TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

PIA HUMALAJOKI

YDINVOIMALAITOKSEN VIKA-ANALYYSIT

Diplomityö

Tarkastaja: lehtori Risto Mikkonen
Tarkastaja ja aihe hyväksytty
Tieto- ja sähkötekniikan tiedekunta-neuvoston kokouksessa 9. syyskuuta 2015

TIIVISTELMÄ

PIA HUMALAJOKI: Ydinvoimalaitoksen vika-analyysit
Tampereen teknillinen yliopisto
Diplomityö, 82 sivua
Maaliskuu 2016
Sähkötekniikan koulutusohjelma
Pääaine: Vaihtoehtoiset sähköenergiateknologiat
Tarkastaja: lehtori Risto Mikkonen

Avainsanat: ydinvoimalaitos, vika-analyysi, vikasietoisuus, syvyyssuuntainen puolustusperiaate, turvallisuustoiminto

Ydinenergian käytön turvallisuuden varmistaminen tapahtuu syvyyssuuntaisen puolustusperiaatteen mukaisesti toisiaan varmentavilla toiminnallisilla puolustustasoilla. Puolustustasot koostuvat turvallisuustoiminnoista, joiden toteutuminen on varmistettava normaalien käyttötilanteiden lisäksi erilaisissa häiriö- ja onnettomuustilanteissa. Kokonaisvaltaisen turvallisuuden suunnittelussa ja vaatimusten toteutumisen osoittamisessa hyödynnetään erilaisia analyysejä.

Tässä diplomityössä muodostetaan ydinvoimalaitokselle tehtävistä yksittäisistä vika-analyyseistä kokonaisuus ja tarkastellaan yksittäisten analyysien rooleja, kattavuutta, toteutustapaa ja tavoitteita osana tätä kokonaisuutta. Työn esimerkkikokonaisuus koostuu vikaantumisten syitä ja seurauksia selvittävistä analyyseistä, joilla voidaan vastata Säteilyturvakeskuksen YVL-ohjeiden vikasietoisuusvaatimuksiin.

Analyysikokonaisuus perustuu pääosin Olkiluoto 3 -laitoksella käytettyihin analyysimenetelmiin. Analyysit on ryhmitelty sen mukaan, tarkastellaanko niillä yksittäistä laitetta, turvallisuusjärjestelmää, -toimintoa vai arkkitehtuuritason turvallisuutta sekä osoitetaanko niillä toiminnon moninkertaisuus-, erilaisuus- vai erotteluperiaatteen toteutumista. Kokonaisuudessa on huomioitu useiden tekniikanalojen, erityisesti prosessi- ja automaatiotekniikan, analyysejä ja niiden vaikutuksia toisiinsa.

Työssä esitettävä analyysikokonaisuus muodostuu vika- ja vaikutusanalyyseistä, aiheettomien toimintojen analyyseistä, yhteisvika-analyyseistä, vikakriteerien analyyseistä sekä alkutapahtumien ja niistä aiheutuvien riippuvuuksien tunnistamiseen tähtäävistä analyyseistä. Yksittäiset analyysitulokset toimivat toisten vika-analyysien lähtötietoina muodostaen yhden laajan kokonaisuuden. Vika-analyysikokonaisuutta hyödynnetään pohjatietona deterministisen turvallisuusanalyysien ja todennäköisyysperusteisen riskianalyysin laadinnassa. Työssä muodostettua analyysikokonaisuutta voidaan hyödyntää osana yksittäisten analyysien tavoitteiden täyttymisen arviointia.

ABSTRACT

PIA HUMALAJOKI: Failure Analyses of Nuclear Power Plant
Tampere University of Technology
Master of Science Thesis, 82 pages
March 2016
Master's Degree Programme in Electrical Engineering
Major: Alternative Electric Energy Technologies
Examiner: lecturer Risto Mikkonen

Keywords: Nuclear Power Plant, failure analysis, failure tolerance, Defence in Depth, safety function

Defence in Depth -concept is used for ensuring the safety of Nuclear Power Plants. Defence in Depth -levels include a variety of safety functions, which must work despite different failures. This must be demonstrated with different analyses.

This Master's Thesis gathers together different failure analyses of Nuclear Power Plant and explains the roles, coverages, methods and purpose of each analysis. These analyses fulfill the YVL guides requirements of Finnish nuclear authority STUK.

Used examples consists mostly of Olkiluoto 3 project's analyses. Analyses are grouped based on their focus: redundancy, diversity or separation of one safety system, safety function or architectural safety. The examples are about process or I&C techniques.

Created collection of analyses contains failure mode and effect analysis, spurious action analysis, common cause failure analysis, failure criterion analysis and initiating event's analysis. Often the results of one analysis are inputs to the other so they have to be handled together. Results of failure analyses are also needed as inputs to deterministic safety analyses and probabilistic risk assessment.

ALKUSANAT

Tämä diplomityö tehtiin Säteilyturvakeskuksen Ydinvoimalaitosten valvonta -osaston Riskianalyysit-toimistolle. Työn ohjaajana toimi Säteilyturvakeskukselta johtava asiantuntija Ilkka Niemelä ja tarkastajana lehtori Risto Mikkonen Tampereen teknillisen yliopiston Sähkötekniikan laitokselta.

Ennen kaikkea haluan kiittää työni ohjaajaa Ilkkaa asiantuntevista neuvoista ja johdatuksesta mielenkiintoiseen ja laajaan aiheeseen. Erityiskiitokset kuuluvat myös Nina Lahtiselle ja Petteri Suikkaselle uusien näkökulmien avaamisesta. Kiitos myös muille, etenkin STUKin Riskianalyysit ja Sähkö- ja automaatiojärjestelmät -toimistojen työntekijöille, jotka ovat työssäni auttaneet sekä ulkopuolisille tahoille, joiden materiaalia ja asiantuntemusta olen saanut työssäni hyödyntää.

Erityisesti kiitän myös perhettäni, joka on aina kannustanut ja tukenut minua – sekä opinnoissa että muussa elämässäni. Kiitos myös ystävilleni, joita ilman opiskeluvuoteni Tampereella ja diplomityöurakka Helsingissä eivät olisi olleet yhtä ikimuistettavia kuin ne nyt olivat. Antoisista opiskelijavuosista kiitän myös minulle erittäin tärkeiksi muodostuneita Sähkökiltaa, ylioppilaskuntaa ja yliopistoa. Suurimmat kiitokset kuuluvat kuitenkin Akselille, joka on jaksanut kannustaa ja rohkaista minua jatkuvasti, pitää huolta niin hyvinä kuin huonompinakin hetkinä.

Helsingissä, 18.2.2016

Pia Humalajoki

SISÄLLYSLUETTELO

1. JOHDANTO 1
2. JÄRJESTELMÄN VIKASIETOISUUS 3
2.1 Vikaantumisen lähtökohdat 5
3. YDINVOIMALAITOKSEN TURVALLISUUSPERIAATTEET 7
3.1 Painevesilaitoksen turvallisuustoiminnot 8
3.2 Syvyyssuuntainen puolustusperiaate 10
3.2.1 Tapahtumien suunnitteluperusteluokitus 13
3.3 Ydinvoimalaitoksen suunnitteluperiaatteita 14
3.3.1 Järjestelmien turvallisuusluokitus 16
3.3.2 Vikasietoisuus ja vikakriteerit 17
3.3.3 Toimintojen priorisointi 18
3.4 Viranomaisvaatimukset ja -ohjeet 19
4. VIKA-ANALYYSIEN ROOLI TURVALLISUUSTOIMINTOJEN ANALYSOINNISSA 21
4.1 Vika-analyysit 22
4.1.1 Vika-analyysit osana suunnitteluprosessia 23
4.1.2 Vika-analyysien työllistävyys ja laajuus 25
4.2 Deterministiset turvallisuusanalyysit 26
4.2.1 PRA:n onnistumiskriteerit 27
4.3 Todennäköisyysperusteinen riskianalyysi 28
4.3.1 Tapahtuma- ja vikapuut 29
5. VIKA-ANALYYSIMENETELMIÄ 32
5.1 Vika- ja vaikutusanalyysi 32
5.2 Aiheettomien toimintojen analyysi 34
5.2.1 Poikkeamatarkastelu 36
5.3 Vikakriteerien analyysi (N+1, N+2 -analyysi) 36
5.4 Yhteisvika-analyysi 38
5.5 Alkutapahtuma-analyysit 39
5.5.1 Sisäisten uhkien analyysit 40
5.5.2 Ulkoisten uhkien analyysit 41
6. TURVALLISUUSTOIMINNON VIKAANTUMISEN TARKASTELU 43
6.1 Yksittäisen järjestelmän vikaantuminen 45
6.1.1 Järjestelmien rajapinnat ja vuorovaikutukset 45
6.1.2 Yksittäisen laitteen tai järjestelmän vikaantumismahdollisuudet 48
6.2 Turvallisuustoimintojen moninkertaisuus 53
6.2.1 Toimintoketjun vikakriteerit ja vikasietoisuus 53
6.3 Turvallisuustoimintojen erilaisuus 55
6.3.1 Yhteisvian mahdollisuus 56
6.3.2 Erilaisuusperiaate tukitoiminnoissa 58

7. ARKKITEHTUURITASON VIKAANTUMISEN TARKASTELU 61
7.1 Yksittäisen puolustustason vahvuus 63
7.1.1 Fyysinen erottelu 63
7.1.2 Informaatiovirtojen erottelu 66
7.1.3 Sähkönsyötön saatavuus 67
7.1.4 Rakenteellinen kestävyys 68
7.2 Puolustustasojen välinen erottelu 69
7.2.1 Puolustustasojen riippumattomuus 70
7.2.2 Vakavien onnettomuuksien hallinnan erillisyys 71
7.2.3 Puolustustasojen säilyminen tukijärjestelmissä 72
8. YHTEENVETO JA JOHTOPÄÄTÖKSET 76
LÄHTEET 79

LYHENTEET JA MERKINNÄT

CCF	Yhteisvika (Common Cause Failure)
CCI	Yhteisvika-alkutapahtuma (Common Cause Initiator)
DBC	Suunnitteluperusteluokka (Design Basis Conditions)
DEC	Suunnitteluperusteen laajennus -luokka (Design Extension Category)
DID	Syvyyssuuntainen puolustusperiaate (Defence In Depth)
EYT	Ei ydinteknisesti turvallisuusluokiteltu
FMEA	Vika- ja vaikutusanalyysi, VVA (Failure Mode and Effect Analyses)
HAZOP	Poikkeamatarkastelu (Hazard and operability study)
HBS	Langoitettu turvallisuusautomaatiojärjestelmä OL3-suunnittelussa (Hardwired Backup System)
IAEA	Kansainvälinen atomienergiajärjestö (International Atomic Energy Agency)
IE	Alkutapahtuma (Initiating Event)
I&C	Automaatio (Instrumentation and Control)
LOCA	Jäähdytteenmenetysonnettomuus (Loss of Coolant Accident)
LOOP	Ulkoisen sähköverkon menetys (Loss Of Offsite Power)
OL	Olkiluoto
PAC	Toimilaitteiden prioriteettien hallinta- ja ohjausjärjestelmä OL3-suunnittelussa (Priority Actuator and Control System)
PAS	Prosessiautomaatiojärjestelmä OL3 suunnittelussa (Process Automation System)
PICS	Ohjelmistopohjainen, visuaalinen pääkäyttöliittymäjärjestelmä OL3-suunnittelussa (Process Information and Control System)
PRA/PSA	Todennäköisyysperusteinen riskianalyysi (Probabilistic Risk Assessment, Probabilistic Safety Assessment)
PS	Reaktorin suojausjärjestelmä OL3-suunnittelussa (Protection System)
RCSL	Ehkäisevä reaktorin säätö-, valvonta- ja rajoitusjärjestelmä OL3-suunnittelussa (Reactor Control, Surveillance and Limitation System)

SA	Vakava onnettomuus (Severe Accident)
SA I&C	Vakavien onnettomuuksien hallintajärjestelmä OL3-suunnittelussa (Severe Accident Instrumentation and Control)
SAHARA	Periaate, jonka mukaan turvallisuus on pidettävä niin korkealla tasolla kuin käytännöllisin toimenpitein on mahdollista (Safety as High as Reasonably Achievable)
SAS	Turvallisuusautomaatiojärjestelmä OL3-suunnittelussa (Safety Automation System)
SBO	Oletettu onnettomuustilanne, jossa ulkoinen sähkönsyöttö ja hätädieselgeneraattorit eivät tuota turvallisuusjärjestelmien tarvitsemaa käyttösähköä (Station Black Out)
SC	Turvallisuusluokka (Safety Class)
SICS	Turvallisuuskäyttöliittymä OL3-suunnittelussa (Safety Information and Control System)
STUK	Säteilyturvakeskus
TGI	Turbiinigeneraattorin automaatiojärjestelmä OL3-suunnittelussa (Turbine Generaton I&C)
TTKE	Turvallisuustekniset käyttöehdot
TXP	Teleperm XP automaatiotuoteperhe
TXS	Teleperm XS automaatiotuoteperhe
VTT	Teknologian tutkimuskeskus VTT Oy
VVA	Vika- ja vaikutusanalyysi (Failure Mode and Effect Analyses, FMEA)
WENRA	Länsi-Euroopan ydinturvallisuusviranomaisten järjestö (Western European Nuclear Regulators Association)
YVL-ohjeet	Säteilyturvakeskuksen julkaisemat yksityiskohtaiset ydinvoimalaitoksen turvallisuusvaatimukset

a	vuosi
f	taajuus
Cs-137	Cesium-137
TBq	terabecquerel

1. JOHDANTO

Ydinenergian tuotantoon liittyy turvallisuusriski, joka aiheutuu käytettävän polttoaineen sisältämistä radioaktiivisista aineista, jotka voivat olla vahingollisia ihmiselle, ympäristölle tai omaisuudelle. Tämän vuoksi ydinenergian käyttö on luvanvaraista ja tarkoin valvottua. (Ydinenergialaki 990/1987, 8 §). Suomessa ydinvoimalaitosten turvallisuusvalvonnasta vastaa Säteilyturvakeskus *(STUK)* tavoitteenaan varmistaa voimayhtiöiden vaatimustenmukainen toiminta. STUKin valvonnan piiriin kuuluvat Suomen käytössä olevat neljä ydinvoimalaitosyksikköä – kaksi Loviisassa ja kaksi Olkiluodossa, rakenteilla oleva Olkiluodon kolmas yksikkö, suunnitteilla oleva laitosyksikkö Pyhäjoen Hanhikivelle sekä Espoon VTT:n tutkimusreaktorin käytöstä poisto. Lisäksi valvonnan piiriin kuuluvat ydinmateriaalien ja -jätteiden käsittely, varastointi ja loppusijoitus.

Huolellisen suunnittelun lisäksi ydinenergian käytön turvallisuuden varmistamiseksi on varauduttava onnettomuuksiin. STUKin määräyksen (Y/1/2016, 3 §) mukaan ydinvoimalaitoksen turvallisuuden ja sen turvallisuusjärjestelmien teknisten ratkaisujen arviointiin ja perusteluun on käytettävä analyyttisiä ja kokeellisia menetelmiä, kuten deterministisiä turvallisuusanalyysejä, vika-analyysejä ja todennäköisyysperusteista riskianalyysiä. Yksityiskohtaiset turvallisuusvaatimukset esitetään STUKin julkaisemissa ohjeissa *(YVL)*.

Turvallisuuden arvioimiseksi ydinvoimalaitoksilla tehdään useita erilaisia vika-analyysejä. Yksittäinen analyysi tarkastelee tiettyä osaa ydinvoimalaitoksesta ja sen vikaantumismahdollisuuksista omasta näkökulmastaan. Näkökulmia ovat esimerkiksi automaatiojärjestelmät ja automaatioarkkitehtuuri, prosessijärjestelmät sekä laitoksen fyysinen arkkitehtuuri. Tarkastelu voi kohdentua toimintoihin, yksittäisiin laitteisiin tai laajempaan kokonaisuuteen. Olkiluoto 3 -laitos on Suomen ensimmäinen ydinvoimalaitos, jonka toiminta perustuu ensisijaisesti digitaaliseen ohjaukseen, mikä on asettanut haasteita erityisesti automaatiojärjestelmien vikaantumismahdollisuuksien ja vikaantumisen seurausten analysoinnille.

Diplomityön tavoitteena on luoda kokonaiskuva näistä eri näkökulmista. Tavoitteena on esittää analyysikokonaisuus, joka huomioi eri tekniikanalojen analyysit sekä hahmottaa kunkin analyysin peittävyys, jotta YVL-ohjeissa esitetyt vikasietoisuusvaatimukset tulisivat kattavasti analysoiduiksi. Tavoiteltavan analyysikokonaisuuden myötä hahmotetaan yksittäisten analyysien rooli ja tavoite. Esitettävä analyysikokonaisuus toimii esimerkkinä siitä, millaisilla analyyseillä vaatimuksiin voidaan vastata. Analyysimenetelmien valinta ja käyttö on luvanhaltijan vastuulla ja riippuu esimerkiksi tarkasteltavan

laitoksen tyypistä, joten tämän työn analyysikokonaisuutta ei suoraan voi soveltaa muihin kohteisiin.

Aluksi työn luvussa 2 määritellään ydinvoimalaitoksen luotettavuuteen liittyvät termit sekä erilaiset järjestelmien ja toimintojen vikaantumistavat. Jo itsessään *järjestelmä*-käsite voidaan määritellä usealla eri tavalla näkökulmasta riippuen, minkä vuoksi määritelmien selkiyttäminen on tarpeellista. Luvussa 3 esitellään ydinvoimalaitoksen vikaantumiseen liittyviä turvallisuusperiaatteita ja Suomessa onnettomuuksien varalle suunniteltuja järjestelmiä ja niitä koskevia luokituksia ja vaatimuksia.

Luvussa 4 selvennetään ja verrataan tässä työssä tarkasteltavien vika-analyysien roolia ja tavoitetta muihin ydinvoimalaitoksen turvallisuustoiminnoille tehtäviin analyyseihin – deterministisiin onnettomuusketjuja kuvaaviin analyyseihin sekä tapahtumien todennäköisyyttä ja seurauksia mallintavaan todennäköisyysperusteiseen riskianalyysiin. Luvussa 5 esitellään tarkemmin vika-analyysimenetelmiä, jotka myöhemmin liitetään YVL-ohjeiden vaatimuksiin. Analyysimenetelmistä osa on hyvin perinteisiä ja laajasti käytettyjä ja osa on täysin ydinvoimalaitoksiin keskittyviä analyysejä, joita ei muilla aloilla sovelleta.

Luvuissa 6 ja 7 kootaan esimerkkikokonaisuus analyysimenetelmistä, joiden avulla YVL-ohjeiden vika-analyysivaatimuksiin pyritään vastaamaan. Luvut koostuvat aihealueittain jaotelluista YVL-ohjeiden vika-analyysivaatimuksista edeten yksittäisestä järjestelmästä yhden turvallisuustoiminnon toteutuksen kautta koko laitosarkkitehtuurin kattavaan tarkasteluun. Jokaisen aihealueen analyysejä koskevat vaatimukset on koottu lukujen alkuun, jonka jälkeen esitetään esimerkkimenetelmät, kuinka vaatimukset voidaan osoittaa täytetyiksi.

Työn esimerkit viittaavat enimmäkseen Olkiluoto 3 -laitokselle tehtyihin analyyseihin ja painottuvat automaatioon kohdistuviin analyyseihin. Analyysit ovat osa laitosdokumentaatiota, eivätkä siten julkisesti saatavilla. Dokumentaation lisäksi työssä on hyödynnetty henkilökohtaisia tiedonvaihtoja asiantuntijoiden kanssa sekä STUKin sisäisiä materiaaleja. Tämän vuoksi työn analyysikuvaukset ovat yksinkertaistuksia ja esimerkeistä on poistettu yksityiskohtaiset laitoksia koskevat tiedot. Työssä esitetyt analyysit ovat vain yksittäisiä esimerkkejä analyysien toteutustavoista ja vaihtoehtoja näille on useita.

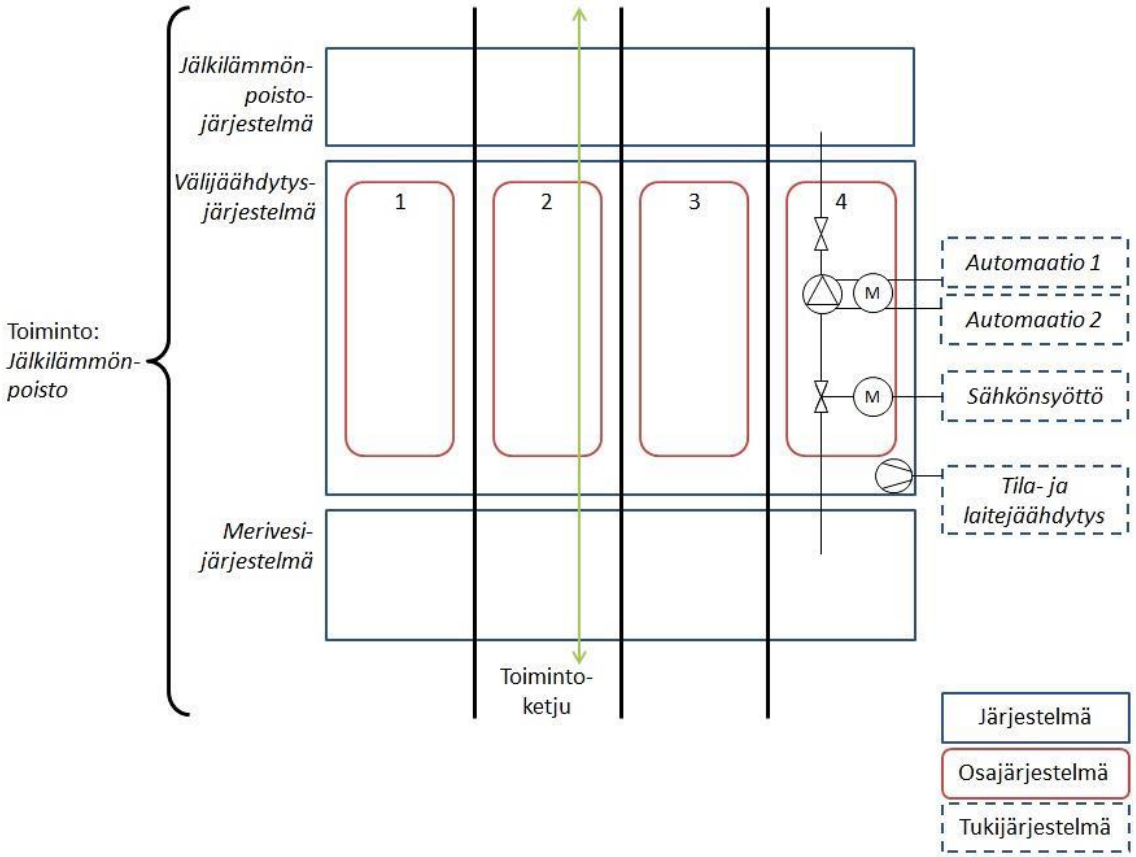
2. JÄRJESTELMÄN VIKASIETOISUUS

Vikasietoisuuteen *(Failure tolerance, Fault tolerance)* liittyvä käsitteistö ei ole ydinvoima-alalla täysin vakiintunutta, mutta yleisesti sillä tarkoitetaan järjestelmän kykyä jatkaa toimintaansa, vaikka siinä olisi vikoja. Vikasietoisuutta voidaan verrata järjestelmän luotettavuuteen ja käyttövarmuuteen, joilla tarkoitetaan teknisen järjestelmän kykyä toimia häiriöittä ja ilman käyttökeskeytyksiä. Käyttövarmuuteen vaikuttavat järjestelmän eri rakenneosien käyttövarmuus, merkitys järjestelmän toiminnalle ja miten osat on liitetty toisiinsa, sekä kuinka nopeasti ja miten hyvin niiden viat pystytään korjaamaan. Laitteen vikaantuminen saattaa aiheuttaa vaaratilanteita ja onnettomuuksia, joiden aiheuttama riski riippuu laitteen käyttövarmuudesta ja toimintaympäristöstä. Käyttövarmuuden turvallisuusmerkitys korostuu onnettomuuksia estävissä ja niiden seurauksia rajoittavissa valvonta-, suojaus- ja turvajärjestelmissä. (Ervamaa 1979, 11–13).

Kuva 2.1 selventää työn kannalta oleellisen yksittäisen toiminnon toteuttamiseen liittyvän terminologian. Toiminnolla tarkoitetaan yhden halutun tehtävän, esimerkiksi ydinreaktorin jälkilämmönpoiston, toteuttamista. Toiminto toteutetaan yhdellä tai usealla järjestelmällä, esimerkissä jälkilämmönpoistoon osallistuvat jälkilämmönpoistojärjestelmä, välijäähdytysjärjestelmä ja merivesijärjestelmä. Yksi järjestelmä voi myös osallistua useaan eri toimintoon. Esimerkiksi Olkiluoto 1 ja 2 -laitoksilla suojarakennuksen lauhdutusjärjestelmän tehtävänä on normaalikäytössä ottaa vastaan päähöyryputkien ja ulospuhallusjärjestelmän vuotoja ja polttoaineenvaihdon aikana toimia väliaikaisena allasvesivarastona (TVO 2008).

Kuvan 2.1 järjestelmät on jaettu neljään rinnakkaiseen osajärjestelmään. Osajärjestelmistä tarvittava määrä osallistuu ensisijaisesti toiminnon toteutukseen ja loput toimivat varalla. Varajärjestelmänä voi toimia myös toinen järjestelmä. Yksittäinen osajärjestelmä sisältää erilaisia laitteita, jotka koostuvat komponenteista. Osajärjestelmät voivat olla keskenään identtisiä tai erilaisia. Yhtä osajärjestelmien kokonaisuutta, jolla toiminto voidaan toteuttaa, kutsutaan toimintoketjuksi.

Tukijärjestelmäksi kutsutaan järjestelmää, jota tarvitaan käynnistämään, ohjaamaan, jäähdyttämään tai käyttämään turvallisuustoimintoa suorittavaa järjestelmää tai muuten ylläpitämään sen toimintaedellytyksiä (YVL B.1, 43). Tukijärjestelmä voi liittyä osajärjestelmän toimintaan suoraan, kuten sähkönsyöttöjärjestelmä, tai järjestelmän sijainnin kautta, kuten huonetilan jäähdytysjärjestelmä. Tukijärjestelmät voidaan jakaa muiden järjestelmien tavoin osajärjestelmiin.



Kuva 2.1. *Työssä käytettävät toimintoon liittyvät termit.*

Kaikki viat eivät ole laitoksen toiminnan kannalta yhtä merkittäviä, vaan tiettyjen järjestelmien käyttökuntoisuus on laitoskokonaisuuden kannalta tärkeämpää kuin toisten. Toiminnon vikasietoisuus kuvaa sitä, kuinka monta ja miten sijoittuvia yksittäisiä siihen liittyviä vikoja voi olla samanaikaisesti, jotta vaadittu toiminto voidaan edelleen toteuttaa. Järjestelmä voi sisältää esimerkiksi neljä osajärjestelmää, joista yhden toimiminen riittää vaaditun toiminnon toteutukseen. Tällaisessa tilanteessa yhdessä, kahdessa tai kolmessa eri osajärjestelmässä esiintyvien vikojen määrällä ei ole merkitystä, mutta jos jokaisessa osajärjestelmässä on yksikin vika, estää se koko toiminnon toteutumisen. Laitoksen turvallisuuden kannalta on oleellista, että turvallisuustoimintojen toteuttamiseen vaaditut määrät toimintoketjuja toimivat tarkoitetulla tavalla.

Kaikkea vikaantumista ei voida hyvästä suunnittelusta, valmistuksesta ja käytönaikaisista toimenpiteistä huolimatta välttää, eivätkä kaikki vikaantumiset johda järjestelmän toimimattomuuteen tai muihin ei-toivottuihin seurauksiin, kuten laitoksen käyttökatkoon tai onnettomuuteen. Vikasietoisuusanalyysien tarkoituksena on selvittää, millainen vaikutus yksittäisellä vikaantumisella on haluttuun toimintoon ja onko vaikutus hyväksyttävissä. Vikaantuminen voidaan hyväksyä, jos se ei estä toiminnon toteuttamista tarvetilanteessa.

2.1 Vikaantumisen lähtökohdat

Laitteet voivat vikaantua toisistaan riippumatta tai vikojen välillä voi ilmetä riippuvuuksia. Riippuvuudet voivat aiheutua toista vioista tai laitteista. Yksittäisviaksi kutsutaan muista tekijöistä riippumatonta satunnaisvikaa, jonka seurauksena yksi laite, järjestelmä tai rakenne ei pysty toteuttamaan sille määrättyä tehtävää. Mikäli vian aiheuttaa laitteen ulkopuolinen tapahtuma tai toisen laitteen, järjestelmän tai rakenteen vika, kyse on seurausviasta. (YVL B.1, 42, 44). Seurausvika voi syntyä systemaattisesti tietyn tapahtuman yhteydessä, esimerkiksi samassa huoneessa olevan tulipalon seurauksena. Seurausvika voi olla myös satunnaista, jonka todennäköisyyttä tietyt laitteen ulkopuoliset tapahtumat lisäävät.

Jos kaksi tai useampi laitetta, järjestelmää tai rakennetta vikaantuu samasta tarkasteltavan laitteen sisäisestä syystä, puhutaan yhteisviasta (*Common Cause Failure, CCF*). Yhteisvialle ei ole käytössä yksiselitteisestä määritelmää, mutta tässä työssä yhteisvialla tarkoitetaan todennäköisyysperusteisessa riskianalyysissä *(Probabilistic Risk Assessment, PRA)* käytetyn määritelmän mukaisesti *”tilannetta, jossa seuraavat kolme asiaa toteutuvat:*

1. *Kaksi tai useampi yksittäistä järjestelmää, laitetta tai rakennetta on vikaantunut tai heikentynyt niin, että ne eivät täytä toimintavaadetta tarvetilanteessa.*
2. *Viat ovat ajallisesti päällekkäin niin, että onnistumiskriteerien täyttyminen satunnaisessa tarvetilanteessa on epävarmaa.*
3. *Viat aiheutuvat yhteisestä syystä tai mekanismista, mutta eivät ole seurausvikoja.”* (YVL A.7, 11).

Todennäköisyysperusteisen riskianalyysin ulkopuolella yhteisviaksi voidaan kutsua myös saman ulkoisen tapahtuman tai syyn aiheuttamia seurausvikoja.

Järjestelmien välinen yhteisvika voi syntyä kahden toimintoketjun yhteisten tai samankaltaisten järjestelmien välille. Yhteisillä järjestelmillä tarkoitetaan järjestelmiä, joita kaksi tai useampi rinnakkaista toimintoketjua käyttää samaan tarkoitukseen, ja näin ollen järjestelmän vikaantuminen vaikuttaa molempiin toimintoketjuihin. Yhteisvikamahdollisuus ilmenee myös tilanteessa, jossa kahdessa tai useammassa järjestelmässä käytetään saman tyypin komponentteja tai merkittävästi samankaltaisia osia sisältäviä laitteita samaan tarkoitukseen. Yhteisvika voi tällöin aiheutua esimerkiksi suunnittelu- tai asennusvirheestä tai komponentin materiaaliin liittyvästä kulumisesta.

Vikaantuminen voi ilmetä laitteen, järjestelmän tai rakenteen toiminnallisena tai rakenteellisena muutoksena tai puutteena, aktiivisena tai passiivisena vikaantumisena. Passiivinen vikaantuminen aiheuttaa laitteen kokonaisen tai osittaisen suorituskyvyn puutteen kun taas aktiivinen vikaantuminen ilmenee virhetoimintoina (YVL B.1 2013, 40–42). Perinteisesti vikaantumista on tarkasteltu passiivisen vikaantumisen näkökulmasta, jol-

loin laite ei toimi *(”Loss of”)* tarvetilanteessa. Digitalisoituminen on kasvattanut vaikutusten laajuutta vikaantumisissa, joissa tarkasteltava kokonaisuus toimii tarkoitukseensa nähden väärin tai aiheettomasti *(”Spurious actuation”)*. Passiivisen vian tavoin väärät tai aiheettomat toiminnot voivat aiheuttaa häiriö- tai onnettomuustilanteita tai estää turvallisuusjärjestelmän toiminnan.

Yhdellä laitteella voi olla useita vikaantumistapoja, kuten esimerkiksi venttiilillä vuoto, tarpeeton avautuminen tai sulkeutuminen ja avautumatta tai sulkeutumatta jääminen. Samaan vikaantumistapaan voivat johtaa erilaiset syyt, kuten venttiilin vuotoon komponentin löystyminen tai materiaalin haurastuminen. Venttiilin rakenteellinen vika ilmenee esimerkiksi vuotona putkilinjasta ulos. Jos vuoto taas tapahtuu putkilinjan sisällä kiinni olevan venttiilin läpi, kyse on toiminnallisesta viasta.

Vika voi paljastua heti syntyessään tai se voi olla piilevä vika. Piilevä vika paljastuu vasta laitteen käyttötilan muuttuessa tai sen testauksen aikana. (Ervamaa 1979, 21). Esimerkiksi normaalissa tehokäytössä kiinni oleva venttiili voi juuttua kiinni-asentoon, ja vika havaitaan vasta, kun venttiili pitäisi aukaista.

Alkutapahtumalla *(Initiating Event, IE)* tarkoitetaan yksilöityä tapahtumaa, joka johtaa odotettavissa oleviin käyttöhäiriöihin tai onnettomuustilanteisiin (YVL B.1, 40). Järjestelmän vikaantuminen voi aiheuttaa alkutapahtuman, se voi ilmetä toisen alkutapahtuman seurauksena tai satunnaisesti yhtä aikaa toisen alkutapahtuman kanssa. Vikaantumisen syntymekanismin ja vikaantumisen ilmentymän välillä ei aina ole yksiselitteistä riippuvuutta, mikä voi vaikeuttaa vikaantumisten analysointia. Esimerkiksi ohjelmistovirhe voi aiheuttaa väärän ohjauksen, mutta vian vaikutukset riippuvat ohjattavan järjestelmän järjestelmä- ja komponenttitason suunnittelusta.

3. YDINVOIMALAITOKSEN TURVALLISUUSPERIAATTEET

Ydinenergian käytön riskit aiheutuvat laitoksilla käytettävistä radioaktiivisista aineista. Ihmisten ja ympäristön suojelemiseksi ydinenergian käytön aiheuttamilta haitallisilta vaikutuksilta, tulee huomio kiinnittää säteilyaltistuksen ja radioaktiivisten päästöjen kontrollointiin, radioaktiiviseen päästöön johtavien tapahtumien todennäköisyyden rajoittamiseen sekä seurausten lieventämiseen radioaktiivisen päästön tapahtuessa (IAEA 2006, 4–5).

Kansainvälisesti käytetyn SAHARA-periaatteen *(Safety As High As Reasonably Achievable)* mukaan ydinenergian käytön turvallisuus on pidettävä niin korkealla tasolla, kuin käytännöllisin toimenpitein on mahdollista (IAEA 2006, 10; Ydinenergialaki 990/1987, 7 a §). Onnettomuuksien ja häiriöiden mahdollisuutta ei voida sulkea täysin pois, joten niiden estämiseen ja rajoittamiseen on varauduttava erilaisin turvallisuusjärjestelmin. Ydinvoimalaitoksen turvallisuus voidaan varmistaa pienentämällä onnettomuustilanteiden taajuutta tilanteen syntyyn liittyvien järjestelmien, rakenteiden ja laitteiden laadun parantamisella sekä lieventämällä onnettomuustilanteiden mahdollisia seurauksia luotettavilla turvallisuustoiminnoilla. (Sandberg 2013, 95–96; STUK 2015a, 2–3).

Turvallisuusajattelun lähtökohtana on, että käyttäjän virheet tai useatkaan laiteviat yksinään eivät voi aiheuttaa ydinvoimalaitokselle vakavaa onnettomuutta (TVO 2013, 51). Virheisiin ja vikoihin varaudutaan käyttämällä peräkkäisiä, toisiaan varmentavia järjestelmiä ja menettelytapoja, niin kutsuttua syvyyssuuntaista puolustusperiaatetta *(Defence In Depth, DID)*. Syvyyssuuntaisella puolustusperiaatteella varaudutaan laitoksen turvallisuutta ja käyttöä uhkaaviin sekä laitoksen sisäisiin että sen toimintaympäristön tapahtumiin, ulkoisiin uhkiin. Sisäisiä uhkia muodostavat esimerkiksi laiteviat, tulipalot, käyttöhenkilökunnan virheet ja laitosprosessin häiriöt. Ulkoisia uhkia ovat esimerkiksi laitoksen läheiset metsäpalot, maanjäristykset ja poikkeukselliset sääolosuhteet. (STUK Y/1/2016, 14–15 §).

Ydinvoimalaitoksen ja sen järjestelmien ja laitteiden suunnitteluun ja toimintaan liittyvät vaatimukset, määrittelyt ja perusteet normaaleissa käyttötilanteissa ja onnettomuuksissa muodostavat laitoksen suunnitteluperusteen *(Design Basis)* (YVL A.11, 23). Suunnitteluperuste sisältää esimerkiksi laitoksen sijaintipaikalla todennäköiseksi arvioidun suurimman maanjäristyksen, alhaisimman ja korkeimman ilman lämpötilan ja merenpinnan korkeuden, joista laitoksen on vähintään selviydyttävä. Suunnitteluperuste

sisältää myös alkutapahtumien oletetut taajuudet laitoksen käytön aikana. Onnettomuuksien todennäköisyyden on oltava sitä pienempi, mitä vakavampi onnettomuuden seuraus saattaisi olla, ja turvallisuusvaatimukset ja -toimenpiteet on mitoitettava ja kohdennettava tämän mukaisesti oikeassa suhteessa riskeihin (Ydinenergialaki 990/1987, 7 a, d §).

3.1 Painevesilaitoksen turvallisuustoiminnot

Turvallisuustoiminnot *(Safety functions)* ovat ydinvoimalaitoksen turvallisuuden kannalta tärkeitä toimintoja, joiden tarkoituksena on hallita häiriötilanteita, ehkäistä onnettomuustilanteiden syntyminen tai eteneminen tai lieventää onnettomuustilanteiden seurauksia (STUK Y/1/2016, 2 §). Järjestelmää, joka osallistuu turvallisuustoiminnon toteuttamiseen, kutsutaan turvallisuusjärjestelmäksi *(Safety system)* (YVL B.1, 43). Turvallisuusjärjestelmät voivat olla passiivisia rakenteita, kuten suojarakennus, tai aktiivisia tai passiivisia prosessi-, ilmastointi-, automaatio- tai sähköjärjestelmiä (Sandberg 2013, 56–57).

Yleisin ydinvoimalaitostyyppi on kevytvesireaktori, jossa neutronien hidastamiseen ja polttoaineen jäähdyttämiseen käytetään vettä (Sandberg 2013, 43). Kevytvesilaitokset voidaan jakaa painevesi- ja kiehutusvesilaitoksiin: esimerkiksi Loviisan ydinvoimalaitokset sekä Olkiluoto 3 -laitos ovat painevesilaitoksia ja Olkiluodon 1 ja 2 -laitokset kiehutusvesilaitoksia. Painevesilaitoksessa on kaksi erillistä jäähdytyspiiriä: primääripiiri ja sekundääripiiri. Reaktorisydämen läpi virtaavan primääripiirin lämpö siirretään erilliseen sekundääripiiriin höyrystimissä, joissa syntyvä höyry johdetaan turbiineille. Kiehutusvesireaktorissa osa jäähdytteenä käytetystä vedestä höyrystyy suoraan reaktorissa ja syntynyt höyry johdetaan turbiineille ilman erillisiä höyrystimiä. (Sandberg 2013, 43–51).

Kevytvesilaitoksen ydinturvallisuuden takaamiseksi turvallisuusjärjestelmien tehtävä on varmistaa sekä laitoksen normaalin käytön että häiriö- ja onnettomuustilanteiden aikana

- reaktorin pysäytys ja sen kriittisyydenhallinta,
- polttoaineen jäähdytys ja jälkilämmön poisto sekä
- radioaktiivisten aineiden leviämisen estäminen ja säteilyaltistukselta suojelu (Areva 2004a; Sandberg 2013, 56–57).

Yllä mainitut turvallisuuspäämäärät voidaan jakaa niiden hallinnan helpottamiseksi pienempiin osiin, painevesilaitoksella esimerkiksi taulukossa 3.1 esitettyihin turvallisuustavoitteisiin ja niitä toteuttaviin turvallisuustoimintoihin. Tavoitteiden ja toimintojen yksityiskohtainen nimeäminen ja jaottelu on yksilöllistä jokaisella laitoksella, eikä taulukossa 3.1 esitetty kokonaisuus kuvaa suoraan minkään todellisen laitoksen suunnittelua. Turvallisuustoiminnot voidaan edelleen jakaa niitä toteuttaviin erilaisiin turvallisuusjärjestelmiin, jotka vaihtelevat laitostyypistä riippuen.

Taulukko 3.1. *Painevesilaitoksen turvallisuustavoitteet ja niitä toteuttavat turvallisuustoiminnot.*

Turvallisuustavoite	**Turvallisuustoiminto**
Reaktiivisuuden hallinta	Reaktorin pysäytys Pitkäaikainen kriittisyydenhallinta
Primääripiirin massatase	Hätäjäähdytys
Lämmönsiirto sekundääripiiriin	Luonnonkierto Pakotettu virtaus pääkiertopumpuilla
Sekundääripiirin lämmönpoisto	Höyrystimen syöttövesi Höyrystimen ylipainesuojaus Höyrystimen höyrynpoisto
Primääripiirin tai suojarakennuksen lämmönpoisto	Lämmönpoisto primääripiiristä tai suojarakennuksesta jälkilämmönpoistojärjestelmillä Lämmönpoisto polttoainealtaasta
Primääripiirin ylipaineensuojaus	Paineistimen ruiskutus Paineistimen varoventtiilit tai muut varoventtiilit
Radioaktiivisten aineiden leviämisen estäminen	Suojarakennuksen eristys

Reaktiivisuuden hallinnalla tarkoitetaan, että reaktori voidaan tarvittaessa pysäyttää ja pitää alikriittisenä *(Subcritical state)*, eli tilassa, jossa ei tapahdu fissioissa vapautuvien neutronien ylläpitämää ketjureaktiota (YVL B.4, 8). Painevesilaitoksella reaktorin pysäytyksestä ja krittisyydenhallinnasta huolehtivat pikasulkujärjestelmä (säätösauvat), boorinsyöttöjärjestelmä, hätäruiskutusjärjestelmä sekä lisävesi- ja uloslaskujärjestelmät (Areva 2004a; Toivonen 1988, 511–513).

Ydinpolttoaineeseen kertyy käytön aikana radioaktiivisia fissiotuotteita, joiden hajotessa vapautuvaa energiaa kutsutaan jälkilämmöksi. Jälkilämpöä syntyy edelleen reaktorin pysäyttämisen jälkeen, ja polttoaineen eheyden säilyttämiseksi se on poistettava reaktorista. (Sandberg 2013, 58). Painevesilaitoksen polttoaineen jäähdytys ja jälkilämmön poisto voidaan jakaa toisistaan riippuvaisiin primääripiirin massataseesta huolehtimiseen, lämmönsiirtoon primääripiiristä sekundääripiiriin ja lopulliseen lämmönpoistoon. Primääripiirin massatase, eli sydämen jäähdytykseen tarvittavaa vesimäärä, varmistetaan hätäjäähdytystoiminnolla, jonka toteutukseen osallistuvat matala- ja keskipaineinen hätäjäähdytysjärjestelmä ja paineakut. Lämmönsiirto primääripiiristä sekundääripiiriin perustuu ensisijaisesti lämpötilaerojen aiheuttamaan luonnonkiertoon. Jälkilämpö poistetaan reaktorista tai suojarakennuksesta jälkilämmönpoistojärjestelmillä tai sekundääripiirin kautta hätä- tai apusyöttövesijärjestelmän ja höyrystimien paineenalennusjärjestelmällä. Reaktorin paineen hallinta hoidetaan paineistimen ruiskutuksella ja varoventtiileillä. (Areva 2004a; Toivonen 1988, 511–513).

Onnettomuuden seurausten lieventämiseksi on huolehdittava suojarakennuksen eristyksestä ja radioaktiivisten aineiden päästöjen rajoittamisesta. Painevesilaitoksen suojarakennuksen eristys suoritetaan sulkemalla eristysventtiilit suojarakennuksen läpikulke-

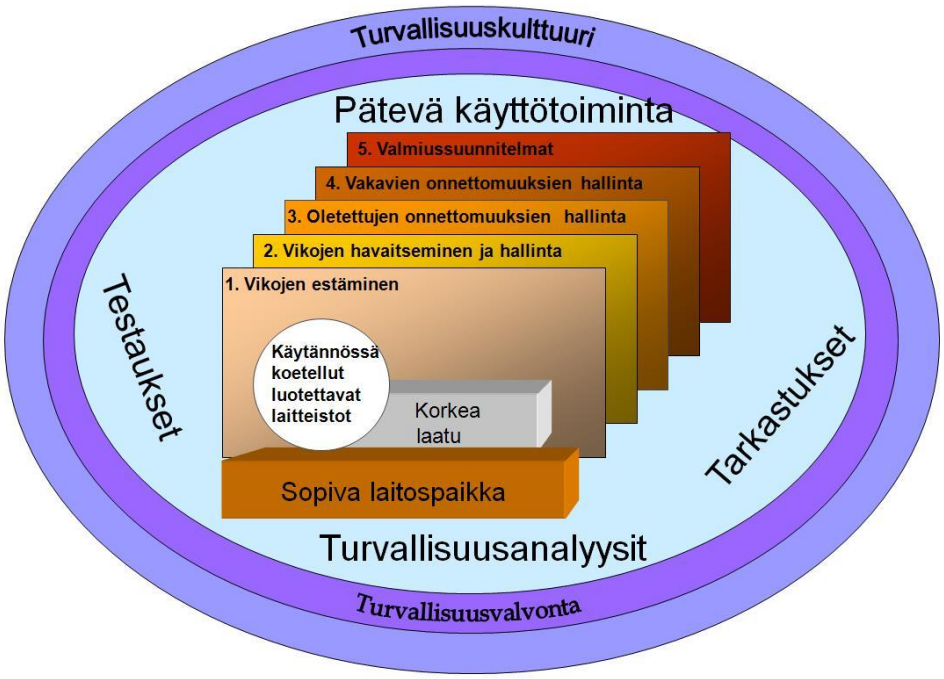
vissa putkissa (Areva 2004a). Radioaktiivisia päästöjä rajoitetaan myös suodatetulla ilmastoinnilla.

Vakavien onnettomuuksien hallintaan käytetään erillisiä turvallisuustoimintoja. Vakavissa reaktorionnettomuuksissa tavoitteena on erityisesti säilyttää suojarakennuksen eheys huolehtimalla erillisillä järjestelmillä suojarakennuksen jälkilämmönpoistosta, estää sydämen korkeapaineinen sulaminen primääripiirin paineenalennusventtiilien avulla ja hallita onnettomuuden aikana syntyviä palavia kaasuja, kuten vetyä.

Turvallisuusjärjestelmän vikaantumista analysoitaessa on huomioitava kyseisen järjestelmän lisäksi sen tukijärjestelmät ja muut riippuvuudet. Usein eri järjestelmien välillä esiintyy suunnittelemattomia riippuvuuksia esimerkiksi järjestelmien fyysisen sijoittelun seurauksena. Luvussa 6 esiteltävät vika-analyysit laaditaan erikseen jokaiselle turvallisuustoiminnolle.

3.2 Syvyyssuuntainen puolustusperiaate

Polttoainevaurioiden ja säteilyn haitallisten vaikutusten estäminen varmistetaan usealla peräkkäisellä, toisiaan varmistavalla toiminnallisella tasolla ja peräkkäisillä leviämisesteillä. Syvyyssuuntaisen puolustusperiaatteen *(Defence In Depth, DID)* ajatuksena on, että mikäli onnettomuuden ensimmäisten tasojen ennaltaehkäisy epäonnistuu, jälkimmäiset tasot suojaavat laitosta, sen käyttäjiä ja ympäristöä onnettomuuden haitallisilta vaikutuksilta sekä lieventävät niitä. (IAEA 2012, 6–8). Puolustustasojen tulee olla toisistaan riippumattomia, eikä yhden tason menetys saa heikentää muiden tasojen toimintaa (STUK Y/1/2016, 9 §). Toiminnalliset puolustusperiaate jaetaan kuvan 3.1 mukaisesti viiteen tasoon. Tasojen vahvuus varmistetaan pätevällä käyttötoiminnalla, testauksilla ja tarkastuksilla ja todennetaan turvallisuusanalyyseillä. Syvyyssuuntainen puolustusperiaate luo pohjan turvallisuussuunnittelulle, johon turvallisuusvalvonta kohdistuu. Turvallisuussuunnittelu ja -valvonta puolestaan kuuluvat kokonaisvaltaiseen turvallisuuskulttuuriin.



Kuva 3.1. *Syvyyssuuntainen puolustusperiaate (Reiman 2007).*

Ensimmäisen, vikoja ennaltaehkäisevän tason tarkoitus on varmistaa laitoksen luotettava käyttö ja estää poikkeamat normaaleista käyttöolosuhteista. Tämän varmistamiseksi laitoksen järjestelmien, rakenteiden ja laitteiden suunnittelussa, valmistuksessa, asennuksessa, käyttöönotossa, tarkastuksessa, koestuksessa, huollossa ja käyttötoiminnassa sovelletaan korkeita laatuvaatimuksia, luotettavuusvaatimuksia ja riittäviä varmuusmarginaaleja. (IAEA 2012, 6–8; YVL B.1, 13).

Toisella tasolla varaudutaan laitoksen huolellisesta suunnittelusta ja käytöstä huolimatta syntyviin häiriötilanteisiin sellaisin järjestelmin, joiden tehtävänä on havaita häiriöt ja rajoittaa häiriötilanteiden kehittymistä onnettomuuksiksi sekä ohjata laitos tarvittaessa hallittuun tilaan (IAEA 2012, 6–8; YVL B.1, 13). Näillä järjestelmillä taataan polttoaineen suojakuoren eheys varmistamalla reaktorin pysäytys, reaktorisydämen jäähdytys ja jälkilämmön poisto (Sandberg 2013, s. 101). Hallitulla tilalla *(Controlled State)* tarkoitetaan tilaa, jossa reaktori on sammutettu ja sen jälkilämmön poisto on turvattu. Kun edellisten lisäksi reaktori on paineeton, on se turvallisessa tilassa *(Safe State)*. (STUK Y/1/2016, 2 §).

Jos ensimmäisen ja toisen tason toimista huolimatta tai niiden epäonnistuessa onnettomuuden etenemistä ei saada pysäytettyä, sen seurauksia on lievennettävä. Onnettomuustilanteiden hallintaan on varauduttava sellaisin automaattisesti käynnistyvin luotettavin järjestelmin, jotka suojaavat radioaktiivisten aineiden leviämistä pidättäviä esteitä, estävät vakavien polttoainevaurioiden syntymisen ja onnettomuuden kehittymisen vakavaksi onnettomuudeksi. Kolmas taso jaetaan kahteen osaan, 3a ja 3b: 3a-tason tavoite on hallita yksittäisistä alkutapahtumista ja niiden seurausvaikutuksista johtuvia oletettuja

onnettomuuksia. 3b tasolla hallitaan käyttöhäiriöitä ja oletettuja onnettomuuksia, joiden yhteydessä niiden hallintaan suunnitellussa järjestelmässä ilmenee yhteisvika tai kyseessä on todennäköisyysperusteisen riskianalyysin perusteella valittu vikayhdistelmä tai harvinainen ulkoinen tapahtuma. (IAEA 2012, 6–8; YVL B.1, 13).

Syvyyssuuntaisen puolustusperiaatteen neljännen, vakavien onnettomuuksien hallinnan -tason tavoite on päästön rajoittaminen vakavissa onnettomuuksissa. Tasolla varmistetaan suojarakennuksen eheys ja tiiveys niin, että vakaville onnettomuuksille asetetut päästöjen raja-arvot eivät ylity. (IAEA 2012, 6–8; YVL B.1, 13).

Viimeinen, viides taso tähtää seurausten lieventämiseen tilanteessa, jossa laitokselta pääsee ympäristöön huomattavia määriä radioaktiivisia aineita. Tasolla varaudutaan huolehtimaan väestöön kohdistuvien säteilyvaikutusten rajoittamisesta erilaisin valmius- ja pelastusjärjestelyin. (IAEA 2012, 6–8; YVL B.1, 13).

Toiminnallisten tasojen lisäksi syvyyssuuntainen turvallisuusajattelu näkyy ydinvoimalaitoksilla radioaktiivisten aineiden eristämisessä ympäristöstä. Eristäminen toteutetaan kuvassa 3.2 esitetyillä viidellä sisäkkäisellä vapautumisesteellä. Ensimmäinen este on polttoaineen kiinteä keraaminen olomuoto, joka pitää sisällään syntyviä fissiotuotteita. Normaalikäytössä pieni osa fissiotuotteista vapautuu polttoaineesta, mutta jää toisena esteenä toimivan polttoainesauvan sisälle. Mikäli polttoainesauvan suojakuori rikkoutuu, radioaktiiviset aineet jäävät kolmanteen esteeseen, primäärisen jäähdytyspiirin sisäpuolelle. Neljäntenä esteenä toimii paineenkestävä ja kaasutiivis suojarakennus, joka primääripiirin vaurioituessa pitää sisällään radioaktiivisen höyryn ja veden. Viimeinen leviämiseste on reaktorin ulompi suojarakennus eli reaktorirakennus, jonka ilmansuodattimiin jäävät mahdollisesti sisemmästä suojarakennuksesta vuotavat radioaktiiviset aineet. Reaktorirakennus myös suojaa laitosta ulkoisilta uhkilta, kuten lentokoneentörmäyksiltä. (STUK 2008, 3–4).

Kuva 3.2. *Moninkertaiset radioaktiivisten aineiden vapautumisesteet (TVO 2013, 51).*

Häiriö- ja onnettomuustilanteiden analysoinnissa kiinnitetään huomio etenkin kolmeen keskimmäiseen vapautumisesteeseen. Esimerkiksi häiriö- ja onnettomuustilanteiden luokittelun yhtenä perusteena käytetään polttoainesauvan suojakuoren, primääripiirin ja suojarakennuksen eheyttä (YVL B.1, 41).

3.2.1 Tapahtumien suunnitteluperusteluokitus

Ydinvoimalaitoksen suunnittelussa on otettava huomioon mahdolliset muutokset ympäristöolosuhteissa ja muut tapahtumat, jotka voivat vaarantaa turvallisuustoimintojen toteuttamisen. Normaalit käyttötilanteet ja niistä poikkeavat laitostilanteet, häiriöt ja onnettomuudet luokitellaan perustuen tilanteen oletettuun esiintymistaajuuteen taulukon 3.2 mukaisesti. Luokittelu mukailee syvyyssuuntaisen puolustusperiaatteen tasoja. (STUK 2015a, 2).

Suunnitteluperusteluokkaan DBC 1 *(Design Basis Condition)* kuuluvat laitoksen normaalia toimintaa kuvaavat tilat kuten tuotantokäyttö ja laitoksen käynnistys-, pysäytys- ja seisokkitilanteet. DBC 2 -luokkaan kuuluvat odotettavissa olevat käyttöhäiriöt, joiden oletettu esiintymistaajuus f on kerran tai useammin sadassa käyttövuodessa a, eli noin kerran laitoksen käyttöiän aikana. (YVL B.1, 41; STUK 2015a, 9).

Oletetut onnettomuudet ovat sellaisia yksittäisen alkutapahtuman aiheuttamia poikkeamatilanteita, joista ydinvoimalaitoksen edellytetään selviävän ilman vakavia polttoainevaurioita. Oletetut onnettomuudet, joiden oletetaan esiintyvän harvemmin kuin kerran sadassa mutta vähintään kerran tuhannessa käyttövuodessa kuuluvat luokkaan DBC 3 ja harvemmin kuin kerran tuhannessa vuodessa luokkaan DBC 4. (YVL B.1, 41).

Taulukko 3.2. *Tapahtumien suunnitteluperusteluokitus. Muokattu lähteestä (STUK 2015a, 9).*

Suunnittelu-perusteluokka	**Puolustus-taso**	**Laitostilanteen luokka**	**Esiintymistaajuus (*)**
DBC 1	1	Normaalit käyttötilanteet	
DBC 2	2	Odotettavissa oleva tapahtuma	$f > 10^{-2}/a$
DBC 3	3a	Yksittäisen tapahtuman aiheuttama oletettu onnettomuus - luokka 1	 $10^{-2}/a > f > 10^{-3}/a$
DBC 4		- luokka 2	$f < 10^{-3}/a$
DEC	3b	Tyyppi A: odotettavissa oleva tapahtuma tai luokan 1 oletettu onnettomuus turvallisuus-järjestelmän yhteisvikaan yhdistettynä	$f < 10^{-4}/a$
		Tyyppi B: moninkertaisia vikoja sisältävä tapahtuma	$f < 10^{-5}/a$
		Tyyppi C: harvinainen tapahtuma	

(*) Puolustustasojen 2 ja 3a osalta alkutapahtuman esiintymistaajuus ja tason 3b osalta alkutapahtuman ja oletettujen lisävikojen kokonaisesiintymistaajuus.

Oletetun onnettomuuden laajennuksella, DEC-luokkaan *(Design Extension Category)* kuuluvilla tapahtumilla tarkoitetaan tilanteita, jotka aiheutuvat harvinaisesta ulkoisesta tapahtumasta tai joiden aiheuttamiseen tarvitaan alkutapahtuman lisäksi turvallisuusjärjestelmien yhteisvika tai monimutkainen vikayhdistelmä, josta laitos kuitenkin selviää ilman vakavaa polttoainevauriota. DEC-tapahtumien taajuudelle määritetyt arvot ovat suuntaa-antavia. DEC-A-luokkaan kuuluvat tapahtumat, joissa odotettavissa olevaan käyttöhäiriöön (DBC 2) tai DBC 3 -luokan oletettuun onnettomuuteen liittyy turvallisuusjärjestelmissä esiintyvä yhteisvika. DEC-B-luokan tapahtumiksi luokitellaan monimutkaiset vikayhdistelmät. DEC-C-luokan tapahtumat aiheutuvat harvinaisista ulkoisista tapahtumista, kuten äärimmäisistä sääilmiöistä tai lentokoneen törmäyksestä. (YVL B.1, 42).

Vakavassa reaktorionnettomuudessa *(Severe Accident, SA)* huomattava osa reaktorissa olevasta polttoaineesta vaurioituu menettäen alkuperäisen rakenteensa. Odotusarvo reaktorisydämen vaurioitumistaajuudelle tulee olla pienempi kuin 10^{-5}/vuosi. Lisäksi sellaisen onnettomuuden, jossa radioaktiivinen Cs-137-päästö ylittää 100 TBq, taajuuden odotusarvon tulee olla pienempi kuin 5.0×10^{-7}/vuosi. (YVL A.7, 4).

Suunnitteluperusteluokkiin liitetään raja-arvoja tapahtumien aiheuttamille sallituille seurauksille, kuten radioaktiivisten päästöjen suuruudelle, polttoainevaurioille sekä ylipainesuojaukselle. Luokitusta hyödynnetään turvallisuusjärjestelmien mitoituksessa ja muiden suunnitteluvaatimusten määrittelyssä, jotta asetetut raja-arvot eivät ylity. (STUK 2015a, 19). Luokituksesta seuraa myös tapahtumien analyysivaatimuksia sekä analyyseissä käytettäviä oletuksia. Esimerkiksi luokkiin DBC 2 tai DBC 3 kuuluville alkutapahtumille on laadittava yhteisvika-analyysi ja oletettujen onnettomuuksien analysoinnissa on huomioitava ulkoisen sähköverkon menetys, mikäli se voi pahentaa alkutapahtuman seurauksia. (YVL B.1, 9; YVL B.3, 6).

3.3 Ydinvoimalaitoksen suunnitteluperiaatteita

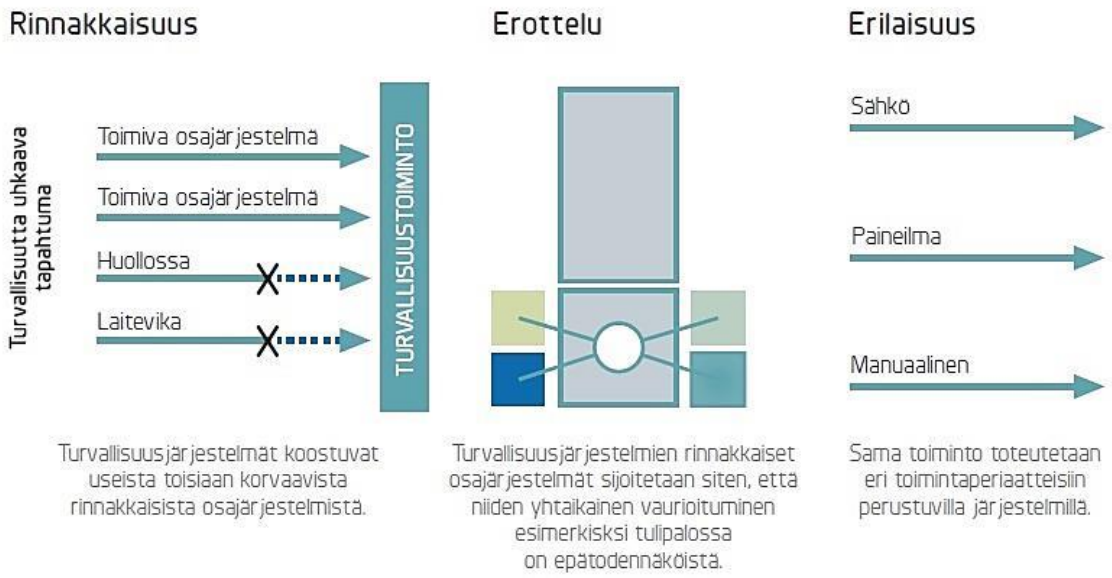
Ydinvoimalaitosten turvallisuussuunnittelua koskevan YVL B.1 -ohjeen mukaan *”[414.] Ydinvoimalaitoksen suunnittelussa on otettava huomioon tapahtumat, jotka voivat saada aikaan laitoksen parametrien poikkeamisen normaaliarvoistaan, sekä tapahtumat, jotka voivat vaarantaa turvallisuustoimintoja toteuttavien laitteiden tai järjestelmien käyttövalmiuden…”* (s. 12). Näihin tapahtumiin varaudutaan turvallisuustoiminnoilla.

Turvallisuustoimintojen varmistamiseksi on laitoksen suunnitteluratkaisuissa ensisijaisesti hyödynnettävä luontaisia turvallisuusominaisuuksia, jotka perustuvat reaktorin tehon kasvua hillitseviin fysikaalisiin takaisinkytkentöihin. Jos luontaisia turvallisuusominaisuuksia ei voida käyttää, tulee järjestelmät ja -laitteet toteuttaa ensisijaisesti niin, että ne eivät tarvitse ulkoista käyttövoimaa tai ne käyttövoiman menetyksen seurauksena asettuvat turvallisuuden kannalta edulliseen tilaan. Tätä periaatetta kutsutaan turvalli-

sen tilan periaatteeksi. (STUK Y/1/2016, 11 §). Jos järjestelmä osallistuu usean toiminnon toteuttamiseen, turvallisuuden kannalta edullinen tila ei välttämättä ole yksiselitteinen. Tällöin toiminnot voidaan asettaa tärkeysjärjestykseen niiden menetyksestä aiheutuvien seurausten ja toiminnon tarpeen todennäköisyyden mukaan (Toivonen 1988, 512).

Jotta turvallisuudelle tärkeät toiminnot tapahtuvat luotettavasti, turvallisuusjärjestelmien suunnittelussa sovelletaan turvallisen tilan periaatteen lisäksi kuvassa 3.3 esitettyjä rinnakkais-, erottelu- ja erilaisuusperiaatteita (IAEA 2012, 26). Rinnakkais- eli moninkertaisuusperiaatteella *(redundancy)* tarkoitetaan, että on olemassa useita rinnakkaisia osajärjestelmiä, joista toiminnon toteuttamiseksi riittää esimerkiksi yhden osajärjestelmän toimiminen kolmesta tai kahden neljästä (Sandberg 2013, 102). Moninkertaisuusperiaatteella taataan, että mikään turvallisuustoiminto ei voi estyä yksittäisen osajärjestelmän tai laitteen vian seurauksena.

Toinen suunnitteluperiaate on erotteluperiaate *(separation)*, joka pitää sisällään fyysisen ja toiminnallisen erottelun (IAEA 2012, 26). Fyysinen erottelu tarkoittaa, että rinnakkaiset osajärjestelmät sijoitetaan eri tiloihin, riittävän kauas toisistaan tai asetetaan niiden välille suojaavia rakenteita. Tällä pyritään estämään, että esimerkiksi tulipalo tai tulva ei tuhoa useaa osajärjestelmää samanaikaisesti. Fyysisen erottelun lisäksi rinnakkaisten järjestelmien vuorovaikutukset estetään toiminnallisella erottelulla, kuten sähköisellä erottelulla ja järjestelmien välisen informaation käsittelyn erottelulla, jotta yhden järjestelmän vika ei vaikuta haitallisesti toisiin järjestelmiin. (STUK Y/1/2016, 2 §; YVL B.1, 43).



Kuva 3.3. *Turvallisuusjärjestelmien suunnitteluperiaatteet. Muokattu lähteestä (TVO 2013, 52).*

Kolmas suunnitteluperiaate, erilaisuusperiaate *(diversity)* tarkoittaa, että sama turvallisuustoiminto voidaan toteuttaa eri toimintaperiaatteisiin perustuvilla järjestelmillä tai laitteilla. Näin pienennetään yhteisvikojen mahdollisuutta ja parannetaan toiminnon luotettavuutta. Reaktorin sammuttaminen on esimerkiksi mahdollista säätösauvojen tai reaktoriin syötettävän booriliuoksen avulla. (Sandberg 2013, 102–104).

Turvallisuustoimintojen, joita tarvitaan käyttöhäiriöiden tai oletettujen onnettomuuksien alkuvaiheessa, tulee käynnistyä automaattisesti. Suojausjärjestelmän automaattisesti käynnistämien toimintojen tulee pitää laitos hallitussa tilassa niin kauan, että operaattorille jää riittävästi harkinta-aikaa jatkotoimenpiteiden aloitukselle. (Sandberg 2013, 104–105).

3.3.1 Järjestelmien turvallisuusluokitus

Ydinvoimalaitoksen järjestelmät, laitteet ja rakenteet luokitellaan niiden ydinturvallisuusmerkityksen mukaan turvallisuusluokkiin *(Safety Class, SC)* 1, 2, 3 ja luokkaan EYT *(ei ydinteknisesti turvallisuusluokiteltu)*. Luokittelu perustuu deterministisiin turvallisuusanalyyseihin ja todennäköisyysperusteisiin riskianalyyseihin sekä asiantuntijaarvioihin. Luokittelun mahdollistamiseksi laitos jaetaan rakenteellisiin ja toiminnallisiin kokonaisuuksiin eli järjestelmiin, jotka jaetaan edelleen rakenteisiin ja laitteisiin. (YVL B.2, 3). Pääsääntöisesti turvallisuusluokka määrittää, mitä luvussa 3.3.2 esitettävistä vikakriteereistä kuhunkin järjestelmään sovelletaan.

Rakenteiden turvallisuusluokan määrää rakenteen kestävyys, eheys ja tiiveys, joka vaaditaan turvallisuustoiminnon toteuttamiseksi tai radioaktiivisten aineiden leviämisen estämiseksi. Korkein rakenteellinen turvallisuusluokka on 1. Turvallisuusluokkaan 1 kuuluvat ydinpolttoaine, reaktoripainesäiliö sekä ne primääripiirin osat, joiden vaurioituminen voi aiheuttaa reaktorin eheyttä vaarantavan onnettomuuden ja vaatia turvallisuustoimintojen välittömän käynnistymisen, eikä niitä voi korvata laitoksen normaaliin käyttöön liittyvillä järjestelmillä. Loput rakenteet kuuluvat turvallisuusluokkiin 2 tai 3 tai luokkaan EYT. (YVL B.2, 5–6).

Toiminnallinen turvallisuusluokitus perustuu järjestelmän merkitykseen laitoksen turvallisuustoimintojen luotettavuudelle alkutapahtuman hallinnan kannalta, huomioiden syvyyssuuntaisen turvallisuusajattelun. Toiminnallisesti korkein turvallisuusluokka on 2, johon kuuluvat turvallisuustoimintoja toteuttavat järjestelmät, jotka oletettujen onnettomuuksien tilanteissa saattavat laitoksen hallittuun tilaan ja pitävät sen siinä edellytetyn ajan. Loput järjestelmät luokitellaan turvallisuusluokkaan 3 tai luokkaan EYT. Järjestelmän osat, yksittäiset rakenteet tai laitteet, voivat kuulua myös koko järjestelmän turvallisuusluokkaa ylempään tai alempaan turvallisuusluokkaan. (YVL B.2, 4–5).

Ydinvoimalaitoksen järjestelmät, rakenteet ja laitteet luokitellaan lisäksi maanjäristysluokkiin niiden toimintovaatimusten perusteella. Korkeimpaan maanjäristysluokkaan S1

kuuluvien järjestelmien tulee pysyä ehjinä, tiiviinä, toimintakykyisinä ja oikealla paikallaan suunnitteluperusteen mukaisen maanjäristyksen aiheuttamasta kuormituksesta huolimatta. Maanjäristysluokkaan S2A luokitellaan järjestelmät, joiden toimintakyvyn ja eheyden säilyttäminen ei ole välttämätöntä, mutta jotka voivat maanjäristyksen seurauksena vahingoittaa S1-luokkaan kuuluvien järjestelmien toimintaa, esimerkiksi romahtamalla tai aiheuttamalla tulvan. Kaikki muut järjestelmät luokitellaan maanjäristysluokkaan S2B. (YVL B.2, 6–7).

3.3.2 Vikasietoisuus ja vikakriteerit

Järjestelmiltä vaadittava vikasietoisuus määritetään N+1 ja N+2-vikakriteereillä. Vikasietoisuutta kasvatetaan moninkertaistamalla saman toiminnon toteuttavia järjestelmiä ja laitteita. Vikakriteereiden tarkoituksena on huomioida vikaantumisten ohella huoltojen ja korjausten vaikutus järjestelmien toimintakuntoisuuteen.

Yksittäisvikakriteerin N+1 mukaan vaadittu turvallisuustoiminto on pystyttävä toteuttamaan, vaikka mikä tahansa toiminnossa vaadittava yksittäinen laite vikaantuisi (YVL B.1, 43). N+1-vikakriteerin mukaiset järjestelmät toteutetaan vähintään kaksiredundanttisina (2x100 %), eli kahdella rinnakkaisella osajärjestelmällä, joista kumpikin pystyy itsenäisesti toteuttamaan vaaditun toiminnon. Toinen vaihtoehto on 3x50%-periaatteen käyttö, jolloin yhden osajärjestelmän vikaantuessa jäljelle jäävien kahden osajärjestelmän toiminta yhdessä riittää toiminnon toteuttamiseen. Yksittäisvikakriteeriä sovelletaan normaalikäyttöön osallistuville turvallisuusluokan 3 järjestelmille (STUK 2015a, 20).

Turvallisuusluokan 2 turvallisuusjärjestelmissä noudatetaan N+2-vikakriteeriä, jonka mukaan järjestelmän tulee pystyä toteuttamaan tehtävänsä, vaikka mikä tahansa yksittäiseen osajärjestelmään kuuluva laite tai sen tukijärjestelmän laite vikaantuisi ja samanaikaisesti toinen osajärjestelmä olisi poissa käytöstä, esimerkiksi huollossa tai korjauksessa (Sandberg 2013, 102). N+2-vikakriteerin mukaiset järjestelmät toteutetaan 3x100 % tai 4x50 % -periaatteella. Kun N+2-vikakriteerin lisäksi huomioidaan mahdollisen alkutapahtuman aiheuttama seurausvika rinnakkaiseen osajärjestelmään, osajärjestelmien moninkertaisuusvaade kasvaa 4x100%:iin.

Vaihtoehtona N+2-kriteerille on käyttää (N+1 & D+1)-periaatetta, joka tarkoittaa, että turvallisuustoiminto voidaan toteuttaa kahdella rinnakkaisella erilaisuusperiaatteen (D+1) mukaisella järjestelmällä, joista molemmat täyttävät itsenäisesti yksittäisvikakriteerin. Toteutustapana voidaan myös käyttää (N+2 & D+1)-periaatetta, esimerkiksi jos ensisijaisen järjestelmän sisällä esiintyy mahdollisuus yksittäisvian laajenemiseen kahden osajärjestelmän väliseksi yhteisviaksi. Tilannetta havainnollistetaan esimerkillä luvussa 6.3.1.

3.3.3 Toimintojen priorisointi

Yksi prosessijärjestelmä voi osallistua sekä turvallisuustoiminnon että normaalikäytön toimintojen toteuttamiseen. Tämä aiheuttaa tarpeen priorisoida toiminnot ja järjestelmiä ohjaavat signaalit, jotta järjestelmä osallistuu kulloinkin laitoksen turvallisuuden kannalta merkittävimpiin toimintoihin. Turvallisuustoiminnot priorisoidaan kuvan 3.4 mukaisesti korkeammalle kuin normaalikäytön toiminnot. Yksittäiset järjestelmät saattavat osallistua myös useampaan kuin yhteen turvallisuustoimintoon, jolloin onnettomuustilanteessa saattaa syntyä yhteisiä järjestelmiä hyödyntävien toimintojen yhtäaikainen käyttötarve. Tätä varten myös turvallisuustoimintojen keskinäinen tärkeysjärjestys ratkaistaan osana prosessisuunnittelua.

Toimintojen tärkeysjärjestyksen määrittämisen lisäksi järjestelmiä ohjaavat signaalit priorisoidaan. Ydinvoimalaitoksen automaatiojärjestelmät jaetaan normaaleissa käyttötilanteissa käytettävään käyttöautomaatioon sekä onnettomuuksien estämiseen ja seurausten lieventämiseen suunniteltuun suojausautomaatioon. Toiminnot allokoidaan niiden tarkoituksen mukaisesti eri automaatiojärjestelmille. Lähtökohtaisesti ohjaajien valvomossa tekemä toimenpide tai jonkin muun järjestelmän toiminta ei saa estää tai pysäyttää suojausautomaatiolta käynnistyskäskyn saanutta järjestelmää toteuttamasta turvallisuustoimintoa ennen kuin toiminto on toteutettu loppuun tai toiminnon käynnistäneet parametrit ovat palautuneet normaalialueelle. (YVL B.1, 22).

Järjestelmää ohjaavista toimintojen signaaleista ensisijaiseen toimintoketjuun kuuluvat ohjaussignaalit ovat prioriteetiltaan korkeammalla kuin saman toiminnon varaketjujen ohjaukset. Jos ensisijaiseen toimintoon liittyvä ohjaussignaali on esimerkiksi pulssimainen, tulee priorisoinnilla estää ensisijaisen käskyn kumoaminen varatoiminnon eriaikaisella käskyllä. Jos kuitenkin prioriteetiltaan korkeampi toimintoketju on vikaantunut, tulee varatoiminnon prioriteetti voida nostaa tätä korkeammaksi. Esimerkiksi, jos kuvan 3.4 tilanteessa laite on saanut pysäytyskäskyn turvallisuustoiminnon ensisijaisesta toimintoketjusta, pysyy laite lähtökohtaisesti pysäytettynä niin kauan, kunnes pysäytyskäsky kumotaan.

Kuva 3.4. *Yhden järjestelmän toimintojen ja niiden ohjaussignaalien priorisointi.*

Priorisointia tulee voida muuttaa esimerkiksi valvomon menetystilanteissa, jolloin valvomosta saattaa lähteä järjestelmille vääriä ohjaussignaaleja. Tällöin varavalvomosta lähetetyt signaalit tulee voida priorisoida ensisijaisen valvomon lähettämiä signaaleja korkeammalle. Priorisointi on yksinkertaisimmillaan, jos toimintoketjut on toteutettu täysin toisistaan erillisillä järjestelmillä sekä prosessitasolla että ohjausten suhteen. Usein näin ei kuitenkaan ole, mikä monimutkaistaa priorisointia.

3.4 Viranomaisvaatimukset ja -ohjeet

Kansainvälisellä tasolla ydinenergian rauhaomaista ja turvallista käyttöä edistää Kansainvälinen atomienergiajärjestö *(International Atomic Energy Agency, IAEA)*, jonka eräänä tehtävänä on laatia ydin- ja säteilyturvallisuutta koskevia ohjeita. IAEA:n Turvallisuusstandardien julkaisusarja *(IAEA Safety Standards Series)* jaetaan kolmeen osaan: Turvallisuusperusteet-sarjassa *(Safety Fundamentals)* esitetään turvallisuutta koskevat perustavoitteet ja -periaatteet. Turvallisuusvaatimukset-sarja *(Safety Requirements)* käsittää vaatimukset, joita noudattamalla turvallisuustavoitteet saavutetaan. Turvallisuusoppaat-sarja *(Safety Guides)* kuvaa suositeltavia menettelytapoja turvallisuusvaatimusten täyttämiseksi. (IAEA 2006, 4–5). IAEA:n ohjeistot eivät ole laillisessa mielessä jäsenvaltioita sitovia, mutta esimerkiksi Suomessa ohjeita käytetään merkittävänä lähdeaineistona kotimaisen turvallisuussäännöstön laadinnassa (Sandberg 2013, 365).

Euroopan unionin ydinlaitosten turvallisuutta koskeva direktiivi ohjaa sen jäsenmaiden turvallisuuslainsäädäntöä. WENRA *(Western European Nuclear Regulators Association)* on ydinvoimaa käyttävien Euroopan unionin jäsenmaiden ja Sveitsin turvallisuusviranomaisten yhteistyöfoorumi. WENRA:n eräänä tavoitteena on kehittää ja yhdenmukaistaa ydinturvallisuuden kansainvälisiä vaatimuksia. Tätä varten WENRA on laatinut niin sanotut referenssivaatimukset, joita myös Suomen kansalliset vaatimukset noudattavat. (EU 2014, WENRA 2015).

Suomessa ydinvoiman turvallisuudesta määrää ydinenergialaki (990/1987) sekä lukuisat tarkentavat määräykset ja ohjeet. Vuoden 2016 alusta alkaen STUKin määräykset ovat korvanneet vanhat ydinturvallisuutta koskevat valtioneuvoston asetukset (STUK 2016). Yksityiskohtaiset ydinvoimalaitoksen turvallisuusvaatimukset esitetään STUKin laatimissa ydinvoimalaitosohjeissa *(YVL)* (YVL A.1, 10). YVL-ohjeet velvoittavat luvanhaltijoita toteuttamaan niissä esitetyt vaatimukset, kuitenkin niin, että luvanhaltijalla on oikeus esittää muunkinlainen kuin ohjeissa esitetty menettelytapa tai ratkaisu, jos se toteuttaa vaaditun turvallisuustason (990/1987, 7 r §). YVL-ohjeissa asetetaan kriteerit laitosten järjestelmien ja toimintojen vikasietoisuudelle sekä vaatimukset vikasietoisuuden analysoinnille.

Laitoskohtaisissa turvallisuusteknisissä käyttöehdoissa *(TTKE)* esitetään ne tekniset ja hallinnolliset vaatimukset, joilla varmistetaan yksittäisen laitoksen suunnitteluperusteiden ja turvallisuusanalyysien mukainen käyttö ja turvallisuuden kannalta tärkeiden jär-

jestelmien, rakenteiden ja laitteiden toimintakyky (YVL A.1, 22–23). TTKE:n vaatimukset koskevat esimerkiksi testauksia ja sallittuja korjausaikoja. Lisäksi TTKE esittää ne rajoitukset, joita on noudatettava laitteiden vikaannuttua.

4. VIKA-ANALYYSIEN ROOLI TURVALLISUUS-TOIMINTOJEN ANALYSOINNISSA

Tässä työssä käsiteltävät vika-analyysit ovat yksi osakokonaisuus ydinvoimalaitoksen turvallisuustoimintojen vikaantumista tarkastelevaa analyysikokonaisuutta. Kokonaisuus voidaan jakaa kuvassa 4.1 hahmoteltaviin deterministisiin turvallisuusanalyyseihin, vika-analyyseihin ja todennäköisyysperusteiseen riskianalyysiin *(Probabilistic Risk Assessment, PRA)*. Deterministiset menetelmät on tarkoitettu kuvaamaan vian tai häiriön etenemistä järjestelmässä, vika-analyysit vikaantumisten syntymistä ja seurauksia ja PRA huomioi vikaantumisten todennäköisyyden. Usein menetelmiä käytetään toistensa tukena laatien tapahtuman syntyä ja etenemistä kuvaava analyysi, johon liitetään tapahtuman ja seurausten todennäköisyydet.

Deterministiset turvallisuusanalyysit luovat pohjan turvallisuustoimintojen analysoinnille. Niillä osoitetaan, että laitoksen ja sen järjestelmien suunnittelu täyttää tekniset turvallisuustavoitteet ja -vaatimukset. Deterministisillä analyyseillä osoitetaan, että laitos pystyy toteuttamaan siltä vaaditut turvallisuustoiminnot häiriö- ja onnettomuustilanteissa, eikä sillä ole ominaispiirteitä, jotka merkittävästi pahentaisivat häiriöitä tai onnettomuuksia tai lisäisivät niiden aiheuttamia vaurioita. (STUK 2015b). Deterministiset turvallisuusanalyysit hyödyntävät lähtötietoinaan vika-analyyseillä selvitettyjä vikaantumismahdollisuuksia.

Vika-analyyseillä selvitetään vikojen syyt ja niiden vaikutukset järjestelmien toiminnalle. Tavoitteena on osoittaa, että turvallisuustoiminnot voivat toteuttaa tehtävänsä häiriö- ja onnettomuustilanteissa ja että ne täyttävät niille deterministisillä turvallisuusanalyyseillä määritetyt vikasietoisuusvaatimukset.

Kuva 4.1. *Analyysikokonaisuuksien roolit turvallisuustoimintojen analysoinnissa.*

Todennäköisyysperusteinen riskianalyysi kokoaa deterministisen turvallisuusanalyysien ja vika-analyysien tuloksista laitoksen riskimallin. Analyysillä tutkitaan, missä tilanteissa ja millä todennäköisyydellä deterministisillä turvallisuusanalyyseillä määritetyt onnistumismiskriteerit eivät täyty. PRA:lla tarkastellaan turvallisuustoimintojen epäluotettavuutta ja tunnistettuihin onnettomuus- ja häiriötilanteisiin liittyviä todennäköisyyksiä: tunnistetaan tapahtumayhdistelmät, jotka voivat tilanteisiin johtaa, sekä kyseisten tapahtumien esiintymistodennäköisyydet ja seurausten todennäköisyydet (IAEA 1992, 2–3). Tapahtumayhdistelmien tunnistamisessa hyödynnetään vika-analyyseillä selvitettyjä vikaantumismahdollisuuksia. PRA:ssa tunnistetut monimutkaiset vikayhdistelmät toimivat edelleen syötteenä deterministisille turvallisuusanalyyseille.

4.1 Vika-analyysit

Vika-analyysien tarkoituksena on tunnistaa laitteiden, järjestelmien, toimintojen ja koko arkkitehtuuritason laajuisia vikaantumismahdollisuuksia ja niiden aiheuttamia turvallisuustoimintotarpeita. Laitteiden, järjestelmien ja toimintojen vikasietoisuus osoitetaan vika-analyyseillä. Vika-analyysejä voidaan kuvata asiantuntija-arvioiksi, joissa hyödynnetään esimerkiksi muissa yhteyksissä laadittuja onnettomuuslaskuja. Vika-analyysit voivat olla itsenäisiä analyysimenetelmiä tai osa deterministisiä turvallisuusanalyysejä tai todennäköisyysperusteista riskianalyysiä. Esimerkiksi paloanalyysit sisältävät sekä deterministisiä palosimulointeja, vika-analyyseihin kuuluvia tilakohtaisia analyysejä että todennäköisyysperusteisen syiden ja seurausten riskiarvioinnin.

Taulukkoon 4.1 on koottu YVL B.1 -ohjeen vaatimuksia vikasietoisuuden osoittamisesta ja vika-analyyseistä sekä Olkiluoto 3 -laitosdokumentaation perustuvia analyysejä, joilla voidaan osoittaa tiettyyn aihepiiriin liittyvät vaatimukset täytetyiksi.

Taulukko 4.1. *YVL B.1-ohjeen vaatimuksia ja niihin vastaavat vika-analyysit.*

AIHE	KOHDE	ANALYYSI	YVL B.1	LUKU
Vika-analyysiavaruus	Tapahtumat, laitosvaste	Alkutapahtuma-analyysit	352	6
Yksittäisen laitteen/ järjestelmän vikaantuminen	Mekaaniset laitteet	Vika- ja vaikutusanalyysit	352, 432	6.1.2
		Inhimillisten virheiden analyysit	STUK Y/1/ 2016, 6 §	
	Automaatio	Aiheettomien toimintojen analyysit	5236	
Turvallisuus-toiminnon moninkertaisuus	Järjestelmät, tukijärjestelmät	Vikakriteerien analyysit (N+1, N+2)	351, 352	6.2.1
Turvallisuustoi-minnon sisäinen ja osatoimintojen erilaisuus	Mekaaniset laitteet	Yhteisvika-analyysit	351, 432	6.3.1
	Tukijärjestelmät	Tukijärjestelmien erilaisuus-analyysit	351	6.3.2
		Automaation erilaisuusanalyysit	5229	
		Mittausten erilaisuusanalyysit	5230	
Puolustustason vahvuus, turvallisuus-lohkojen erottelu	Pohjapiirros	Sisäisten uhkien analyysit	434, 437	7.1.1
	Tukijärjestelmät	Erottelulla hallitut automaatio-kokonaisuudet	5238 5244	7.1.2
		Sähkönsyötön erotteluanalyysit	STUK Y/1/ 2016, 11 §	7.1.3
	Rakenteet	Ulkoisten uhkien analyysit	435, 501	7.1.4
Puolustustasojen erottelu	Puolustustasot	Seurausvikojen leviämisen analyysit	351, 426	7.2.1
	SA-järjestelmät	Vakavien onnettomuuksien hallinnan erillisyysanalyysit	431	7.2.2
	Tukijärjestelmät	- Sähköjärjestelmien riippumat-tomuusanalyysit - Automaation erilaisuus ana-lyysit (erottelulla hallitut koko-naisuudet)	427	7.2.3

Esitetyt vaatimukset ja niihin vastaavat analyysit käsitellään taulukon mukaisesti tämän työn luvuissa 6 ja 7. Vika-analyysien lähtötietoina tulee tuntea käsiteltävän laitteen, järjestelmän tai toimintoketjun rajapinnat ja käsiteltävän kohteen sisäiset ja ulkoiset vuorovaikutukset. Tätä varten luvussa 6 esitellään analyysien ohessa myös järjestelmäkuvauksia ja rajapintamäärittelyjä, vaikka ne eivät ole varsinaisia vika-analyysejä.

4.1.1 Vika-analyysit osana suunnitteluprosessia

Ydinvoimalaitostoiminnan luvanvaraisuuden vuoksi uuden voimalaitoksen rakentamiseen kuuluu useita lupavaiheita. Kaikkiin lupavaiheisiin liittyy oleellisena osana myös vikaantumisen ja vikasietoisuuden analysointi. Turvallisuustoimintojen vika-analyysejä hyödynnetään läpi suunnitteluprosessin: Alkuvaiheessa osoitetaan, että suunnittelussa

on huomioitu vikasietoisuusvaatimukset ja laitos voidaan toteuttaa niiden mukaisesti. Suunnittelun edetessä yksityiskohtaisiin järjestelmäsuunnitelmiin ja laitevalintoihin, analyysit tarkentuvat ja niillä osoitetaan, että vaatimukset tulevat täytetyiksi. Analyyseillä tunnistetut turvallisuusriskit huomioidaan suunnittelussa prosessin jokaisessa vaiheessa ja tarvittaessa suunnitteluun tehdään muutoksia.

Ydinvoimalaitoksen rakentamisen periaatepäätöstä haettaessa on luvanhaltijan toimitettava STUKille esimerkiksi laitoksen turvajärjestelmien osalta suunnitteluperiaatteet ja toiminnan kuvaus, periaatteelliset suunnitelmat onnettomuustilanteisiin varautumisesta sekä yhteenveto laitostyyppiä koskevista turvallisuusanalyyseistä ja mahdollisten onnettomuuksien ympäristövaikutusanalyyseistä. STUK valmistelee toimitetun materiaalin perusteella alustavan turvallisuusarvion. (YVL A.1, 6–7, 33). Tässä vaiheessa esimerkiksi ulkoisten uhkien analyysejä hyödynnetään osana laitospaikan valintaa, sen olosuhteiden kartoittamista ja suunnitteluperusteiden määrittämistä.

Rakentamislupahakemuksen yhteydessä STUKille toimitetaan hyväksyttäväksi muun muassa alustava turvallisuusseloste, suunnitteluvaiheen todennäköisyysperusteinen riskianalyysi sekä turvallisuuden kannalta tärkeiden rakenteiden, järjestelmien ja laitteiden luokittelu niiden turvallisuusmerkityksen perusteella (Ydinenergia-asetus 161/1988, 35 §). Rakentamislupavaiheessa suunnitteluperusteet täsmentyvät ja analyysit tarkentuvat arkkitehtuuritasolle. Analyysien avulla tunnistetaan esimerkiksi, kuinka monelle rinnakkaiselle sähkönsyöttöjärjestelmälle on tarve ja kuinka eri puolustustasojen järjestelmät näille allokoidaan. Edellä mainittuja ulkoisten uhkien analyysejä hyödynnetään esimerkiksi rakenteiden kestävyyden arvioinnissa.

Ydinenergialain (990/1987, 20 §) mukaan ydinvoimalaitokselle voidaan myöntää käyttölupa, kun sille on myönnetty rakentamislupa ja se täyttää kyseisen lain turvallisuusvaatimukset. Käyttölupaa varten laaditaan lopullinen turvallisuusseloste, joka sisältää esimerkiksi täsmälliset järjestelmäkuvaukset, joiden yhteydessä on laadittu yksityiskohtaiset vika-analyysit. Järjestelmä-, laite- ja komponenttitasolla ulkoisten uhkien analyysejä voidaan hyödyntää esimerkiksi yksittäisten laitteiden kiinnityksien suunnittelussa. Käyttöönotto edellyttää myös STUKin arviota turvallisuusvaatimusten täyttymisestä, riittävistä turvajärjestelyistä, valvonnan toteutuksesta ja varautumisesta ydinvahinkoihin. Laitostoimittajan ja voimayhtiön laatimat vika-analyysit toimivat yhtenä perusteena STUKin arvioille turvallisuusvaatimusten täyttymisestä. Laadittujen vika-analyysien perusteella STUK voi vielä vaatia suunnitelmiin muutoksia, mikäli turvallisuusvaatimukset eivät ole täyttyneet tai analyysitulokset muutoin antavat tälle aihetta. Tavoite kuitenkin on, että analyysejä hyödynnetään mahdollisimman laajasti jo suunnittelun aikana, ja STUKille toimitettavat analyysien tulokset eivät enää antaisi aihetta muutoksiin.

Vika-analyysejä laaditaan myös käynnissä oleville ydinvoimalaitoksille esimerkiksi korjausten ja laitosmuutosten yhteydessä sekä käyttökokemusten perusteella. Pienenkin

yksityiskohdan muuttaminen voi vaikuttaa useisiin toimintoihin ja edellyttää monien analyysien tarkentamista tai päivittämistä. Tällöin on hyödyksi, jos suunnittelun ja rakentamisen aikaiset analyysit ovat huolellisesti dokumentoituja ja päivitettävissä, jotta analyysejä ei tarvitse toistaa kokonaisuudessaan alusta asti. Käyville laitoksille tehtävät vika-analyysit ja niiden päivitykset voivat myös osoittaa tarpeen uusille laitosmuutoksille.

4.1.2 Vika-analyysien työllistävyys ja laajuus

Vika-analyysit ovat laajoja kokonaisuuksia, joiden työmäärän arviointi on vaikeaa. Analyysit ovat kiinteä osa suunnittelua ja täydentyvät jatkuvasti suunnitelmien täsmentyessä, eikä yhden analyysin työmäärää näin ollen voi täsmällisesti määrittää irrallisena suunnitteluprosessista ja muista analyyseistä. Tässä luvussa esitetään STUKin näkökulmasta arvioita analyysien työmääristä, perustuen Olkiluoto 3 -laitokselle tehtyihin analyyseihin. Työmääriä arvioitaessa analyysin laatijan oletetaan tuntevan ennalta laitoksen järjestelmät ja toiminnot yksityiskohtaisesti.

Jokaisen työssä käsiteltävän analyysin laatimiseen voidaan arvioida käytettäväksi vähintään yksi henkilötyövuosi ja yhteensä uuden ydinvoimalaitoksen vika-analyyseihin laitoksen valmisteluvaiheessa ennen rakentamislupapäätöstä luokkaa 100 henkilötyövuotta. Vertailukohtana esimerkiksi Olkiluoto 3 -projektin työllistävyysvaikutuksen on arvioitu olevan kokonaisuudessaan yli 30 000 henkilötyövuotta ja omakotitalon rakentamisen hieman alle viisi henkilötyövuotta (TVO 2016; Rakennustutkimus RTS 2015).

Ensimmäisen PRA-mallin laatimiseen saattaa kulua kymmenen henkilötyövuotta ja työmäärä voi kolminkertaistua ennen laitoksen käynnistystä. Myös laitoksen käytön aikana PRA:n päivitykseen osallistuu jatkuvasti useita henkilöitä. Deterministiset turvallisuusanalyysit, sisältäen suunnittelun lähtökohtana pidettävien vikakriteerien analysoinnin, puolestaan voidaan laatia muutamassa henkilötyövuodessa edellyttäen, että laitoksen toimintoja kuvaava laitosmalli on tehty.

Vika-analyysimenetelmistä laajimman yksittäisen kokonaisuuden muodostavat vika- ja vaikutusanalyysit. Vika- ja vaikutusanalyysit laaditaan kaikille laitoksen turvallisuusluokitelluille prosessi- ja tukijärjestelmille ja niiden komponenteille. Esimerkiksi jo Olkiluoto 3 -laitoksen yksittäisten komponenttien analysointiin kuluu arviolta yli kymmenen henkilötyövuotta. Tämän lisäksi vika- ja vaikutusanalyysejä laaditaan myös järjestelmätasolla. Yhteisviat vaaditaan analysoitavaksi vain komponenteilta, jotka saattavat vaikuttaa turvallisuustoimintojen toteutumiseen, joten tähän kuluva työmäärä on hieman vika- ja vaikutusanalyysejä pienempi (YVL B.1, 9–10). Aiheettomien toimintojen analyysi koskee arviolta muutamia tuhansia automaatiotoimintoja. Kun huomioidaan automaation jakaminen erottelulla hallittuihin kokonaisuuksiin, alkutapahtumat ja järjestelmät, joihin toiminnot vaikuttavat, työtä lienee vähintään yhdeksi henkilötyövuodeksi.

Myös sisäisten ja ulkoisten uhkien analysointi on pienempi kokonaisuus, arviolta muutaman henkilötyövuoden kokoluokkaa.

Suunnitteluratkaisujen muuttuessa analyysejä päivitetään, jotta ne ovat jatkuvasti ajan tasalla. Päivitysten lukumäärä vaikuttaa suoraan analyysien työmäärään. Työmäärä riippuu myös siitä, voidaanko analyyseissä hyödyntää vastaavien laitosten analyysejä vai täytyykö työ aloittaa tyhjästä, jopa uusien analyysimenetelmien kehittämisestä. Analyysiin käytetty työmäärä ei kuitenkaan suoraan vaikuta analyysin tulosten merkittävyyteen tai hyödynnettävyyteen. Jos analyysiin on käytetty paljon aikaa, voi se olla merkki siitä, että analyysi on suuritöinen, tai siitä, että on tehty suunnittelumuutoksia analyysin aiempien tulosten perusteella, ja näin ollen analyysiä on jouduttu päivittämään useasti.

4.2 Deterministiset turvallisuusanalyysit

Deterministiset turvallisuusanalyysit ovat häiriöiden ja onnettomuuksien etenemistä kuvaavia ja niiden seurauksia mallintavia analyysejä, jotka perustuvat fysikaalisiin malleihin ja kokeellisiin tai yleisesti tunnettujen korrelaatioiden laskentamenetelmiin. Laitoksen käyttäytyminen mallinnetaan analyysein kattavasti alkutapahtumasta alkaen onnettomuus- tai häiriötilanteeseen ja laitoksen ajamiseen takaisin hallitun tilan kautta turvalliseen tilaan. (YVL B.3, 4–5; IAEA 2009, 8). Deterministisiä analyysejä ovat esimerkiksi termohydrauliset häiriö- ja onnettomuusanalyysit, suojarakennusanalyysit, vakaviin onnettomuuksiin liittyvät analyysit, ympäristöön ja ihmisten säteilyaltistukseen liittyvät annos- ja päästöanalyysit, kuormitusanalyysit sekä laitteiden ja rakenteiden lujuusanalyysit (STUK 2015b).

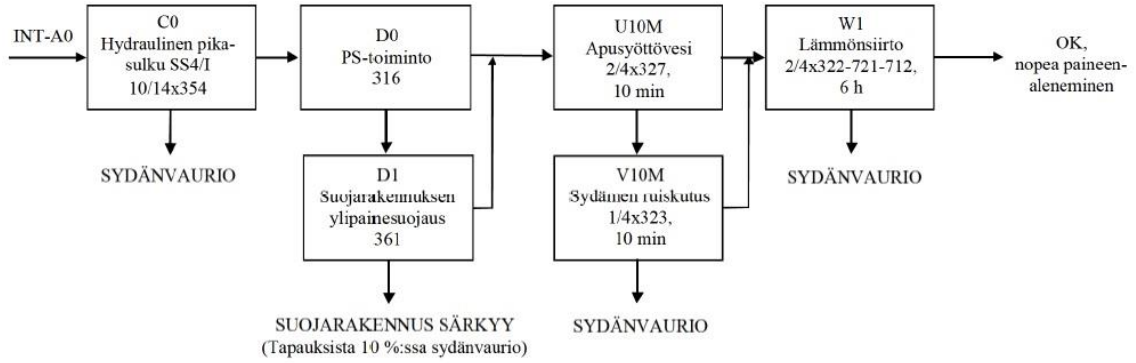
Deterministiset turvallisuusanalyysit tarkastelevat analyysikohteen ajallista ja tilariippuvaista käyttäytymistä valittujen alkutapahtumien seurauksena (IAEA 2009, 8). Analyysimenetelmät jaetaan konservatiivisiin ja parhaan arvion -menetelmiin. Konservatiivisissa analyyseissä käytettävät laskentamallit ja alkuoletukset valitaan niin, että tapahtuman seuraukset ovat hyvällä varmuudella lievempiä kuin analyysitulos osoittaa, kun taas parhaan arvion -menetelmässä alkuoletukset valitaan mahdollisimman realistisesti (YVL B.3, 12). Konservatiivisia analyysejä täydennetään herkkyystarkasteluilla, eli selvittämällä lähtötietojen ja laskentamenetelmien muutosten vaikutus laskennan lopputulokseen (Sandberg 2013, 96). Parhaan arvion -menetelmän yhteydessä laaditaan tilastomatemaattisesti perusteltavissa oleva epävarmuusanalyysi (IAEA 2009, 10–11).

Deterministisiä turvallisuusanalyysejä hyödynnetään turvallisuustoimintoja toteuttavien järjestelmien mitoituksessa ja luotettavuuden parantamisessa, esimerkiksi huoltovirheiden ja inhimillisten virheiden analysoinnissa (YVL B.3, 4). Analyyseillä osoitetaan täytetyiksi järjestelmien hyväksymiskriteerit sekä alkutapahtumiin liittyvät onnistumiskriteerit. Vika-analyysien avulla selvitetään onnistumiskriteerien täyttymiseen vaikuttavat viat.

4.2.1 PRA:n onnistumiskriteerit

Onnistumiskriteerit kuvaavat turvallisuusjärjestelmien minimijoukkoa, jonka toimintakuntoisuus vaaditaan tarkasteltavasta alkutapahtumasta selviämiseen (Ahonen 2011, 28). Onnistumiskriteerit luovat pohjan tapahtumien syy-seurausyhteyksien hahmottamiselle, ja niitä hyödynnetään vika-analyysien lähtötietoina.

Kuvassa 4.2 on esitetty Olkiluodon 1 ja 2 -laitosten *(OL1/OL2)* ison jäähdytteenmenetysonnettomuuden *(Loss Of Coolant Accident, LOCA)* onnistumiskriteerit lohkokaaviona. Kaaviossa alkutapahtumana *INT-A0* on iso LOCA, eli suojarakennuksen sisäpuolinen primääripiirin höyryvuoto, jonka vuotokohdan halkaisija on suurempi kuin 200 mm. (TVO 2010b). Laatikoiden ensimmäisellä rivillä olevat kirjain–numero-yhdistelmät *(C0, D0…)* kuvaavat kyseiseen toimintoon liittyvää vikapuuta. Vikapuita käsitellään osana todennäköisyysperusteista riskianalyysiä luvussa 4.3.1.



Kuva 4.2. *OL1/OL2-laitosten ison LOCAn onnistumiskriteerit (TVO 2010b).*

Kuvan 4.2 esimerkissä pikasulku onnistuu, jos 10/14 hydraulisesta pikasulkuryhmästä *354* toimii. Mikäli toiminto epäonnistuu, aiheutuu sydänvaurio. Tämän lisäksi PS-toiminnon lauhdutusjärjestelmän *316* tai suojarakennuksen ylipainesuojausjärjestelmän *361* on onnistuttava tehtävässään. Jos molemmat toiminnot epäonnistuvat, seurauksena on suojarakennuksen särkyminen, joka 10% todennäköisyydellä johtaa sydänvaurioon. (TVO 2010b).

Mikäli suojarakennuksen paine onnistutaan edellä kuvatuilla toimilla alentamaan hallitusti, reaktorisydämen jäähdytykseen riittää kaksi toimivaa apusyöttövesipiiriä *327* neljästä tai yksi reaktorisydämen ruiskutusjärjestelmän *323* piiri. Molemmissa tilanteissa järjestelmän toiminnan alkaminen vaaditaan 10 minuutin kuluessa alkutapahtumahetkestä. Lauhdutusaltaan jäähdyttämiseksi vaaditaan vielä kahden neljästä suojarakennuksen ruiskutusjärjestelmästä *322*, pysäytetyn reaktorin välijäähdytysjärjestelmän *721* ja pysäytetyn reaktorin merivesijärjestelmän *712* toiminnan alkaminen viimeistään kuuden tunnin kuluttua alkutapahtumahetkestä. Jäähdytykselle ei ole varmentavaa toimintoa. Alkutapahtumasta selvitään, kun lohkokaaviossa kuvattujen toimien kautta päädytään lopputilanteeseen *OK*. (TVO 2010b).

4.3 Todennäköisyysperusteinen riskianalyysi

Todennäköisyysperusteinen riskianalyysi *(Probabilistic Risk/Safety Assessment, PRA/PSA)*, on laskentamalli, joka täydentää deterministisiä turvallisuusanalyysejä tapahtumaketjujen todennäköisyyksillä. Sen tavoitteena on tunnistaa laitoksen tärkeimmät riskitekijät niin laitteita, järjestelmiä, toimintoja, alkutapahtumia kuin myös ihmisen toimintoja tarkasteltaessa. Tunnistuksen perusteella voidaan kiinnittää huomio laitoksen turvallisuuden tehokkaaseen kehittämiseen sekä suunnitteluvaiheessa että käytön aikana. (Sandberg 2013, 126, 135).

PRA koostuu kolmesta eri tasosta. Ensimmäinen taso sisältää reaktorisydämen vaurioitumiseen johtavat tapahtumaketjut ja vaurioitumisen todennäköisyyden. Ensimmäisen tason yhteydessä laitoksesta luodaan myöhempien analyysien pohjana käytettävä malli perustuen mahdollisiin polttoainevaurioon johtaviin tilanteisiin normaalien käyttötilanteiden aikana. PRA:n toinen taso sisältää laitokselta ympäristöön tapahtuvan radioaktiivisten aineiden päästön todennäköisyyden, suuruuden ja ajoittumisen. Kolmas taso sisältää radioaktiivisten aineiden päästön aiheuttamat riskit ihmisille, ympäristölle ja omaisuudelle. (Sandberg 2013, 130–131). Tason 3 PRA:a ei vaadita suomalaisilta ydinvoimalaitoksilta.

PRA:n tavoitteena on mallintaa sydänvaurioon johtavat tapahtumaketjut ja niiden todennäköisyydet sekä sydänvaurion kokonaistodennäköisyys mahdollisimman tarkasti. Mallinnus perustuu loogisiin ja fysikaalisiin malleihin: Loogisilla malleilla kuvataan sydänvaurioon johtavia tapahtumayhdistelmiä ja vikojen vaikutusten etenemistä laitosjärjestelmissä sekä näiden yhdistelmien yleisyyttä. Fysikaalisilla malleilla kuvataan onnettomuuden tai vaurioitumisen etenemistä ja onnettomuuden seurauksia. Analyysiä varten laaditaan vika- ja tapahtumapuita hyödyntäen vika-analyysien tuloksia ja muita tunnettuja tietoja muun muassa laitoksen suunnittelusta, käytöstä, käyttöhistoriasta, komponenttien luotettavuudesta, ihmisen toimenpiteiden luotettavuudesta, sydämen vaurioitumisen fysikaalisesta kehittymisestä, radioaktiivisten aineiden käyttäytymisestä ja mahdollisista terveys- ja ympäristöhaitoista. (Sandberg 2013, 128).

PRA-laskennan tuloksena tunnistetaan todennäköisimmät vakaviin onnettomuuksiin johtavat minimikatkosjoukot. Katkosjoukko on komponentti- tai laitevikojen yhdistelmä, josta seuraa järjestelmän toimimattomuus. Minimikatkosjoukko on lyhin komponenttivikojen yhdistelmä, joka johtaa huipputapahtumaan *(Top Event)*, eli järjestelmän vioittumiseen tai vaaratilanteeseen. Jos minimikatkosjoukosta yksikin komponentti vaihdetaan toimivaksi, ei katkosjoukko enää johda järjestelmän vikaantumiseen. (Ervamaa 1979, 31, 132). Järjestelmän luotettavuutta parannettaessa huomio tulee kiinnittää ennen kaikkea minimikatkosjoukkoihin ja näihin kuuluvien toimintojen varmentamiseen. Minimikatkosjoukoista tunnistetaan herkkyys- ja epävarmuusanalyysit huomioiden riskin kannalta merkittävimmät alkutapahtumat, turvallisuustoiminnot ja järjestelmät. Harvinaiset sääilmiöt ja muut ulkoiset tekijät, kuten tulipalot, aiheuttavat lähtötie-

toihin epävarmuutta. Epävarmuustekijöitä liittyy myös sydänvaurion kehittymiseen, sulan sydämen käyttäytymiseen ja fissiotuotteiden kulkeutumiseen ja käyttäytymiseen. (Sandberg 2013, 127–135).

PRA:a hyödynnetään ydinvoimalaitoksen suunnittelussa ja kehitettäessä sen käyttötoimintaa ja teknisiä ratkaisuja. Suunnitteluvaiheen PRA toimii riskiarviona ydinvoimalaitoksen sisäisille ja ulkoisille alkutapahtumille. Suunnitteluvaiheen PRA:n avulla arvioidaan järjestelmien ja tukijärjestelmien välisiä kytkentöjä, vuorovaikutuksia ja yhteisiä vianaiheuttajia niin toiminto-, järjestelmä- kuin laitetasollakin, jotta laitoksen turvallisuus voidaan suunnitella vaaditulle tasolle. Laitoksen käytön aikana PRA:a käytetään laitoksen käytön turvallisuutta koskevien päätösten tukena ja osana turvallisuuden valvontaa. PRA:a hyödynnetään esimerkiksi laitoksen turvallisuuteen liittyvien tarkastusten, ohjeistomuutosten, huoltotoiminnan, koulutusten ja laitosmuutosten suunnittelussa. (Sandberg 2013, 135–137).

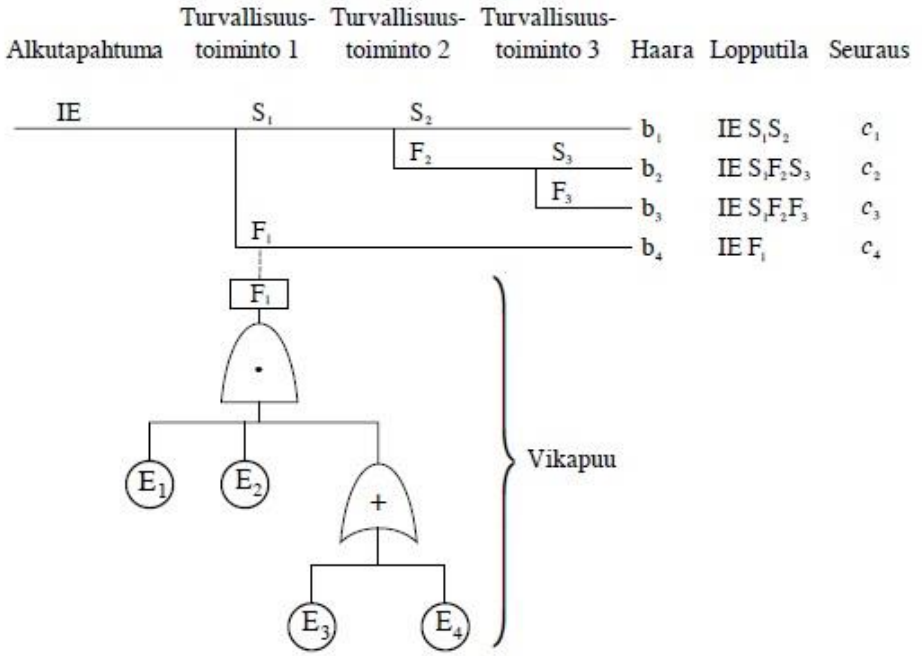
4.3.1 Tapahtuma- ja vikapuut

Tapahtumapuulla määritetään systemaattisesti aikajärjestyksessä tietystä alkutapahtumasta lähtevät tapahtumaketjut loogisen kaavion avulla. Tapahtumapuun laatiminen aloitetaan alkutapahtuman valinnasta. Alkutapahtumasta alkaa onnistumiskriteerien mukainen tapahtumaketju, jonka yksittäiset toiminnot joko onnistuvat tai epäonnistuvat. Vikaantumistodennäköisyyksien avulla voidaan ratkaista todennäköisyys ja riski alkutapahtuman eri seurauksille. (Ervamaa 1979, 141–142). Usein tapahtumien estämiseen käytetyt turvallisuustoiminnot ovat riippuvaisia toisistaan tai keskenään samoista järjestelmistä, jolloin onnettomuusketjuista on muodostettava yksi vikapuu, joka ratkaistaan minimikatkosjoukkojen avulla.

Kuvan 4.3 yläosassa on havainnollistava esimerkki yksinkertaisesta tapahtumapuusta. Alkutapahtuman *IE* etenemistä torjutaan peräkkäisillä turvallisuustoiminnoilla, joita mallinnetaan tapahtumapuun haarautumiskohtina, toiminnon onnistumisena S_1 ... S_3 tai epäonnistumisena F_1 ... F_3. Haarautumistodennäköisyydet, eli tarkasteltavan turvallisuustoiminnon onnistumisen tai epäonnistumisen todennäköisyydet voidaan arvioida hyödyntäen vikapuita. Tapahtumapuussa syntyy haarat b_1 ... b_4, jotka johtavat seurauksiin c_1 ... c_4. Tapahtumapuiden avulla voidaan ratkaista monimutkaistenkin tapahtumaketjujen eteneminen sekä alkutapahtuman ja yksittäisen vikaantumisen E_1 ... E_4 välinen yhteys.

Kuva 4.3 havainnollistaa vikapuun ja tapahtumapuun yhden haarautumiskohdan välistä yhteyttä. Vikapuu on järjestelmän vikatilaa kuvaava Boolen algebraa hyödyntävä looginen malli, joka kuvaa järjestelmävikaan johtavia vikayhdistelmiä. (Vaurio 2006, 105). Vikapuuanalyysissä laaditaan looginen kaavio siitä, kuinka järjestelmän osien E_1 ... E_4 vikaantuminen johtaa huipputapahtumaan, kuvan esimerkissä 1. turvallisuustoiminnon

epäonnistumiseen F_1. (Ervamaa 1979, 130–132). Järjestelmän osat yhdistetään toisiinsa loogisilla porteilla, joista •-merkki kuvaa JA-porttia ja +-merkki TAI-porttia.



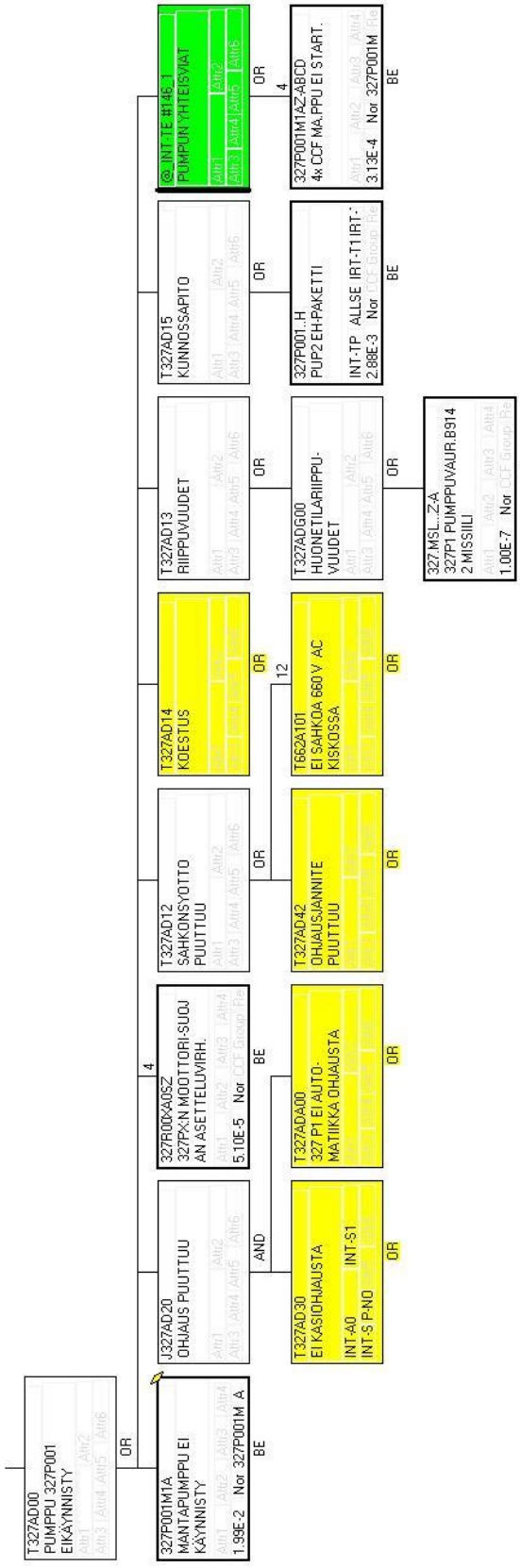
Kuva 4.3. *Tapahtumapuun ja vikapuun välinen yhteys (Laitonen 2010, 26).*

Vikapuun laatiminen alkaa tarkasteltavan järjestelmän määrittelyllä ja käsiteltävien huipputapahtumien valinnalla. Kullekin huipputapahtumalle laaditaan oma vikapuunsa. Valinnan jälkeen selvitetään, mitkä tapahtumat tai tapahtumayhdistelmät voivat kyseisen huipputapahtuman aiheuttaa. Huipputapahtuman aiheuttajat, perustapahtumat, selvitetään vikaantumisketjujen avulla niin pitkälle kuin on tarpeellista. Usein perustapahtumat ovat esimerkiksi järjestelmään kuuluvien komponenttien vikaantumisia, joiden vikaantumistodennäköisyys tunnetaan. (Ervamaa 1979, 131–133). Vikapuiden laadinta edellyttää sekä täsmällistä järjestelmän tuntemusta sekä luotettavuustekniikan osaamista.

Vikapuu on kvalitatiivinen kuvaus järjestelmän vikaantumisen perussyistä, jonka tavoitteena on löytää järjestelmän heikot kohdat ja merkittävät vikayhdistelmät. Vikapuun avulla voidaan laskea järjestelmän vikaantumisen todennäköisyys, kun perustapahtumien esiintymistodennäköisyys on tiedossa. Huipputapahtuman todennäköisyys saadaan ratkaisemalla kaikki huipputapahtumaan johtavat vikapuun haarat. (Ervamaa 1979, 133–134).

Ydinvoimalaitosten tapahtuma- ja vikapuita laaditaan näihin tarkoitetuilla tietokoneohjelmilla. Kuvassa 4.4 on esimerkki FinPSA-ohjelmalla laaditun vikapuun yksittäisen mäntäpumpun ”ei käynnisty”- vioittumistavan portista. Useimmat portin haarat eli vikaantumiseen johtavat syyt on selvitetty vika- ja vaikutusanalyysin avulla. Vihreän haa-

ran kuvaamat ”pumpun yhteisviat” huomioidaan vikapuussa yhteisvika-analyysin perusteella. Vikapuun keltaiset haarat ovat esimerkkiä varten katkaistuja.



Kuva 4.4. *Vikapuun portti ”Mäntäpumppu ei käynnisty”. (STUK 2015c).*

5. VIKA-ANALYYSIMENETELMIÄ

Vika-analyysit ovat selvityksiä, joilla kartoitetaan, tunnistetaan ja mallinnetaan onnettomuuksien ja tapaturmien syntyyn ja etenemiseen vaikuttavia tekijöitä ja näiden seurauksia. Yksittäiset menetelmät vastaavat eri tarpeisiin ja etenkin monimutkaisten järjestelmien ja toimintojen analysoinnissa haluttuun lopputulokseen pääsemiseksi on yhdisteltävä useita menetelmiä tavoitteesta ja tarkasteltavasta kohteesta riippuen. Vika-analyysimenetelmien tavoite vaihtelee vikaantumisen syiden tunnistamisesta vian seurausten tai tarkasteltavan kohteen vikasietoisuuden määrittämiseen. Analyysit tuottavat erilaisia tuloksia riippuen käytetyistä menetelmistä, tarkasteltavasta kohteesta, analyysin ja analysoitavan kohteen laajuudesta sekä suunnitteluprosessin vaiheesta, johon analyysi sijoittuu.

Analysoitava kohde, analyysin tavoite ja saatavilla oleva aineisto vaikuttavat analyysin yksityiskohtaisuuteen. Esimerkiksi suunnittelun alkuvaiheessa suoritettavat analyysit on syytä tehdä ensin karkealla tasolla ja suunnittelun edetessä lisätä analyyseissä huomioitavia yksityiskohtia. Analyysit voivat olla luonteeltaan kvalitatiivisia tai kvantitatiivisia. Usein analysointi aloitetaan laadullisella eli kvalitatiivisella, tekijän näkemykseen perustuvalla, vaarojen ja onnettomuustekijöiden tutkimisella ja luokittelulla. Analyysit voidaan toteuttaa induktiivisesti eli aineistolähtöisesti, jolloin tarkoituksena on muodostaa yksittäisistä havainnoista yleistys tai teoria tai deduktiivisesti, jolloin analyysi etenee tunnetusta teoriasta kohti yksittäistapauksia. Kvantitatiiviset eli määrälliset, tilasto- ja historiatietoihin perustuvat onnettomuuksien mallintamiset ja niiden seurausten ja taajuuden arvioinnit täydentävät kvalitatiivisia analyysejä. (Palukka 2008, 2–3).

Tässä luvussa esitellään erilaisten suomalaisilla ydinvoimalaitoksilla käytettyjen vika-analyysimenetelmien käyttötarkoituksia ja toteutustapoja. Kattavassa analyysikokonaisuudessa hyödynnetään useita menetelmiä toistensa tukena. Vaikka osa analyyseistä voidaan asettaa selvästi etenemisjärjestykseen, usein menetelmiä käytetään toistensa kanssa rinnakkain. Ydinvoimalaitosten analysointiin käytettävät menetelmät eivät rajoitu tässä luvussa esitettyihin menetelmiin, vaan esitetyt menetelmät ovat esimerkkejä eräistä käytetyistä analyyseistä.

5.1 Vika- ja vaikutusanalyysi

VVA eli vika- ja vaikutusanalyysi *(Failure Mode and Effect Analysis, FMEA)* on luonteeltaan kvalitatiivinen, systemaattinen menetelmä, jolla tunnistetaan yksittäisiä laite- ja materiaalivikoja sekä niiden syitä ja seurauksia. VVA:n tarkoituksena on löytää tarkasteltavan järjestelmän tai komponentin kaikki mahdolliset vioittumistavat ja tunnistaa

näihin johtavat syyt ja niiden vaikutukset tarkasteltavan kohteen toimintaan. Perinteisessä VVA:ssa tarkastellaan järjestelmiä tai komponentteja toisistaan riippumattomina – muiden paitsi tarkasteltavan kohteen oletetaan toimivan normaalisti. (Ervamaa 1979, 105–114). Analyysi voi kuitenkin olla tarpeen tehdä myös vikatilannekohtaisesti huomioiden järjestelmän toimintaan vaikuttavat muiden järjestelmien vikaantumiset.

Vika- ja vaikutusanalyysit laaditaan järjestelmäkohtaisesti kaikille turvallisuusluokitelluille järjestelmille huomioiden niihin kuuluvat laitteet, komponentit ja tukijärjestelmät. Analyysi kattaa tarkasteltavan järjestelmän toimintaan vaikuttavat yksittäis- ja seurausviat huomioiden laitoksen eri käyttötilanteet. Analyysiä hyödynnetään suunnittelun alkuvaiheessa ja se muodostaa pohjan kvantitatiivisille luotettavuus- ja käytettävyysanalyyseille. (Ervamaa 1979, 105–114).

Analyysin toteutus

Ennen analyysin aloittamista määritellään analysoitava kohde, kuvataan järjestelmän tai laitteen toiminta ja ympäristöolosuhteet. Varsinainen analyysi aloitetaan selvittämällä tarkasteltavien komponenttien mahdolliset vioittumisen syyt tyyppivikataulukoiden tai komponenttikohtaisen vika- ja vaikutusanalyysin avulla. Tämän jälkeen täytetään esimerkiksi taulukon 5.1 mukainen taulukko kaikista järjestelmään kuuluvista komponenteista ja niiden vioittumistavoista. Taulukossa 5.1 esitetään vain yhden komponentin *(mäntäpumppu)* yksi vioittumistapa *(ei käynnisty)*.

Taulukko 5.1. *Vika- ja vaikutusanalyysi -taulukko. Muokattu lähteestä (TVO 2008).*

VVA **Järjestelmä:** Apusyöttövesijärjestelmä				
KOMPONENTTI	**VIKA**			
	VIOITTUMISTAPA	**SYY**	**VAIKUTUKSET**	**PALJASTUMISTAPA**
Mäntäpumppu	Ei käynnisty	**1** Ohjaus puuttuu **2** Mekaaninen vika; esim. kiilahihnat viallisia, venttiilit viallisia **3** Sähkönsyöttö puuttuu **4** Riippuvuudet **5** Koestus/ kunnossapito	Ei vettä reaktoriin	Kontaktorin/katkaisijan asennon osoitus. Amperimittarin näyttö. **2** Viallisista kiilahihnoista ei tule tietoa valvomoon, koska kierroslukuvahti on moottorin akselilla. **3A** Tyyppivikahälytys F3 (Kytkinlaitosvika) tulee ylivirrasta. **3B** 662 A101 kiskosta alijännitehälytys. **3C** Kytkinlaitoksen ohjausjännitteen suojakytkimen laukeamisesta hälytys. **3D** Jos ALG-katkaisijan jousi ei virity, tulee tyyppivikahälytys F3 (Kytkinlaitosvika). **3E** Elektroniikkajännitteen puuttuessa tulee tyyppivikahälytys F1 (24V suojakytkin lauennut).

Taulukon ensimmäiseen sarakkeeseen listataan analysoitavan järjestelmän komponentit ja sen tekniset tiedot, joilla on analyysin kannalta merkitystä. Toiseen sarakkeeseen kerätään kaikki mahdolliset vioittumistavat ja seuraavaan sarakkeeseen selvitetyt mahdolliset vikaantumisen syyt. Mahdollisia syitä voivat olla esimerkiksi satunnaisviat, suunnitteluvirheet, ympäristötekijät (esimerkiksi lämpötila tai kosteus) tai huoltovirheet. Neljänteen sarakkeeseen kirjataan kunkin vioittumistavan välittömät seuraukset ja mahdollisesti omaan sarakkeeseensa vian aiheuttamat vaikutukset koko järjestelmän toimintaan. Seuraavaan sarakkeeseen merkitään tapa, jolla vika paljastuu – esimerkiksi merkkivalo tai määräaikaiskoestus. Taulukkoon voidaan lisätä oma sarake käytetyille oletuksille, kommenteille ja muille huomioille, kuten vikapuumallintamiseen liittyville tiedoille. (Ervamaa 1979, 109–110). Analyysissä hyödynnetään analyysiryhmän asiantuntemuksen lisäksi analysoitavan kohteen piirustuksia, valokuvia, tilastoja ja standardeja (Palukka 2008, 45).

VVA toimii merkittävänä lähtötietona laitteiden vikapuiden laatimisessa. Taulukon 5.1 mäntäpumpun ”ei käynnisty”-vikaa kuvaava vikapuu esitettiin luvun 4.3.1 kuvassa 4.4. Jokainen VVA:ssa löydetty vikaantumisen syy luo vikapuuhun oman haaransa.

5.2 Aiheettomien toimintojen analyysi

Ohjelmistopohjaisen automaation lisääntyneestä käytöstä on ydinenergia-alalle syntynyt tarve kehittää aktiivisten vikojen analyysimenetelmiään. Ohjelmistopohjainen automaatiojärjestelmä voi ohjata samanaikaisesti useita eri toimintoja ja laitteita, jolloin yksittäisen vian vaikutukset voivat levitä laajalle vaikeuttaen vian tarkastelua. Väärien ja aiheettomien toimintojen analyysissä oleellista on huomioida toiminnon seuraukset käsiteltävää järjestelmäkokonaisuutta laajemmin koko laitostasolla.

Aiheettomien toimintojen analyysin tavoitteena on tunnistaa erottelulla hallittujen automaatiokokonaisuuksien väärät ja aiheettomat toiminnot ja niiden seuraukset. Erottelulla hallittua kokonaisuutta nimitetään jatkossa entiteetiksi, joka ei kuitenkaan ole alalla vakiintunut termi. Entiteetillä tarkoitetaan tarkasteltavaa kohdetta, jota kyseisessä tilanteessa voidaan pitää yhtenä, muista entiteeteistä erotettuna kokonaisuutena. Entiteetit määritetään niin, että tarkastelun kannalta merkittävä tiedonvaihto ja vikaantumisvaikutukset rajoittuvat niiden rajapintoihin. Merkittävän ja merkityksettömän tiedonvaihdon rajaamiseksi ei kuitenkaan ole määritelty yleisiä kriteereitä tai menetelmiä. Kohteesta riippuen entiteetin voi muodostaa esimerkiksi yksi automaatiojärjestelmä, useat automaatiojärjestelmät, joiden välillä on tiedonvaihtoa tai kaikki samaan automaatioalustaan kuuluvat järjestelmät. Myös järjestelmää pienempi kokonaisuus voi muodostaa oman entiteettinsä: entiteetti voi koostua esimerkiksi vain yhdestä prosessikortista, jonka toteuttamien toimintojen erillisyyttä kortin sisällä on vaikea osoittaa. Entiteettien määrittäminen ei ole yksiselitteistä ja vaatii tarkasteltavan laitoksen sekä prosessi- että automaatiojärjestelmien tuntemusta. (Suikkanen 2015).

Virheellisten toimintojen vaikutukset laitoksen turvallisuudelle selvitetään määritettyjen entiteettien avulla. Analyysi kattaa kaikki entiteettiin kohdistuvat aktiiviset viat tarkasteltavan entiteetin laajuudessa. Analyysillä tunnistetaan entiteetin pahin mahdollinen vikaantuminen ja siihen liittyvät seurausviat. Pahinta vikaantumismahdollisuutta pyritään mahdollisuuksien mukaan pienentämään suunnitteluratkaisuilla.

Aiheettomien toimintojen analyysin yhteydessä tulee huomioida myös ohjausten priorisointi. Priorisoinnilla voidaan määrittää, minkä automaatiojärjestelmän ohjaukset laite toteuttaa. Prioriteetiltaan korkeamman automaatiojärjestelmän tulee tarvittaessa voida kumota alemman prioriteetin automaatiojärjestelmän virheelliset ohjaukset.

Automaation analysointi prosessijärjestelmistä irrallaan ei riitä, vaan virheellisen tai aiheettoman toiminnon vaikutukset laitoksen turvallisuudelle on selvitettävä. Tämän vuoksi analyysissä huomioidaan automaation vikaantumisen aiheuttamat mahdolliset seuraukset tarkasteltavan entiteetin ohjaamille prosessijärjestelmille ja entiteettien rajapintojen kautta muihin automaatiojärjestelmiin.

Analyysin toteutus

Aiheettomien toimintojen analysoinnille ei ole ydinenergia-alalla vakiintuneita menetelmiä. Tässä luvussa esitetään kuvaus eräänlaisesta menetelmästä, jolla entiteetit ja niiden pahimmat mahdolliset vikaantumiset voidaan määrittää. Menetelmä etenee seuraavien vaiheiden mukaisesti:

1. Määritetään entiteetti.
2. Määritetään ja kuvataan entiteetin yksittäiset automaatiotoiminnot ja niiden aikaansaamat vaikutukset.
3. Ryhmitellään automaatiotoiminnot niiden vaikutusten perusteella. Ryhmittelyssä hyödynnetään esimerkiksi turvallisuuden kannalta merkittäviä laitosparametreja.
4. Kiinnitetään huomio laitoksen turvallisuuden kannalta oleellisiin vaikutuksiin.
5. Huomioidaan sekä passiiviset että aktiiviset vikaantumistavat.
6. Määritetään vaikutusten laitosvaste ja ryhmitellään samanlaiset vasteet.
7. Arvioidaan entiteetin useiden aiheettomien toimintojen seuraukset ja tunnistetaan pahin mahdollinen vikaantuminen.
8. Arvioidaan seuraukset myös alkutapahtumien yhteydessä. Alkutapahtumia voidaan ryhmitellä niiden käsittelyn helpottamiseksi.
9. Tarkastellaan, kattavatko olemassa olevat analyysit kohdassa 8 tunnistetut tilanteet; jos ei, laaditaan tarvittavat termohydrauliset tai muut vastaavat analyysit.
10. Verrataan analyysituloksia hyväksymiskriteereihin. (Suikkanen 2015).

Kohdissa 2–5 käsitellään yhtä automaatiotoimintoa kerrallaan. Näiden kohtien tuloksia voidaan hyödyntää jo sellaisenaan deterministisen turvallisuusanalyysien syötteenä. Analyysin tuloksena tunnistettua entiteetin pahinta mahdollista vikaantumista pienennetään tarvittaessa muuttamalla laitos- tai automaatiosuunnittelua havaittujen tarpeiden

mukaisesti. Muutosten jälkeen analyysi toistetaan. Tätä jatketaan niin kauan, kunnes pahin mahdollinen vikaantuminen on hyväksyttävissä rajoissa.

5.2.1 Poikkeamatarkastelu

Poikkeamatarkastelu *(Hazard and Operability Study, HAZOP)* on prosessiteollisuudessa käytetyin järjestelmien vaaratekijöiden tunnistusmenetelmä. Poikkeamatarkastelussa etsitään systemaattisesti järjestelmään häiriöitä tai vaaraa aiheuttavia toimintaparametrien muutoksia, niiden syitä ja seurauksia. (Vaurio 2006, 119). Ydinvoimalaitosten turvallisuustoimintojen analysoinnissa ei hyödynnetä suoraan poikkeamatarkastelua, mutta yllä luvussa 5.2 esitelty automaation aiheettomien toimintojen analyysi muistuttaa poikkeamatarkastelua.

Poikkeamatarkastelu laaditaan laitekokonaisuuskohtaisesti. Analyysillä tunnistetaan yksittäisiä laitteeseen liittyvien prosessisuureiden poikkeamia, jotka saattavat aiheuttaa esimerkiksi laitevian. Monimutkaisista järjestelmistä tehdään yksinkertaistettuja malleja, mikä vaikeuttaa vaaratekijöiden yksityiskohtaista tunnistamista (Fieandt 1983, 20–21). Poikkeamatarkastelua voidaan hyödyntää sekä laitoksen suunnittelu- että käyttövaiheessa teknisiin järjestelmiin, joiden häiriöt tyypillisesti näkyvät toimintaparametrien muutoksina. Suunnittelun lisäksi analyysiä voidaan hyödyntää esimerkiksi henkilökunnan koulutuksessa. (Fieandt 1983, 8–10).

Analyysin toteutus

Tarkasteltava järjestelmä jaetaan kemiallisten tai fysikaalisten toimintaprosessien mukaisiin laitteisiin tai laitekokonaisuuksiin, joiden prosessisuureita tarkastellaan yksitellen esimerkiksi prosessi-, instrumentointi- tai virtauskaavioiden avulla (Fieandt 1983, 8). Tarkasteltavia prosessisuureita ovat esimerkiksi virtaus, lämpötila, paine ja kemiallinen koostumus. Analyysissä tarkasteltavaan suureeseen liitetään avainsana, kuten ”vähemmän” tai ”enemmän”, jolloin syntyy poikkeama, jonka vaikutukset järjestelmään arvioidaan. Avainsanan ja prosessisuureen yhdistelmistä tarkasteltaviksi poikkeamiksi muodostuu esimerkiksi ”enemmän painetta”, ”päinvastainen virtaus” tai ”alhaisempi lämpötila” verrattuna normaalitilaan. (Palukka 2008, 23–25).

Tyypillisesti analyysistä laaditaan taulukko, jossa luetellaan avainsanat, niihin liittyvät poikkeamat, poikkeamiin johtavat syyt ja niiden aiheuttamat seuraukset. Analyysin pohjalta laaditaan parannustoimenpiteitä, jotka ensisijaisesti tähtäävät poikkeaman estämiseen. (Palukka 2008, 23–25).

5.3 Vikakriteerien analyysi (N+1, N+2 -analyysi)

Ydinvoima-alalla käytetään erillisiä analyysejä osoittamaan, onko turvallisuustoiminnon toteutukseen suunniteltu riittävä määrä rinnakkaisia järjestelmiä tai osajärjestelmiä niin,

että toiminnolta vaadittu vikasietoisuus täyttyy. Analyysejä voidaan kutsua vikakriteerianalyyseiksi tai N+1, N+2 -analyyseiksi. Vikasietoisuutta ja vikakriteerejä on käsitelty luvussa 3.3.2.

Analyyseillä varmistetaan, että turvallisuustoimintovaade voidaan tarvittaessa täyttää, vaikka osa toimintoon kuuluvista järjestelmistä tai osajärjestelmistä olisi tarvehetkellä käyttökunnottomia. Tavoitteena on tunnistaa, voidaanko saman turvallisuustoiminnon toteuttavia toimintoketjuja menettää yhtäaikaisesti yksittäisvioista ja alkutapahtumista syntyneistä seurausvioista johtuen. Lisäksi kartoitetaan, tehdäänkö järjestelmille ennakkohuoltoja tai korjauksia, joiden vuoksi osajärjestelmät eivät ole jatkuvasti käytettävissä. Kun tiedossa on, kuinka monta rinnakkaista osajärjestelmää vaaditaan toiminnon toteuttamiseen, saadaan analyysin tuloksena selville, riittääkö suunniteltu kapasiteetti toiminnon toteuttamiseen.

Analyysin toteutus

Analyysi laaditaan alkutapahtumakohtaisesti jokaiselle turvallisuustoiminnolle, esimerkiksi taulukossa 5.2 esitetyllä tavalla. Taulukkoon kirjataan kaikki turvallisuustavoitteet ja niitä toteuttavat toiminnot ja järjestelmät. Jokaisen turvallisuusjärjestelmän kohdalle taulukkoon kerätään tiedot siitä, tarvitaanko kyseistä toimintoa tarkasteltavan alkutapahtuman yhteydessä ja kuinka moninkertaisena järjestelmä on toteutettu *(Kapasiteetti (%))*. Tämän jälkeen taulukkoon kirjataan esimerkkirivin mukaisesti, voiko järjestelmä vikaantua alkutapahtuman seurauksena, yksittäisviasta tai voiko se olla huollon vuoksi käyttökunnottomana. Tietojen avulla selvitetään, mikä on jäljelle jäävä kapasiteetti, jos järjestelmässä ilmenee yhtä aikaa useita mahdollisia vikatyyppejä. Järjestelmiä, jotka eivät osallistu kyseisestä alkutapahtumasta selviämiseen, ei tarvitse analysoida. (Areva 2004b, liite 1).

Taulukko 5.2. *N+1, N+2 -analyysitaulukko.*

TAPAHTUMA: *Esimerkki*

Turvallisuus-tavoite	**Turvallisuus-toiminto**	**Turvallisuusjär-jestelmä**	**Järjestelmä vaaditaan**	**Kapasiteetti (%)**	**Seurausvika**	**Yksittäisvika**	**Huolto**	**Jäljelle jäävä kapasiteetti (%)**
Esimerkki	*Esimerkki*	*Esimerkki*	***x***	*3x 100*	*-*	*x*	*x*	***100***
Reaktiivisuuden hallinta	Sammutus	Säätösauvat	x					
	Kriittisyyden-hallinta	Lisävesi- ja ulos-lasku	-					
		Booraus	x					
		Hätäruiskutus	-					

Taulukko 5.2 on esimerkki suunnittelun alkuvaiheen analyysistä, jolla osoitetaan, että suunnitelluilla järjestelmillä voidaan vastata vikasietoisuusvaatimuksiin. Samat toiminnot analysoidaan uudelleen täsmällisemmin, kun toimintoja toteuttavat järjestelmät, laitteet ja komponentit on suunniteltu. Täsmällisemmässä analyysissä huomioidaan esimerkiksi järjestelmien sisäinen osajärjestelmien moninkertaisuus sekä yhteisvian mahdollisuus.

5.4 Yhteisvika-analyysi

Turvallisuustoimintoja toteuttavien kahden tai useamman osajärjestelmän yhteisvian välttämiseksi laaditaan erillisiä yhteisvika-analyysejä. Erilaisen arkkitehtuurin ja käyttötavan vuoksi yhteisvika-analyysit toteutetaan erikseen prosessijärjestelmille, sähköjärjestelmille sekä automaatiojärjestelmille. Yhteisvika-analyysien tavoitteena on tunnistaa osajärjestelmien tai rinnakkaisten järjestelmien yhteisvikamahdollisuudet.

Yhteisvikamahdollisuuksien analysointia varten selvitetään alkutapahtumakohtaisesti turvallisuustoimintojen toteutuminen, huomioiden niitä toteuttavien järjestelmien erilaisuus- ja moninkertaisuusperiaatteet. Analyysi kohdistuu turvallisuustoimintoihin, jotka voidaan toteuttaa kahdella tai useammalla rinnakkaisella toimintoketjulla tai yksittäinen toimintoketju sisältää rinnakkaisia, toisiaan varmentavia järjestelmiä. Tavoitteena on tunnistaa toimintoketjujen väliset yhteisviat, joiden seurauksena koko toiminnon toteutuminen vaarantuu.

Mikään yksittäisen ydinvoimalaitoksen laitetyypin yhteisvika ei saa johtaa tilanteeseen, jossa laitosta ei voida ajaa hallittuun tilaan ja siitä edelleen turvalliseen tilaan (YVL B.1, 9). Analyysin erityishuomio kiinnitetään aktiivisiin komponentteihin, joiden tulee onnettomuustilanteessa vaihtaa tilaansa tai pysyä käynnissä. Passiivisten komponenttien kohdalla tulee varmistaa, että onnettomuustilanteessa komponentin tila on oikea.

Analyysin toteutus

Yhteisvikamahdollisuudet toimintoketjujen välillä tunnistetaan esimerkiksi laatimalla järjestelmälliset rinnakkaiset listat turvallisuustoiminnon toteutukseen osallistuvista osajärjestelmistä. Jokainen turvallisuustoiminto tarkastellaan erikseen. (Areva 2014c). Rinnakkaisia listoja vertaamalla voidaan tunnistaa järjestelmät, joita käytetään molemmissa toimintoketjuissa, saman tyyppiset komponentit sekä riippuvuudet esimerkiksi yhteisistä tukijärjestelmistä. Tunnistettujen yhteneväisyyksien kohdalla tarkastellaan erikseen, onko yhteisen järjestelmän sisällä riittävää moninkertaisuutta ja erilaisuutta, tai onko järjestelmä sellainen, jonka toimimattomuus ei estä koko toiminnon toteuttamista.

5.5 Alkutapahtuma-analyysit

Alkutapahtuma-analyyseillä tarkoitetaan alkutapahtumien tunnistamista ja alkutapahtumien seurausvaikutusten eli alkutapahtumariippuvuuksien määrittämistä. Analyysin ensimmäisen osan tarkoituksena on tunnistaa kattava joukko mahdollisten häiriöiden tai onnettomuuksien aiheuttajia. Tämän jälkeen määritetään laitteet, järjestelmät ja rakenteet, joiden toimintaan kyseinen alkutapahtuma vaikuttaa. Todennäköisyysperusteisessa riskianalyysissä näitä kutsutaan alkutapahtumariippuvuuksiksi. Alkutapahtumariippuvuuksia hyödynnetään esimerkiksi alkutapahtumassa tarpeellisten turvallisuustoimintojen vikojen tunnistamisessa. Alkutapahtuma-analyyseissä yhdistyy sekä deterministisiä että todennäköisyyspohjaisia piirteitä. Muut vika-analyysit perustuvat usein alkutapahtuma-analyyseihin.

Analyysin toteutus

Alkutapahtumia tunnistetaan historiatiedon, käyttökokemusten, tehtyjen vaaratilannekartoitusten ja tehtyjen vika-analyysien perusteella. Laitoskohtaisten alkutapahtumien tunnistamisessa hyödynnetään myös Kansainvälisen atomienergiajärjestön *(International Atomic Energy Agency, IAEA)* laatimia alkutapahtumaluetteloja (IAEA 1993). Tarkoituksena on löytää laitoksen turvallisuuden vaarantavia vikaantumismahdollisuuksia, jotka aiheuttavat turvallisuustoimintovaateen. Samalla ne saattavat estää turvallisuustoiminnon suorittamisen.

Käsiteltävien alkutapahtumien määrän hallitsemiseksi alkutapahtumat ryhmitellään ja niitä voidaan yhdistellä, mikäli ne edellyttävät samojen järjestelmien toimintaa tai ne voidaan sisällyttää toiseen alkutapahtumaan, jolla on vastaavat seuraukset (Fortum 2014). Alkutapahtumat ryhmitellään jäähdytteenmenetysonnettomuuksiin *(Loss Of Coolant Accident, LOCA)*, häiriötapahtumiin *(Transient)* ja yhteisvika-alkutapahtumiin *(Common Cause Initiator, CCI)* (IAEA 1993, 18). Tämä ryhmittely ei huomioi kattavasti uusien, digitaalisten laitosten automaatiojärjestelmien aiheuttamia, useaan toimintoon yhtä aikaa vaikuttavia aktiivisia vikoja. Digitaalisen automaation aiheuttamat aktiiviset viat luovat oman alkutapahtuma-ryhmän ja ne tulee analysoida erikseen.

Tunnistetuille alkutapahtumille määritetään esiintymistaajuudet hyödyntäen tilastollisia analyysejä. Taajuuden määrittämiseen käytettävät menetelmät riippuvat alkutapahtuman tyypistä: määrittäminen voi perustua analysoitavan sekä samankaltaisten laitosten käyttökokemuksiin ja historiatietoihin, kirjallisuuteen tai laitteiden valmistustietoihin perustuviin laskuihin. Laitoksen ulkoisia alkutapahtumia arvioidaan esimerkiksi säätilastojen avulla. (TVO 2011b).

Tunnistetuille alkutapahtumille määritetään laitteet, järjestelmät ja rakenteet, joiden toimintaan kyseinen alkutapahtuma vaikuttaa. Tällainen seurausvika voi syntyä toiminnallisista riippuvuuksista tai ympäristövaikutuksista. Lisäksi tavoitteena on tunnistaa

laitteet, joiden suojaus alkutapahtumaa vastaan on olennaista järjestelmän toiminnan kannalta. (STUK 2015a, 6).

5.5.1 Sisäisten uhkien analyysit

Sisäiset uhat ovat laitoksen sisällä esiintyviä tapahtumia, jotka voivat vaikuttaa haitallisesti laitoksen turvallisuuteen tai käyttöön (YVL B.1, 42). Tyypillistä on, että sisäisten uhkien aiheuttamat suorat vaikutukset rajoittuvat laitoksen tiettyyn fyysiseen osaan, mutta seurausvaikutukset voivat levitä koko laitoksen laajuuteen. Muun muassa palo-, tulva- ja missiilialkutapahtumat ovat sisäisiä uhkia (YVL B.7, 8). Missiilillä tarkoitetaan laitteista irtoavia lentäviä osia, jotka voivat rikkoa muita laitteita. Analyyseillä tunnistetaan, mitkä laitteet vikaantuvat ja osoitetaan, että laitoksen turvallisuustoimintojen luotettavuus ei vaarannu, minkä tahansa mahdolliseksi arvioidun sisäisen uhan seurauksena.

Sisäisten uhkien analyysissä tarkastellaan laitosarkkitehtuuria kaikilla puolustustasoilla. Tunnistetut sisäiset uhat huomioidaan alkutapahtumien aiheuttajina. Sisäisiin uhkiin varaudutaan esimerkiksi laitoksen tila- ja sijoitussuunnittelulla *(layout-suunnittelulla)* ja laitteiden ja rakenteiden lujuusteknisellä mitoituksella (YVL B.7, 6–7). Sisäisten uhkien analyysissä hyödynnetään sekä deterministisiä että todennäköisyyspohjaisia menetelmiä.

Analyysien toteutus

Paloanalyyseissä tarkastellaan palon syttymisen taajuutta, leviämisreittejä ja sen aiheuttamia alkutapahtumia sekä vikoja turvajärjestelmiin ja -laitteisiin. Analyysissä kartoitetaan huonetilat ja niiden sisältämä palava materiaali, kuten laitteet, kaapelit ja palavat nesteet. Palon leviämisen mallinnuksessa on huomioitava esimerkiksi palon leviäminen yksittäisestä kaapista koko huoneeseen, ilmanvaihtojärjestelmien vaikutukset sekä inhimillisten erehdyksien seurauksina aukinaiset palo-ovet, minkä seurauksena palo saattaa levitä määriteltyä palo-osastoa laajemmalle. Varsinaisen palon lisäksi analysoidaan esimerkiksi savun, lämmön ja sammutusveden aiheuttamat riskit.

Putkirikko, säiliön murtuminen tai pumpun virheellinen toiminta voi aiheuttaa laitoksen sisäisen tulvan ja alkutapahtuman. Tulva voi peittää allensa turvallisuustoiminnoissa tarvittavia laitteita tai esimerkiksi putkirikon aiheuttama vesi- tai höyrysuihku voi rikkoa laitteita kasvattaen tulva-alkutapahtuman seurauksia. Tulva-analyysi sisältää tulvalähteiden kartoituksen, vuototaajuuden määrittämisen, laitteiden sietokykyanalyysit sekä tulvan etenemisen mallintamisen. (Fortum 2014). Tulvalähteitä ja -reittejä tunnistetaan huonetilakohtaisesti suunnitteluvaiheessa esimerkiksi 3D-malleilla ja käyvillä laitoksilla esimerkiksi laitoskäynneillä.

Sisäisten uhkien analyysiin kuuluu myös missiililähteiden, kuten pyörivien koneiden ja mahdollisten räjähdysten kartoittaminen. Lisäksi kartoitetaan esimerkiksi raskaat nostot, joiden taakkojen putoaminen saattaa vaarantaa turvallisuuden kannalta tärkeitä järjestelmiä, laitteita tai rakenteita (YVL B.7, 8). Näihin liittyvät seurausvaikutukset huomioidaan laitteiden vika- ja vaikutusanalyyseissä.

5.5.2 Ulkoisten uhkien analyysit

Laitoksen turvallisuuteen tai käyttöön haitallisesti vaikuttavat laitoksen ympäristössä esiintyvät tilanteet ja tapahtumat, kuten poikkeukselliset sääilmiöt, laitoksen ulkopuoliset tulvat ja maanjäristykset, ovat ulkoisia uhkia (YVL B.7, 24). Luonnon aiheuttamat ulkoiset uhat ovat harvinaisia, minkä vuoksi niiden taajuuksien määrittämiseen liittyy suuria epävarmuuksia. Myös tahallinen, laitoksen turvallisuutta tai käyttöä uhkaava toiminta voidaan tulkita ulkoiseksi uhaksi, mutta kyseiseen toimintaan varaudutaan ja sitä analysoidaan erillisillä menetelmillä.

Ulkoiset uhat vaikuttavat koko laitosalueeseen, -arkkitehtuuriin ja useisiin puolustustasoihin. Laajuuden vuoksi pelkästään toimintojen sijoittaminen eri puolille laitosta ei takaa turvallisuustoiminnon toteutumista, vaan ulkoisiin uhkiin varaudutaan esimerkiksi erilaisuus- ja moninkertaisuusperiaatteiden mukaisilla järjestelmillä ja huomioimalla uhat laitoksen suunnitteluperusteessa. Sisäisten uhkien tavoin ulkoisten uhkien analysointi sisältää sekä deterministisiä että todennäköisyyspohjaisten analyysien piirteitä, ja havaitut uhat huomioidaan alkutapahtumien aiheuttajina.

Ulkoisista uhkista analysoidaan sääilmiöt, maanjäristykset ja poikkeuksellisen meriveden pinnankorkeuden aiheuttamat tulvat. Sääilmiötä ovat esimerkiksi poikkeuksellisen kova tuuli, lumisade, ukkonen, korkea meriveden lämpötila, jääesiintymät tai korkean lämpötilan aiheuttamat leväesiintymät. Ulkoiset uhkat voivat esiintyä yksittäisinä tai yhteisilmiöinä. (TVO 2011a). Usein laitokselle haitalliset ulkoiset alkutapahtumat ovat yhteisilmiöitä, kuten samanaikainen tuuli ja meriveden korkea leväpitoisuus tai tuuli ja lumisade (TVO 2011c). Ulkoisten uhkien analyysissä huomioidaan myös ilmiön yhtäläisyydet muihin tapahtumiin: esimerkiksi lentokoneen törmäykseen ja myrskytuuleen varautumista voidaan osittain verrata toisiinsa ja rakenteiden kestävyys molemmissa tilanteissa käsitellä samassa analyysissä. Mikäli ulkoiset uhkat ovat hyvin ennustettavissa ja laitos ehditään ajaa turvallisesti tilaan, esimerkiksi seisokkiin, jossa poikkeuksellisesta ilmiöstä ei ole laitokselle haittaa, ei ilmiötä käsitellä ulkoisena alkutapahtumana.

Analyysien toteutus

Ulkoisten uhkien analyysi alkaa ilmiöiden tunnistuksella ja karsintakriteerien määrityksellä. Tavoitteena on tunnistaa esimerkiksi kokemuksiin ja kirjallisuuteen perustuen kaikki mahdolliset laitosta koettelevat ulkoiset uhkat, mutta toisaalta karsia pois ilmiöt, joiden ei katsota voivan aiheuttaa alkutapahtumaa tai haastetta laitoksen turvallisuudel-

le. Esimerkiksi Suomessa ydinvoimalaitokset rakennetaan peruskallion päälle, minkä seurauksena maanvyöryjä tai maan poikkeuksellista kohoamista ei ole tarpeen analysoida. Käsiteltävien alkutapahtumien karsintaan käytetään asiantuntijoiden taajuus- ja voimakkuusarvioita sekä alustavia laitosvaikutusten arvioita. Tämän perusteella määritetään alkutapahtumaluokat ja niiden taajuudet, joiden pohjalta PRA:ssa mallinnetaan ja arvioidaan sydänvaurioriski kullekin ulkoiselle uhalle. (TVO 2011c).

Maanjäristysanalyysissä selvitetään laitoksen ympäristön mahdollisten maanjäristysten taajuus, toistuvuus ja maksimi- ja minimivoimakkuudet maanjäristysvyöhykkeiden perusteella. Analyysissä mallinnetaan esimerkiksi maaperän liikkeet, kiihtyvyysspektri ja huippukiihtyvyys. Lisäksi tunnistetaan maanjäristyksissä tarvittavat rakennukset, turvallisuustoiminnot ja -järjestelmät komponentteineen ja määritetään niiden kestävyydet, tuennat sekä niihin kohdistuvat rasitukset. (TVO 2009).

6. TURVALLISUUSTOIMINNON VIKAANTUMISEN TARKASTELU

Vika-analyyseillä osoitetaan, että ydinvoimalaitokselta vaaditut, luvussa 3.1 esitellyt turvallisuustoiminnot voidaan tarvetilanteessa toteuttaa. Tämä tarkoittaa, että yksittäisen turvallisuusjärjestelmän, laitteen tai rakenteen vikaantuminen voi olla hyväksyttävissä, mikäli sen toteuttama tehtävä on korvattavissa esimerkiksi rinnakkaisella osajärjestelmällä, eli se ei estä turvallisuustoiminnon toteutumista. Vika-analyysit suoritetaan turvallisuustoimintokohtaisesti ja niiden tulee tarkastella kaikkia turvallisuusjärjestelmiä ja turvallisuuteen liittyviä järjestelmiä sekä niiden sisältämiä osajärjestelmiä ja laitteita, joiden viat saattavat vaikuttaa kyseisen turvallisuustoiminnon onnistumiseen.

Olennaisena osana vika-analyyseihin kuuluu käsiteltävän järjestelmän rajapintojen määrittäminen. Saman järjestelmän rajapintojen määrittely voi vaihdella analyysikohtaisesti, riippuen siitä, tarkastellaanko järjestelmää itsenäisenä vai osana tiettyä kokonaisuutta. Itsenäinen tarkastelu tarkoittaa esimerkiksi järjestelmän sisäisten vikojen tunnistamista, jolloin on oleellista tuntea järjestelmään kuuluvien laitteiden vuorovaikutukset ja rajaukset. Tarkasteltaessa useasta järjestelmästä koostuvan toiminnon vikaantumista, yksittäisen järjestelmän sisäisiä rajapintoja ei yleensä tarvitse huomioida.

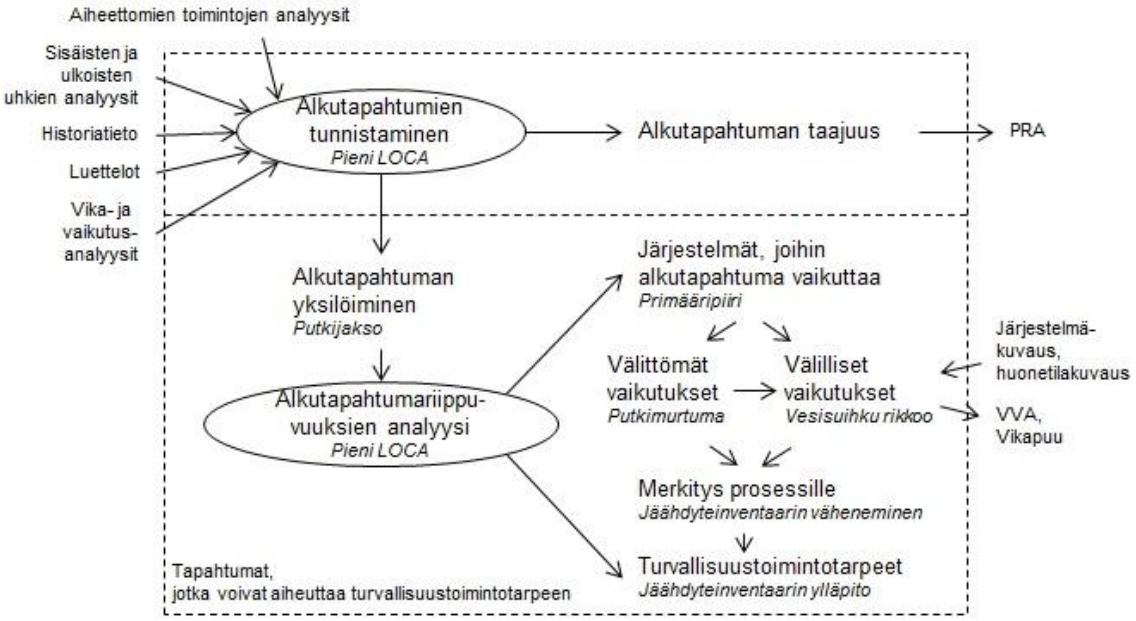
Tässä luvussa esitetään esimerkkejä analyyseistä, joilla tarkastellaan yksittäisen turvallisuustoiminnon vikaantumista ja vikasietoisuutta. Esimerkkianalyysit esitetään aihealueittain, alkaen yksittäisen toiminnon toteuttamiseen osallistuvien laitteiden ja järjestelmien vikaantumisesta ja edeten turvallisuustoiminnon toteutumisen varmistamiseen toimintoketjujen, järjestelmien ja laitteiden moninkertaisuuden ja erilaisuuden avulla. Alalukujen alussa esitetään YVL B.1 -ohjeen vaatimus kyseisestä aiheesta.

Alkutapahtuma-analyysit

Alkutapahtumakohtaisesti vaihtelee, minkä turvallisuustoimintojen toimintaa tarvitaan. Tämän vuoksi analyysien lähtökohtana pidetään alkutapahtumia, jotka on tunnistettu luvussa 5.5 esitetyin menetelmin. Turvallisuustoimintojen vikasietoisuutta tarkastelevat analyysit laaditaan alkutapahtumakohtaisesti ja huomioiden alkutapahtumien seurausviat ja -vaikutukset.

Alkutapahtuma-analyysit voidaan jakaa kuvan 6.1 mukaisesti kahteen osaan: alkutapahtumien tunnistamiseen sekä alkutapahtumariippuvuuksien määrittämiseen. Molemmilla osilla on oma tavoite ja lähtötiedot. Tunnistettuja ja yksilöityjä alkutapahtumia käytetään lähtötietona alkutapahtumien riippuvuuksien määrittämiselle. Alkutapahtumien

yksilöinnillä tarkoitetaan alkutapahtuman täsmällistä määrittelyä, esimerkiksi kyseisessä analyysissä tarkasteltavaa putkijaksoa, jolle alkutapahtumaksi tunnistettu putkirikko oletetaan.



Kuva 6.1. *Alkutapahtuma-analyysien lähtötiedot ja analyyseillä saatavat tulokset.*

Alkutapahtumariippuvuuksien analyysin jälkeen oletetaan tunnistetuiksi järjestelmät ja laitteet, jotka tapahtuman seurauksena menetetään, joiden ei voida olettaa toimivan halutulla tavalla alkutapahtuman yhteydessä tai joiden suojaus alkutapahtumaa vastaan on olennaista järjestelmän toiminnan kannalta (STUK 2015a, 6). Alkutapahtuma voi vaikuttaa tunnistettuihin laitteisiin välittömästi eli suoraan tai välillisesti, esimerkiksi putkirikosta aiheutuneen vesisuihkun rikkoessa samassa huonetilassa olevia laitteita. Alkutapahtumasta riippuvaisten järjestelmien ja laitteiden tunnistamisen avulla voidaan määrittää alkutapahtuman aiheuttamat prosessivaikutukset ja turvallisuustoimintotarpeet sekä turvallisuustoimintojen toteuttamista haittaavat seurausvaikutukset.

Turvallisuustoimintojen alkutapahtumakohtaisille analyyseille asetetaan oletuksia, joiden päälle analyysit rakentuvat. Analyysien lähtökohtana oletetaan, että tarkasteltava järjestelmä on käyttövalmiudessa ja käynnistyy halutulla tavalla, eikä siihen vaikuta muita poikkeuksia kuin tarkasteltava alkutapahtuma. Järjestelmän käyttöolosuhteet, kuten lämpötila, oletetaan suunnitteluperusteen ja käyttöohjeiden mukaisiksi. Myös muiden järjestelmien toiminta oletetaan normaaliksi. Huoltojen aikana järjestelmille aiheutuu suunniteltua epäkäytettävyyttä, jonka vaikutukset selvitetään erillisissä seisokkianalyyseissä (TVO 2008).

6.1 Yksittäisen järjestelmän vikaantuminen

”[352.] Vikasietoisuusanalyysissä on tarkasteltava toiminnallista kokonaisuutta kerrallaan ottaen huomioon sekä turvallisuustoimintoa toteuttava järjestelmä, että sen tukijärjestelmät. Analyysissä tulee tarkastella jokaista laitetta, jonka viat saattavat vaikuttaa järjestelmän suorittaman turvallisuustoiminnon onnistumiseen jonkin alkutapahtuman jälkeen. Kaikkien turvallisuustoimintoa toteuttavaan järjestelmään vaikuttavien laitteiden kaikki vikaantumistavat on käytävä analyysissä läpi…” (YVL B.1, 9).

Jotta järjestelmän vikaantumismahdollisuudet voidaan vaatimuksen mukaisesti tunnistaa, on määriteltävä siihen kuuluvat laitteet ja osajärjestelmät, sekä tunnistettava niiden väliset vuorovaikutukset ja tukijärjestelmät. Järjestelmän vikaantumismahdollisuudet analysoidaan siihen liittyviä laitteita, osajärjestelmiä ja tukijärjestelmiä tarkastelemalla.

6.1.1 Järjestelmien rajapinnat ja vuorovaikutukset

Ydinvoimalaitoksen järjestelmät koostuvat luvun 2 mukaisesti osajärjestelmistä, jotka voivat olla usean laitteen yhdistelmiä ja sisältää tukijärjestelmiä. YVL B.1 -ohjeen mukaisesti *”[322.]… järjestelmät ja laitteet on jaettava riittävän pieniin kokonaisuuksiin (konfiguraatioyksiköihin) siten, että ne ovat helposti tunnistettavissa, seurattavissa ja hallittavissa.”* (s. 7). Näiden kokonaisuuksien väliset vuorovaikutukset ja riippuvuudet on tunnistettava, jotta järjestelmän vikaantuminen voidaan hallita ja mallintaa, kuinka järjestelmän toiminta muuttuu, jos sen yksittäinen osajärjestelmä vikaantuu.

Järjestelmän sisäisten vikojen analysoinnissa oleellista on tuntea osajärjestelmien, laitteiden ja tukijärjestelmien väliset vuorovaikutukset. Järjestelmältä vaaditun toiminnon toteuttamisen epäonnistumisen syynä voi olla yksittäisen osajärjestelmän tai laitteen viasta aiheutunut järjestelmän sisäinen seurausvika, häiriö osajärjestelmien välisissä kytköksissä tai yksittäisen komponentin rikkoutuminen. Järjestelmän sisäinen seurausvika voi ilmetä esimerkiksi pumpun toimimattomuutena, joka johtuu kyseisen järjestelmän pienestä putkimurtumasta. Vaikka murtuma ei estäisi putken toimintaa, saattaa murtumasta aiheutuva vesisuihku vikaannuttaa esimerkiksi järjestelmän sisällä olevan elektroniikan.

Tietyn turvallisuustoiminnon toteuttavaan toimintoketjuun osallistuu yksi tai useampi järjestelmä. Yksittäisten järjestelmien ja laitteiden vikojen analysoinnin lisäksi on huomioitava vikojen leviämismahdollisuudet järjestelmän rajapintojen ulkopuolelle. Järjestelmän rajapinnat ja vuorovaikutukset toisiin järjestelmiin mahdollistavat vikojen leviämisen niin yhdessä toiminnossa kuin myös useiden toimintojen välillä, mikäli sama järjestelmä osallistuu useaan toimintoon.

Huomioitavia vuorovaikutuksia syntyy kahden järjestelmän välille, jos ne vaikuttavat huomattavasti toistensa toimintaan, joko molemminpuolisesti tai yksisuuntaisesti. Tyy-

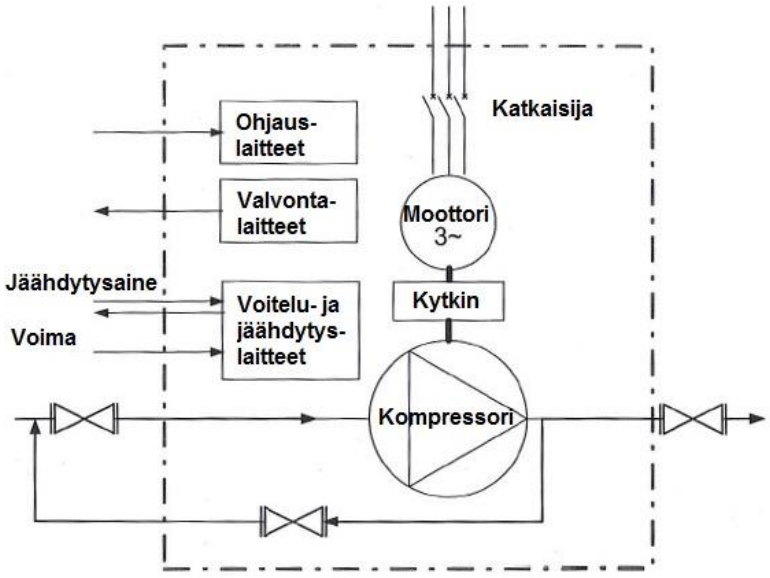
pillisesti yksi turvallisuustoiminto toteutetaan peräkkäisillä järjestelmillä, joissa toiminto etenee järjestelmästä toiseen ketjumaisesti. Näiden peräkkäisten järjestelmien lisäksi tulee huomioida ketjun eri vaiheisiin osallistuvat tukijärjestelmät. Esimerkiksi automaation arkkitehtuurille on syytä laatia oma yleiskuvaus, jossa esitetään käytettävät automaatioalustat, pääautomaatiojärjestelmät ja niiden toiminta, mittaus- ja toimilaitejärjestelmät, erillisjärjestelmät sekä hälytykset ja näiden rajapinnat muihin järjestelmiin. *"[5242.] Järjestelmien väliset rajapinnat on määriteltävä osana automaatioarkkitehtuurin suunnittelua."* (YVL B.1, 23).

Vikojen eteneminen järjestelmän ja yhden toimintoketjun sisällä johtuu tyypillisesti suunnitelluista riippuvuuksista. Suunnitelluilla riippuvuuksilla tarkoitetaan esimerkiksi järjestelmien välisten toimintoon kuuluvan informaatiovaihdon, prosessisuureiden etenemisen tai tukijärjestelmien aikaansaamia riippuvuuksia. Eri toimintoketjujen ja toimintojen väliset riippuvuudet taas voivat olla joko suunniteltuja tai suunnittelemattomia. Suunnittelemattomat riippuvuudet voivat ilmetä esimerkiksi samaan tilaan sijoitettujen järjestelmien välillä huoneen kosteus- tai lämpötilamuutosten välityksellä.

Yksityiskohtainen järjestelmäkuvaus

Prosessi- ja automaatiojärjestelmien tuntemista ja suunnitteluperusteiden dokumentointia varten laaditaan järjestelmäkohtaiset kuvaukset niiden teknisestä toteutuksesta sekä toiminnallisuudesta. Järjestelmään kuuluvat laitteet, komponentit ja niiden rajapinnat määritellään yksityiskohtaisesti, jotta niiden väliset vuorovaikutukset voidaan tunnistaa. (TUD-Kansliet 2010). Järjestelmäkuvaus sisältää tiedon järjestelmän toiminnasta, sen laitteiden tilat eri käyttötilanteissa ja millaisilla ohjauksilla ja minkälaiseksi sen tila voi muuttua käyttötilanteiden aikana. Laitteen tilalla eri käyttötilanteissa tarkoitetaan esimerkiksi sitä, onko venttiili tehokäytön aikana auki vai kiinni. Normaalien käyttötilanteiden lisäksi turvallisuustoimintoihin osallistuvista järjestelmistä määritellään niiden täsmälliset tehtävät häiriö- ja onnettomuustilanteissa sekä turvallisuustoiminnon käynnistävät signaalit. Myös toiminnon pysäyttämismahdollisuudet huomioidaan. (TVO 2008).

Kuvassa 6.2 esitetään esimerkkinä kompressorin kuvaus ja sen rajapinnat. Katkoviiva kuvaa laitteen rajapintaa, jonka läpi voi kulkea fyysisiä (esimerkiksi jäähdytysaine) tai signaaliohjausten muodostamia kytköksiä (esimerkiksi ohjaussignaalit ohjauslaitteille) muihin laitteisiin. Kuvaa täydentämään laaditaan kirjallinen selvitys, jossa kuvataan laitteen toiminta osana järjestelmää ja yksittäisten komponenttien vikaantumismahdollisuudet.



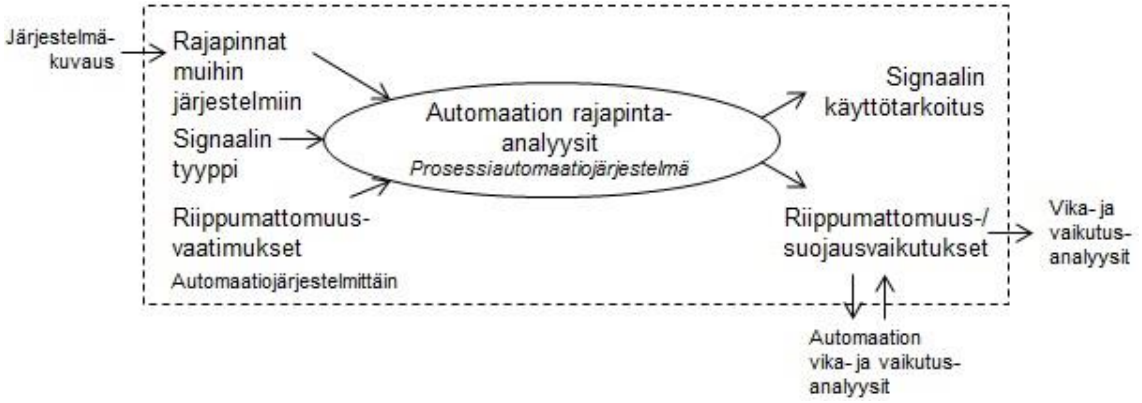
Kuva 6.2. *Kompressorin rajapinnat. Muokattu lähteestä (TUD-Kansliet 2010, 87).*

Järjestelmäkuvauksia hyödynnetään useiden analyysien laadinnassa. Samalle laitteelle tai järjestelmälle saattaa olla tarve laatia usean tasoisia kuvauksia eri analyysejä varten: esimerkiksi kompressorin vika- ja vaikutusanalyysissä voidaan hyödyntää tietoa laitteen sisältämistä komponenteista (moottori, liitännät), kun taas yhteisvika-analyyseissä kompressori voidaan mieltää yhdeksi laitekokonaisuudeksi tai tarkastella sen eri osien yhteisvikoja.

Järjestelmien väliset rajapinnat: automaation rajapinta-analyysit

Järjestelmien sisäisten laitteiden ja rajapintojen määrittämisen lisäksi tule huomioida järjestelmien väliset vuorovaikutukset ja rajapinnat sekä järjestelmään tulevat ja siitä lähtevät signaalit. Kuvassa 6.3 esitetään automaatiojärjestelmien välisten rajapintojen analyysin tavoitteita ja tarvittavia lähtötietoja.

Automaation rajapinta-analyysejä varten on tunnistettava yksityiskohtaisesti järjestelmien väliset rajapinnat, niihin liittyvät signaalit ja ovatko signaalit tyypiltään langoitettuja vai verkkopohjaisia. Analyysissä signaaleista tunnistetaan esimerkiksi niiden käyttötarkoitus, kuten hälytys- tai näyttötoiminto, sekä kuinka niille asetetut riippumattomuusvaatimukset toteutuvat. Tavoitteena on tunnistaa mahdollisuudet, joissa viat tai virheellinen informaatio saattavat levitä rajapintojen kautta järjestelmästä toiseen. Jos rajapintojen tehtävä on rajoittaa vikojen leviämistä, varmistetaan yksityiskohtaisemmin tarkasteluin, että ne toteuttavat asetetut suojausvaikutukset. (Areva 2015).



Kuva 6.3. *Automaation rajapinta-analyysin lähtötiedot ja analyysillä saatavat tulokset.*

Automaation rajapinta-analyyseissä tarkastellaan rajapinnan läpi kulkevia signaaleja ja niiden vikoja olettaen, että rajapinta toimii suunnitellusti. Myös rajapinnan vikaantumista tulee tarkastella joko osana rajapinta-analyysejä tai esimerkiksi automaation vika- ja vaikutusanalyyseillä. Rajapinta-analyysien avulla voidaan varmistaa, että järjestelmän vika- ja vaikutusanalyyseissä on huomioitu järjestelmään rajapinnan kautta vaikuttavat oikeanlaiset viat.

6.1.2 Yksittäisen laitteen tai järjestelmän vikaantumismahdollisuudet

”[432.] Mikään odotettavissa oleva yksittäisen toiminnassa olevan laitteen vikaantuminen tai virhetoiminto laitoksen normaalin käytön aikana ei saa johtaa sellaiseen tilanteeseen, joka edellyttää oletettujen onnettomuuksien hallintaan suunniteltujen järjestelmien käyttämistä.” (YVL B.1, 14). Tämän vuoksi laitteiden vikaantumissyyt ja -tavat on tunnistettava kattavasti ja vikaantumismahdollisuuksiin on liitettävä mahdollisen vikaantumisen aiheuttamat seuraukset kyseiselle laitteelle ja koko järjestelmälle. Vikaantumismahdollisuuksien tarkastelu voi kohdistua yksittäisen laitteen sijaan koko järjestelmään, mikäli laitekohtainen tarkastelu ei ole turvallisuustoiminnon toteutumisen kannalta merkittävää.

Yksittäisen laitteen tai järjestelmän vikaantumismahdollisuuksia tarkasteltaessa tavoitteena on tunnistaa sekä aktiiviset että passiiviset viat, joiden takia tarkasteltava laite tai järjestelmä ei pysty toteuttamaan sille määrättyä toimintoa tai toteuttaa virhetoiminnon. Analyysein huomioidaan sekä satunnaiset että systemaattiset viat ja tarkasteltavan kohteen rajapinnan sisäisistä ja ulkopuolisista syistä aiheutuvat viat. Järjestelmän laitteiden ja rakenteiden laadun tulee olla sitä korkeampi, mitä suurempi järjestelmän turvallisuusmerkitys on. (STUK 2015a, 3, 13).

Vikaantumismahdollisuuksien tunnistamisessa on huomioitava neljä erilaista järjestelmän vikaantumistilannetta suhteessa alkutapahtumaan:

1. Tarvetilanteena toimivaa alkutapahtumaa ei ole ja laite tai järjestelmä vikaantuu passiivisesti. Vikaantumista ei välttämättä havaita välittömästi.
2. Tarvetilanteena toimivaa alkutapahtumaa ei ole, mutta laitteen tai järjestelmän vikaantuminen aiheuttaa alkutapahtuman.
3. Laite tai järjestelmä vikaantuu passiivisesti tarvetilanteena olevaan alkutapahtumaan nähden, eli järjestelmä ei toimi tarvetilanteessa.
4. Automaatio vikaantuu aktiivisesti, ja vaikuttaa alkutapahtumaan mahdollisesti pahentaen alkutapahtuman seurauksia.

Kaikki tilanteet voivat syntyä niin prosessi- kuin automaatiojärjestelmien yhteydessä, mutta tilanteista 2. ja 4. koskevat erityisesti automaatiojärjestelmien vikaantumista. *”[5236.] Automaatiosuunnittelussa on otettava huomioon satunnaiset vikaantumiset (esimerkiksi laiteviat), systemaattiset virheet ja vikaantumiset (esimerkiksi ohjelmistoviat) sekä niiden seurauksena syntyvät passiiviset ja aktiiviset viat.”* (YVL B.1, 22).

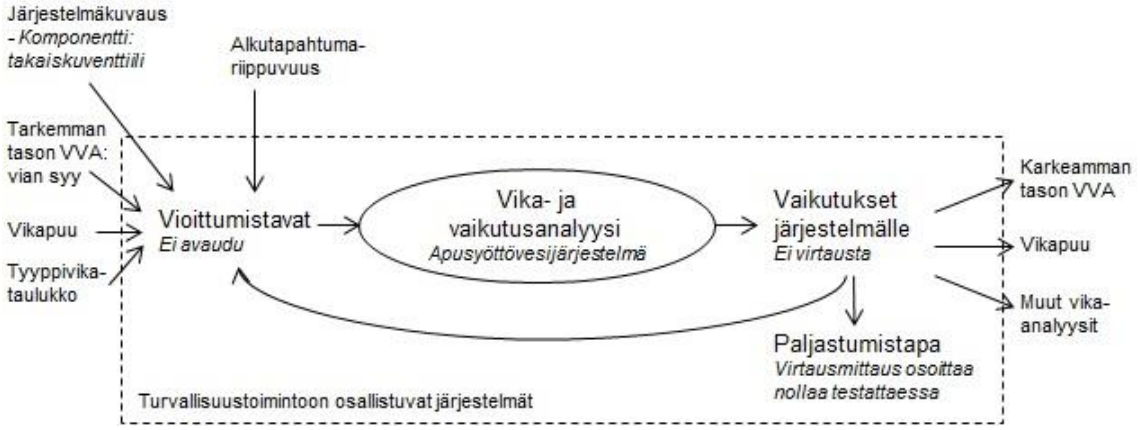
Yksittäisen laitteen vikaantumistarkastelussa huomioidaan vikaantumisen aiheuttamat häiriöt järjestelmälle sekä käyttö- ja kunnossapitohenkilöstön turvallisuudelle. Yksittäisten vikaantumistapojen tunnistamismenetelmänä käytetään esimerkiksi järjestelmäkohtaista vika- ja vaikutusanalyysiä tai laitetyyppikohtaisia tyyppivikaluetteloita. Jos tunnistettu vikaantuminen johtuu käytetyn komponentin tyypistä, huomioidaan tunnistettu vikaantumistapa myös muiden samanlaisia komponentteja tai laitteita sisältävien järjestelmien vikaantumistapana yhteisvika-analyysin avulla.

Seuraavissa kappaleissa laitteiden ja järjestelmien vikaantumisten analysointia käsitellään kolmesta näkökulmasta vian aiheuttajan perusteella. Vika voi johtua tarkasteltavan kohteen sisäisestä viasta, rajapinnan ulkopuolisista syistä tai aiheettomista ohjauksista.

Laitteen sisäinen vikaantuminen: vika- ja vaikutusanalyysit

Luvussa 5.1 esitetty vika- ja vaikutusanalyysi on yleisesti käytetty menetelmä tarkasteltavan järjestelmän tai laitteen rajapinnan sisäisten, suunnitelluista riippuvuuksista aiheutuvien vikaantumisten analysoinnissa. Analyysin tavoitteena on koota yhteen kuvan 6.4 mukaisesti järjestelmän toimintaan vaikuttavat vikaantumistavat ja selvittää niiden vaikutukset järjestelmälle. Kuvan 6.4 esimerkissä analyysi on laadittu apusyöttövesijärjestelmälle, jonka vioittumistavat, esimerkiksi takaiskuventtiilien jumiutuminen, on saatu tarkemman tason eli yksittäisten laitteiden tai komponenttien vika- ja vaikutusanalyysien tuloksista ja venttiilien tyyppivikataulukoista.

Vika- ja vaikutusanalyysiä varten on määriteltävä tarkoin, mitä tarkoitetaan käsiteltävällä järjestelmällä. Analyyseistä voidaan muodostaa ketju, jossa karkeamman tason analyysi pohjautuu yksityiskohtaisemman tason analyysin tuloksiin. Laitetason vika- ja vaikutusanalyysin lähtötietoina voidaan hyödyntää yksittäisten komponenttien analyysejä, ja laitetason analyysin tuloksia voidaan käyttää järjestelmätason analyysin lähtötietoina.



Kuva 6.4. *Vika- ja vaikutusanalyysin lähtötiedot ja analyysillä saatavat tulokset.*

Yksityiskohtaisin vika- ja vaikutusanalyysi laaditaan komponenttitasolla. Järjestelmän yksittäisen toiminnon toteuttamiseen liittyvät kaikki yksittäiset komponentit käydään läpi, ja niiden erilaiset vikaantumistavat selvitetään hyödyntäen komponenttien tyyppivikataulukoita ja järjestelmäkuvauksia. Myös alkutapahtumariippuvuudet huomioidaan. Tunnistetut komponenttien vikaantumistavat voidaan kirjata esimerkiksi taulukon 6.1 kaltaiseen taulukkoon. Taulukkoon liitetään viittaus järjestelmätason vika- ja vaikutusanalyysin riveihin, joiden syötteenä komponenttitason analyysin tulokset toimivat. Analyysissä käydään läpi erilaiset satunnaiset sekä systemaattiset syy-seurausyhdistelmät. Sama vika voi olla seurausta useasta eri syystä: esimerkiksi jos takaiskuventtiili ei avaudu, syynä voi olla mekaaninen vika tai vaurioituminen asennusvaiheessa. Kun vioittumistavat on selvitetty, kartoitetaan vian vaikutukset järjestelmän toiminnalle. (Areva 2014b).

Syiden ja vaikutusten lisäksi vika- ja vaikutusanalyysissä pyritään tunnistamaan ja esittämään vikojen paljastumistavat. Järjestelmän käyttötarkoituksesta ja vikaantumisen vaikutuksista riippuen vika voi olla piilevä tai välittömästi mittausten tai toiminnan muutoksen perusteella paljastuva vika. Piilevä vioittumistapa voi olla esimerkiksi mittaustulos, joka ei reagoi muutoksiin tai on väärä, mutta asetettujen raja-arvojen sisällä.

Taulukko 6.1. *Komponenttitason vika- ja vaikutusanalyysitaulukko.*

VVA

Järjestelmä: *Esim. Suojausjärjestelmä*
Järjestelmän toiminto: *Esim. Ilmastointi*

Komponentti	**Vioittumistapa**	**Yhteys järjestelmän vika- ja vaikutusanalyysiin**
Esimerkki	*Paljastuva/Piilevä: mittaustulos asteikon sisällä/ulkopuolella, ei reagoi muutoksiin tms…*	*Järjestelmän VVA:n rivit XX*
Mittalaite		
Mittaustiedon lähetyskomponentti		

Laitteen vikaantuminen ulkopuolisesta syystä: inhimillisten virheiden analyysit

Jos laitteen tai järjestelmän vikaantuminen johtuu sen rajapinnan ulkopuolisesta syystä, puhutaan seurausviasta. Seurausvikoja ovat esimerkiksi tietyssä huoneessa tulipalon vuoksi tuhoutuneet laitteet tai laitteen rikkoutuminen sen käyttämän sähköjärjestelmän vian aiheuttaneen ylijännitteen vuoksi. Tarkasteltavaan järjestelmään vaikuttavat muiden järjestelmien seurausvaikutukset huomioidaan vika- ja vaikutusanalyyseissä, mutta seurausvaikutuksille voidaan laatia myös erillisiä analyysejä, kuten luvussa 7.1.1 käsiteltävä paloanalyysi.

Yksittäisen laitteen vika voi aiheutua myös käyttöhenkilökunnan inhimillisestä virheestä tai huollon aikaisesta virheestä. ”*Virheiden mahdollisuus on otettava huomioon ydinvoimalaitoksen ja sen käyttö- ja kunnossapitotoiminnan suunnittelussa siten, että inhimilliset virheet ja niiden aiheuttamat poikkeamat laitoksen normaalista toiminnasta eivät vaaranna laitoksen turvallisuutta tai johda yhteisvikoihin.”* (STUK Y/1/2016, 6 §). Virheisiin varautumiseksi ja niiden havaitsemiseksi laaditaan inhimillisten virheiden analyysejä kuten huoltovirhe-analyysejä ja kuvan 6.5 mukaisia palautuspoikkeamien analyysejä.

Kuva 6.5. *Palautuspoikkeamien analyysin lähtötiedot ja analyysillä saatavat tulokset.*

Palautuspoikkeamien analyysissä käydään läpi järjestelmään kohdistuvat huollot ja muut toimenpiteet, joiden toteuttamiseen liittyy virheen mahdollisuus. Analyysiä varten kartoitetaan kuvien 6.5 ja 6.6 mukaisesti toimenpiteet ja niiden toteutusväli, joista voi aiheutua poikkeama, eli järjestelmä ei toimenpiteen jälkeen palaudu normaaliin tilaansa. Poikkeaman palautusmahdollisuudet määritetään koestus tai tarkastusmenettelytavan ja toistuvuuden avulla. Palautusmahdollisuuksia analysoitaessa huomioidaan myös, onko palautus mahdollista häiriön aikana. Todennäköisyysperusteista riskianalyysiä *(Probabilistic Risk Assessment, PRA)* varten lasketaan palautuspoikkeamien aiheuttama epäkäytettävyys laitteelle. (TVO 2008). Analyysin tarkoituksena on tunnistaa normaaliin käyttötoimintaan kuuluvat toimenpiteet, joiden epäonnistuminen saattaa tehdä järjestelmän toimintakunnottomaksi.

Tekijä: ENi

PALAUTUSPOIKKEAMIEN ANALYYSI

Laitepaikka	Poikkeaman aiheuttava toimenpide		Palautusmahdollisuudet		
	Palautuspoikkeama ja toimenpide, jossa se aiheutuu	Toimen-pideväli	Koestus, perustilautus tai muu tarkastusmenettely	Koestusväli	Palautus häiriön aikana
327V117 327V217 327V317 327V417	Venttiili jää auki 1 pumpun 327P1-P4 EH-ohjel-man mukaisen huollon tai 2 pumpun 327P1-P4 siirrettä-vän korjauksen (kts. liite 5.4) jälkeisen ilmauksen jälkeen. (327-13 "Pumppujen ilmaus järjestelmän tyhjennyksen jälkeen")	4 vuotta 2 vuotta	Ei havaita MA-kokeissa. Pal-jastuu seuraavassa pumppujen ilmauksessa.	16 kk	Ei. P=1,0

Kuva 6.6. *Esimerkki apusyöttövesijärjestelmän palautuspoikkeamien analyysistä. (TVO 2008).*

Inhimillisten virheiden analyysien tuloksia hyödynnetään esimerkiksi työvälineiden valinnassa ja ohjeiden laadinnassa. Selkeyden ja täsmällisyyden lisäksi voidaan esimerkiksi ohjeistaa eri osajärjestelmille tehtävän saman työn jakamisesta eri henkilöille, jolloin yhden työntekijän inhimillinen virhe vältetään toistamasta rinnakkaisissa järjestelmissä.

Aiheettomien ohjausten seuraukset: aiheettomien toimintojen analyysi

Aiheettomat tai väärät signaalit voivat aiheuttaa prosessijärjestelmien vääriä toimintoja tai rikkoa järjestelmiä tai laitteita. Laitteille tulevien signaalien ja ohjausten muutosten seurauksia voidaan tarkastella poikkeamatarkastelun kaltaisella, luvussa 5.2 esitetyllä aiheettomien toimintojen analyysillä. Jos automaatiojärjestelmä voi aiheuttaa aiheettoman toiminnon, sen seuraukset kartoitetaan sekä selvitetään, ovatko ne hyväksyttäviä (Areva 2015). Aiheettomien toimintojen analyysillä tarkastellaan, mitä yhden erottelulla hallitun automaatiokokonaisuuden vikaantumisesta voi seurata. Yksittäisiä automaatiolaitteita, kuten mitta- ja instrumentointilaitteita voidaan tarkastella muiden laitteiden tavoin vika- ja vaikutusanalyyseillä.

Yksittäisen mekaanisen laitteen virhetoimintojen ja vikaantumismahdollisuuksien tarkastelussa on huomioitava automaation aiheettomien toimintojen seuraukset. Esimerkiksi aiheettoman tai väärän signaalin aiheuttama ylijännite tai ylikuumeneminen saattaa rikkoa laitteen. Nämä mahdollisen vikaantumisen syyt voidaan huomioida vian aiheuttajina esimerkiksi laitteen vika- ja vaikutusanalyysissä. Yhden laitteen vikaantumisen tarkastelussa on huomioitava sen saamat kaikki ohjaukset, jolloin sen virhetoimintaan saattavat vaikuttaa useat eri automaatiokokonaisuudet.

Vaikka toisen järjestelmän vikaantuminen ei vikaannuttaisi tarkasteltavaa järjestelmää, voi se saada aikaan tarkasteltavalle järjestelmälle epätoivotun seuraustoiminnon. Usein virheelliset seuraustoiminnot aiheutuvat vääristä automaatio-ohjauksista. Mekaanisen laitteen vikaantuminen saattaa myös aiheuttaa virheellisiä automaatiosignaaleja, joista

voi seurata vääriä prosessiohjauksia. Esimerkiksi venttiili voi avautua väärään aikaan, jos se saa vääränlaisen avautumiskäskyn. Tällöin venttiilin toiminnassa ei ole vikaa, vaan virheellinen toiminto aiheutuu ohjausjärjestelmän tai sen yksittäisen komponentin, kuten ulostulokortin, virheestä. Jos virheellinen toiminto voi vaarantaa laitoksen turvallisuuden, huomioidaan virheelliset seuraukset luvussa 5.2 esitetyssä aiheettomien toimintojen analyysissä ja automaatiolla ohjattavien järjestelmien ja laitteiden vika- ja vaikutusanalyyseissä.

6.2 Turvallisuustoimintojen moninkertaisuus

”[433.] Vikaantumisiin on varauduttava siten, että turvallisuustoiminnon toteuttavat järjestelmät koostuvat kahdesta tai useammasta moninkertaisuusperiaatetta toteuttavasta rinnakkaisesta järjestelmästä tai järjestelmän osasta niin, että kyseinen turvallisuustoiminto voidaan toteuttaa, vaikka mikä tahansa näistä olisi käyttökunnoton.” (YVL B.1, 14). Turvallisuustoimintojen moninkertaisuuden analysoinnin tarkoituksena on osoittaa, että kaikki turvallisuustoimintoja ja turvallisuuteen vaikuttavia toimintoja toteuttavat järjestelmät ja niiden tukijärjestelmät täyttävät niille asetetut moninkertaisuutta eli rinnakkaisuutta vaativat vikakriteerit.

Myös tukijärjestelmien moninkertaisuuden toteutuminen analysoidaan. Jos rinnakkaiset osajärjestelmät ovat keskenään samanlaisia, kasvaa todennäköisyys, jolla suunnittelu- ja ohjelmistovirheet johtavat osajärjestelmien systemaattiseen vikaantumiseen. Virheellinen automaation syötetieto voidaan torjua esimerkiksi mittausten moninkertaistamisella, jolloin yksittäiset virheelliset mittaukset erottuvat oikeiden joukosta. Virheellisten mittausten vaikutusta voidaan vähentää myös sillä, että toiminto toteutuu vasta, kun esimerkiksi kolme neljästä rinnakkaisesta mittauksesta ylittää raja-arvon.

6.2.1 Toimintoketjun vikakriteerit ja vikasietoisuus

”[351.] Vikasietoisuusanalyyseillä on osoitettava, että

- *kaikki turvallisuustoimintoja toteuttavat järjestelmät ja niiden tukijärjestelmät täyttävät tämän ohjeen [YVL B.1] luvussa 4.3 esitetyt vikakriteerit…*

[352.]… Analyysissä oletetaan vaaditusta vikakriteeristä riippuen yksi tai useampi vika kerrallaan ja selvitetään niiden vaikutus järjestelmän toimintaan.” (YVL B.1, 9).

Vikakriteerien analyysissä tarkastellaan yksitellen toimintoketjun toimintaa, kun sen järjestelmiin tai tukijärjestelmiin oletetaan vaadittujen vikakriteerien mukaiset viat ja alkutapahtumariippuvuudet. Vikakriteerit on esitelty luvussa 3.3.2. Järjestelmältä vaaditut vikakriteerit, N+1 tai N+2, riippuvat toiminnosta, jonka toteuttamiseen järjestelmä osallistuu. Jos järjestelmä osallistuu usean toiminnon toteuttamiseen, tulee sen täyttää jokaista toimintoa koskevat kriteerit. Vikakriteerianalyysi toteutetaan järjestelmäkohtai-

sesti niin, että tarkasteltavan järjestelmän lisäksi huomioidaan sen tukijärjestelmät ja niiden aiheuttamat viat (YVL B.1, 9). Tarvittaessa tukijärjestelmien viat analysoidaan erillisillä analyyseillä (STUK 2015a, 6).

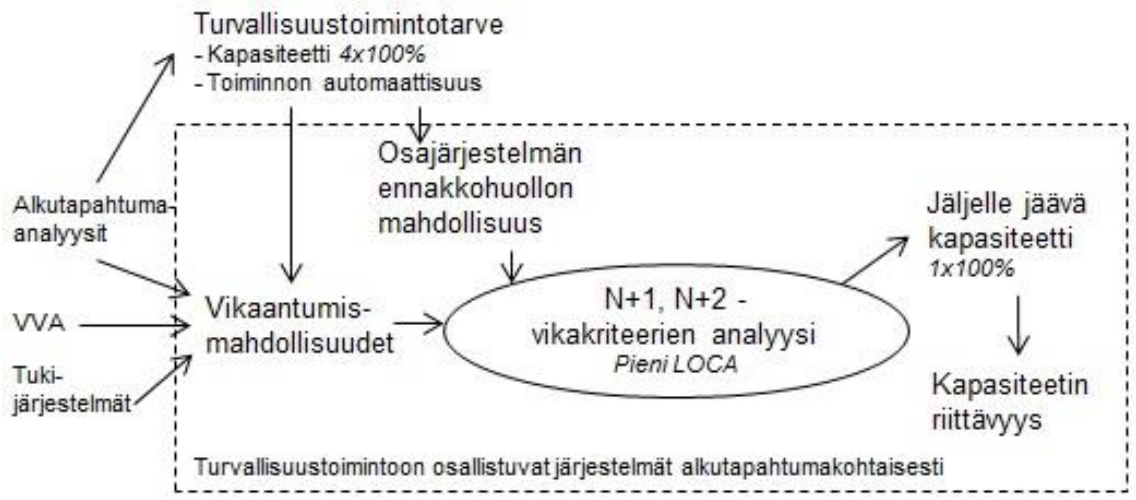
Vikakriteerien täyttymisen analysointi perustuu alkutapahtuma-analyyseillä tunnistettuihin häiriö- ja onnettomuustilanteisiin. Tilanteesta selviytymiseen vaadittujen turvallisuustoimintojen tarpeellisuutta arvioidaan yksitellen osana tunnistettuja käyttötilanteita. Turvallisuustoiminnon toteuttamiseen osallistuvien järjestelmien tulee täyttää niiltä vaaditut rinnakkaisuuskriteerit riittävän kapasiteetin varmistamiseksi. Erilaisin analyysein varmistetaan turvallisuustoiminnon toteutuminen, vaikka sen käyttämiin järjestelmiin kohdistuisi yksittäis-, yhteis- tai seurausvikoja. (Areva 2004b).

Yksittäisten järjestelmien analysoinnin lisäksi tulee huomioida järjestelmän asema vaaditun toiminnon toteutuksessa. Yksittäisten järjestelmien vikakriteerien täyttyminen ei välttämättä takaa koko toiminnon vikakriteerien täyttymistä, joten järjestelmien lisäksi toimintoketjut kokonaisuudessaan tulee analysoida erikseen. Esimerkiksi tilanteessa, jossa eri sähkönsyöttöjä käyttävät osajärjestelmät osallistuvat ristikkäin toistensa kanssa samoihin toimintoketjuihin, eivät toiminnon vikakriteerit välttämättä täyty.

Toimintoketjun vikaantumista analysoitaessa on huomioitava se, mihin tilaan sen osana oleva järjestelmä joutuu, kun sen laitteita tai muita osia huolletaan. Huollon aikana järjestelmä voi olla esimerkiksi epäkäytettävä tai saatettuna turvalliseen tilaan. (STUK 2015a, 7). Tämä vaikuttaa käytettävissä olevien rinnakkaisten toimintoketjujen lukumäärään, ja otetaan huomioon vikakriteerien määrittämisessä.

Moninkertaisuuden riittävyys: N+1, N+2 -vikakriteerianalyysi

Kuvassa 6.7 esitetään vikakriteerianalyysin pohjana olevat lähtötiedot sekä tulokset. Turvallisuustoiminnon toteutumisessa kiinnitetään huomio järjestelmiltä vaadittavaan kapasiteettiin sekä siihen, kuinka nopeasti toiminto tulee pystyä suorittamaan, eli vaaditaanko sen käynnistyminen automaattisesti. Toiminnon vikaantumismahdollisuudet saadaan esimerkiksi toimintoon osallistuville järjestelmille ja sen tukijärjestelmille laadituista vika- ja vaikutusanalyyseistä sekä alkutapahtumariippuvuuksien analyysistä. Vikaantumisten lisäksi järjestelmien käyttökunnottomuus esimerkiksi huollon vuoksi vaikuttaa toiminnon vikasietoisuuteen. Analyysin tuloksena selviää, onko rinnakkaisia järjestelmiä suunniteltu riittävän monta toteuttamaan tarvittavaa toimintoa, kun tiedetään mahdollisesti samanaikaisesti käyttökunnottomina olevien osajärjestelmien määrä.



Kuva 6.7. *N+1 ja N+2-vikakriteerianalyysin lähtötiedot ja analyysillä saatavat tulokset.*

Vikasietoisuuden analysoinnin osana tulee tarkastella myös tukijärjestelmien moninkertaisuutta jokaisen turvallisuustoiminnon kohdalla. Turvallisuustoimintojen tukijärjestelmien on noudatettava vastaavia vikakriteereitä, kuin varsinaisten järjestelmien.

6.3 Turvallisuustoimintojen erilaisuus

"[407.] Suunnitteluratkaisuissa on pyrittävä riippumattomuuteen yksittäisestä teknologiasta." (YVL B.1, 11). Mikäli yksittäinen turvallisuustoiminnon toteuttava toimintoketju vikaantuu eikä kykene suorittamaan siltä vaadittua toimintoa, on toiminnolle suunnitellun moninkertaisuusperiaatteen mukaisen varatoiminnon noudatettava myös erilaisuus- eli diversiteettiperiaatetta: järjestelmien on oltava toisistaan mahdollisimman riippumattomia ja mahdollisuuksien mukaan pohjauduttava eri teknologioihin (YVL B.1, 11). Erilaisuusperiaatetta osoittavat yhteisvika-analyysit laaditaan kaikille laitteille, jotka osallistuvat odotettavissa olevien käyttöhäiriöiden *(DBC 2)* tai luokan 1 oletettujen onnettomuuksien *(DBC 3)* alkutapahtumien hallintaan (YVL B.1, 9–10). Analyyseillä on osoitettava ensisijaisen ja varatoteutuksen riippumattomuus toisistaan niin, että ne eivät voi vikaantua samasta sisäisestä syystä. Yhteisestä ulkoisesta syystä johtuvaa vikaantumista tarkastellaan luvussa 7.1.1.

Sekä osajärjestelmien välisen että toiminnon ja sen varatoiminnon välisen riippumattomuuden osoittamiseksi tulee tarkastella järjestelmien yhteisvikoja, yhteisiä järjestelmiä sekä rinnakkaisten järjestelmien määrällistä riittävyyttä vikakriteerien mukaisesti. Toimintoketjun ja sen järjestelmien analyysissä tulee huomioida myös toimintoon osallistuvat tukijärjestelmät. Tukijärjestelmät on suunniteltava niin, että järjestelmän erilaisuus säilyy eikä yhteisen tukijärjestelmän käyttö aiheuta uusia riippuvuuksia muuten eroteltujen osajärjestelmien välille. Järjestelmä-, laite- ja rakennetasolla erilaisuusperiaatetta voidaan soveltaa esimerkiksi käyttämällä toisiaan korvaavissa osissa vähintään kahta riittävän erityyppistä järjestelmätoteutusta, rakennetta tai laitetta (STUK 2015a, 14).

6.3.1 Yhteisvian mahdollisuus

”[432.] Mikään odotettavissa oleva yksittäisen toiminnassa olevan laitteen vikaantuminen tai virhetoiminto laitoksen normaalin käytön aikana ei saa johtaa sellaiseen tilanteeseen, joka edellyttää oletettujen onnettomuuksien hallintaan suunniteltujen järjestelmien käyttämistä.” (YVL B.1, 14). Jos sama järjestelmä osallistuu usean toiminnon toteuttamiseen, on sen eri osajärjestelmien laitteiden erilaisuus analysoitava erityisen tarkoin, sillä *”[351.] vikasietoisuusanalyyseillä on osoitettava, että …*

> • *minkään yksittäisen laitetyypin (esim. samanlainen takaiskuventtiili, sama tyyppi ja valmistaja) yhteisvika ei estä ydinvoimalaitoksen ajamista hallittuun tilaan ja siitä edelleen turvalliseen tilaan.”* (YVL B.1, 9).

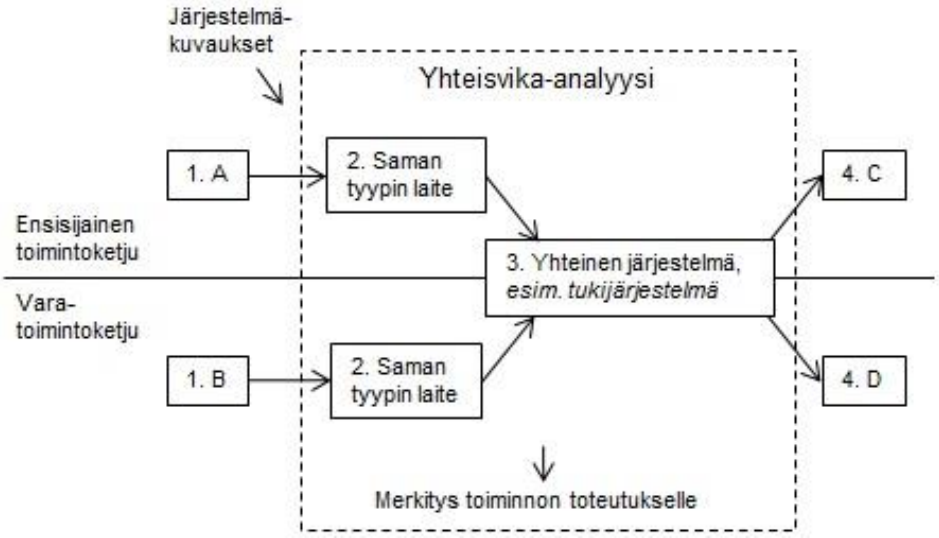
Tämän lisäksi on analysoitava yhteisviat, joiden vaikutuksesta sekä järjestelmä että sen varajärjestelmä saattavat vikaantua yhtä aikaa. Myös usean järjestelmän toimintaan vaikuttavien tukijärjestelmien synnyttämät yhteisvikamahdollisuudet tulee analysoida. Oleellista on tarkastella yhteisvikoja, jotka voivat vikaannuttaa järjestelmiä, joiden toiminta on tarkasteltavassa alkutapahtumassa vaaditun turvallisuustoiminnon kannalta kriittistä.

Inhimilliset virheet ovat yksi yhteisvikamahdollisuuden aiheuttajista. Jos sama työntekijä esimerkiksi avaa huoltoseisokkia varten tehdyn lukituksen väärin, on todennäköistä, että hän tekee työtehtävänsä väärin jokaisessa rinnakkaisessa järjestelmässä. Inhimillisistä virheistä johtuvat yhteisviat käsiteltiin luvussa 6.1.2 esitellyssä inhimillisten virheiden analyysissä.

Yhteisvikamahdollisuuden tunnistaminen: yhteisvika-analyysit

Yhteisvika-analyysin tavoitteena on tunnistaa yhden toiminnon toteuttamiseen käytetyt järjestelmät ja laitteet, jotta voidaan varmistua toimintoketjujen erilaisuudesta. Analyysi voidaan toteuttaa esimerkiksi laatimalla jokaisesta turvallisuustoiminnosta toiminnallinen ketju, jossa kuvataan siihen osallistuvat järjestelmät ja tukijärjestelmät sekä niiden yksittäiset laitteet ja komponentit, kuten luvussa 5.4 on esitetty. Vertaamalla toisiinsa ensisijaista ja varatoimintoketjuja, voidaan tunnistaa kohteet, joiden yhteisvikaantuminen vaikuttaa molempien ketjujen toimintaan. (Areva 2014c).

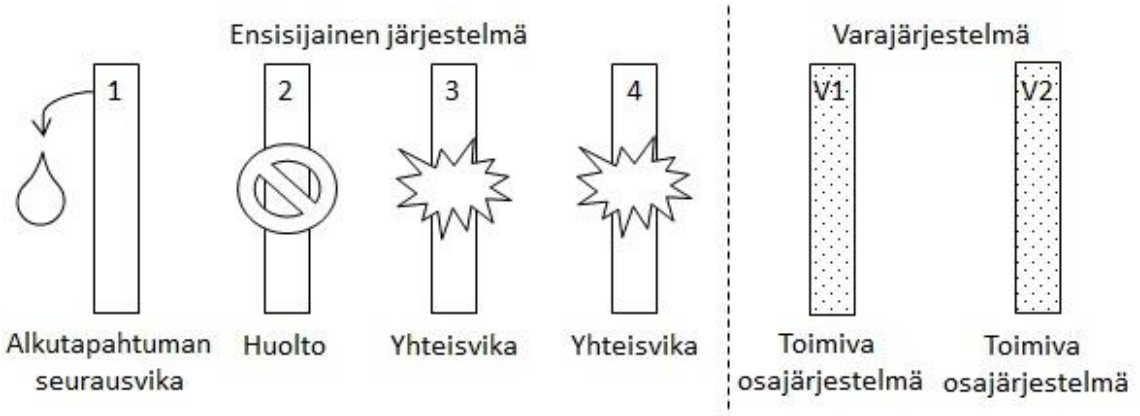
Kuvan 6.8 katkoviivalla erotettu osio esittää yhteisvika-analyysin kattavuutta. Lähtötietoina käytetyt toimintoon osallistuvat järjestelmät ja laitteet saadaan järjestelmä- ja toimintokuvauksista, joiden perusteella laaditaan ensisijaisen ja varatoiminnon toiminnalliset ketjut. Analyysin tavoite on tunnistaa ketjujen sisältämät samantyyppiset laitteet *(2)* ja yhteiset järjestelmät *(3)*, kuten tukijärjestelmät. Kun saman tyyppiset laitteet ja yhteiset järjestelmät on tunnistettu, selvitetään voiko mahdollinen yhteisvika vaarantaa toiminnon toteutuksen.



Kuva 6.8. *Yhteisvika-analyysin kattavuus turvallisuustoimintokohtaisesti.*

Yhteisvika-analyysien tarkoituksena on tunnistaa laitteet joilla on yhteisvian mahdollisuus ja vian merkitys toiminnon toteuttamiselle, mutta ei vikojen tarkempia syitä. Vikaantumisen syyt tunnistetaan tarvittaessa erikseen vika- ja vaikutusanalyyseissä. Sähkö- ja automaatiojärjestelmien yhteisviat analysoidaan erikseen luvun 6.3.2 mukaisesti. Yhteisvika-analyysien perusteella voidaan todeta tarve lisätä rinnakkaisien toimintoketjujen tai järjestelmien määrää.

Suunnittelun aikaisilla yhteisvika-analyyseillä voidaan esimerkiksi tunnistaa tarve käyttää (N+2 & D+1)-suunnitteluperiaatetta, jossa neliredundanttisen järjestelmän rinnalle suunnitellaan erilaisuusperiaatteen mukainen varajärjestelmä. Kuva 6.9 havainnollistaa tilannetta, jossa ensisijaisen järjestelmän kaksi osajärjestelmää vikaantuu yhteisviasta, jolloin ensisijainen järjestelmä ei välttämättä kykene toteuttamaan siltä vaadittua tehtävää, kun huomioidaan myös alkutapahtuman seurausvika sekä huoltomahdollisuus.



Kuva 6.9. *Yhteisvian vaikutus vaadittavien rinnakkaisten osajärjestelmien määrään.*

Kuva 6.9 esittää esimerkiksi hätäjäähdytystoimintoon osallistuvaa järjestelmää ja sen varajärjestelmää osajärjestelmineen. Mikäli toiminnon toteutumista tarkastellaan osana jäähdytteenmenetysalkutapahtumaa, yksi osajärjestelmistä syöttää vettä vuotavaan putkilinjaan, ja näin ollen on poissa käytöstä alkutapahtuman seurauksena, vaikka tarkasteltava osajärjestelmä itsessään olisi toimiva. N+2-kriteerin mukaisesti varaudutaan siihen, että toinen osajärjestelmä on huollossa. Jos osajärjestelmät keskenään ovat erilaisuusperiaatteen mukaisia, kolmannen osajärjestelmän yksittäisvian jälkeen olisi vielä yksi käyttökuntoinen osajärjestelmä. Jos osajärjestelmien välistä erilaisuutta ei kuitenkaan ole, tulee varautua yksittäisvian sijaan kahden osajärjestelmän yhteisvikaan. Mikäli yhteisvikaan ei varauduta järjestelmän sisällä osajärjestelmien erilaisuudella, tulee järjestelmälle suunnitella erillinen varajärjestelmä, joka täyttää erilaisuusvaatimukset.

6.3.2 Erilaisuusperiaate tukitoiminnoissa

Analyysien avulla tulee osoittaa, että erilaisuusperiaate säilyy niin osajärjestelmien kuin koko turvallisuustoimintoketjujen välillä myös niihin osallistuvissa tukitoiminnoissa, kuten sähkönsyötössä, automaatio-ohjauksissa, ilmastoinnissa ja laitteiden jäähdytyksessä. Järjestelmien riippuvaisuus tukitoiminnoista ei saa heikentää turvallisuustoimintojen erilaisuusperiaatteen toteutumista – yhden tukijärjestelmän vika ei saa estää koko toiminnon toteutumista.

Erilaisuusperiaate tulee huomioida tukitoimintojen välillä sekä toimintoketjun sisällä että ensisijaisen ja varatoimintoketjun toteutuksen välillä. Sähkönsyötön ja automaatiotoimintojen erilaisuusanalyysit voidaan laatia erikseen sen jälkeen, kun pääjärjestelmän analyysit ovat valmiita. Muut tukijärjestelmät huomioidaan osana pääjärjestelmää sen analyyseissä.

Sähkönsyötön erilaisuus: sähköjärjestelmien erilaisuusanalyysit

Sähkönsyöttöjärjestelmät ovat itsenäisiä kokonaisuuksia, jotka kuitenkin ovat välttämättömiä useiden muiden järjestelmien toiminnalle. Jotta järjestelmien erilaisuusperiaate säilyy, tulee myös niiden sähkönsyöttö toteuttaa erilaisuusperiaatteen mukaisesti: samaa turvallisuustoimintoa toteuttavan ensisijaisen ja sen varatoimintoketjun sähkönsyöttö on varmistettava eri sähkönsyöttöjärjestelmällä, jos niiden välillä ei muutoin ole riittävää erilaisuutta ja moninkertaisuutta. Sähköjärjestelmien analyyseillä tarkastellaan erikseen ulkoisen sähkönsyötön menetystilannetta ja järjestelmien sähkönsaantia muissa alkutapahtumissa. (YVL B.1, 26–28). Molemmissa tilanteissa selvitetään sähkönsyöttöjärjestelmien vikaantumisten aiheuttamat seuraus- ja yhteisvikavaikutukset.

Ulkoisen sähkönsyötön menetyksen *(Loss Of Offsite Power, LOOP)* aikana turvallisuudelle tärkeiden toimintojen sähkönsyöttö on varmistettava erilaisuusperiaatteen mukaisten omakäyttösähköjärjestelmien, kuten dieselgeneraattorien avulla (YVL B.1, 27). Vertaamalla järjestelmäkuvauksissa esitettyjä rajapintoja voidaan tunnistaa, mihin eri pro-

sessi-, automaatio- tai muihin järjestelmiin yhden sähkönsyöttöjärjestelmän vikaantuminen vaikuttaa. Tunnistetuista järjestelmistä analysoidaan, voidaanko niiltä vaaditut toiminnot toteuttaa eri sähkönsyöttöä käyttävillä järjestelmillä tai onko niille suunniteltu varasähkönsyöttö toisesta sähkönsyöttöjärjestelmästä.

Muiden alkutapahtumien yhteydessä sähköjärjestelmien analyysien tavoitteena on tunnistaa sähkönsyöttöjärjestelmien aiheuttamat seurausviat ja yhteisvikamahdollisuudet. Analyysit laaditaan luvussa 6.3.1 esitetyin menetelmin. Tavoitteena on tunnistaa yhteisviat, joiden vuoksi usean rinnakkaisen toimintoketjun sähkönsyöttö menetetään samasta syystä.

Automaation erilaisuus: automaation erilaisuusanalyysit

Automaation erilaisuusperiaatteen analyysit sisältävät ohjaus-, mittaus- ja priorisointijärjestelmien vikaantumisen vaikutusten analysoinnin. Automaation erilaisuuden analysoinnissa tulee huomioida sekä automaatiojärjestelmistä että yksittäisistä signaaleista ja niissä käytetystä tekniikasta johtuvat yhteisvikamahdollisuudet. Analyyseissä huomioidaan myös operaattorin ja automaation väliset rajapinnat.

Analyyseillä osoitetaan, että automaatiojärjestelmät ja niiden varajärjestelmät on allokoitu erilaisille automaatioalustoille niin, etteivät ne vahingoita pääjärjestelmien välistä erilaisuusperiaatteen toteutumista. Analyysissä käydään alkutapahtumakohtaisesti läpi jokainen turvallisuustoiminto, ja selvitetään niissä käytettäviin ensisijaiseen ja varajärjestelmään vaikuttavat automaatio-ohjaukset ja signaalien mittaustavat. Ohjausjärjestelmien erilaisuusanalyyseillä osoitetaan, että turvallisuustoimintojen ohjaus säilyy luotettavana yhden automaatiojärjestelmän tai sen osajärjestelmän vikaantumisesta huolimatta. Analyysillä tarkastellaan sekä ohjausjärjestelmän osajärjestelmien että sen ensisijaisten ja varajärjestelmien välisiä yhteyksiä ja samanlaisia toteutustapoja, vastaavasti kuin luvussa 6.3.1 on esitetty prosessijärjestelmille. Jotta erilaisuus ohjausten välillä säilyy, tulee niiden toiminnan perustua eri teknologioihin tai toimia eri automaatioalustoilla. Automaatiojärjestelmien perustumista eri teknologioihin esitellään luvussa 7.2.3.

Turvallisuustoimintoja käynnistävien ohjausjärjestelmien erilaisuusanalyyseillä tulee myös osoittaa, että saman toiminnon käynnistävät mittaukset perustuvat keskenään erilaisiin tekniikoihin. *”[5229.] Suojausautomaation turvallisuustoiminnon on käynnistyttävä vähintään kahdesta eri prosessisuureesta … [5230.] Mikäli kahden eri prosessisuureen määrittäminen turvallisuustoiminnon käynnistämistä edellyttävän tapahtuman tunnistamiseksi ei ole mahdollista, kyseisen tunnistamisessa käytettävän yksittäisen prosessisuureen mittaamisessa on käytettävä vähintään kahta eri mittausperiaatetta.”* (YVL B.1, 22). Mittausten yhteisvika-analyysiä varten on tunnistettava viat, joiden seurauksena mittalaite esimerkiksi osoittaa virheellisesti mittaukselle mahdollista maksimi- tai minimiarvoa tai se ei reagoi mitattavan suureen muutoksiin, vaan jää paikalleen osoittamaan tiettyä arvoa. Seurauksena saattaa syntyä esimerkiksi aiheeton toiminto tai

aiheellinen signaali jäädä huomioimatta. (Areva 2005, liite A). Tätä torjutaan moninkertaisilla mittauksilla. Mittausperiaatteiden erilaisuuden osoittamisen lisäksi mitta- ja toimilaitteiden väliset rajapinnat kartoitetaan, jotta voidaan varmistaa niiden keskinäinen erilaisuus tai muuten sulkea pois mahdollisuus toimintaan vaikuttavaan yhteisvikaan.

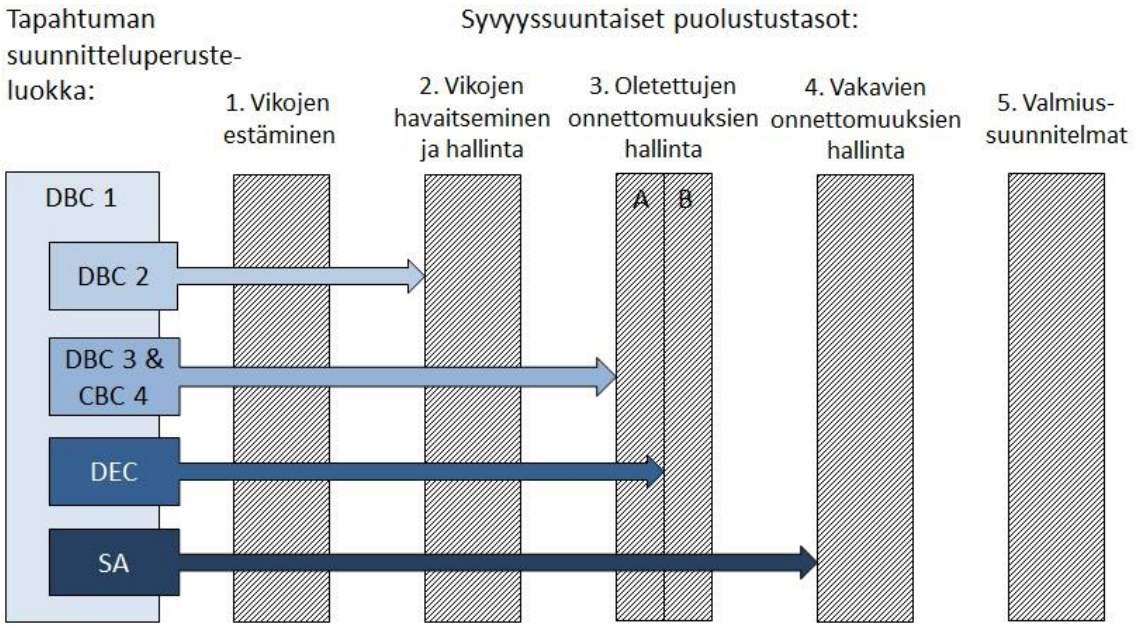
Automaation erilaisuusperiaatteen analyyseihin kuuluu myös toimintojen priorisoinnin analysointi. Esimerkiksi Olkiluoto 3 -laitoksella automaatiotoimintojen priorisointi toteutetaan erillisillä toimilaitteiden prioriteettien hallinta- ja ohjausjärjestelmillä *(Priority Actuator and Control System, PACS)* jotka koostuvat useista yksittäisistä PAC-moduuleista. Toimilaite ja sitä ohjaava PAC-moduuli on sijoitettu samaan turvallisuuslohkoon, ja PAC-moduuliin on kiinteästi ohjelmoitu järjestys, jonka mukaan moduuli välittää ohjaukset toimilaitteelle. PAC moduulit jaetaan kahteen eri teknologiaan perustuvaan ryhmään, A ja B, siten, että laitos selviää toisen ryhmän passiivisesta vikaantumisesta.

7. ARKKITEHTUURITASON VIKAANTUMISEN TARKASTELU

Luvussa 3 esiteltiin ydinvoimalaitoksen turvallisuussuunnittelussa sovellettavat syvyyssuuntainen puolustusperiaate, suunnitteluperusteluokitus ja järjestelmien turvallisuusluokitus. Näiden periaatteiden toteutumisen analysointi ei onnistu turvallisuustoiminnoittain, vaan on tarkasteltava arkkitehtuuritasolla useampaa toimintoa yhtä aikaa huomioiden niiden keskinäiset vuorovaikutukset.

Kuvassa 7.1 esitetään, kuinka syvyyssuuntaisen puolustusperiaatteen mukaiset tasot 1–5 estävät eri suunnitteluperusteluokkien *(DBC 2–4, DEC)* mukaisten ja suunnitteluperusteen ylittävien *(SA)* laitostapahtumien etenemisen. DBC 1 -luokka kuvaa laitoksen normaaleja käyttötilanteita ilman vikoja, josta vian ilmetessä siirrytään vikaa vastaavaan suunnitteluperusteluokkaan. Luvun 6 yksittäistä turvallisuustoimintoa käsittelevät analyysit keskittyvät DBC 3–4 ja DEC-tapahtumien pysäyttämiseen, eli puolustustasoon 3.

Syvyyssuuntaisen puolustusperiaatteen tasojen tulee olla toisistaan riippumattomia niin toiminnallisesti kuin fyysisestikin, jotta yhdellä tasolla tapahtuva häiriö tai vikaantuminen ei etene muille tasoille. Toisaalta yksittäisen tason tulee olla riittävän vahva toteuttamaan tehtäväänsä itsenäisesti. (YVL B.1, 14).

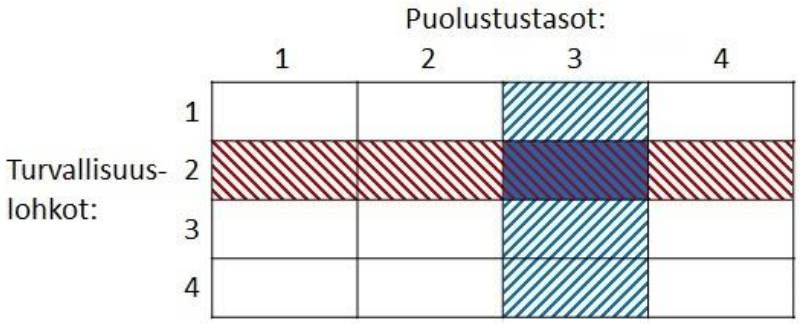


Kuva 7.1. *Laitostapahtumien suunnitteluperusteluokkien ja syvyyssuuntaisten puolustustasojen yhteys. Muokattu lähteestä (Holmberg 2015).*

Yksi puolustustaso voi koostua eri turvallisuusluokkiin luokitelluista turvallisuustoimintoja toteuttavista järjestelmistä: 1. Puolustustason järjestelmät voivat kuulua turvallisuusluokkiin 1, 2, 3 tai EYT. Puolustustasoilla 2, 4 ja 5 on turvallisuusluokan 3 järjestelmiä. Puolustustaso 3 koostuu turvallisuusluokkaan 2 kuuluvista turvallisuusjärjestelmistä, joilla laitos saadaan hallittuun tilaan ja turvallisuusluokan 3 järjestelmistä, joilla laitos saadaan hallitusta tilasta turvalliseen tilaan tai jotka ovat oleellisia onnettomuus- ja häiriötilanteiden hallinnan kannalta. (STUK 2015a, 19).

Kuva 7.2 esittää kaksi erilaista mahdollisuutta, kuinka vika voi vaikuttaa laitokseen arkkitehtuuritasolla. Kuvan 7.2 sarakkeet esittävät syvyyssuuntaisen puolustuksen neljää ensimmäistä tasoa ja rivit laitoksen jakoa neljään turvallisuuslohkoon *(Safety Division)*. Turvallisuuslohkolla tarkoitetaan laitoksen toiminnallisesti ja fyysisesti eroteltua osaa ja sen sisältämiä laitteita ja rakenteita, joka koostuu kunkin turvallisuusjärjestelmän yhdestä moninkertaisuusperiaatetta toteuttavasta osasta (YVL B.1, 43). Turvallisuuslohkoja havainnollistetaan lisää kuvassa 7.3.

Kuvan 7.2 mukaisesti yhdessä sarakkeessa eli puolustustasossa esiintyvä vika saattaa vaikuttaa kaikkien turvallisuuslohkojen toimintaan yhteis- tai seurausvikojen välityksellä. Koska tilanteessa vaarantuu kokonainen syvyyssuuntaisen puolustuksen taso, oleellista on, että vika ei leviä muille tasoille vaan ne säilyttävät toimintakuntoisuutensa. Kuvan 7.2 yhden rivin eli kokonaisen turvallisuuslohkon luotettava toiminta taas voidaan menettää esimerkiksi tulipalon seurauksena. Koko turvallisuuslohkoa koskevaan vikaan varautumiseksi tulee huolehtia turvallisuuslohkojen välisestä erottelusta, puolustustasojen vahvuudesta, jotta muiden lohkojen toimintakuntoisuus säilyy ja ne pystyvät huolehtimaan syvyyssuuntaisen puolustuksen kaikista tasoista.



Kuva 7.2. *Yksittäisen syvyyssuuntaisen puolustustason tai yhden turvallisuuslohkon vikaantuminen.*

Yksittäisen puolustustason vahvuus tulee analysoida huomioiden tason toiminnallinen sekä rakenteellinen kestävyys. Lisäksi vika-analyysein on osoitettava, että eri syvyyssuuntaiset puolustustasot säilyttävät erillisyytensä ja riippumattomuutensa toisistaan. Puolustustasojen, vakavien onnettomuuksien hallintaa lukuun ottamatta, ei vaadita olevan järjestelmien osalta täysin toisistaan riippumattomia, kunhan vikojen leviäminen tasolta toiselle on estetty. Myös vakavien onnettomuuksien hallinnan tason toimintoja

saa perustellusti hyödyntää oletettujen onnettomuuksien laajennustilanteissa (DEC), jos tämä ei vaaranna järjestelmän kykyä hoitaa varsinaista tehtäväänsä, mikäli tilanne kehittyy vakavaksi onnettomuudeksi (YVL B.1, 14).

7.1 Yksittäisen puolustustason vahvuus

Luvussa 6.2 esitetty turvallisuustoiminnon moninkertaisuus on tärkeä osa yksittäisen puolustustason vahvuutta. Kun järjestelmät ovat moninkertaistettuja, on huolehdittava myös niiden erottelusta, jotta esimerkiksi seurausviat tai alueelliset tapahtumat, kuten tulipalot tai tulvat, eivät vaaranna koko turvallisuustoiminnon toteuttamista. Tämän takaamiseksi turvallisuusjärjestelmän moninkertaisuutta toteuttavat eri osat sijoitetaan eri turvallisuuslohkoihin, eli toisistaan fyysisesti eroteltuihin tiloihin (YVL B.1, 15). *”[436.] Minkään turvallisuuslohkon ja sen sisältämien laitteiden menettäminen ei saa johtaa minkään turvallisuustoiminnon menetykseen.”* (YVL B.1, 15).

Yksittäistä puolustustasoa vahvistaa turvallisuuslohkojen välinen vahva erottelu niin fyysisesti, sähköisesti kuin myös informaationvälityksen osalta. Turvallisuuslohkoihin jaon tarkoituksena on vähentää seurausvikoja niin, että vaikka yksi lohko toimisi virheellisesti tai se menetettäisiin kokonaan, voidaan samat toiminnot toteuttaa edelleen jäljelle jääneiden lohkojen avulla. Automaatiojärjestelmien kohdalla tämä vaatii erityistä huomiota, sillä eri turvallisuuslohkoissa voidaan käyttää yhteisiä automaatioalustoja, -järjestelmiä ja mittauksia, jolloin vikojen leviäminen sekä turvallisuuslohkojen että puolustustasojen välillä mahdollistuu.

Samaan puolustustasoon, mutta eri turvallisuusluokkaan kuuluvien laitteiden välinen erottelu tulee analysoida, jotta *”[440.]… alemman turvallisuusluokan järjestelmän, rakenteen tai laitteen toimintatapa tai vikaantuminen ei aiheuta ylemmässä turvallisuusluokassa olevan järjestelmän, rakenteen tai laitteen vikaantumista eikä toiminnan menetystä.”* Liitettäessä yhteen eri turvallisuusluokkiin kuuluvia järjestelmiä, on ne erotettava toisistaan toiminnallisesti ja niiden rajapinnat suunniteltava niin, että niiden välinen yhteys ei vaaranna turvallisuustoimintoa toteuttavan järjestelmän toimimista. (YVL B.1, 15).

7.1.1 Fyysinen erottelu

”[434.] Turvallisuustoimintoja toteuttavan järjestelmän moninkertaisuusperiaatetta toteuttavat osat on sijoitettava eri turvallisuuslohkoihin… [437.] Turvallisuusjärjestelmien moninkertaisuusperiaatetta toteuttavia osia sisältävien turvallisuuslohkojen on oltava eri rakennuksissa, tai ne on erotettava muista samassa rakennuksessa olevista turvallisuuslohkoista omiksi osastoikseen siten, että viat eivät voi levitä järjestelmän yhdestä moninkertaisuusperiaatetta toteuttavasta osasta toiseen laitoksen sisäisten (esim. tulipalo, tulva tai dynaamiset vaikutukset) tai ulkoisten tapahtumien seurauksena…” (YVL B.1, 14–15). Turvallisuuslohkojen erotteluvaatimus koskee myös kaikkia

turvallisuustoiminnon toteuttamiseen tarvittavien järjestelmien tukijärjestelmiä ja esimerkiksi niihin liittyviä kaapelointeja ja mittausjärjestelmiä (YVL B.1, 15).

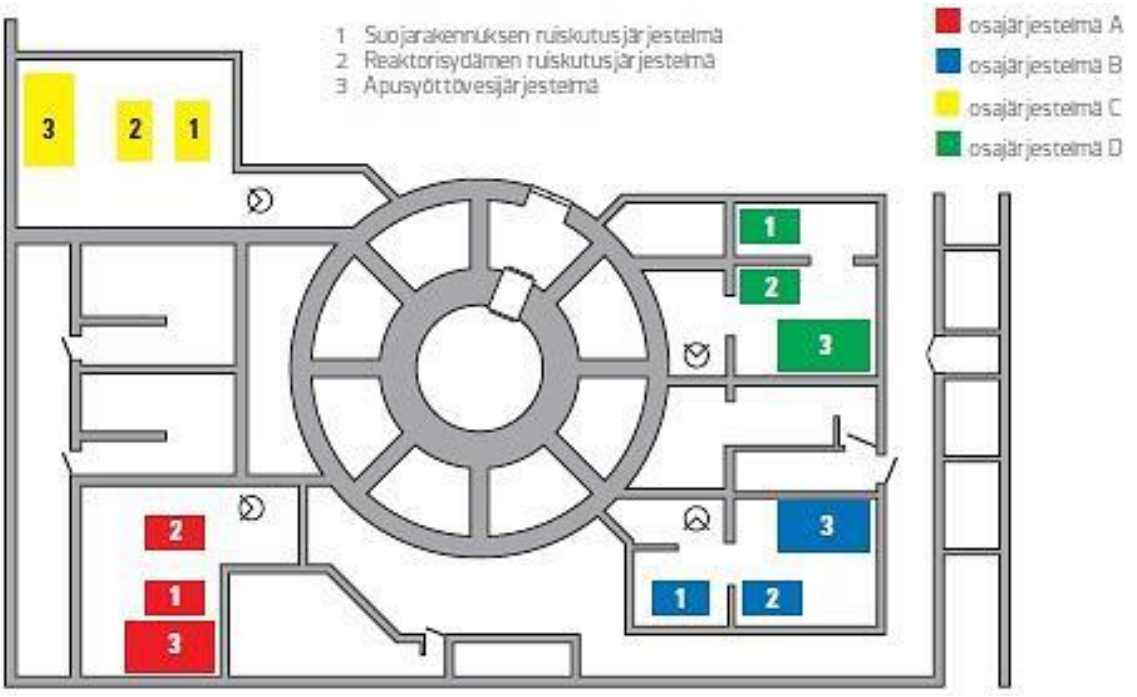
Turvallisuuslohkojen fyysisellä erottelulla varaudutaan laitoksen sisäisiin ja ulkoisiin tapahtumiin ja niiden seurausvaikutuksiin, jotka voisivat vikaannuttaa usean toimintoketjun samanaikaisesti. Jotta turvallisuustoiminnon toteutuminen taataan, tulee rinnakkaiset osajärjestelmät sijoittaa eri turvallisuuslohkoihin (YVL B.1, 15).

Turvallisuuslohkojen ja palo-osastojen määrittäminen: laitoksen pohjapiirustus

Laitosarkkitehtuurin suunnittelussa määritetään laitoksen turvallisuuslohkot, fyysisesti toisistaan erotellut tilat, laitteet ja rakenteet. Kunkin turvallisuusjärjestelmän moninkertaisuus- eli rinnakkaisperiaatetta toteuttavat osat sijoitetaan eri turvallisuuslohkoihin. (YVL B.1, 43). Turvallisuuslohkoilla pyritään estämään vikojen leviäminen rakenteellisesti. Turvallisuuslohkot jaetaan edelleen toisistaan erillisiin palo-osastoihin osastojen käyttötapaan tai palokuormaan perustuen. Esimerkiksi valvomo, tietokonetilat, sähkö- ja kytkintilat, kaapelitilat ja akkuhuoneet voivat olla omia palo-osastojaan. (YVL B.8, 10–11).

Turvallisuuslohkoista ja niihin kuuluvista tiloista laaditaan piirrokset, joissa kuvataan tilassa olevat järjestelmät ja laitteet sekä tilan läpi kulkevat kaapelit, vaikka ne eivät toiminnallisesti liittyisi kyseisen turvallisuuslohkon järjestelmiin. Piirrosten perusteella osoitetaan turvallisuuslohkojen välistä erottelua koskevat vaatimukset täytetyiksi. Esimerkiksi Olkiluoto 1 ja 2-laitosten turvallisuusjärjestelmien eri osajärjestelmät on sijoitettu eri puolilla reaktorirakennusta sijaitsevaan neljään erilliseen tilaan, joita havainnollistetaan kuvassa 7.3.

Kuvasta 7.3 voidaan havaita, kuinka turvallisuusjärjestelmärakennukset eli turvallisuuslohkot ovat fyysisesti eri puolilla reaktorirakennusta. Jokainen turvallisuuslohko sisältää turvallisuustoimintojen yhden osajärjestelmän. Esimerkiksi kuvan vasemman alareunan turvallisuuslohkon tulipalo voi tuhota esitetyistä ruiskutus- ja apusyöttövesijärjestelmistä osajärjestelmät *A*, mutta muut osajärjestelmät kykenisivät edelleen toteuttamaan vaaditut toiminnot. Piirroksia hyödynnetään osajärjestelmien välisen erottelun toteutumisen varmistamisessa.

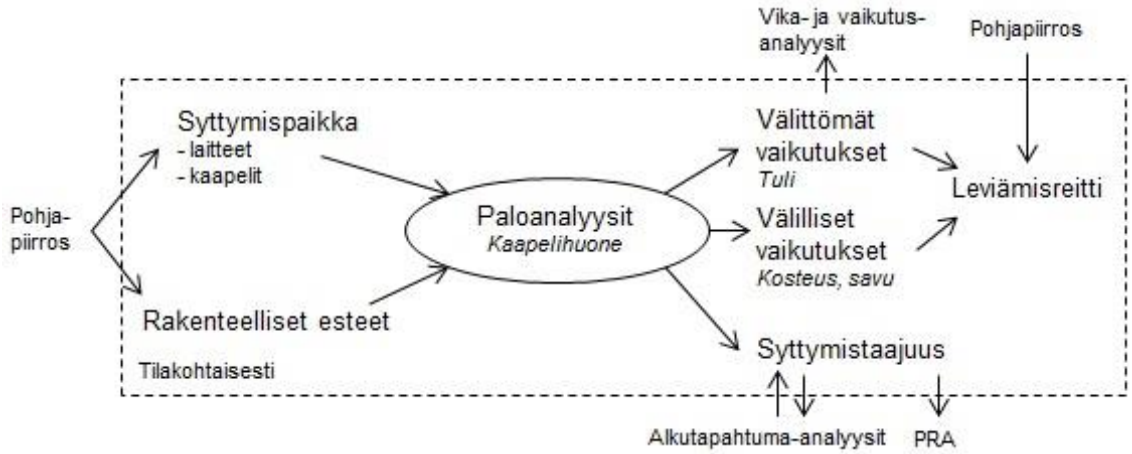


Kuva 7.3. *Olkiluoto 1 ja 2 -laitosten neljä toisistaan fyysisesti eroteltua turvallisuusjärjestelmärakennusta eli turvallisuuslohkoa (TVO 2013, 53).*

Onnettomuuden leviäminen: sisäisten uhkien analyysit

Luvussa 5.5.1 kuvataan sisäisten uhkien analyysien, kuten palo- ja tulva-analyysien, suoritustavat. Muiden alkutapahtuma-analyysien tavoin sisäisten uhkien analyysien tavoitteena on tunnistaa häiriö- tai onnettomuustilanteiden syntymismahdollisuudet ja -taajuudet ja yksilöidä tilanne palojen ja tulvien yhteydessä tiettyyn huonetilaan ja laitteisiin. Kuvassa 7.4 esitetään paloanalyysien lähtötiedot ja tulokset, joita voidaan soveltaa myös muiden sisäisten uhkien analysointiin.

Leviämislaajuuden ja vikaantuvien järjestelmien, laitteiden ja rakenteiden tunnistamiseksi selvitetään onnettomuuden leviämisreitti, joka perustuu muun muassa pohjapiirroksiin ja rakenteellisiin esteisiin, kuten palo-ovien ja ilmastointikanavien sijoitteluun. Leviämisellä tarkoitetaan sekä tulipalon leviämistä että palon aiheuttamien sivuvaikutusten, kuten savun ja kosteuden aiheuttamien vaikutusten leviämistä.



Kuva 7.4. *Paloanalyysien lähtötiedot ja analyyseillä saatavat tulokset.*

Analyysien tuloksia hyödynnetään esimerkiksi osana muita vika-analyysejä ja todennäköisyysperusteisesta riskianalyysiä *(PRA)* sekä suoraan suunnitteluratkaisujen tekemisessä. Analyyseillä voidaan esimerkiksi tunnistaa tarve muuttaa järjestelmien suojauskonsepteja tai sijoittelua. Tavoitteena on tunnistaa esimerkiksi paljon öljyä sisältävien moottoreiden vuotomahdollisuudet, jotta öljypalon mahdollisuutta voidaan pienentää ja leviämislaajuutta rajoittaa.

7.1.2 Informaatiovirtojen erottelu

”[5238.] Ydinvoimalaitosta ohjaavat automaatiojärjestelmät on suunniteltava sellaisiksi, että niiden vikaantuminen ei estä alkutapahtuman hallintaa” (YVL B.1, 22). Käyttöautomaation tai muun alemman tuvallisuusluokan automaatiojärjestelmän vikaantuminen ei saa estää oletettujen onnettomuuksien hallintaan suunniteltuja turvallisuusjärjestelmiä toteuttamasta turvallisuustoimintoja: *”[5244.] Suojausjärjestelmä on erotettava toiminnallisesti muista automaatiojärjestelmistä siten, että informaatiovirta suojausjärjestelmästä muihin automaatiojärjestelmiin on toteutettu yksisuuntaisesti käyttäen fyysisesti yhdensuuntaistavaa erotuslaitetta”* (YVL B.1, 23). Vastaavasti automaatioarkkitehtuuri tulee erottaa fyysisin erotuslaittein hallinnollisista tietojärjestelmistä niin, että tiedonsiirto on mahdollista yhdensuuntaisesti vain automaatioarkkitehtuurista tietohallintojärjestelmiin (YVL B.1, 23).

Sekä käyttö- että suojausautomaation arkkitehtuuri on suunniteltava siten, että sen turvallisuusluokka vastaa korkeinta siihen liittyvän järjestelmän turvallisuusluokkaa. Käyttö- tai suojausautomaatiojärjestelmän vikaantuminen ei saa estää alkutapahtumien hallintaa eikä automaatiojärjestelmässä esiintyvä yksittäisvika saa aiheuttaa käyttöhäiriötä pahempaa alkutapahtumaa. Turvallisuustoiminnoissa ei saa käyttää langattomaan tiedonsiirtoon perustuvia ratkaisuja ja turvallisuusautomaation tiedonsiirtojärjestelmien on kestettävä pahimmatkin mahdolliset kuormitustilanteet. (YVL B.1, 20–22).

Automaation erottelu: erottelulla hallittujen kokonaisuuksien määrittäminen

Jotta voidaan varmistaa, että alemman turvallisuusluokan automaatiojärjestelmien vikaantuminen ei estä suojausjärjestelmää toteuttamasta turvallisuustoimintoja, erotetaan eri turvallisuusluokkiin kuuluvat järjestelmät toisistaan toiminnallisesti. Tätä erottelua analysoidaan osana aiheettomien toimintojen analyysiä. Analyysi alkaa erottelulla hallittujen kokonaisuuksien, *entiteettien*, ja niihin liittyvien automaatiotoimintojen määrittelystä kuvan 7.5 mukaisesti. Aiheettomien toimintojen analyysiä sekä entiteettejä ja niiden määrittelyn vaikeutta on käsitelty luvussa 5.2. Entiteettien määrityksen jälkeen selvitetään niihin liittyvien toimintojen sekä koko entiteetin toimintojen yhteisvaikutusten pahimmat mahdolliset vikaantumisvaikutukset ja vaikutusten laajuus.

Kuva 7.5. *Aiheettomien toimintojen analyysin lähtötiedot ja analyysillä saatavat tulokset.*

Erottelulla hallittujen kokonaisuuksien määrittäminen on tärkeä osa automaation analysointia, sillä niiden avulla voidaan tarkastella automaatiovikojen laajuuksia. Määritetyt entiteetit toimivat lähtökohtana pahimman mahdollisen vikaantumisen tunnistamiselle sekä sellaisenaan voivat osoittaa automaation erotteluvaatimukset täytetyiksi.

7.1.3 Sähkönsyötön saatavuus

STUKin määräyksen (Y/1/2016, 11 §) mukaan *”6. Ydinvoimalaitoksella on oltava häiriö- ja onnettomuustilanteiden varalta ulkoinen ja sisäinen sähkötehon syöttöjärjestelmä. Turvallisuustoiminnoissa tarvittava sähköteho on voitava syöttää kumpaa tahansa järjestelmää käyttämällä.”* Sekä ulkoinen että sisäinen sähkönsyöttöjärjestelmä on suunniteltava siten, että se yksinään riittää turvallisuustoimintojen toteuttamiseen vaadittavien järjestelmien sähkötehon lähteeksi (YVL B.1, 26).

Yksittäisen puolustustason vahvistamiseksi rinnakkaisten, toisiaan varmistavien järjestelmien on käytettävä keskenään eri sähkönjakelujärjestelmiä. Myös yksittäisen turvallisuustoiminnon erilaisuusperiaatetta toteuttavien eri toimintoketjujen sähkönsyöttö on varmistettava erilaisuusperiaatteen mukaisilla sähkönsyötöillä. Turvallisuustoimintojen sähkönsyötön varmistamiseen liittyviä erilaisuusperiaatteen analyysejä on tarkasteltu luvussa 6.3.2. Sähkönsyöttöjärjestelmien sijoittelua analysoidaan muiden järjestelmien tavoin, kuten luvussa 7.1.1 esitettiin.

Yhden sähköjärjestelmän vika ei saa levitä ristikytkentöjen kautta toisiin moninkertaisuutta toteuttaviin järjestelmiin eivätkä sähköjärjestelmän taajuus- ja jännitevaihtelut saa vaarantaa turvallisuustoimintojen toteutumista. Sähköjärjestelmien käyttökunnottomuusaika, esimerkiksi huoltojen yhteydessä, on pidettävä niin lyhyenä kuin mahdollista. Myös normaalioloissa käyttämättömien varavoimajärjestelmien jatkuva toimintavalmius on varmistettava (YVL B.1, 26).

Turvallisuusluokiteltujen sähkö- ja automaatiojärjestelmien, -laitteiden ja niiden kaapelointien sijoittelussa on huomioitava myös suojautuminen sekä jatkuvilta että lyhytaikaisilta sähkömagneettisten häiriökenttien vaikutuksilta. Laitteet ja kaapelit on sijoiteltava myös siten, etteivät ne itse aiheuta haitallisia sähkömagneettisia häiriöitä ympäristöönsä. (YVL B.1, 29).

7.1.4 Rakenteellinen kestävyys

Ydinvoimalaitoksen suunnittelussa on huomioitava, kuinka ulkoiset olosuhteet ja tapahtumat vaikuttavat häiriö- ja onnettomuustilanteista selviämiseen, esimerkiksi rakenteiden kestävyytenä ja järjestelmien toimintakuntoisuutena. *”[501.] Ydinlaitoksen järjestelmien, laitteiden ja rakenteiden suunnittelussa on otettava huomioon laitospaikalla mahdollisiksi arvioidut luonnonilmiöt ja muut laitokseen kohdistuvat ulkoiset uhat.”* (YVL B.7, 16).

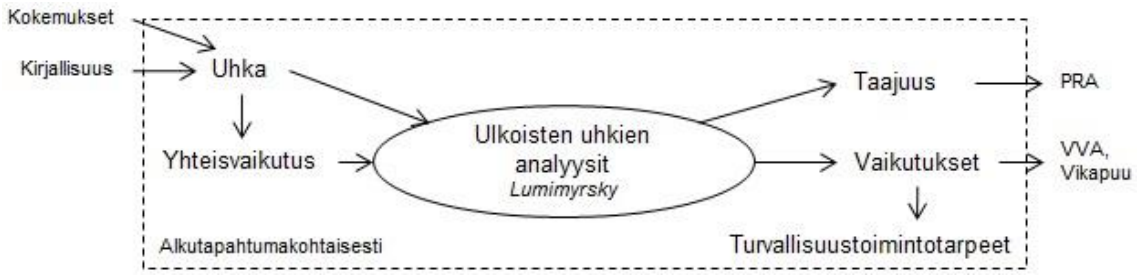
Suunnitteluratkaisuilla on varmistettava, että sääilmiöt, kuten jäätyminen tai lumi eivät aiheuta tukkeutumista tai estä jäähdytysilman saantia turvallisuuden kannalta tärkeille järjestelmille. Laitoksen ulkoisista syistä syntyvien tulvien etenemisreitit on kartoitettava ja merivesijärjestelmien tukkeutumismahdollisuudet on analysoitava ja niihin on varauduttava tarkoitukseen soveltuvilla puhdistusjärjestelmillä. Suunnittelussa on huomioitava myös laitoksen ulkopuoliset räjähdykset ja tulipalot ja niiden aiheuttamien lämmön ja savun vaikutukset. Myös eläinten ja kasvuston aiheuttamat uhat laitokselle on huomioitava. Ulkoisten uhkien huomioiminen on osoitettava analyyseillä. (YVL B.7, 18–19)

Ulkoisten uhkien vaikutukset järjestelmien toimintakuntoisuuteen analysoidaan laitosarkkitehtuuritasolla, sillä vaikutus voi kohdistua varsinaisen laitteen tai järjestelmän lisäksi esimerkiksi sen kaapelointiin tai kytkentöihin. *”[435.] Sähkö- ja automaatiolaitteiden tyyppitesteihin on sisällytettävä suunnittelumaanjäristykseen verrattuna riittävät vaatimukset mekaanisen rasituksen kestosta. Laitteiden välisten kaapelointien ja kytkentöjen kestävyys on osoitettava analyysein ja/tai kokein.”* (YVL B.7, 14).

Laitospaikan aiheuttamat riskit: ulkoisten uhkien analyysit

Ulkoisten uhkien analyysi käsittää sää-, tulva- ja seismisten ilmiöiden ja niiden taajuuksien tunnistamisen sekä laitosvaikutusten arvioinnin luvun 5.5.2 mukaisesti. Ilmiöiden

tunnistamisessa hyödynnetään kirjallisuutta ja historiatietoja, kuten kuvassa 7.6 havainnollistetaan.



Kuva 7.6. *Ulkoisten uhkien analyysien lähtötiedot ja analyyseillä saatavat tulokset.*

Ulkoisten uhkien analyysin tarkoituksena on tunnistaa laitoksen ulkopuoliset ilmiöt, jotka saattavat aiheuttaa alkutapahtuman, sekä näiden mahdolliset seurausviat. Vaikka ulkoisten uhkien aiheuttamat alkutapahtumat voivat vaikuttaa useassa fyysisesti erotellussa turvallisuuslohkossa samanaikaisesti, analyysin tavoitteet ja tulosten hyödyntäminen eivät poikkea muista alkutapahtuma-analyyseistä.

7.2 Puolustustasojen välinen erottelu

STUKin määräyksen (Y/1/2016) 9 §:n mukaan syvyyssuuntaisen puolustusperiaatteen *”puolustustasojen on oltava toisistaan niin riippumattomia kuin käytännöllisin toimenpitein on mahdollista saavuttaa.”* Näin ollen yhdellä puolustustasolla esiintyvä vika ei saa vaikuttaa muihin tasoihin, eikä yhden puolustustason menetys heikentää muiden tasojen toimintaa. Vaatimuksen toteutumisen osoittamiseksi *”[351.] vikasietoisuusanalyyseillä on osoitettava, että…*

- *syvyyssuuntaisen turvallisuusperiaatteen mukaan eri puolustustasoille sijoitetut järjestelmät on toiminnallisesti erotettu toisistaan siten, että yhdellä tasolla tapahtuva vika ei vaikuta muihin tasoihin…”* (YVL B.1, 9).

Toiminnallisen erottelun lisäksi samaan turvallisuuslohkoon sijoitetut eri puolustustasoihin kuuluvat järjestelmät on eroteltava toisistaan fyysisesti käyttäen etäisyyttä tai suojaavia rakenteita (YVL B.1, 14).

Fyysisen ja toiminnallisen erottelun tarve tulee analyysein peilata alkutapahtumiin sekä tilannekohtaisesti sisäisiin ja ulkoisiin uhkiin. Mikäli samaa turvallisuustoimintoa toteuttavat eri turvallisuusjärjestelmät on suunniteltu eri puolustustasoille, on niiden ja niiden tukijärjestelmien riippumattomuus varmistettava osana puolustustasojen riippumattomuutta. (STUK 2015a, 17).

7.2.1 Puolustustasojen riippumattomuus

”[426.] Riippumattomuuden on perustuttava toiminnallisen erottelun, erilaisuusperiaatteen sekä fyysisen erottelun riittävään soveltamiseen puolustustasojen välillä.” (YVL B.1, 14). Puolustustasojen välistä fyysistä erottelua tarkastellaan turvallisuusluokittain vastaavasti kuin luvussa 7.1.1 kuvatuin yksittäisen puolustustason vahvuutta osoittavin menetelmin. Puolustustasojen välistä riippumattomuutta tarkasteltaessa analysoidaan samassa tilassa sijaitsevien eri puolustustasoille kuuluvien toimintojen välisiä fyysisiä esteitä ja välimatkoja. Toiminnallinen erottelu ja erilaisuusperiaate puolustustasojen välillä tarkoittaa, että yhdellä tasolla ilmenevä vika ei aiheuta seurausvikoja muille tasoille.

Vian leviäminen puolustustasosta toiseen: seurausvikojen analysointi

Yksittäisen järjestelmän vikaantuminen voi aiheuttaa seurausvikoja useille puolustustasoille. Puolustustasojen välisten seurausvikojen mahdollisuuksien analysointiin voidaan käyttää vastaavia menetelmiä, kuin yksittäisen puolustustason vahvuuden analysointiin: puolustustasojen välisten seurausvikojen analysoinnin on huomioitava niin fyysinen ja rakenteellinen erottelu, kuin myös informaatio- ja sähkövirtojen kautta mahdollistuvat seurausviat.

Esimerkiksi taulukon 7.1 kaltaisella analyysillä voidaan osoittaa, että tietyn alkutapahtuman seurausten lieventämiseen on varauduttu usealla puolustustasolla eikä näiden puolustustasojen välillä ole ristikkäisyyksiä. Esimerkki kuvaa automaatiotoimintojen riippumattomuuden tarkastelua. Kun oletetaan, että yksittäisten puolustustasojen vahvuudet on analysoitu, voidaan analyysillä osoittaa, että yhden tason menetys ei estä tarkasteltavan onnettomuuden ehkäisyä tai rajoittamista. (Areva 2014a, liite A).

Taulukko 7.1. *Automaation syvyyssuuntaisten puolustustasojen riippumattomuusanalyysitaulukko.*

RIIPPUMATTOMUUSTARKASTELU **Tapahtuma:** *Esim. Pieni jäähdytteenmenetysonnettomuus*					
Automaatio-toiminto	**Puolustus-taso**	**I&C -järjestelmä**	**Automaatio-toiminto (vara)**	**Puolustus-taso**	**I&C -järjestelmä**
Esimerkkitoiminto	*2.*	*PS*	*Esimerkkitoiminnon korvaava varatoiminto*	*3.*	*HBS*
Automaattinen hätäsyöttövesijärjestelmän käynnistys			Manuaalinen hätäsyöttövesijärjestelmän käynnistys		

Esimerkissä tarkastelu suoritetaan vertaamalla toisiinsa taulukkoon alkutapahtumakohtaisesti kirjattuja kyseisen alkutapahtuman hallinnassa käytettäviä ensisijaiseen ja varatoimintoketjuun osallistuvia automaatiojärjestelmiä ja niiden puolustustasoja. Esimerkki automaation syvyyssuuntaisen puolustuksen tasoista ja automaatiojärjestelmistä esitellään luvussa 7.2.3. Taulukon 7.1 kaltaisesta analyysistä voidaan esimerkkirivin tavoin kuitenkin nähdä, että tarkasteltavan alkutapahtuman seurauksia voidaan ehkäistä kahden eri toimintoketjun toiminnoilla, joita ohjaavat eri puolustustasojen *(2. ja 3.)* automaatiojärjestelmät *(PS ja HBS)*. Taulukkoon voidaan kirjata myös kriteerit toiminnon käynnistymiselle, esimerkiksi höyrystimen pinnankorkeuden tai paineen nousu tai lasku tietyn rajan yli tai alle. (Areva 2014a, liite A).

7.2.2 Vakavien onnettomuuksien hallinnan erillisyys

”[431.] Vakavien onnettomuuksien hallintaan tarkoitetut järjestelmät (syvyyssuuntaisen puolustusperiaatteen taso 4) on erotettava toiminnallisesti ja fyysisesti normaaliin käyttöön, häiriötilanteisiin ja oletettujen onnettomuuksien sekä oletettujen onnettomuuksien laajennustilanteiden hallintaan tarkoitetuista järjestelmistä (tasot 1, 2 ja 3a sekä 3b). Vakavien reaktorionnettomuuksien hallintaan syvyyspuolustuksen tasolla 4 tarkoitettuja järjestelmiä voi perustellussa tapauksessa käyttää myös vakavien sydänvaurioiden estämiseen oletettujen onnettomuuksien laajennustilanteissa, mikäli tämä ei vaaranna järjestelmien kykyä hoitaa varsinainen tehtävänsä tilanteen mahdollisesti kehittyessä vakavaksi reaktorionnettomuudeksi.” (YVL B.1, 14).

Vakavien onnettomuuksien hallinnan -tason riippumattomuus on huomioitava myös tukijärjestelmissä. Käyttöenergian, kuten sähkön ja paineilman, syöttölähteiden on oltava riippumattomia laitoksen muista syöttölähteistä ja jakelujärjestelmistä. (YVL B.1, 27). Vakavien onnettomuuksien varalle voidaan esimerkiksi suunnitella omat akustot, joita voidaan käyttää muiden sähkönsyöttöjärjestelmien vikaantuessa. Sama erotteluvaatimus koskee automaatiojärjestelmiä: *”[5240.] … 8. Vakavien reaktorionnettomuuksien hallintaan käytettävän instrumentoinnin ja ohjausjärjestelmien on oltava riippumattomia laitoksen muista automaatiojärjestelmistä. Muiden automaatiojärjestelmien vikaantuminen ei saa häiritä vakavien onnettomuuksien hallintatoimenpiteitä.”* (YVL B.1, 23).

Vakavien onnettomuuksien hallinnan riippumattomuuden analysointi

Vakavien onnettomuuksien hallintaan käytettävien järjestelmien analyysit eivät poikkea luvussa 6 esitetyistä muiden turvallisuusjärjestelmien analyyseistä. Vakavien onnettomuuksien hallintaan käytettäviltä järjestelmiltä kuitenkin vaaditaan täydellisempää riippumattomuutta muista järjestelmistä kuin muiden tasojen välillä. Mikäli samoja järjestelmiä tai niiden osia käytetään myös muilla tasoilla, tulee vakavien onnettomuuksien hallintaan tarkoitettujen toimenpiteiden olla priorisoituna korkeimmalle niin, etteivät muiden tasojen toimenpiteet vaaranna näiden toteuttamista.

Taulukossa 7.2 on esitetty esimerkki vakavien onnettomuuksien hallinnan *(Severe Accident, SA)* -tason erillisyyden analyysistä. Tason riippumattomuuden analysoinniksi on ensin tunnistettava vakavien onnettomuuksien hallintaan kuuluvat turvallisuustoiminnot. Turvallisuustoiminnoille on määritetty onnistumiskriteerit. Lopuksi on analysoitu, voivatko muiden järjestelmien, tässä esimerkissä automaatiojärjestelmien, viat estää onnistumiskriteerien täyttymisen. Yhteen turvallisuustoimintoon voi liittyä useita onnistumiskriteereitä. (Areva 2014a, liite C).

Taulukko 7.2. *Vakavien onnettomuuksien hallinnan -tason automaation riippumattomuusanalyysitaulukko. Muokattu lähteestä (Areva 2014a, liite C).*

SA-TASON AUTOMAATION RIIPPUMATTOMUUSTARKASTELU **Tapahtuma:** *Esim. Pieni jäähdytteenmenetysonnettomuus*			
Turvallisuus-toiminto	**Onnistumiskriteeri**	**Onnistumiskriteerin estävä, muun kuin SA-tason automaatiovika**	
		Analyysi	**Tulos**
Esimerkki-toiminto	*Esim. Lämpötilan osoitus SA I&C -järjestelmälle.*	*Mittaus toteutettu SA I&C -järjestelmällä / mittaustulokset lähetetty suoraan SA I&C -järjestelmälle / tms …*	*Aiheeton muun tason järjestelmän automaatiovika ei voi vaikuttaa onnistumiseen: OK*
Paineenalennuksen käynnistys	Lämpötila mitataan ja osoitetaan SA I&C:lle.		
Paineenalennuksen valvonta	Paine osoitetaan SA I&C:lle.		

Analyysissä on huomioitava muiden järjestelmien aiheuttamat sekä aktiiviset että passiiviset vaikutukset. Jos analyysillä havaitaan, että muiden puolustustasojen järjestelmien viat voivat estää onnistumiskriteerien täyttymisen, muutetaan suunnittelua. Analyysi on hyväksyttävissä vasta, kun sillä osoitetaan vakavien onnettomuuksien hallinnan tason riittävä erillisyys jokaisen onnistumiskriteerin kohdalla.

7.2.3 Puolustustasojen säilyminen tukijärjestelmissä

”[427.] Riippuvuus turvallisuustoimintoja syvyyssuuntaisen puolustuksen eri tasoilla tukevista järjestelmistä on otettava huomioon. Riippuvuus ei saa tarpeettomasti heikentää syvyyssuuntaisen puolustuksen luotettavuutta.” (YVL B.1, 14). Puolustustasojen erillisyyden säilyminen huomioitaessa prosessijärjestelmiin vaikuttavat tukijärjestelmät, on analysoitava erikseen, sillä riippumattomuuden osoittaminen ei ole yhtä suoraviivaista kuin pelkkiä prosessijärjestelmiä tarkasteltaessa. Kuten myös yksittäisen turvallisuustoiminnon tukijärjestelmien erilaisuustarkasteluissa luvussa 6.3.2, voidaan puolustustasojen erottelun säilyminen analysoida jälkikäteen sähkö- ja automaatiojärjestelmien kohdalla.

Sähköjärjestelmien sijoittuminen eri puolustustasoille

Syvyyssuuntainen puolustusperiaate näkyy sähköjärjestelmissä erillisinä syöttöinä ja eri jännitetasoilla olevien energiansiirtoteiden sähköisenä erotteluna. Esimerkiksi Olkiluoto 3 -laitoksen omakäyttösähkö saadaan ulkoisesta 400 kV verkosta tai siitä riippumattomasta 110 kV:n verkosta. Turvallisuudelle tärkeiden laitteiden sähkönsyöttö on varmistettu turvallisuuslohkojen omilla varavoimadieselgeneraattoreilla (4 kappaletta), kahdella SBO-dieselgeneraattorilla *(Station Black Out)* sekä erilaisilla akustoilla. (TVO 2010a, 50–51). Eri luokkien onnettomuuksiin varautuvien sähköjärjestelmien välinen erillisyys analysoidaan ja osoitetaan suunnittelun yhteydessä.

Automaation puolustustasot ja automaatioalustan vikaantumisen tarkastelu

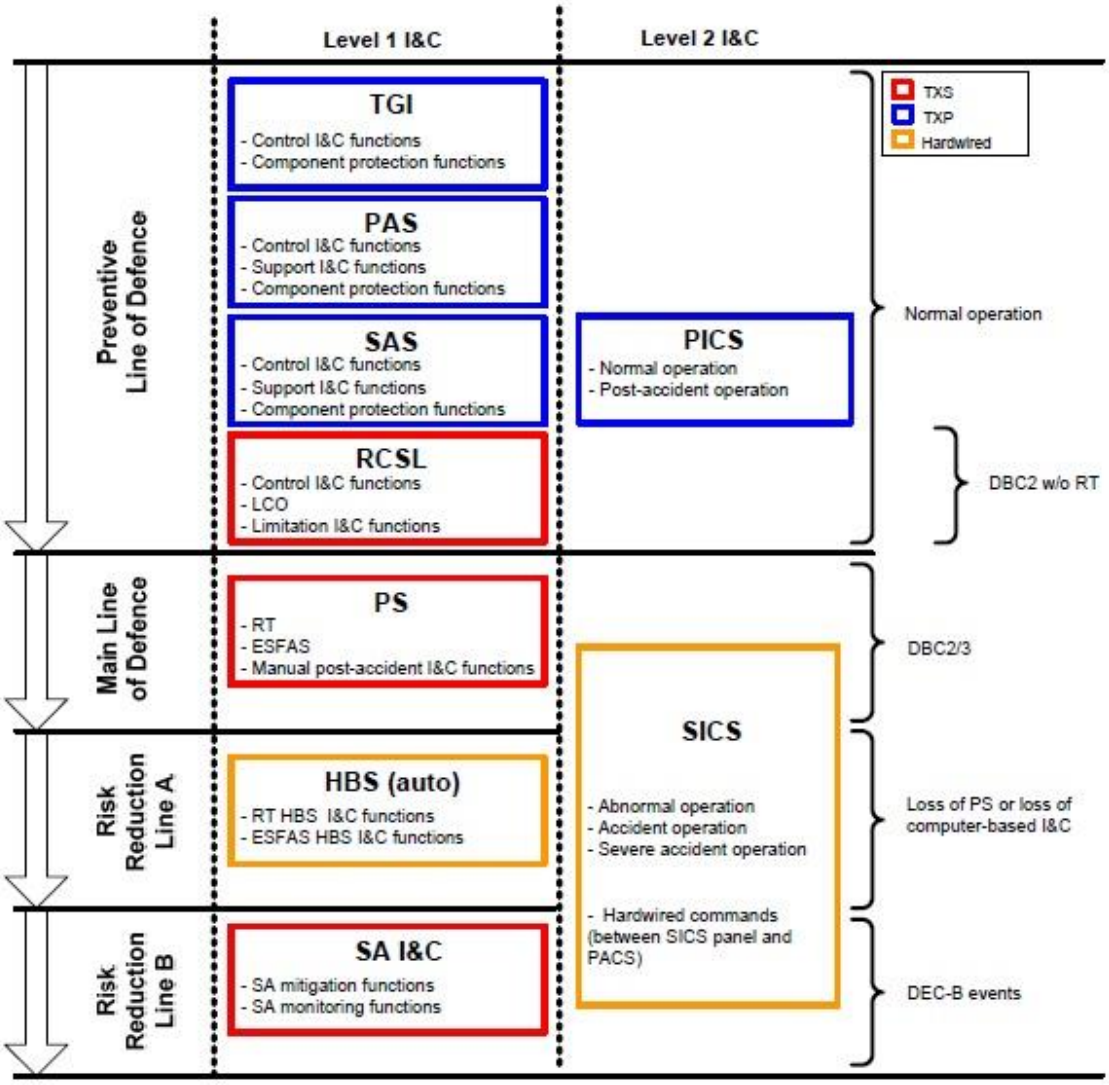
Automaatioalusta on tyypillisesti tietyn valmistajan keskenään yhteensopivista automaatiotuotteista koostuva kokonaisuus, jonka päälle erilaiset automaatiojärjestelmät rakennetaan. Vaikka automaatiojärjestelmiä kutsutaan omiksi järjestelmikseen, samalla alustalla toimivat järjestelmät voivat muodostaa turvallisuusmielessä yhden teknisen kokonaisuuden. Yhtenäinen kokonaisuus muodostuu esimerkiksi järjestelmien välisten teknisten sidoksien, kuten yhteisten väylien ja palvelimien, vuoksi. Puolustustasojen erillisyys ja erilaisuus on analysoitava sekä automaatiojärjestelmä- että automaatioalustatasolla.

Olkiluoto 3 -laitoksen automaatiojärjestelmissä käytetty syvyyssuuntainen puolustusmalli esitetään kuvassa 7.7. Automaation syvyyssuuntainen puolustus jaetaan seuraavasti neljään tasoon, jotka mukailevat yleisiä puolustustasoja:

1. a) Vikoja estävät prosessiautomaatiojärjestelmät *(Turbine Generator I&C, TGI, Process Automation System, PAS,* ja *Safety Automation System, SAS)*, jotka ohjaavat ja säilyttävät laitoksen tilan normaalien käyttöparametrien puitteissa (DBC 1).
   b) Rajoittavat automaatiojärjestelmät *(Reactor Control, Surveillance and Limitation System, RCSL)*, jotka korjaavat laitoksen tilan takaisin normaaliksi, jos normaalit käyttöparametrit ylitetään (DBC 2).
2. Pääpuolustuslinja koostuu reaktorin suojausjärjestelmästä *PS (Protection System)*, joka käynnistää automaattisesti tarvittavat turvallisuustoiminnot (reaktorin pikasulku ja suojausjärjestelmän käynnistämät tilannekohtaiset toiminnot), jos parametrit ylittävät jonkin suojausjärjestelmän kynnysarvoista (DBC 2–4).
3. DEC-tilanteita varten laitos on varustettu ohjelmistopohjaisen automaation menetystä ja suojausjärjestelmän vikaantumista vastaan erilaisuusperiaatteen puitteissa langoitetulla turva-automaatiojärjestelmällä *HBS (Hardwired Backup System)*, jonka ohjaustoimenpiteet operaattorit toteuttavat käsiohjauksella.
4. Vakavien reaktorionnettomuuksien (SA) hallitsemiseksi laitoksella on edellä mainituista järjestelmistä riippumaton vakavien onnettomuuksien automaatiojär-

jestelmä *SA I&C (Severe Accident Instrumentation and Control)*. (Areva 2013; TVO 2010a, 48–49).

Kuvasta 7.7 nähdään, että automaatiojärjestelmät on sijoitettu eri puolustustasoille ja näin ollen tasojen välinen erillisyys automaatiojärjestelmiä tarkasteltaessa säilyy. Neljän tason syvyyssuuntaista erottelua ei kuitenkaan sovelleta käyttöliittymä- tai prosessirajapinnoissa: Kuvan toisessa sarakkeessa esitettyä PICS-järjestelmää (Process Information and Control System) käytetään vakavia onnettomuuksia lukuun ottamatta kaikissa laitostilanteissa, joten se ohjaa kaikkien puolustustasojen, paitsi vakavien onnettomuuksien, järjestelmiä. SICS-järjestelmä (Safety Information and Control System) on tarkoitettu käytettäväksi vain silloin, kun PICS ei ole käytettävissä. Prosessi–instrumentaatiorajapinnassa mittaukset puolestaan ryhmitellään suoraan mittausta tarvitsevan järjestelmän mukaisiksi tai mikäli ne ohjaavat useaa järjestelmää, prioriteettimoduulin avulla.



Kuva 7.7. *Olkiluoto 3 -laitoksen automaation syvyyssuuntainen puolustus (Areva 2013).*

Puolustustasojen erottelun lisäksi tunnistetaan erikseen automaatiojärjestelmillä ohjattavat järjestelmät ja analysoidaan tilanteet, joissa ohjattava järjestelmä sijoittuu eri tasolle kuin ohjausjärjestelmä. Analysoinnin apuna voidaan hyödyntää erottelulla hallittujen kokonaisuuksien määrittämistä, jota on käsitelty luvussa 7.1.2.

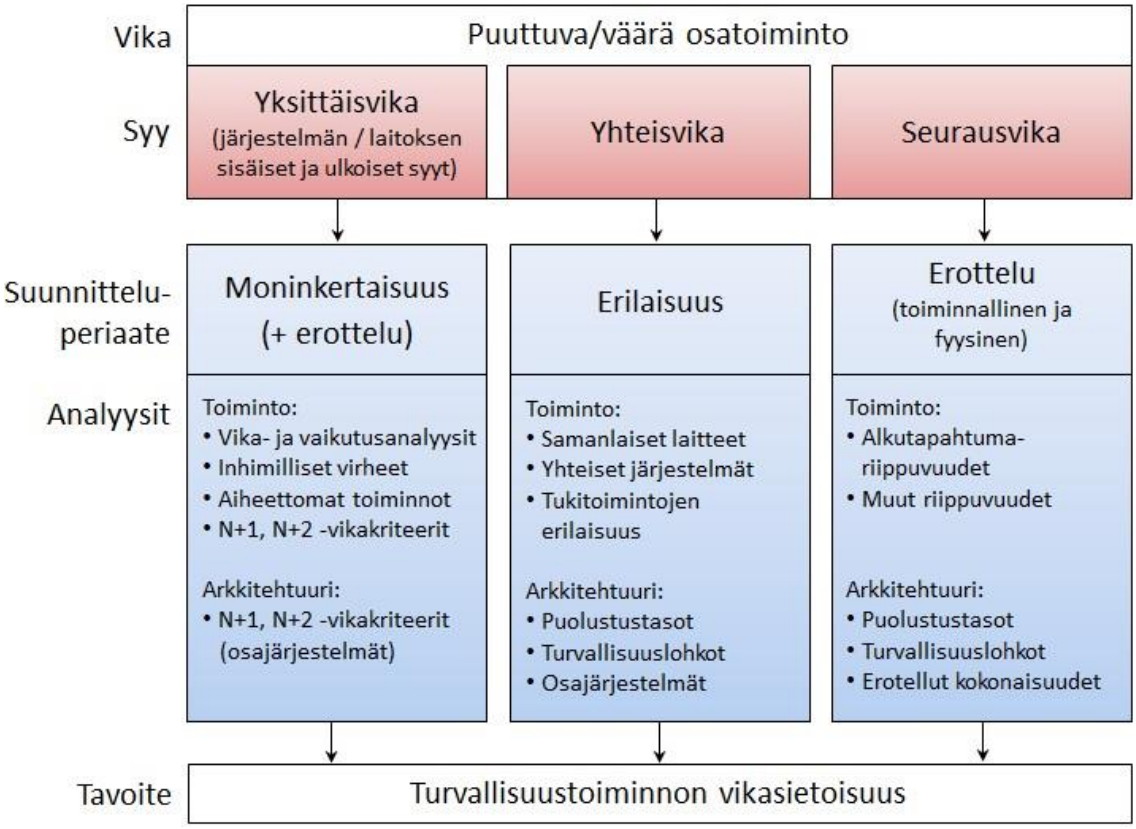
Automaation syvyyssuuntaisten puolustustasojen lisäksi kuvassa 7.7 esitetään Olkiluoto 3 -laitoksen automaatiojärjestelmien allokointi eri automaatioalustoille. TGI, PAS ja SAS-järjestelmät toteutetaan Teleperm XP automaatiotuoteperheen alustalla *(TXP)* ja loput automaatiojärjestelmät Teleperm XS -alustalla *(TXS)*, joista HBS-järjestelmä kovalangoitettuina. Vika-analyysien perusteella osoitetaan, että laajakaan automaatioalustan vikaantuminenkaan ei estä yhtäaikaisesti kaikkien puolustustasojen toimintaa.

8. YHTEENVETO JA JOHTOPÄÄTÖKSET

Osana ydinvoimalaitosten turvallisuuden varmistamista tulee tuntea niiden rakenteiden, järjestelmien ja laitteiden vikaantumismahdollisuudet ja vikojen vaikutukset. Tätä varten ydinvoimalaitoksille laaditaan lukuisia erilaisia vika-analyysejä laitosten suunnittelun, rakentamisen ja käytön aikana. Analyysejä tulisi hyödyntää kattavasti osana suunnitteluprosesseja, mutta niillä myös osoitetaan Säteilyturvakeskukselle sen laatimien YVL-ohjeiden vaatimusten täyttyminen. Tässä työssä on laadittu vika-analyyseistä esimerkkikokonaisuus, soveltaen pääosin Olkiluoto 3 -laitokselle tehtyjä analyysejä. Työssä on tarkasteltu yksittäisten analyysien eri ominaisuuksia, tavoitteita, kattavuuksia, toteutustapoja ja suhteita muihin analyyseihin.

Ydinvoimalaitoksen turvallisuustoimintojen vika-analyyseillä selvitetään niiden vikaantumismahdollisuudet sekä vikasietoisuudet. Vikasietoisuutta lisätään hyödyntämällä kolmea suunnitteluperiaatetta: toimintojen moninkertaisuutta, erilaisuutta ja erottelua. Jokainen turvallisuustoiminto ja sen järjestelmät analysoidaan periaatteisiin vastaavilla analyyseillä, huomioiden vikaantumismahdollisuudet yhden toiminnon sisällä sekä laajemmin arkkitehtuuritasolla syvyyssuuntaisen puolustuksen mukaisesti. Deterministiset turvallisuusanalyysit ja todennäköisyysperusteiset riskianalyysit tarkastelevat vikaantumisten etenemistä ja niihin liittyviä todennäköisyyksiä perustuen muun muassa vika-analyyseillä selvitettyihin vikaoletuksiin.

Ydinvoimalaitoksen turvallisuustoiminnot voivat vikaantua aktiivisesti tai passiivisesti yksittäisvian, yhteisvian tai seurausvian johdosta. Vikojen analysointi tapahtuu osissa, jolloin yhdellä analyysillä voidaan keskittyä tietyn tyyppisten vikojen tai niiden seurausten tunnistamiseen. Työssä esitetty analyysikokonaisuus on yksi esimerkki siitä, minkälaisia analyysejä voidaan hyödyntää vikasietoisuuteen vaikuttavien suunnitteluperiaatteiden analysoinnissa. Analyysien yhteisenä tavoitteena on tunnistaa kaikki viat, jotka voivat heikentää turvallisuustoimintojen toteuttamista. Kuten kuvassa 8.1 esitetään, yksittäisvikasietoisuutta kasvatetaan ensisijaisesti järjestelmien rinnakkaisuudella, yhteisvikasietoisuutta järjestelmien erilaisuudella sekä seurausvikojen sietoisuutta järjestelmien erottelulla niin fyysisesti kuin toiminnallisestikin. Jokaisen suunnitteluperiaateen toteutumista analysoidaan siihen soveltuvilla menetelmillä.



Kuva 8.1. *Turvallisuustoimintojen vikasietoisuuteen vaikuttavat suunnitteluperiaatteet ja niitä osoittavat vika-analyysit.*

Yksittäisten vikojen ja niiden seurausten tunnistamiseen käytettyjä menetelmiä ovat järjestelmien, tukijärjestelmien ja niiden komponenttien vika- ja vaikutusanalyysit, inhimillisten virheiden analyysit ja aiheettomien toimintojen analyysit. Näillä analyyseillä tunnistettuja vikoja hyödynnetään toimintojen N+1 ja N+2 -vikakriteerien täyttymisen tarkastelussa, jonka tavoitteena on tunnistaa mahdollisten yhtäaikaisten vikojen ja esimerkiksi korjausten ja huoltojen jälkeen jäljelle jäävän kapasiteetin riittävyys toteuttaa tarvittavat turvallisuustoiminnot.

Erilaisuus- ja erotteluperiaatteilla pyritään välttämään rinnakkaisten järjestelmien samanaikaista ja samasta syystä johtuvaa vikaantumista. Lähtökohtana oletetaan, että yksittäiset laitteiden ja järjestelmien vikaantumismahdollisuudet ja niidet vaikutukset on jo tunnistettu. Yhteisvika-analyysejä käytetään yhden turvallisuustoiminnon eri toimintoketjujen välisten yhteisvikamahdollisuuksien eli laitteiden tyyppivikojen ja useaan toimintoketjuun vaikuttavien järjestelmien löytämiseen. Tukitoimintojen erilaisuusperiaatteen täyttymisestä laaditaan erilliset analyysinsä, jotta voidaan varmistaa, että tukijärjestelmien käyttö ei heikennä toimintojen välistä erilaisuutta. Lisäksi analyyseillä varmistetaan, että erilaisuusperiaatetta noudatetaan myös arkkitehtuurin suunnittelussa puolustustasojen, turvallisuuslohkojen ja osajärjestelmien välillä.

Kolmas suunnitteluperiaate, erotteluperiaate, sisältää sekä toiminnallisen että fyysisen erottelun. Erotteluperiaate tulee huomioida niin turvallisuustoimintojen, puolustus-

tasojen kuin myös turvallisuuslohkojen välillä. Tärkeää erotteluperiaatteen analysoinnissa on määrittää toimintojen väliset riippuvuudet sekä alkutapahtumien seuraukset. Fyysisen erottelun analysointi liittyy vahvasti arkkitehtuuritasoiseen erotteluun, jonka tarkoituksena on rajoittaa vika fyysisesti yhteen turvallisuuslohkoon, puolustustasoon tai osajärjestelmään. Analysoitaessa vikojen leviämistä järjestelmästä toiseen esimerkiksi informaatiovirtojen yhteydessä, voidaan hyödyntää niin kutsuttuja erottelulla hallittuja automaatiokokonaisuuksia.

Vaikka analyysit laaditaan ja tarkastetaan toisistaan erillisinä kokonaisuuksina, ei niitä voi täysin käsitellä toisistaan irrallisina, koska jokaisen analyysin tuloksia hyödynnetään useiden muiden analyysien lähtötietoina. Yksinkertaistetuissa esimerkeissä analyysit rajoittuvat yksittäisten vikojen tarkasteluun ja oletuksena on, että muut järjestelmät toimivat oikein. Todellisuudessa viat kuitenkin leviävät laitostasolla hyvin nopeasti, ja järjestelmien analysoinnissa tulee huomioida näiden yhtäaikaisten vikojen vaikutukset. Analyyseistä ei kuitenkaan tässä työssä luotu yhtä hierarkkista kokonaisuutta, vaan analyysien yhtymäkohdat muihin analyyseihin käsiteltiin erikseen analyyseittäin. Analyysien työmäärää arvioitaessa huomattiin, että yhden analyysin irrottaminen muusta suunnitteluprosessista ja työmäärän tarkka määrittäminen toisista analyyseistä erillisinä on hankalaa. Analyyseillä käsiteltävien järjestelmien tai toimintojen määrän sekä analyyseillä tuotetun tiedon määrän perusteella työmäärän voidaan kuitenkin olettaa olevan merkittävä, vähintään yksi henkilötyövuosi jokaista analyysiä kohden.

Analyysimenetelmät ovat hyvin monipuolisia ja niitä voidaan soveltaa suunnitteluprosessin eri vaiheissa useilla eri tavoilla. Menetelmiä myös kehitetään jatkuvasti vastaamaan uusiin vaatimuksiin. Etenkin automaatiota tarkastelevat analyysimenetelmät ovat ydinvoima-alalla muihin analyyseihin verrattuna vielä vähän käytettyjä ja vaativat jatkokehitystä. Esimerkiksi erottelulla hallittujen kokonaisuuksien ja vikojen leviämisen rajoittumisen määrittämiseen ei vielä ole yksiselitteisiä ohjeita tai yleisesti käytössä olevia menetelmiä.

Suomalaisilla ydinvoimalaitoksilla noudatetaan keskenään samanlaisia turvallisuusperiaatteita ja samoja YVL-ohjeiden vaatimuksia, mutta täsmälliset turvallisuustoiminnot ja niiden toteutustavat vaihtelevat laitoksittain. Tämän vuoksi työssä esitettyä analyysikokonaisuutta ei voi sellaisenaan suoraan soveltaa uuteen ydinvoimalaitokseen, mutta kokonaisuutta voidaan hyödyntää analyysien tavoitteiden täyttymisen arvioinnissa.

LÄHTEET

Lainsäädäntö ja viranomaisohjeet

STUK Y/1/2016. Säteilyturvakeskuksen määräys ydinvoimalaitoksen turvallisuudesta. Määräys annettu 22.12.2015.

Ydinenergia-asetus 161/1988. Ajantasainen säädös 755/2013.

Ydinenergialaki 990/1987. Ajantasainen säädös 676/2015.

YVL A.1 Ydinenergian käytön turvallisuusvalvonta. Säteilyturvakeskus 22.11.2013. ISBN 978-952-478-851-9 (pdf). Saatavissa: http://www.finlex.fi/data/normit/41445-YVL_A.1.pdf

YVL A.7 Ydinvoimalaitoksen todennäköisyysperusteinen riskianalyysi ja riskien hallinta. Säteilyturvakeskus 15.11.2013. ISBN 978-952-478-923-3 (pdf). Saatavissa: http://www.finlex.fi/data/normit/41423-YVL_A.7.pdf

YVL A.11 Ydinlaitoksen turvajärjestelyt. Säteilyturvakeskus 15.11.2013. ISBN 978-952-478-935-6 (pdf). Saatavissa: http://www.finlex.fi/data/normit/41427-YVL_A.11.pdf

YVL B.1 Ydinvoimalaitoksen turvallisuussuunnittelu. Säteilyturvakeskus 15.11.2013. ISBN 978-952-478-854-0 (pdf). Saatavissa: http://www.finlex.fi/data/normit/41400-YVL_B.1.pdf

YVL B.2 Ydinlaitosten järjestelmien, rakenteiden ja laitteiden luokittelu. Säteilyturvakeskus 15.11.2013. ISBN 978-952-478-857-1 (pdf). Saatavissa: http://www.finlex.fi/data/normit/41401-YVL_B.2.pdf

YVL B.3 Ydinvoimalaitoksen deterministiset turvallisuusanalyysit. Säteilyturvakeskus 15.11.2013. ISBN 978-952-478-860-1 (pdf). Saatavissa: http://www.finlex.fi/data/normit/41402-YVL_B.3.pdf

YVL B.4 Ydinpolttoaine ja reaktori. Säteilyturvakeskus 15.11.2013. ISBN 978-952-478-663-2 (pdf). Saatavissa: http://www.finlex.fi/data/normit/41403-YVL_B.4.pdf

YVL B.7 Varautuminen sisäisiin ja ulkoisiin uhkiin ydinlaitoksessa. Säteilyturvakeskus 15.11.2013. ISBN 978-952-478-872-4 (pdf). Saatavissa: http://www.finlex.fi/data/normit/41406-YVL_B.7.pdf

Muu aineisto

Ahonen, E. 2011. Vikasietoisuuden tutkiminen todennäköisyysperusteisen riskianalyysin avulla. Diplomityö. Lappeenrannan teknillinen yliopisto. 81 s.

Areva. 2004a. Topical Report 10 – Diversification Document. Areva NP. [Ei julkinen].

Areva. 2004b. Topical Report 90 – N+1, N+2 failure analyses. Areva NP. [Ei julkinen].

Areva. 2005. Topical Report 105 – I&C architecture concept, Independence and diversity. Areva NP. [Ei julkinen].

Areva. 2013. Plant Level I&C Architecture [AD-02.01a]. Areva NP. [Ei julkinen].

Areva. 2014a. DC 131 – I&C Architecture Defence-in-Depth and Diversity analysis. Areva NP. [Ei julkinen].

Areva. 2014b. DC 141 – Protection System: Failure Modes and Effect Analysis. Areva NP. [Ei julkinen].

Areva. 2014c. Topical Report E1005 – Diversification and CCF Analysis. Areva NP. [Ei julkinen].

Areva. 2015. I&C Architecture Analyses – Phase 4. Architecture analyses and SAS FMEA -workshop, esityskalvot 21.10.2015. Areva NP. [Ei julkinen].

Ervamaa, J., Mankamo, T. & Suokas, J. 1979. Luotettavuustekniikka. Insinööritieto Oy, Helsinki. 326 s. ISBN 951-793-055-0.

EU. 2014. Ydinlaitosten ydinturvallisuutta koskevan yhteisön kehyksen perustamisesta annetun direktiivin 2009/71/Euratom muuttamisesta. Neuvoston direktiivi 2014/87/EURATOM, annettu 8.7.2014. Saatavissa: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32014L0087&from=FI

Fieandt, J., Mankamo, T., Reunanen, M. & Salo, R. 1983. Prosessijärjestelmän poikkeamatarkastelu. Valtion teknillinen tutkimuskeskus, Espoo. 24 s. ISBN 951-38-1718-0.

Fortum. 2014. Loviisa 1 Riskitutkimus – Pääraportin luku 2. Fortum Oyj. [Ei julkinen].

Holmberg, J. 2015. Defence-in-depth, PSA and digital I&C. NKS-R MODIG and PLANS -workshop, esityskalvot 29.9.2015. Risk Pilot AB. [Ei julkinen].

IAEA. 1992. Probabilistic Safety Assessment. International Atomic Energy Agency, Wien. 23 s. IAEA Safety Series No. 75-INSAG-6. ISBN 92-0-102492-4.

IAEA 1993. Defining initiating events for purposes of probabilistic safety assessment. International Atomic Energy Agency, Wien. 150 s. IAEA-TECDOC-719.

IAEA. 2006. Fundamental Safety Principles. International Atomic Energy Agency, Wien. 21 s. IAEA Safety Fundamentals No. SF-1. ISBN 92-0-110706-4.

IAEA. 2009. Deterministic safety analysis for nuclear power plants. International Atomic Energy Agency, Wien. 62 s. IAEA Specific safety guide No. SSG-2. ISBN 978-92-0-113309-0.

IAEA. 2012. Safety of Nuclear Power Plants: Design. International Atomic Energy Agency, Wien. 66 s. IAEA Specific Safety Requirements No. SSR-2/1. ISBN 978-92-0-121510-9.

Laitonen, J. 2010. Todennäköisyyspohjainen riskien seuranta ydinvoimalaitosten valvonnassa. Diplomityö. Aalto-yliopisto. 66 s.

Palukka, P. 2008. Luotettavuus- ja riskianalyysi. Opintomoniste. Tampereen teknillinen yliopisto, turvallisuuden johtaminen ja suunnittelu.

Rakennustutkimus RTS. 2015. Omatalorakentaminen työllistää. Rakennustutkimus RTS Oy, Helsinki. Saatavilla: http://www.omatalo.com/wordpress/wp-content/uploads/2015/03/Ostamalla-Omatalon-annat-tyoetae-viidelle.pdf [Luettu 22.1.2016].

Reiman, L. 2007. Ydinvoimalaitoksia koskevat turvallisuusvaatimukset. Verkkojulkaisu 19.11.2007. Säteilyturvakeskus. Saatavilla: http://edu.pyhajoki.fi/lukiouusi/Oppiaineet/Fysiikka/sateily/Ydinvoimalaitosta_koskevat_turvallisuusvaatimukset_Pyhajoki_tiedostot/frame.htm [Luettu 3.2.2016].

Sandberg, J. (toim.). 2013. Ydinturvallisuus. Kirjasarja: Säteily- ja ydinturvallisuus, osa 5. 2. painos. Säteilyturvakeskus, Porvoo. 418 s. ISBN 951-712-500-3.

STUK. 2008. Säteily- ja turvallisuuskatsauksia: Ydinvoimalaitosten turvallisuus. Esite. Säteilyturvakeskus, Helsinki. 7 s.

STUK. 2015a. YVL B.1 Ydinvoimalaitoksen turvallisuussuunnittelu. Perustelumuistio 21.9.2015. Säteilyturvakeskus. Saatavissa: https://ohjeisto.stuk.fi/YVL/B.1-perust.pdf

STUK. 2015b. YTV 4.3.1 Deterministiset turvallisuusanalyysit. STUKin toimintajärjestelmä, ohje 3.2.2015. Säteilyturvakeskus, Helsinki. [Ei julkinen].

STUK. 2015c. FinPSA-tietokoneohjelma. Säteilyturvakeskus. [Ei julkinen].

STUK. 2016. STUKin määräykset korvasivat valtioneuvoston asetukset. Verkkouutinen 7.1.2016. Saatavissa: http://www.stuk.fi/-/stukin-maaraykset-korvasivat-valtioneuvoston-asetukset [Luettu 8.1.2016].

Suikkanen, P. 2015. Failure tolerance analysis. NKS-R MODIG and PLANS - workshop, esityskalvot 29.9.2015. Säteilyturvakeskus. [Ei julkinen].

Toivonen, H. (toim.), Rytömaa, T. & Vuorinen, A. 1988. Säteily ja turvallisuus. Säteilyturvakeskus, Helsinki. 640 s. ISBN 951-860-933-0.

TUD-kansliet. 2010. T-boken – Tillförlitlighetsdata för komponenter i nordiska kraftreaktorer. Vattenfall Power Consultant AB, Stockholm. 358 s. ISBN 978-91-633-6143-2.

TVO. 2008. OL1/OL2 PSA osa 7. Teollisuuden Voima Oyj. [Ei julkinen].

TVO. 2009. OL1/OL2 PSA osa 17. Teollisuuden Voima Oyj. [Ei julkinen].

TVO. 2010a. Ydinvoimalaitosyksikkö Olkiluoto 3. Esite. Teollisuuden Voima Oyj, Eura. 61 s.

TVO. 2010b. OL1/OL2 PSA osa 6. Teollisuuden Voima Oyj. [Ei julkinen].

TVO. 2011a. OL1/OL2 PSA osa 2. Teollisuuden Voima Oyj. [Ei julkinen].

TVO. 2011b. OL1/OL2 PSA osa 5. Teollisuuden Voima Oyj. [Ei julkinen].

TVO. 2011c. OL1/OL2 PSA osa 16. Teollisuuden Voima Oyj. [Ei julkinen].

TVO. 2013. OL1 & OL2 Ydinvoimalaitosyksiköt. Esite. Teollisuuden Voima Oyj, Helsinki. 58 s.

TVO. 2016. TVO työnantajana – Henkilöstö. Verkkosivu. Teollisuuden Voima Oyj. Saatavissa: http://www.tvo.fi/Henkilöstö [Luettu 20.1.2016].

Vaurio, J. 2006. Luotettavuustekniikka. Opintomoniste. Lappeenrannan teknillinen yliopisto, Energia- ja ympäristötekniikan osasto.

WENRA. 2015. Reactor Harmonisation Working Group (RHWG). Verkkosivu. Western European Nuclear Regulators Association. Saatavissa: http://www.wenra.org/harmonisation/reactor-harmonisation-working-group/ [Luettu 21.12.2015].