Ydinvoimalaitoksen turvallisuustoimintojen varmistaminen vikautumisten varalta

Tämä ohje on voimassa 1.7.1996 alkaen toistaiseksi. Ohje kumoaa 6.4.1983 annetun ohjeen YVL 2.7.

Toinen, uudistettu painos
Helsinki 1996
Oy Edita Ab
ISBN 951-712-127-X
ISSN 0783-2338

Valtuutusperiaatteet

Säteilyturvakeskus antaa ydinenergian käytön turvallisuutta koskevat yksityiskohtaiset määräykset ydinenergialain (990/87) 55 §:n 2 momentin 3 kohdan ja ydinvoimalaitosten turvallisuutta koskevista yleisistä määräyksistä annetun valtioneuvoston päätöksen (395/91) 29 §:n nojalla.

YVL-ohjeet ovat sääntöjä, joita yksittäisen luvanhaltijan tai muun kyseeseen tulevan organisaation on noudatettava, ellei Säteilyturvakeskukselle ole esitetty muuta hyväksyttävää menettelytapaa tai ratkaisua, jolla YVL-ohjeessa esitetty turvallisuustaso saavutetaan. Ohje ei muuta Säteilyturvakeskuksen ennen ohjeen voimaantuloa tekemiä päätöksiä, ellei Säteilyturvakeskus ilmoita siitä erikseen.

1 Yleistä

Valtioneuvoston päätöksessä (395/91) esitetään ydinvoimalaitosten turvallisuutta koskevat yleiset määräykset. Ohjeessa YVL 1.0 esitetään puolestaan valtioneuvoston päätöstä täsmentävät ydinvoimalaitosten suunnittelussa noudatettavat turvallisuusperiaatteet.

Valtioneuvoston päätöksen (395/91) 18 §:n mukaan tärkeimpiä turvallisuustoimintoja suorittavien järjestelmien on pystyttävä toteuttamaan tehtävänsä, vaikka mikä tahansa järjestelmän yksittäinen laite olisi toimintakyvytön ja vaikka mikä tahansa turvallisuustoimintoon vaikuttava laite olisi samanaikaisesti poissa käytöstä korjauksen tai huollon vuoksi. Näitä turvallisuustoimintoja käsitellään ohjeessa YVL 1.0.

Päätöksen 18 §:ssä edellytetään myös, että tärkeimpien turvallisuustoimintojen varmistamisessa on käytettävä mahdollisuuksien mukaan eri toimintaperiaatteisiin perustuvia järjestelmiä.

Tässä ohjeessa esitetään edellä mainittuja yleisiä suunnitteluvaatimuksia täydentäviä soveltamisohjeita vikautumisten huomioonottamisesta ydinvoimalaitosten turvallisuustoimintojen varmistamisessa ja periaatteet vikakriteerien soveltamiseksi eri turvallisuustoimintoihin sekä vaatimukset vika-analyysien tekemisestä.

Primääri- ja sekundääripiirin paineenhallintaan käytettävien järjestelmien suunnittelua käsitellään ohjeessa YVL 2.4 sekä turvallisuusjärjestelmät käynnistävien ja niiden toimintaa ohjaavien suojausjärjestelmien ja sähköjärjestelmien suunnittelua ohjeessa YVL 5.5.

Ohjeessa YVL 2.2 käsitellään ydinvoimalaitoksen teknisten ratkaisujen perustelemiseksi vaadittavia häiriö- ja onnettomuusanalyysejä. Ohjeeseen sisältyvät myös vaatimukset siitä, minkälaisia laitevikoja ja ohjaajien virheellisiä toimenpiteitä näissä analyyseissä pitää olettaa.

2 Yleisiä suunnitteluperiaatteita

Valtioneuvoston päätöksen (395/91) 13 §:n mukaan suuriin radioaktiivisten aineiden päästöihin johtavien onnettomuuksien on oltava erittäin epätodennäköisiä. Tämän vaatimuksen täyttämiseksi ydinvoimalaitoksen turvallisuustoimintojen tulee olla hyvin luotettavia. Tärkeimpien turvallisuustoimintojen luotettavuuden suunnittelutavoitteet esitetään ohjeessa YVL 2.8.

Turvallisuusjärjestelmien suunnittelussa tulee käyttää sekä deterministisiä että todennäköisyyspohjaisia suunnitteluperiaatteita. Turvallisuustoimintoihin kohdistuvia luotettavuusvaatimuksia asetettaessa tulee ottaa huomioon alkutapahtuman todennäköisyys ja seurausvaikutusten vakavuus.

Turvallisuustoimintojen varmistamisessa käytettävät yleiset suunnitteluperiaatteet esitetään valtioneuvoston päätöksen (395/91) 18 §:ssä. Rinnakkaisperiaatteen käytöstä seuraa, että turvallisuusjärjestelmä koostuu vähintään kahdesta rinnakkaisesta, samaan tehtävään tarkoitetusta osajärjestelmästä. Turvallisuustoimintojen varmistamisessa on käytettävä erotteluperiaatetta siten, että toisiaan varmistavien turvallisuusjärjestelmien sekä turvallisuusjärjestelmien rinnakkaisten osien vioittuminen samasta ulkoisesta syystä on epätodennäköistä.

Järjestelmän luotettavuuden kannalta saattaa joissakin tapauksissa olla edullista, että muuten erilliset osajärjestelmät voidaan poikkeuksellisessa tilanteessa käyttötoimenpitein kytkeä ristiin. Tällaisessa tapauksessa tulee käyttää luotettavia varmistuksia tarkoituksettoman ristiinkytkennän estämiseksi.

Rinnakkaisperiaatteen käytön avulla saavutettavaa turvallisuustoiminnon luotettavuutta rajoittaa laitteiden yhteisvikojen mahdollisuus. Tämän vuoksi tärkeimmiltä turvallisuus-

toiminnoilta edellytetään valtioneuvoston päätöksen (385/91) 18 §:n mukaisesti mahdollisuuksien mukaan eri toimintaperiaatteisiin perustuvien järjestelmien käyttöä.

3 Vikakriteerien soveltaminen turvallisuustoimintoihin

3.1 Soveltamisperiaatteet

Yksittäisvika tarkoittaa satunnaisvikaa ja sen seurausvaikutuksia, jotka oletetaan tapahtuviksi joko normaalissa käyttötilanteessa tai alkutapahtuman ja sen seurausvaikutuksien lisäksi.

Alkutapahtuman ja yksittäisvian seurausten arvioinnissa on otettava huomioon järjestelmän rinnakkaisten osajärjestelmien mahdollinen riippuvuus. Erityisesti on tarkasteltava osajärjestelmien välisiä ristikytkentöjä ja yhteyksiä järjestelmiin, joilla ei ole ydinteknillistä turvallisuusmerkitystä.

Vikakriteereitä sovellettaessa tulee eräitä poikkeuksia lukuunottamatta tarkastella kahdentyyppisiä vikoja. On otettava huomioon sekä laitteiden toimintoviat eli aktiiviset viat että passiiviset viat, jotka voivat sattua järjestelmän tai laitteen suorittaessa turvallisuustehtäväänsä.

Toimintovika on laitteen tai sen osan tilan muutokseen liittyvä virhetoiminto. Laitteen toimintovika on mahdollinen esimerkiksi silloin, kun laitteen toiminta vaatii jonkin osan mekaanista liikettä. Viitteessä 2 mainitaan esimerkkejä tyypillisistä toimintovioista. Koneteknisen laitteen tai nestettä tai kaasua sisältävän järjestelmän passiivinen vika voi puolestaan olla laitteen tai rakenteen eheyden menetys tai virtaustien tukkeutuminen.

Laitteen aiheeton käynnistys voidaan jättää ottamatta huomioon toimintovikana, mikäli sitä voidaan pitää hyvin epätodennäköisenä esimerkiksi sen johdosta, että laitteen käyttövoima on kytketty pois luotettavalla tavalla.

Sähköteknisissä järjestelmissä ja laitteissa on vikautumistyyppejä, jotka ovat luonteeltaan passiivisia. Vikakriteereitä sovellettaessa ei kuitenkaan sähkö- ja automaatiojärjestelmissä tai turvallisuusjärjestelmien instrumentoinnissa erotella toimintovikoja ja passiivisia vikoja. Niitä varten tehtävissä kohdan 6 tarkoittamissa vika-analyyseissä on käsiteltävä luonteeltaan sekä toimintovikoja että passiivisia vikoja edustavia vikatyyppejä.

Suunnittelussa huomioon otettava passiivinen vika tulee määritellä analysoimalla mahdolliseksi arvioituja vikautumis- ja vuototapoja niin, että järjestelmän käyttöolosuhteet otetaan huomioon asianmukaisella tavalla. Pahimmaksi suunnittelussa huomioon otettavaksi viaksi saatetaan määritellä esimerkiksi pumpun tai venttiilin tiivisteen pettäminen tai pienputken katkeaminen, mikäli järjestelmän käyttöolosuhteiden sekä laitteiden ja rakenteiden suunnittelun, valmistuksen ja tarkastusten perusteella on osoitettavissa, että tätä pahempien vikautumisten todennäköisyys on erittäin pieni.

Passiivinen vika voidaan jättää kokonaan ottamatta huomioon, jos sen todennäköisyys voidaan osoittaa riittävän pieneksi. Passiivisen vian soveltamista arvioitaessa otetaan lisäksi huomioon alkutapahtuman jälkeinen ajanjakso, jonka kuluessa laitetta tai rakennetta tarvitaan, sekä vikautumisen vaikutus turvallisuustoiminnon onnistumiseen ja laitoksen kokonaisriskiin.

Edellytyksenä sille, että passiivista vikaa ei tarvitse ottaa huomioon on, että laite on suunniteltu, valmistettu ja tarkastettu korkeiden laatuvaatimusten mukaisesti ja että sama laatutaso ylläpidetään käytönaikaisen kunnossapidon avulla. Mahdollisia kohteita, joissa nämä edellytykset voivat täyttyä, ovat esimerkiksi rakennukset, vesisäiliöt ja laitteiden tukirakenteet. Mahdollinen passiivisen vian soveltamatta jättäminen tulee perustella edellä mainittujen tekijöiden ja edellytysten osalta kohdan 6 tarkoittamassa vika-analyysissä.

Sovellettaessa vikakriteereitä turvallisuustoimintoja suorittaviin järjestelmiin ja laittei-

siin oletetaan, että näiden toimintakyky voidaan määräajoin testata. Testausmahdollisuus tulee ottaa huomioon järjestelmää suunniteltaessa. Vikaa, jota ei voida luotettavasti havaita määräaikaiskokeissa tai -tarkastuksissa ja joka ei aiheuta laitoksen päävalvomossa hälytystä tai muuta indikaatiota, on pidettävä piilevänä vikana. Mikäli tällaisen piilevän vian mahdollisuus todetaan, ensisijainen toimintatapa on muuttaa järjestelmän suunnittelua tai testaustapaa siten, että viat voidaan havaita helpommin. Mikäli tämä ei ole mahdollista, piilevän vian mahdollisuus tulee ottaa huomioon kohdan 6 tarkoittamissa vika-analyyseissä.

Turvallisuustoimintojen käynnistämisessä tai toiminnassa välttämättömien apujärjestelmien toiminta katsotaan osaksi turvallisuustoimintoa ja siten niiden luotettavuuden tulee vastata turvallisuustoiminnolle asetettuja vaatimuksia.

Sovellettaessa vikakriteereitä turvallisuustoimintoihin voidaan erityisestä syystä tehdä poikkeuksia edellä esitettyihin soveltamisperiaatteisiin. Poikkeaminen tulee perustella kohdan 6 tarkoittamassa vika-analyysissä. Esimerkiksi vikakriteerien täyttämättä jättäminen saattaa olla perusteltua hyvin harvinaisten alkutapahtumien seurausvaikutusten yhteydessä.

3.2 Soveltamissäännöt

Tässä luvussa esitetään, miten valtioneuvoston päätöksen (395/91) 18 §:ssä esitettyjä vikakriteereitä tulee soveltaa eri turvallisuustoimintoihin ohjeessa YVL 1.0 esitettyjen vaatimuksien mukaisesti.

Reaktiivisuuden hallintajärjestelmät on suunniteltava siten, että niistä kumpikin toteuttaa turvallisuustoimintonsa myös yksittäisvikautumisen sattuessa.

Jos vain toinen reaktiivisuuden hallintajärjestelmä pystyy yksinään pitämään reaktorin pysäytettynä kaikissa lämpötiloissa, sen on voitava toteuttaa turvallisuustoimintonsa myös yksittäisvikautumisen sattuessa, vaikka mikä tahansa turvallisuustoimintoon vaikuttava laite olisi samanaikaisesti pois käytöstä korjauksen tai huollon vuoksi.

Reaktiivisuuden hallintajärjestelmät on suunniteltava siten, että säätöjärjestelmän yksittäisvika tai yksittäinen ohjausvirhe ei aiheuta tehon kasvua reaktorin pysäytystä edellyttävälle rajalle.

Reaktorin jälkilämmön poisto ja lämmönsiirto lopulliseen lämpönieluun on voitava toteuttaa käyttötilanteissa ja oletetuissa onnettomuuksissa myös yksittäisvikautumisen sattuessa, vaikka mikä tahansa näihin turvallisuustoimintoihin vaikuttava laite olisi samanaikaisesti pois käytöstä korjauksen tai huollon vuoksi.

Käytetty polttoaine on voitava jäähdyttää myös yksittäisvikautumisen sattuessa.

Reaktorin hätäjäähdytysjärjestelmän tulee toteuttaa tehtävänsä myös yksittäisvikautumisen sattuessa, vaikka mikä tahansa turvallisuustoimintoon vaikuttava laite olisi samanaikaisesti pois käytöstä korjauksen tai huollon vuoksi.

Suojarakennuksen lämmönpoisto on voitava toteuttaa oletetuissa onnettomuuksissa myös yksittäisvikautumisen sattuessa, vaikka mikä tahansa turvallisuustoimintoon vaikuttava laite olisi samanaikaisesti pois käytöstä korjauksen tai huollon vuoksi.

Palavien kaasujen käsittely suojarakennuksessa on voitava toteuttaa oletetuissa onnettomuuksissa myös yksittäisvikautumisen sattuessa.

Suojarakennuksen kaasutilaa on voitava puhdistaa onnettomuuksien aikana myös yksittäisvikautumisen sattuessa.

Turvallisuustoiminnot käynnistävän suojausjärjestelmän on toimittava odotettavissa olevissa käyttöhäiriöissä ja oletetuissa onnettomuuksissa myös yksittäisvikautumisen sattuessa, vaikka mikä tahansa turvallisuustoimintoon vaikuttava laite olisi samanaikaisesti pois käytöstä korjauksen tai huollon vuoksi.

Turvallisuustoimintoja palvelevan sisäisen sähkötehon syöttöjärjestelmän on voitava toteuttaa tehtävänsä odotettavissa olevissa käyttöhäiriöissä ja oletetuissa onnettomuuksissa myös yksittäisvikautumisen sattuessa, vaikka mikä tahansa turvallisuustoimintoon vaikuttava laite olisi samanaikaisesti pois käytöstä korjauksen tai huollon vuoksi.

Reaktorin paineen säätö on suunniteltava siten, että paine voidaan käyttötilanteissa pitää normaalin jäähdytyksen edellyttämissä rajoissa, vaikka jossakin paineen säätöön käytettävässä laitteessa tai säätöjärjestelmässä sattuisi yksittäisvika.

Reaktorin jäähdytysjärjestelmän vuotojen havaitsemiseksi on suunniteltava järjestelmä, joka antaa tiedon vuodosta ja sen suuruudesta riittävän nopeasti myös yksittäisvikautumisen sattuessa ja jonka avulla vuoto voidaan paikallistaa riittävän nopeasti.

Reaktorin jäähdytteen tilavuuden säätö on suunniteltava siten, että jäähdytteen tilavuus primääripiirissä voidaan pitää normaalin jäähdytyksen edellyttämissä rajoissa, vaikka jossakin tilavuuden säätöön vaikuttavassa laitteessa tai säätöjärjestelmässä sattuisi yksittäisvika.

Ydinvoimalaitokseen on suunniteltava järjestelmät, jotka käyttötilanteissa jäähdyttävät primääripiiriä. Näiden järjestelmien on toimittava myös yksittäisvikautumisen sattuessa.

Suojarakennus on voitava eristää onnettomuuksissa myös yksittäisvikautumisen sattuessa.

Niiden ilmastointi- ja suodatusjärjestelmien, jotka vähentävät laitostilojen ilman sisältämien radioaktiivisten aineiden pitoisuuksia, estävät radioaktiivisten aineiden leviämisen muihin laitostiloihin tai rajoittavat radioaktiivisten aineiden pääsyä ympäristöön, tulee toimia suunnitellulla tehollaan myös yksittäisvikautumisen sattuessa käyttötilanteissa ja oletettujen onnettomuuksien aikana.

Ydinvoimalaitoksen valvomon, väestönsuojan ja onnettomuuksien aikana toiminnan johtamiseen tarvittavien tilojen suodattavan tuloilmajärjestelmän on voitava toteuttaa turvallisuustoimintonsa myös yksittäisvikautumisen sattuessa käyttötilanteissa ja onnettomuuksissa.

Onnettomuuksien seurantaan ja hallintaan tarkoitettujen mittausjärjestelmien on toimittava myös yksittäisvikautumisen sattuessa.

Radioaktiivisten aineiden päästöjä suunnitelluilla päästöreiteillä on voitava valvoa myös yksittäisvikautumisen sattuessa käyttötilanteissa ja onnettomuuksien aikana.

Niiden järjestelmien, jotka varmistavat suojarakennuksen eheyttä vakavan reaktorionnettomuuden yhteydessä, on voitava toteuttaa turvallisuustoimintonsa myös yksittäisvikautumisen sattuessa.

3.3 Palontorjuntaa koskevat erityisvaatimukset

Kohdan 3.2 tarkoittamien odotettavissa olevien käyttöhäiriöiden alkutapahtumina tulee tarkastella myös yhteen palotekniseen osastoon rajoittuvia tulipaloja. Vikakriteerejä sovelletaan tällöin sellaisinaan kohdan 3.2 mukaisesti.

Mikäli voidaan perustellusti osoittaa, että yhteen palotekniseen osastoon rajoittuva tulipalo ei aiheuta alkutapahtumaa, pidetään paloa ja sen aiheuttamia turvallisuuden kannalta tärkeiden järjestelmien vikoja yksittäisvikautumisena. Kohdassa 3.2 esitettyjä vikakriteereitä sovelletaan tällöin sellaisenaan käyttötilanteisiin.

Jos tulipalo jossakin paloteknisessä osastossa voisi aiheuttaa merkittävän radioaktiivisten aineiden vapautumisen laitostiloihin tai ympäristöön, tulee palon havaitseminen ja sammutus tässä osastossa varmistaa palontorjuntajärjestelmillä, jotka voivat toteuttaa tehtävänsä myös yksittäisvikautumisen sattuessa.

Palontorjuntaa koskevia suunnitteluvaatimuksia käsitellään tarkemmin ohjeessa YVL 4.3.

4 Erilaisuusperiaatteen käyttö

Turvallisuusjärjestelmien rinnakkaisten osien laitteiden yhteisviat voivat heikentää järjestelmän toiminnan luotettavuutta. Yhteisvikojen syitä voivat olla esimerkiksi puutteet laitteen suunnittelussa, testauksessa tai huollossa. Samoin laitteiden ympäristöolosuhteet voivat aiheuttaa yhteisvikoja.

Turvallisuusjärjestelmien suunnittelussa ja käyttö- ja huoltotoiminnassa tulee kiinnittää erityistä huomiota yhteisvikojen välttämiseen. Viitteessä /2/ on esitetty laadunvarmistukseen, laitteiden kvalifiointiin ja erotteluperiaatteen käyttöön perustuvia menetelmiä yhteisvikojen estämiseksi. Yhteisvikojen mahdollisuus on kuitenkin otettava huomioon.

Valtioneuvoston päätöksen (395/91) 18 §:n perusteella edellytetään tärkeimpien turvallisuustoimintojen varmistamisessa käytettävän mahdollisuuksien mukaan eri toimintaperiaatteisiin perustuvia järjestelmiä. Erilaisuusperiaatetta tulee noudattaa, mikäli turvallisuustoiminnolta edellytetään ohjeessa YVL 2.8 korkeaa luotettavuutta tai mikäli on erityistä syytä epäillä, että turvallisuustoiminnon luotettavuus voi heikentyä yhteisvikojen vuoksi.

Yhteisvikamahdollisuuden arviointi voi perustua käyttökokemuksiin, kvalitatiiviseen analyysiin laitteiden vikamekanismeista ja todennäköisyyspohjaisen turvallisuusanalyysin tuloksiin. Seuraavassa esitetään eräin tarkennuksin ne turvallisuustoiminnot, joissa ohjeen YVL 1.0 mukaan ainakin tulee käyttää erilaisuusperiaatteeseen perustuvia järjestelmiä.

Reaktiivisuuden hallitsemiseksi tulee suunnitella kaksi toisistaan riippumatonta, eri periaatteilla toimivaa hallintajärjestelmää, joista kumpikin erikseen pystyy pysäyttämään reaktorin käyttötilanteissa.

Mikäli reaktiivisuusonnettomuuden estämisessä tarvitaan laitteiden aktiiviseen toimintaan perustuvia suojaustoimenpiteitä, edellytetään myös näiltä korkeaa luotettavuutta ja erilaisuusperiaatteen käyttöä.

Reaktorisuojausjärjestelmän suunnittelussa tulee noudattaa erilaisuusperiaatetta. Erityisesti vaaditaan, että reaktorin suojausjärjestelmässä tulee mitata vähintään kahta eri prosessisuuretta, jotka ovat molemmat fysikaalisesti häiriötilanteesta tai onnettomuudesta riippuvia ja joiden laukaisurajat voidaan valita siten, että ne saavutetaan riittävän aikaisin. Mikäli tämä ei ole kaikissa suojaustoiminnoissa mahdollista, tulee käyttää eri mittausperiaatteita ko. prosessisuureen mittaamisessa.

Reaktorin jälkilämmön poisto ja lämmönsiirto lopulliseen lämpönieluun tulee suunnitella noudattaen erilaisuusperiaatetta. Erityisesti tulee laitoksen suunnittelussa varautua normaalisti käytettävän lopullisen lämpönielun käytön keskeytymiseen.

Reaktorin jäähdytysjärjestelmän paineenhallinnan suunnittelussa tulee noudattaa erilaisuusperiaatetta ohjeen YVL 2.4 mukaisesti.

Reaktorin hätäjäähdytysjärjestelmän suunnittelussa tulee noudattaa erilaisuusperiaatetta.

Häiriötilanteissa ja onnettomuuksissa laitoksen yleiskuvan ja hälytysinformaation esittämisessä valvomossa käytettävien järjestelmien suunnittelussa tulee noudattaa mahdollisuuksien mukaan erilaisuusperiaatetta.

Ydinvoimalaitoksen suunnittelussa tulee ottaa huomioon se mahdollisuus, että laitoksen ulkoiset ja sisäiset vaihtosähkötehon syöttölähteet menetetään yhtaikaa. Erilaisuusperiaatteen mukaisesti laitoksella tulee olla käytettävissä vaihtosähkön syöttölähde, joka on riippumaton käyttötilanteita ja oletettuja onnettomuuksia varten suunnitelluista sähkötehon syöttölähteistä.

5 Vikakriteerien soveltaminen noudatettaessa erillisyysperiaatetta

Kohdassa 4 vaadittua erilaisuusperiaatetta noudatettaessa vikakriteerejä sovelletaan turvallisuustoimintoihin kohdan 3.2 mukaisesti kuitenkin siten, että samanaikaista huoltoa tai korjausta koskevaa vaatimusta sovelletaan koko turvallisuustoimintoon. Lisäksi edellytetään, että eri toimintaperiaatteisiin perustuvat osajärjestelmät kukin pystyvät toteuttamaan tehtävänsä myös yksittäisvikautumisen sattuessa.

Riippumattoman vaihtosähkötehon syöttölähteen ei tarvitse täyttää vikakriteerejä, jos turvallisuustoimintoihin liittyvät sähköjärjestelmät täyttävät kohdan 3.2 vaatimukset.

Vikakriteerejä sovellettaessa voidaan ottaa huomioon vain ao. toimintoihin suunnitellut, turvallisuusluokitellut järjestelmät. Mikäli erilaisuusperiaatetta noudatettaessa turvallisuustoimintoon ensisijaisesti tarkoitettu järjestelmä yksinään täyttää kohdan 3.2 vaatimukset, voidaan toisen järjestelmän turvallisuusluokkaa alentaa, kuitenkin enintään luokkaan 3.

6 Vika-analyysit

Vika-analyyseillä on osoitettava, että kohdassa 3 esitetyt vikakriteerit ja kriteereihin liittyvät vaatimukset täyttyvät ja turvallisuustoiminnot voidaan toteuttaa. Vika-analyysit tehdään osana laitoksen ja sen järjestelmien turvallisuuden arviointia. Todennäköisyyspohjaisen turvallisuusanalyysin tekeminen ei poista vaatimusta vika-analyysien tekemisestä, mutta tällaista turvallisuusanalyysiä voidaan käyttää perusteena vikakriteerien soveltamiseen liittyville poikkeamille sekä yhteisvikojen huomioonottamiselle.

Kunkin laitteen mahdollisiksi arvioidut vikatyypit on käytävä analyysissä läpi, kunnes kaikki turvallisuustoimintoon liittyvät laitteet on analysoitu. Analyysissä oletetaan yksi satunnaisvika ja sen aiheuttamat seurausvaikutukset kerrallaan. Vika-analyysin tulee kattaa turvallisuustoimintoihin liittyvien turvallisuusjärjestelmien lisäksi näiden tarvitsemat apujärjestelmät.

Vika-analyysi voidaan tehdä seuraavan jaottelun mukaisesti.

1. Määritellään laitoksen suunnitteluperusteena olevat alkutapahtumat, joiden yhteydessä kohdassa 3.2 esitettyä turvallisuustoimintoa tarvitaan laitoksen turvallisuuden varmistamiseksi, sekä arvioidaan näiden alkutapahtumien seurausvaikutukset.
2. Tunnistetaan turvallisuustoimintoihin liittyvät järjestelmät ja laitteet, joiden on toimittava oikein kunkin alkutapahtuman yhteydessä.
3. Turvallisuustoimintoihin liittyvien laitteiden satunnaisvioista sekä huollosta ja korjauksesta tehdään oletukset kohtien 3.1 ja 3.2 mukaisesti. Satunnaisvikojen seurausvaikutukset arvioidaan. Tutkitaan piilevien vikojen mahdollisuudet ja mikäli niitä ei voida luotettavasti estää, tehdään niitä koskevat oletukset. Osoitetaan, että turvallisuustoiminto voidaan toteuttaa normaalikäytön tai alkutapahtumien yhteydessä näiden oletusten vallitessa.
4. Tunnistetaan turvallisuustoimintoihin liittyvät käyttöhenkilökunnan toimenpiteet ja analysoidaan inhimillisten virheiden vaikutus turvallisuustoimintoon. Vika-analyysissä käsitellään vain ohjaajien valvomossa tekemiä ohjausvirheitä, kuten käyttöohjeen mukaisen toimenpiteen tekemättä jättämistä tai virheellistä suoritusta. Tilanteen tunnistamiseen ja päätöksentekoon liittyviä ohjaajien virheitä käsitellään todennäköisyyspohjaisessa turvallisuusanalyysissä. Ohjausvirhettä käsitellään yksittäisvikautumisena. Turvallisuustoiminnon toteutuminen on osoitettava edellisen kohdan mukaisesti.

Yhteenveto vika-analyysien tuloksista tulee esittää järjestelmäkohtaisesti alustavassa ja lopullisessa turvallisuusselosteessa ja yksityiskohtaiset analyysit turvallisuusselosteeseen liittyvissä aihekohtaisissa raporteissa.

Turvallisuustoimintoon liittyvien laitteiden yhteisvioista ja piilevistä vioista on turvallisuusselosteeseen liittyvässä aihekohtaisessa raportissa arvioitava kunkin järjestelmän tällaiset vikamahdollisuudet sekä esitettävä selvitys siitä, miten erilaisuusperiaatetta noudatetaan turvallisuustoiminnon luotettavuuden varmistamiseksi.

7 Määritelmät

Alkutapahtuma on yksittäinen tapahtuma, jonka vaikutuksesta laitos joutuu pois normaalista käyttötilasta. Alkutapahtuma voi olla laitoksen sisäinen tai ulkoinen tapahtuma, kuten laitevika, luonnonilmiö tai ihmisen toiminnasta johtuva vaaratilanne. Alkutapahtumien määrittelyä käsitellään viitteen /1/ liitteessä.

Erilaisuusperiaate tarkoittaa rinnakkaisten järjestelmien tai laitteiden käyttämistä toteuttamaan samaa turvallisuustoimintoa siten, että nämä järjestelmät tai laitteet eroavat toisistaan jonkin ominaisuuden suhteen. Tällaisia ominaisuuksia voivat olla erilainen toimintaperiaate, erilainen valmistusmenetelmä tai eri fysikaalisten parametrien käyttö.

Ohjausvirhe on yksittäinen virheellinen toimenpide tai toimenpiteen poisjäänti ohjaajan yrittäessä tehdä turvallisuustoimintoon liittyvää ohjaustoimenpidettä.

Passiivinen vika tarkoittaa jonkin laitteen tai rakenteen eheyden menetystä tai jonkin prosessin virtaustien tukkeutumista.

Piilevä vika tarkoittaa identifioitua vikaa, joka ei aiheuta hälytystä ja jota ei havaita suunnitelmien mukaisissa testauksissa tai tarkastuksissa.

Satunnaisvika on vika, jonka esiintyminen on tilastollisesti riippumaton muiden samantyyppisten laitteiden vioista. Tilastolliset vaihtelut materiaalissa, valmistusmenetelmissä, käyttöolosuhteissa, huolloissa ja testauksissa voivat saada laitteen käyttäytymään muista samantyyppisistä laitteista poikkeavalla tavalla.

Toimintovika (josta käytetään myös nimitystä aktiivinen vika) on laitteen tai sen osan toimintatilan muutokseen liittyvä virhetoiminto. Esimerkkejä tyypillisistä toimintovioista löytyy viitteestä /2/.

Turvallisuusjärjestelmä on jotakin tämän ohjeen luvussa 3 mainittua turvallisuustoimintoa suorittava järjestelmä.

Yhteisvika tarkoittaa usean laitteen tai rakenteen vikautumista saman yksittäisen tapahtuman tai syyn seurauksena.

Yksittäisvika tarkoittaa satunnaisvikaa ja sen seurausvaikutuksia, jotka oletetaan tapahtuviksi joko normaalissa käyttötilanteessa tai alkutapahtuman ja sen seurausvaikutuksien lisäksi.

8 Viitteet

1 IAEA Safety Series No. 50-C-D (Rev. 1), Code on the Safety of Nuclear Power Plants: Design, 1988.

2 IAEA Safety Series No. 50-P-1, Application of the Single Failure Criterion, 1991.

3 IAEA Safety Series No. 50-SG-D1, Safety Functions and Component Classification for BWR, PWR and PTR, 1979.