä. On täysin mahdollista, että kaikissa kolmessa luokassa havainnot olisivat hyväksyttävyyden ylärajalla, jolloin yksittäin arvioituna mikään ei viittaisi riskin kannalta poikkeukselliseen vuoteen. Kokonaisuutta ajatellen tällainen vuosi olisi silti poikkeava. Kaikkien vuoden aikana sattuneiden käyttötapahtumariskien (eli ΔCCDP) summa jaettuna vakavan onnettomuuden todennäköisyydellä antaa kokonaiskuvan näiden käyttötapahtumien riskimerkityksestä. Simulaatiotulosten avulla myös tälle prosessille voidaan laskea jakauma ja verrata sitä havainnoista laskettuihin arvoihin. Tämä on esitetty kuvassa 5.5.



Kuva 5.5: Käyttötoiminnasta aiheutunut vuotuinen kokonaisriski. Oikealla 2000 simulaatiokierroksella saatu jakauma ja vasemmalla jakaumasta lasketut yksisuuntaiset fraktiilit sekä havaintojen perusteella lasketut arvot. Olkiluoto 1:n osalta vuosi 2008 erottuu selvästi, jolloin laitoksella paljastui dieselgeneraattoreiden yhteisvika.

Simulaation tuottama jakauma on siinä mielessä yllättävä, että vain 2000 simulaatiokierroksella muutama näyte tuottaa lähes 2.5-kertaisen riskin lisäyksen. Tämä ei tosin näy kuvasta 5.5, sillä selkeyden vuoksi käyttötoiminnasta aiheutuneen riskin lisäyksen asteikko on rajattu 50 %:iin. Laitteiden vioilla voi siis olla huomattavan suuri vaikutus vuosittaiseen onnettomuusriskin vaihteluun. Lisäksi on muistettava,

että simulaatiossa ei huomioitu päällekäisiä vikoja muuten kuin yhteisvikojen avulla. Jakauman vertailu havainnoista lasketuihin arvoihin osoittaa simulaation tuottavan samansuuntaisia tuloksia kuin havainnot. Konservatiivisuus ei siis näy yhtä voimakkaasti kokonaisriskiä kuvaavassa jakaumassa.

Kuvasta 5.5 näkee, että havainnot pysyttelevät miltei jatkuvasti mediaanin alapuolella mutta vuoden 2008 tapaukset Olkiluoto 1:ssä aiheuttivat poikkeavan tilanteen. Tämä tilanne ei ollut havaittavissa kuvasta 5.4, missä itseasiassa kaikkien luokkien osalta tilanne oli edellistä vuotta parempi. Poikkeava tapaus johtui dieselgeneraattoreiden yhteisviasta, joka oli pysynyt piilevänä jonkin aikaa ja havaittiin vasta koestuksessa. Dieselgeneraattorit ovat turvallisuuden kannalta tärkeitä laitteita ja niiden viat aiheuttavat huomattavan osan merkittävimmistä tapahtumista. Tämä on todettu niin vikaraporttien perusteella kuin myös tehdyssä simulaatiossa, jossa ne aiheuttivat 79 % merkittävimmistä tapahtumista.

5.3.3 Vyöhykesääntöjen soveltaminen poikkeamien havaitsemiseen

Edellisessä kappaleessa esiteltyjen fraktiilien avulla voidaan arvioida havainnon todennäköisyyttä eli ottaa kantaa siihen, onko kulunut vuosi ollut riskimerkitykseltään satunnaisuudesta poikkeava. Prosessiteollisuudessa vastaavaa menetelmää käytetään tilastollisessa laadunvalvonnassa, jossa prosessin lopputuoteen ominaisuuksia seurataan ja mitataan. Tyypillisesti seurattava ominaisuus oletetaan normaalijakautuneeksi, jonka parametrit estimoidaan tuotteiden avulla sisäänajovaiheen (burn-in) jälkeen. Tämän jälkeen määritetään sallitut vyöhykkeet eli rajat, joiden avulla voidaan päätellä, onko tuotantoprosessi kontrollissa eli aiheutuuko tuotteen laatua kuvaavan ominaisuuden vaihtelu vain satunnaisuudesta. Esimerkiksi Western Electric Handbookin vyöhykesääntöjen mukaan tarkkailtava prosessi ei ole kontrollissa, jos yksikin seuraavista säännöistä pätee:

- Yksi piste on kolmen sigman rajojen ulkopuolella
- Kaksi peräkkäistä kolmesta pisteestä on kahden sigman rajojen ulkopuolella
- Neljä peräkkäistä viidestä pisteestä on yhden sigman rajojen ulkopuolella
- Kahdeksan peräkkäistä pistettä on samalla puolella keskiviivaa

Normaalijakaumaoletusta käyttäen, kolmen sigman rajojen ulkopuolella on noin 0.27 %, kahden sigman rajojen ulkopuolella noin 4.55 % ja yhden sigman rajojen ulkopuolella noin 31.73 % tapauksista.

Esitettyjä vyöhykesääntöjä soveltamalla voitaisiin muodostaa myös kuvien 5.4 ja 5.5 seurantaprosesseille säännöt, joiden mukaan laitostapahtumia ja niiden riskiä seurattaisiin. Sääntöjen soveltamisessa on tietysti otettava huomioon ydinvoimateollisuudessa voimakkaasti vaikuttava konservatiivinen turvallisuusajattelu. Lisäksi kiinnostuksen kohteena on etenkin riskirajan ylitys, eikä niinkään poikkeama jostain tavoitearvosta. Vyöhykesääntöjen täsmällistä määrittelyä ennen simulaatiomallin parametreja tulisi kuitenkin tarkentaa, jotta malli noudattaisi paremmin todellisuutta.

Luku 6

Yhteenveto ja johtopäätökset

Ydinturvallisuuden varmistamisessa käytetään sekä deterministisiä periaatteita että riskitietoista turvallisuusajattelua. Nykyään riskitietoista ajattelua hyödynnetään yhä enemmän laitosten suunnittelussa ja käytön aikaisessa valvonnassa. Tärkeimpien riskitekijöiden tunnistamisessa ja harvinaisten tapahtumien todennäköisyyksien arvioinnissa käytetään todennäköisyyspohjaista riskien arviointia, PRA:ta, jonka käyttö ydinvoimaloiden turvallisuuden arvioinnissa on Suomessa lainsäädännöllinen edellytys.

Työssä esiteltiin aluksi todennäköisyyspohjaista riskianalyysia ydinvoimasovelluksiin painottuen, määriteltiin riskimitta ja käsiteltiin varsin kattavasti PRA:n laskentamenetelmiä, koska näiden käsitteiden riittävä hallinta on edellytys PRA:n erilaisten käyttösovellusten ymmärtämiselle. Eräs tällainen sovellus on todennäköisyyspohjainen riskien seuranta, jonka erityispiirteisiin tässä työssä keskityttiin.

Todennäköisyyspohjaisella riskien seurannalla lasketaan PRA-perustaisesti jo sattuneille laitostapahtumille kvantitatiivinen riskimitta ja näin arvioidaan ”läheltä piti” -tilanteen vakavuus. Tämä jälkikäteislaskenta sisältää ehdolliseen todennäköisyyteen liittyvän teoreettisen ongelman: Jos tapahtuman kulku jo tunnetaan täysin, voiko sen lopputulokseen enää liittyä epävarmuutta? Onko siis onnettomuuden todennäköisyyttä mahdollista laskea tapahtumalle, jonka tiedetään olleen vain ”läheltä piti” -tapaus? Työssä käsiteltiin tätä ongelmaa ja sen teoreettisia perusteita sekä esiteltiin keino alkutapahtumien ja vikatilanteiden kvantifioinnille.

Säteilyturvakeskuksen tekemä todennäköisyyspohjainen riskien seuranta on ollut pääasiassa käyttötapahtumien riskimerkityksen arviointia PRA-perustaisesti ja tulokset ovat tiivistyneet kolmeen riskikategoriaan luokieltujen käyttötapahtumien lukumäärien tilastointiin. Tästä syystä vikojen tarkempi seuranta, esimerkiksi laitteiden vanhenemisesta johtuva vikataajuuksien mahdollinen kasvu, sekä vanhojen tapahtumien syy-seuraus -suhteiden tarkastelu on hyvin hankalaa ja työlästä. Lisäksi riskien seurannan tulosten avulla on ollut vaikea päätellä, onko vaihtelussa kyse vain vikaantumisprosessin satunnaisvaihtelusta vai mahdollisesti voimayhtiön löystyneestä turvallisuuskulttuurista. Nämä syyt heikentävät oleellisesti Säteilyturvakeskuksen nykymuotoisen riskien seurannan arvoa päätöksentekoa ja turvallisuusvalvontaa ajatellen.

Työssä esiteltiin keino simuloida uusiutumisprosessin avulla ydinvoimalaitoksessa sattuvia käyttötapahtumia ja yhdessä PRA-mallin rakennefunktion avulla näille tapahtumille voidaan määrittää niiden riskimerkitys eli ehdollisen sydänvauriotodennäköisyyden kasvun suuruus. Toistamalla simulaatiota kullekin riskikategorialle saadaan aikaiseksi jakauma, jonka avulla voidaan arvioida vuoden aikaisten käyttötapahtumien poikkeuksellisuutta. Näin todennäkösyyspohjaisen riskien seurannan käyttö turvallisuusvalvonnan ja päätöksenteon apuvälineenä saa lisää arvoa. Menetelmän sovellettavuutta rajoittaa tosin tällä hetkellä parametrien epätarkkuus ja konservatiivisuus. Tätä ongelmaa voidaan vähentää johdonmukaisemmalla vikatapahtumien seurannalla ja tilastoinnilla, jolloin tiedon lisääntyessä parametreja olisi mahdollista tarkentaa. Parametreihin liittyvä epävarmuus voitaisiin myös sisällyttää simulaatioon käyttämällä kiinteiden arvojen sijasta jakaumista poimittuja satunnaislukuja. Lisäksi tarkkuuden parantamiseksi simulaatiossa tulisi käyttää nykyisen 2000 kierroksen sijasta useampia simulaatiokierroksia, jotta voitaisiin tutkia harvinaisten tapahtumien vaikutusta.

Vaikka työssä esitetystä teoriasta ja tuloksista voi saada erilaisen kuvan, on todettava, että todennäköisyyspohjaisen riskien seurannan päätarkoitus ei ole tuottaa yksittäiselle tapahtumalle kvantitatiivista riskimittaa. Tärkeämpää on tapahtumien systemaattinen seuranta ja huolellinen analysointi, jolloin voidaan havaita onnettomuutta ennakoivia merkkejä ja ottaa opiksi vakavimmista tapahtumaketjuista esimerkiksi kehittämällä ohjeistuksia tai muuttamalla laitoksen turvallisuusjärjestelmiä. Näin voidaan edelleen parantaa ydinvoiman käytön turvallisuutta.

Lähdeluettelo

[1] Power Reactor Information System (PRIS). International Atomic Energy Agency. Viitattu 18.12.2009, URL: http://www.iaea.org/programmes/a2/.

[2] Säteilyturvakeskus. *Säteily- ja ydinturvallisuuskatsauksia: Ydinvoimalaitosten turvallisuus*, 2008.

[3] J. Sandberg (toim.). *Ydinturvallisuus.* Säteilyturvakeskus, 2004. Kirjasarjan *Säteily- ja ydinturvallisuus* viides osa.

[4] Säteilyturvakeskus. *YVL-ohje 2.2: Ydinvoimalaitosten teknisten ratkaisujen perusteleminseksi tehtävät häiriö- ja onnettomuusanalyysit*, 2004.

[5] International Nuclear Safety Advisory Group. *Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1: INSAG-12*, 1999.

[6] E. Kainulainen (toim.). *Ydinenergian käytön turvallisuusvalvonta: vuosiraportti 2007.* Säteilyturvakeskus, 2008.

[7] International Nuclear Safety Advisory Group. *Defence in Depth in Nuclear Safety : INSAG-10*, 1996.

[8] Säteilyturvakeskus. *YVL-ohje 1.0: Ydinvoimalaitoksen suunnittelussa noudatettavat turvallisuusperiaatteet*, 1996.

[9] N. Rasmussen et al. *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants.* U.S. NRC, 1975.

[10] M. Modarres. *Risk Analysis in Engineering: Techniques, Tools, and Trends.* Taylor & Francis, New York, 2006.

[11] L. Lederman, F. Niehaus ja B. Tomic. Probabilistic safety assessment past, present and future: An IAEA perspective. *Nuclear Engineering and Design*, 160(3):273–285, 1996.

[12] M. Hayns. The evolution of probabilistic risk assessment in the nuclear industry. *Process Safety and Environmental Protection*, 77(3):117–142, 1999.

[13] T. Bedford ja R. Cooke. *Probabilistic Risk Assessment: Foundations and Methods*. Cambridge University Press, Cambridge, 2003.

[14] M. Modarres. Advanced nuclear power plant regulation using risk-informed and performance-based methods. *Reliability Engineering and System Safety*, 94(2):211–217, 2009.

[15] P. Hakkinen. Seveso Disaster, and the Seveso and Seveso II Directives. Teoksessa *Encyclopedia of Toxicology, 2nd edition*. Elsevier Inc., 2005.

[16] E. Broughton. The Bhopal disaster and its aftermath: a review. *Environmental Health: A Global Access Science Source*, 4:6, 2005.

[17] A. Julin. Todennäköisyyspohjaisen turvallisuusanalyysin käyttö viranomaistyön tukena. 1995. Diplomityö, Lappeenrannan teknillinen korkeakoulu.

[18] Säteilyturvakeskus. *YVL-ohje 2.8: Todennäköisyyspohjaiset turvallisuusanalyysit (PSA) ydinvoimalaitosten turvallisuuden hallinnassa*, 2003.

[19] M. Röwekamp, J. Lanore ja P. De Gelder. Probabilistic Safety Assessments: Going beyond desing limits. Teoksessa *Eurosafe Tribune #012: Probabilistic Safety Assessment*. EUROSAFE initiative, GRS & IRSN, 2008.

[20] J. Vaurio. Luotettavuustekniikka, 2006. Luentomoniste, Lappeenrannan teknillinen yliopisto, Energia- ja ympäristötekniikan osasto.

[21] T. Kivirinta. Ydinvoimalaitoksen sallittujen korjausaikojen riskitietoinen tasapainottaminen. 2005. Diplomityö, Teknillinen korkeakoulu.

[22] *T-boken – Tillförlitlighetsdata för komponenter i nordiska kraftreaktorer*. TUD-kansliet, 2005.

[23] P. O'Connor. *Practical Reliability Engineering*. John Wiley & Sons, Chichester, 2002.

[24] A. Hoyland ja M. Rausland. *System Reliability Theory – Models and Statistical Methods*. John Wiley & Sons, New York, 1994.

[25] R. Durret. *Essentials of Stochastic Processes*. Springer-Verlag, New York, 2001.

[26] V. Hoepfer, J. Saleh ja K. Marais. On the value of redundancy subject to common-cause failures: Toward the resolution of an on-going debate. *Reliability Engineering and System Safety*, 94:1904–1916, 2009.

[27] J. Kupila. Inhimillisen luotettavuuden arviointi osana todennäköisyyspohjaista turvallisuusanalyysia. 2002. Diplomityö, Teknillinen korkeakoulu.

[28] Nuclear Energy Agency. *CSNI Technical Opinion Papers No. 6: PSA-based Event Analysis*, 2004.

[29] J. Holmberg, K. Björkman ja P. Hellström. *Methods for risk follow-up and handling CCF events in PSA applications*. Valtion teknillinen tutkimuskeskus, 2009. Tutkimusraportti, VTT-R-11463-08.

[30] J. Holmberg. Risk follow-up by probabilistic safety assessment—experience from a Finnish pilot study. *Reliability Engineering and System Safety*, (53):3–15, 1996.

[31] E. Arjas ja J. Holmberg. Marked point process framework for living probabilistic safety assessment and risk follow-up. *Reliability Engineering and System Safety*, (49):59–73, 1995.

[32] J. Johnson ja D. Rasmuson. The US NRC's accident sequence precursor program: an overview and development of a Bayesian approach to estimate core damage frequency using precursor information. *Reliability Engineering and System Safety*, (53):205–216, 1996.

[33] M. Hulsmans ja P. De Gelder. Probabilistic analysis of accident precursors in the nuclear industry. *Journal of Hazardous Materials*, (111):81–87, 2004.

[34] Proceedings of the 12th technical meeting on experiences with risk-based precursor analysis. Electrabel, 2009. Konferenssimateriaali.