STUK

OHJE **YVL B.1** / 15.11.2013

YDINVOIMALAITOKSEN TURVALLISUUSSUUNNITTELU

jatkuu

Uusien ydinlaitosten osalta tämä ohje on voimassa 1.12.2013 alkaen toistaiseksi. Rakenteilla olevilla ja käyvillä ydinlaitoksilla tämä ohje saatetaan voimaan erillisellä STUKin päätöksellä. Ohje kumoaa ohjeet YVL 1.0, YVL 2.0, YVL 2.7, YVL 5.2, YVL 5.5 ja YVL 5.6.

Ensimmäinen painos
Helsinki 2013

ISBN 978-952-478-853-3 (nid.) Kopijyvä Oy 2013
ISBN 978-952-478-854-0 (pdf)
ISBN 978-952-478-855-7 (html)

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

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

Valtuutusperusteet

Ydinenergialain (990/1987) 7 r §:n mukaan Säteilyturvakeskuksen tehtävänä on asettaa ydinenergialain mukaisen turvallisuustason toteuttamista koskevat yksityiskohtaiset turvallisuusvaatimukset.

Soveltamissäännöt

YVL-ohjeen julkaiseminen ei sinänsä muuta Säteilyturvakeskuksen ennen ohjeen julkaisemista tekemiä päätöksiä. Vasta kuultuaan asianosaisia Säteilyturvakeskus antaa erillisen päätöksen siitä, miten uutta tai uusittua YVL-ohjetta sovelletaan käytössä tai rakenteilla oleviin ydinlaitoksiin ja luvanhaltijoiden toimintoihin. Uusiin ydinlaitoksiin ohjeita sovelletaan sellaisenaan.

Kun Säteilyturvakeskus harkitsee YVL-ohjeissa esitettyjen, uusien turvallisuusvaatimuksien soveltamista käytössä tai rakenteilla oleviin ydinlaitoksiin, se ottaa huomioon ydinenergialain (990/1987) 7 a §:ssä säädetyt periaatteet: *Ydinenergian käytön turvallisuus on pidettävä niin korkealla tasolla kuin käytännöllisin toimenpitein on mahdollista. Turvallisuuden edelleen kehittämiseksi on toteutettava toimenpiteet, joita käyttökokemukset ja turvallisuustutkimukset sekä tieteen ja tekniikan kehittyminen huomioon ottaen voidaan pitää perusteltuina.*

Ydinenergialain 7 r §:n kolmannen momentin mukaan *Säteilyturvakeskuksen turvallisuusvaatimukset velvoittavat luvanhaltijaa, kuitenkin niin, että luvanhaltijalla on oikeus esittää muunkinlainen kuin vaatimuksissa edellytetty menettelytapa tai ratkaisu. Jos luvanhaltija vakuuttavasti osoittaa, että esitetty menettelytapa tai ratkaisu toteuttaa tämän lain mukaisen turvallisuustason, Säteilyturvakeskus voi sen hyväksyä.*

1 Johdanto

101. Ydinvoimalaitoksen turvallisuussuunnitteluun liittyvät vaatimukset perustuvat syvyyssuuntaiseen puolustusperiaatteeseen. Tässä periaatteessa ydinvoimalaitoksen suunnittelu on reaktorivaurioiden ja säteilyn haitallisten vaikutusten estämiseksi toteutettava useilla peräkkäisillä, toisiaan varmentavilla rakenteilla ja järjestelmillä. Syvyyssuuntaisen puolustusperiaatteen mukaisen rakenteisiin ja turvallisuustoimintoihin liittyvän puolustuksen perustuu viiteen peräkkäiseen tasoon, joista kaksi ensimmäistä tasoa on tarkoitettu ehkäisemään onnettomuuksia ja muut tasot on tarkoitettu suojaamaan laitosta ja sen käyttäjiä sekä ympäristöä onnettomuuden haitallisilta vaikutuksilta eli rajoittamaan onnettomuuksien seurauksia. IAEA:n ja WENRA:n ohjeissa esitetyt vaatimukset perustuvat tähän samaan periaatteeseen. Tässä ohjeessa annetaan vaatimuksia ydinvoimalaitoksen ja turvallisuudelle tärkeiden järjestelmien suunnittelua varten ja täsmennetään valtioneuvoston asetuksessa (717/2013) annettuja suunnitteluvaatimuksia.

102. Ydinvoimalaitoksen turvallisuussuunnitteluun liittyviä vaatimuksia on esitetty lisäksi seuraavissa ohjeissa:

- YVL A.1 Ydinenergian käytön turvallisuusvalvonta
- YVL A.3 Ydinlaitoksen johtamisjärjestelmä
- YVL A.5 Ydinlaitoksen rakentaminen ja käyttöönotto
- YVL A.6 Ydinvoimalaitoksen käyttötoiminta
- YVL A.7 Ydinvoimalaitoksen todennäköisyysperusteinen riskianalyysi ja riskien hallinta
- YVL A.11 Ydinlaitoksen turvajärjestelyt
- YVL B.2 Ydinlaitoksen järjestelmien, rakenteiden ja laitteiden luokittelu.

103. Ydinvoimalaitoksen turvallisuussuunnittelua täydentäviä, yksityiskohtaisia vaatimuksia on esitetty ohjeissa

- YVL A.12 Ydinlaitoksen tietoturvallisuuden hallinta
- YVL B.3 Ydinvoimalaitoksen deterministiset turvallisuusanalyysit
- YVL B.4 Ydinpolttoaine ja reaktori
- YVL B.5 Ydinvoimalaitoksen primääripiiri
- YVL B.6 Ydinvoimalaitoksen suojarakennus
- YVL B.7 Varautuminen sisäisiin ja ulkoisiin uhkiin ydinlaitoksella
- YVL B.8 Ydinlaitoksen palontorjunta
- YVL E.6 Ydinlaitoksen rakennukset ja rakenteet
- YVL E.7 Ydinlaitoksen sähkö- ja automaatiolaitteet
- YVL E.10 Ydinlaitoksen varavoimalähteet
- YVL E.11 Ydinlaitoksen nosto- ja siirtolaitteet.

104. Ydinlaitoksen rakenteellista säteilyturvallisuutta, työntekijöiden ja ympäristön säteilysuojelua sekä säteilymittauslaitteisiin liittyviä vaatimuksia käsitellään ohjeissa

- YVL C.1 Ydinlaitoksen rakenteellinen säteilyturvallisuus
- YVL C.2 Ydinlaitoksen työntekijöiden säteilysuojelu ja säteilyaltistuksen seuranta
- YVL C.3 Ydinlaitoksen radioaktiivisten aineiden päästöjen rajoittaminen ja valvonta
- YVL C.4 Ydinlaitoksen ympäristön säteilyvalvonta
- YVL C.6 Ydinlaitoksen säteilymittaukset.

2 Soveltamisala

201. Tätä ohjetta sovelletaan ydinvoimalaitoksen ja sen turvallisuudelle tärkeiden järjestelmien suunnittelua varten. Ohjetta sovelletaan sekä laitoksen alkuperäiseen suunnitteluun että siihen tehtävien muutosten suunnitteluun. Tätä ohjetta voidaan soveltaa myös muiden ydinlaitosten suunnitteluun.

3 Suunnittelun hallinta

3.1 Suunnittelusta vastaavat organisaatiot

301. Ydinenergialain (muutos 990/1987) 7 f §:n mukaan *turvallisuuden on oltava etusijalla ydinlaitoksen rakentamisessa ja käytössä.* Rakentamis-/käyttöluvan haltija vastaa siitä, että ydinlaitos rakennetaan ja että sitä käytetään turvallisuusvaatimusten mukaisesti.

302. Luvanhakijan/-haltijan on
1. varmistettava, että ydinlaitos ja sen järjestelmät on suunniteltu ja toteutettu turvallisesti ja että ne täyttävät turvallisuusvaatimukset
2. osoitettava ydinlaitoksen ja sen järjestelmien turvallisuus ja turvallisuusvaatimusten täyttyminen.

303. Luvanhakijan/-haltijan on varmistettava laitoksen suunnittelun eheys ja turvallisuus laitoksen suunnittelun, rakentamisen, käytön ja käytöstäpoiston aikana.

304. Luvanhaltijalla on oltava käytettävissään pätevää ja kokenutta henkilöstöä.

305. Luvanhaltijan on ylläpidettävä yksityiskohtaista suunnitteluaineistoa siten, että luvanhaltija pystyy varmistamaan laitoksen suunnittelun eheyden ja turvallisuuden laitoksen koko elinkaaren aikana, mukaan lukien muutosten ja laitteiden vaihtojen suunnittelu.

306. Ydinvoimalaitoksen ja sen turvallisuuden kannalta tärkeiden järjestelmien suunnitteluun osallistuvilla organisaatioilla on oltava johtamisjärjestelmä, jonka on soveltuvin osin täytettävä ohjeessa YVL A.3 asetetut vaatimukset. Suunnitteluorganisaatioiden on lisäksi täytettävä tämän ohjeen luvussa 3 asetetut vaatimukset. Luvanhaltijan tulee osoittaa, että vaatimukset täyttyvät.

307. Suunnitteluorganisaatioilla on oltava käytettävissään tarvittavat resurssit ja osaaminen. Luvanhaltijan on varmistuttava, että resurssit ja osaaminen ovat riittävät.

308. Mikäli ydinvoimalaitoksen ja sen turvallisuuden kannalta tärkeiden järjestelmien suunnitteluun osallistuva organisaatio käyttää alihankkijoita, on sen varmistuttava, että
1. alihankkija pystyy suorittamaan määritellyn tehtävän
2. alihankintana suoritettavaan suunnittelutehtävään liittyvistä turvallisuusvaatimuksista tiedotetaan selvästi ja yksiselitteisesti
3. alihankkijaa ohjataan, käytetään ja valvotaan asianmukaisesti
4. alihankkijan käyttö on läpinäkyvää ja niin yksityiskohtaisesti dokumentoitua, että sen perusteella tarvittaessa voidaan suorittaa suunnittelun riippumattoman kolmannen osapuolen arviointi.

309. Luvanhaltijan on pystyttävä osoittamaan turvallisuusvaatimusten täyttyminen koko suunnittelun alihankintaketjussa.

3.2 Suunnitteluprosessit

310. Valtioneuvoston asetuksen (717/2013) 26 §:n mukaan *ydinvoimalaitoksen turvallisuuden kannalta tärkeiden järjestelmien, rakenteiden ja laitteiden on oltava käyttökuntoisia suunnittelun perustana olevien vaatimusten mukaisesti. Käyttökuntoisuutta ja käyttöympäristön vaikutuksia on valvottava tarkastusten, testien, mittausten ja analyysien avulla. Käyttökuntoisuus on ennakolta varmistettava säännöllisillä huolloilla sekä kunnostamiseen ja korjauksiin on varauduttava käyttökuntoisuuden heikkenemisen varalta. Kunnonvalvonta ja kunnossapito on suunniteltava, ohjeistettava ja toteutettava niin, että järjestelmien, rakenteiden ja laitteiden eheys ja toimintakyky luotettavasti säilyvät koko niiden käyttöiän ajan.*

311. Ydinvoimalaitos ja sen turvallisuuden kannalta tärkeät järjestelmät on suunniteltava käyttäen vaadittuun laatutasoon soveltuvia suunnitteluprosesseja ja -menetelmiä sekä asiaankuuluvia turvallisuusmääräyksiä, ohjeita ja standardeja. Käytettävien standardien ja niiden osien soveltuvuus sekä kattavuus on perusteltava.

312. Turvallisuuden kannalta tärkeän järjestelmän suunnittelun on perustuttava elinkaarimalliin, jonka mukaan suunnittelu ja toteutus jaetaan eri vaiheisiin. Elinkaarimallin on katettava kaikki toisiaan seuraavat vaiheet vaatimusten kokoamisesta käyttövaiheeseen saakka. Elinkaarimallin on erityisesti sisällettävä erillinen vaatimusmäärittelyvaihe, joka edeltää varsinaisia suunnitteluvaiheita.

313. Kuhunkin suunnittelu- ja toteutusvaiheeseen on kuuluttava todentaminen. Todentamistoimenpiteet ja -menetelmät on suunniteltava.

314. Kukin suunnittelu- ja toteutusvaihe on katselmoitava, ennen kuin vaihe katsotaan loppuun suoritetuksi.

315. Luvanhakijan/-haltijan on varattava itselleen mahdollisuus osallistua minkä tahansa vaiheen katselmointiin. Luvanhakijan/-haltijan on osallistuttava turvallisuuden kannalta merkittäviin katselmointeihin. Luvanhakijan/-haltijan on varattava itselleen oikeus kieltää vaiheen vieminen päätökseen, jos on ilmeistä, että turvallisuusvaatimukset eivät täyty.

316. Suunnitteluun osallistuvilla organisaatioilla on oltava kyvykkäät prosessit vaatimustenhallintaa varten.

317. Kun suunnittelutehtävät koskevat useita tekniikan aloja, on järjestettävä yhteydenpitoprosessi, joilla varmistetaan asianmukainen tiedonkulku organisaatiorajapintojen yli.

318. Pätevän henkilökunnan osallistuminen jokaiseen turvallisuuden kannalta merkittävään suunnittelun osa-alueeseen on varmistettava vaihekatselmoinneilla, jotka koskevat useita tekniikan aloja.

3.3 Konfiguraation hallinta

319. Ydinlaitoksen rakentamiseen ja käyttöön liittyvät konfiguraation hallinnan prosessit ja menettelyt on määriteltävä luvanhaltijan johtamisjärjestelmässä.

320. Konfiguraation hallinnan prosessien ja menettelyjen on katettava koko laitoksen elinkaari suunnittelusta käyttöönottoon ja käyttöön.

321. Konfiguraation hallinnan prosessien ja menettelyjen on kuvattava vastuut ja konfiguraation hallinnan valvonnan menettelyt.

322. Ydinlaitoksen järjestelmät ja laitteet on jaettava riittävän pieniin kokonaisuuksiin (konfiguraatioyksiköihin) siten, että ne ovat helposti tunnistettavissa, seurattavissa ja hallittavissa.

323. Laitos, järjestelmäkokonaisuudet, järjestelmät, laitteet, ohjelmistot, apuvälineet ja näihin liittyvä dokumentaatio sekä parametrit (asetukset), sisäiset ja ulkoiset liitynnät sekä rajapinnat on valittava hierarkkisesti konfiguraatioyksiköiksi.

324. Konfiguraation hallinnan menettelyjä tulee soveltaa konfiguraatioyksiköihin ja niiden dokumentaatioon koko konfiguraatioyksiköiden elinkaaren ajan.

325. Ydinlaitoksen suunnittelun tai muutosten yhteydessä konfiguraation perustasot on määriteltävä toimintaprosessien kannalta soveltuviin pisteisiin.

326. Konfiguraation perustasojen välillä muutokset on tehtävä määriteltyjen muutostenhallintamenettelyjen mukaisesti.

327. Konfiguraatioyksiköiden dokumentaatio on päivitettävä muutosten yhteydessä.

328. Jokaisella ydinlaitoksen suunnitteluun ja muutoksiin liittyvällä organisaatiolla on oltava riittävät konfiguraation hallintamenettelyt toimittamiensa tuotteiden konfiguraation hallintaan ja kokonaisuuden yhteensopivuuden varmistamiseen omalta osaltaan.

329. Luvanhaltijan on varmistettava konfiguraation hallintamenettelyjen hyväksyttävyys ja yhteensopivuus, mikäli konfiguraation hallintamenettelyjä on toimitusketjussa useita.

330. Uuden ydinlaitoksen rakentamistoiminnassa ja käytössä olevien ydinlaitosten laajoissa laitosmuutoksissa sovellettavat konfiguraation hallintaprosessit ja ohjeet sekä vastuut ja resurssit on esitettävä projektikohtaisessa konfiguraation hallintasuunnitelmassa. Hallintasuunnitelmassa on esitettävä myös noudatettavat konfiguraation perustasot suhteessa hankkeen edistymiseen ja sen käsittelyyn STUKissa.

3.4 Laatusuunnitelmat

331. Turvallisuudelle tärkeiden järjestelmien ja niiden muutosten suunnittelua ja toteutusta varten on laadittava ja otettava käyttöön järjestelmäkohtainen laatusuunnitelma. Samaa laatusuunnitelmaa voidaan kuitenkin käyttää useita järjestelmiä varten, jos laatutavoitteet,

menetelmät laatutavoitteiden saavuttamiseksi ja suunnitelmaa toteuttava organisaatio ovat kaikissa kyseisissä järjestelmissä samat.

332. Laatusuunnitelmassa on esitettävä
1. järjestelmän suunnitteleva organisaatio vastuineen ja rajapintoineen muihin suunnitteluun liittyviin organisaatioihin
2. suunnittelussa ja toteutuksessa käytettävät standardit ja ohjeet, myös YVL-ohjeet
3. suunnittelu- ja toteutusprosessin vaiheet
4. kunkin suunnitteluvaiheen lähtötietoina käytettävät asiakirjat ja tallenteet ja muut vaihesyötteet
5. kunkin suunnitteluvaiheen tuloksina syntyvät asiakirjat ja tallenteet ja muut vaihetuotteet
6. vaiheiden päätteeksi tehtävät vaihekatselmoinnit, mukaan lukien vaihekatselmoinnin ajoitus, sisältö ja suorittaja, hyväksymiskriteerit sekä sovellettavat päätöksentekomenettelyt ja vastuut
7. alihankkijoiden valvonnassa käytettävät menettelyt
8. konfiguraation ja -muutosten hallinta ja tuotteiden tunnistamismenettelyt
9. vaatimustenmukaisuuden, suunnittelumuutosten ja toteutuspoikkeamien hallinta
10. suunnittelun ja toteutuksen rinnalla hyödynnettävät tukiprosessit ja niihin liittyvät hallinta- ja laatumenettelyt
11. prosessien vastuujako ja päätöksentekomenettelyt mukaan lukien menettelyt laatusuunnitelman muuttamista varten.

333. Järjestelmäkohtainen laatusuunnitelma on laadittava ja toteutettava tämän YVL-ohjeen vaatimusten ja soveltuvan standardin mukaisesti.

334. Standardinmukaisia prosesseja ja suunnitteluorganisaation laatukäsikirjaa käytettäessä prosessien ja ohjeiden soveltaminen on eriteltävä laatusuunnitelmassa.

335. Ohjeessa YVL A.3 esitetään toimittajan johtamisjärjestelmää täydentävää, toimitukseen liittyvää laatusuunnitelmaa koskevat vaatimukset.

3.5 Vaatimusmäärittelyt

336. Ydinlaitoksen turvallisuudelle tärkeän järjestelmän vaatimukset on määriteltävä niin yksityiskohtaisesti, että vaatimusmäärittelyprosessista riippumaton suunnittelija pystyy suorittamaan järjestelmän ja järjestelmän laitteiden käytönaikaisen ylläpidon ja muutosten edellyttämän uudelleen suunnittelun laitoksen elinkaaren ajan.

337. Toiminnallisten vaatimusten lisäksi on määriteltävä myös muut kuin toiminnalliset vaatimukset, kuten laatuvaatimukset ja -standardit.

338. Viitattujen standardien ja ohjeiden riittävyys on perusteltava. Jos esitetyistä standardeista ja ohjeista poiketaan, poikkeaminen on perusteltava ja sen vaikutus arvioitava.

339. Vaatimusmäärittelyjen on oltava yksiselitteisiä, ristiriidattomia ja jäljitettävissä olevia. Vaatimusten täyttyminen on voitava todentaa.

340. Turvallisuudelle tärkeän järjestelmän vaatimusmäärittelyn oikeellisuus, täydellisyys ja ristiriidattomuus tulee arvioida asiantuntijoiden toimesta, jotka ovat riippumattomia suunnittelusta ja toteutuksesta. Arviointiraportissa on esitettävä arvioinnissa tehdyt havainnot sekä perusteltu johtopäätös.

341. Vaatimusten jäljitettävyys eri suunnitteluvaiheissa on voitava osoittaa. Vaatimusten jäljitettävyys eri suunnitteluvaiheissa on osoitettava osana kelpoistusta.

3.6 Suunnitteluorganisaation sisäinen turvallisuusarviointi

342. Suunnitteluorganisaatiossa on tehtävä turvallisuusarviointeja, joilla varmistetaan turvallisuusvaatimusten täyttyminen sekä suunnitteluprosessien asianmukainen toteutus.

343. Turvallisuusarviointien tekijöiden on oltava tehtävään päteviä asiantuntijoita, jotka ovat riippumattomia suunnittelusta ja toteutuksesta. Useaa tekniikan alaa koskevissa arvioinneissa on otettava järjestelmällisesti huomioon poikkitekniset näkökohdat.

344. Suunnittelun turvallisuusarviointi on
1. toteutettava jatkuvana prosessina suunnittelu- ja todentamistoimien aikana
2. raportoitava kaikissa vaiheissa luvanhaltijalle.

345. Jos suunnitteluun osallistuu useita organisaatioita, suunnittelutyön päätoimittaja suorittaa suunnittelun kokonaisturvallisuusarvioinnin luvanhaltijan valvonnassa.

346. Jos järjestelmillä, rakenteilla ja laitteilla on huomattava turvallisuusmerkitys, niiden suunnittelulle on tehtävä turvallisuusarvio riippumattoman kolmannen osapuolen organisaation toimesta.

347. Kaikissa suunnittelun ja suunnittelukatselmointien vaiheissa on käytettävä todennäköisyysperusteista riskianalyysiä. Analyysin on oltava ajantasainen ja vastattava senhetkistä suunnittelua.

3.7 Suunnitteluratkaisujen perustelu

348. Suunnittelussa valittujen ratkaisujen ja menetelmien on perustuttava käytännössä hyväksi havaittuun tekniikkaan ja käyttökokemuksiin ja oltava soveltuvien standardien mukaisia. Suunnittelussa on pyrittävä yksinkertaisuuteen. Jos uusia ratkaisuja esitetään, ne on kelpuutettava tutkimuksella, johon liittyy kokeita ja testejä.

349. Turvallisuustoimintoja toteuttavien järjestelmien suunnittelu on perusteltava deterministisin turvallisuusanalyysein. Näiden analyysien avulla on varmistettava, että turvallisuustoiminnot voidaan toteuttaa suunnitelluilla järjestelmillä ja että laitokselle asetetut turvallisuustavoitteet täyttyvät. Deterministiset turvallisuusanalyysit on tehtävä alkutapahtumille, joiden jälkeen kyseistä turvallisuustoimintoa tarvitaan. Turvallisuustoimintoja toteuttavien järjestelmän toiminnalliset vaatimukset on määriteltävä näiden alkutapahtumien seurausten ja niiden lieventämistarpeiden mukaan. Deterministisiä turvallisuusanalyysejä koskevat yksityiskohtaiset vaatimukset on esitetty ohjeissa YVL B.3 ja YVL B.5.

350. Todennäköisyysperusteisilla riskianalyyseillä (PRA) on arvioitava reaktorisydämen vakavan vaurion todennäköisyyttä, suuren radioaktiivisten aineiden päästön todennäköisyyttä, suunnittelun tasapainoisuutta sekä järjestelmien, rakenteiden ja laitteiden riskimerkitystä. Todennäköisyysperusteista riskianalyysiä koskevat yksityiskohtaiset vaatimukset on esitetty ohjeessa YVL A.7.

351. Vikasietoisuusanalyyseillä on osoitettava, että
- kaikki turvallisuustoimintoja toteuttavat järjestelmät ja niiden tukijärjestelmät täyttävät tämän ohjeen luvussa 4.3 esitetyt vikakriteerit
- syvyyssuuntaisen turvallisuusperiaatteen mukaan eri puolustustasoille sijoitetut järjestelmät on toiminnallisesti erotettu toisistaan siten, että yhdellä tasolla tapahtuva vika ei vaikuta muihin tasoihin
- minkään yksittäisen laitetyypin (esim. samanlainen takaiskuventtiili, sama tyyppi ja valmistaja) yhteisvika ei estä ydinvoimalaitoksen ajamista hallittuun tilaan ja siitä edelleen turvalliseen tilaan.

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. Analyysissä oletetaan vaaditusta vikakriteeristä riippuen yksi tai useampi vika kerrallaan ja selvitetään niiden vaikutus järjestelmän toimintaan.

353. Yhteisvika-analyysi on laadittava alkutapahtumille, jotka kuuluvat suunnitteluperusteluokkiin DBC 2 ja DBC 3. Yhteisvika-analyysiä varten on esitettävä alkutapahtumittain turvallisuustoimintojen toteutus siten, että esityksestä käy ilmi erilaisuus- ja rinnakkaisuusperiaatteen toteuttavien järjestelmien käyttö. Yhteisvika-

analyysissä on tarkasteltava kerrallaan yhtä turvallisuustoimintoa tai sen osaa ottaen huomioon toimintoa toteuttavat järjestelmät ja niiden tukijärjestelmät. Analyysissä on tarkasteltava kaikkien sellaisten laitteiden yhteisvikoja, joiden yhteisviat tai aiheettomat toiminnot saattavat vaikuttaa turvallisuustoiminnon toteutumiseen. Yhteisvika-analyysissä on otettava huomioon alkutapahtuma, alkutapahtumariippuvuudet ja lisäksi yhteisvika sellaisten laitteiden välille, joilla on yhteinen ominaisuus, eli laitteet ovat samankaltaisia tai sisältävät merkittävästi samankaltaisia osia.

354. Vikasietoisuusanalyyseissä on otettava huomioon myös inhimilliset virheet ja osoitettava, että yksittäiset virheet eivät estä turvallisuustoiminnon toteutumista.

3.8 Dokumentaatio

355. Ydinvoimalaitosta, sen järjestelmiä ja niiden suunnitteluvaatimuksia kuvaavan dokumentaation on oltava rakenteeltaan selkeä, kattava sekä suunnittelun, toteutuksen ja käyttövaiheen aikaisia päivityksiä tukeva.

356. Turvallisuusluokitellun järjestelmän suunnittelu- ja toteutusprosessin on oltava kokonaisuudessaan läpinäkyvä, jäljitettävä ja todennettavissa. Työvaiheet tulosaineistoineen on dokumentoitava siten, että

- suunnittelun eri vaiheissa voidaan varmistua siitä, että asetetut vaatimukset siirtyvät oikein lopulliseen käyttöön otettavaan järjestelmään
- ne ovat riippumattoman asiantuntijan arvioitavissa.

357. Dokumentaation on oltava korkealaatuista, yksiselitteistä ja jäljitettävissä.

358. Ajantasaisen ja voimassa olevan dokumentaation on oltava suunnitteluun ja toteutukseen osallistuvien saatavilla.

359. Suunnittelua ja toteutusta koskevan dokumentaation on oltava ristiriidatonta ja jäljitettävissä laitoksen suunnittelun jäädytettyyn perustasoon.

360. Dokumentaatio kaavioineen ja kuvineen (esim. toimintakaaviot) on laadittava käyttäen selkeätä, täsmällistä ja eri laitos- ja järjestelmäsuunnitteluun osallistuvien eri tekniikan alojen asiantuntijoiden ymmärtämää esitystapaa.

361. Ohjelmoitavien järjestelmien versioiden hallitsemiseksi ja inhimillisten virheiden välttämiseksi ohjelma- ja laiteversiot on varustettava yksikäsitteisillä tunnisteilla.

3.9 Kelpoistus

362. Turvallisuudelle tärkeät järjestelmät, rakenteet ja laitteet on kelpoistettava käyttötarkoitukseensa. Kelpoistusprosessissa on osoitettava, että järjestelmät, rakenteet ja laitteet ovat käyttötarkoitukseensa sopivia ja täyttävät niille asetetut turvallisuusvaatimukset. Kelpoistukseen kuuluvat suunnitteluperusteiden oikeellisuuden sekä suunnittelun ja toteutuksen riittävän laadunhallinnan varmistamisen lisäksi ympäristöolosuhdekelpoistus.

363. Kelpoistusprosessin ohjaamiseksi järjestelmälle on laadittava ja toteutettava kelpoistussuunnitelma. Kelpoistussuunnitelmassa on esitettävä

1. järjestelmien, rakenteiden ja laitteiden suunnittelun ja toteutuksen laadunvarmistusvaiheiden (todentaminen ja kelpuutus) yhteydessä tuotettu aineisto, jota käytetään kelpoistuksessa hyväksi
2. kelpoistusta varten suunnitellut ulkopuoliset arviot, testit, analyysit ja koestukset sekä näihin käytetyt menetelmät, niiden soveltuvuus ja suorittaja
3. kelpoistuksen etenemissuunnitelma aikatauluarvioineen ja riippuvuuksineen suhteessa projektin etenemiseen
4. kelpoistusprosessin myötä tuotettu tai tuotettava dokumentaatio ja tämän esittäminen viranomaiskäsittelyyn.

364. Luvanhaltijan on arvioitava kelpoistuksen tulosten hyväksyttävyys ja esitettävä niistä perusteltu johtopäätös.

4 Turvallisuustoimintojen luotettavuuden varmistamista koskevat suunnitteluvaatimukset

4.1 Yleisiä suunnitteluperiaatteita ja -vaatimuksia

401. Ydinenergialain (990/1987) 7 a §:n mukaan ydinenergian käytön turvallisuus on pidettävä niin korkealla tasolla, kuin käytännöllisin toimenpitein on mahdollista (SAHARA-periaate). Korkea turvallisuustaso saavutetaan luotettavilla turvallisuustoiminnoilla ja radioaktiivisten aineiden vapautumista rajoittavilla moninkertaisilla peräkkäisillä rakenteellisilla esteillä.

402. Valtioneuvoston asetuksen (717/2013) 14 §:n ensimmäisen momentin mukaan *turvallisuustoimintojen varmistamisessa on ensisijaisesti käytettävä hyväksi suunnitteluratkaisuin saavutettavissa olevia luontaisia turvallisuusominaisuuksia. Ydinreaktorin fysikaalisten takaisinkytkentöjen yhteisvaikutuksen on oltava sellainen, että se hillitsee reaktorin tehon kasvua.*

403. Valtioneuvoston asetuksen (717/2013) 14 §:n toisen momentin mukaan *jos turvallisuustoiminnon varmistamisessa ei voida käyttää hyväksi luontaisia turvallisuusominaisuuksia, on ensisijaisesti käytettävä järjestelmiä ja laitteita, jotka eivät tarvitse ulkoista käyttövoimaa tai jotka käyttövoiman menetyksen seurauksena asettuvat turvallisuuden kannalta edulliseen tilaan.*

404. Ydinvoimalaitoksen kaikki järjestelmät, rakenteet ja laitteet on suunniteltava siten, että ne toimivat luotettavasti suunnitteluperusteenaan olevissa ympäristöolosuhteissa. Suunnittelussa huomioon otettaviin ympäristöolosuhteisiin voivat tilanteen mukaan kuulua värähtely, lämpötila, paine, sähkömagneettiset vaikutukset, säteily, kosteus ja näiden yhdistelmät.

405. Huoltoa tai tarkastuksia vaativien järjestelmien, rakenteiden ja laitteiden sijoittelua ja materiaaleja suunniteltaessa on otettava huomioon työntekijöiden säteilysuojelu ALARA (As Low As Reasonably Achievable) -periaatteen mukaisesti.

406. Turvallisuustoimintoja toteuttavat järjestelmät on suunniteltava siten, että niiden toimintakuntoisuus voidaan laitoksen käyttövaiheessa testata tai muuten varmentaa mahdollisimman lähellä niitä käyttötilanteita ja toimintaolosuhteita, joita varten ne on suunniteltu. Turvallisuustoiminnon toimintakuntoisuuden kannalta tärkeiden osien on oltava tarkastettavissa.

407. Suunnitteluratkaisuissa on pyrittävä riippumattomuuteen yksittäisestä teknologiasta. Teknologisten murrosten mahdollisuuteen on varauduttava jo ennalta siten, että tarvittavat laitteiden vaihdot voidaan tehdä hallitusti ja hyvissä ajoin.

408. Suunnitteluvaiheessa on kiinnitettävä erityistä huomiota piirteisiin, jotka helpottavat tulevaa jätehuoltoa sekä laitoksen käytöstä poistoa ja purkamista. Erityisesti on kiinnitettävä huomiota materiaalien valintaan, jotta dekontaminointi helpottuu ja tuleva radioaktiivisen jätteen määrä jää niin pieneksi, kuin käytännössä on mahdollista. Suunnitteluun on sisällytettävä käytössä syntyvän radioaktiivisen jätteen käsittelyyn ja varastointiin tarvittavat tilat, ja siinä on varauduttava myös laitoksen tulevassa käytöstäpoistossa syntyvän radioaktiivisen jätteen käsittelyyn.

409. Suunnittelussa on varauduttava turvajärjestelyjen huomioonottamiseen siten että turvallisuuden ja turvajärjestelyjen väliset mahdolliset ristiriidat minimoidaan. Tietoturvallisuus on otettava huomioon ydinvoimalaitoksen suunnittelussa. Turvajärjestelyjä koskevat erityisvaatimukset on esitetty ohjeessa YVL A.11 ja tietoturvallisuutta koskevat ohjeessa YVL A.12.

410. Suunnittelussa on varauduttava vaatimuksiin laitokselle asennettavista IAEA:n ydinmateriaalivalvonnan laitteista. Ydinmateriaalivalvontaan liittyvät vaatimukset on esitetty ohjeessa YVL D.1.

411. Mikäli samalla laitospaikalla sijaitseville ydinvoimalaitosyksiköille suunnitellaan yhteisiä turvallisuuden kannalta tärkeitä rakenteita, järjestelmiä ja laitteita, tulee luotettavuusteknisin tarkasteluin osoittaa, että tämä ei heikennä näiden rakenteiden, järjestelmien ja laitteiden kykyä suorittaa turvallisuustoimintonsa.

412. Mikäli ydinvoimalaitosyksikköjen samaa turvallisuustoimintoa suorittavien järjestelmien välille suunnitellaan ristikytkentöjä, tulee osoittaa, että turvallisuustoiminnot ovat tällä tavoin luotettavampia kuin ilman näitä kytkentöjä.

4.2 Turvallisuustoimintoja toteuttavien järjestelmien suunnitteluperusteet

413. Ydinenergialain (990/1987) 7 d §:n mukaan *ydinlaitoksen suunnittelussa on varauduttava käyttöhäiriöiden ja onnettomuuksien mahdollisuuteen. Onnettomuuden todennäköisyyden on oltava sitä pienempi, mitä vakavampi onnettomuuden seuraus saattaisi olla ihmisille, ympäristölle tai omaisuudelle.*

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. Tällaiset tapahtumat voivat saada alkunsa painelaitteen tai putkiston murtumasta, laiteviasta, virheestä laitoksen toiminnassa tai automaattisessa ohjauksessa tai sisäisestä tai ulkoisesta uhasta.

415. Sisäisinä uhkina on tarkasteltava ainakin laitoksen sisällä syttyviä tulipaloja, laite- tai putkivaurioista johtuvia tulvia, törmäys- ja suihkuvoimia, räjähdyksiä, ylijännitteitä ja mahdollisuuksia tahalliseen vahingon tekoon.

416. Ulkoisina uhkina on tarkasteltava ainakin harvinaisia sääilmiöitä, tulipaloa laitoksen läheisyydessä, korkeaa ja alhaista merenpinnan tasoa, seismisiä ilmiöitä, lämpönielun tukkeutumista jostakin muusta syystä kuin jäätymisen tai seismisen ilmiön seurauksena, lentokonetörmäystä, sähkömagneettisia ilmiöitä, räjähdystä tai myrkyllisiä kaasuja laitosalueella, öljyvuotoa laitoksen läheisellä merialueella sekä luvatonta tunkeutumista laitosalueelle tai laitoksen tietojärjestelmiin.

417. Ydinvoimalaitoksen suunnittelussa huomioon otettavia tapahtumia koskevat yksityiskohtaiset vaatimukset on esitetty ohjeissa YVL B.3, B.5, B.7, B.8, A.11 ja A.12.

4.3 Syvyyssuuntaisen puolustusperiaatteen soveltaminen suunnittelussa

418. Valtioneuvoston asetuksen (717/2013) 14 §:n kolmannen momentin mukaan *onnettomuuksien estämiseksi ja niiden seurausten lieventämiseksi ydinvoimalaitoksessa on oltava järjestelmät reaktorin pysäyttämiseen ja alikriittisenä pitämiseen, reaktorissa syntyvän jälkilämmön poistamiseen sekä radioaktiivisten aineiden pidättämiseen laitoksen sisällä. Kyseisten järjestelmien suunnittelussa on sovellettava moninkertaisuus-, erottelu- ja erilaisuusperiaatteita, joilla varmistetaan turvallisuustoiminnon toteutuminen myös vikaantumistilanteissa.* Valtioneuvoston asetuksen (717/2013) 14 §:n viidennen momentin mukaan *yhteisvikojen vaikutusten laitoksen turvallisuuteen on oltava vähäisiä.*

419. Ydinenergialain (990/1987) 7 b §:n mukaan *ydinlaitoksen turvallisuus on varmistettava peräkkäisillä ja toisistaan riippumattomilla suojauksilla (syvyyssuuntainen turvallisuusperiaate). Tämä periaate on ulotettava laitoksen toiminnalliseen ja rakenteelliseen turvallisuuteen.*

420. Edellä viitattuja ydinenergialain 7 b §:n ja 7 d §:n vaatimuksia täsmennetään valtioneuvoston asetuksen (717/2013) 12 §:ssä seuraavasti: *Odotettavissa olevien käyttöhäiriöiden ja onnettomuuksien ehkäisemiseksi ja niiden seurausten lieventämiseksi ydinvoimalaitoksen suunnittelussa, rakentamisessa ja käyttötoiminnassa on noudatettava toiminnallista syvyyssuuntaista turvallisuusperiaatetta.*

421. Toiminnallisen syvyyssuuntaisen turvallisuusperiaatteen mukaisen turvallisuustoimintojen puolustuksen on perustuttava viiteen peräkkäiseen tasoon, joista kaksi ensimmäistä tasoa on tarkoitettu ehkäisemään onnettomuuksia ja muut tasot on tarkoitettu suojaamaan laitosta

ja sen käyttäjiä sekä ympäristöä onnettomuuden haitallisilta vaikutuksilta. Puolustustasot ovat seuraavat:

1. **Ennalta ehkäiseminen:** Ensimmäisellä tasolla on varmistettava, että laitoksen käyttö on luotettavaa ja poikkeamat normaaleista käyttöolosuhteista ovat harvinaisia. Tämän saavuttamiseksi järjestelmien, rakenteiden ja laitteiden suunnittelussa, valmistuksessa, asennuksessa, käyttöönotossa, tarkastuksessa, koestuksessa ja huollossa sekä laitoksen käyttötoiminnassa on sovellettava korkeita laatuvaatimuksia, luotettavuusvaatimuksia ja riittäviä varmuusmarginaaleja.
2. **Häiriötilanteiden hallinta:** Toisella tasolla on laitoksen huolellisesta suunnittelusta ja käytöstä huolimatta varauduttava poikkeamiin normaaleista käyttöolosuhteista ja varustettava laitos sellaisin järjestelmin, joiden tehtävänä on havaita häiriöt ja rajoittaa häiriötilanteiden kehittymistä onnettomuuksiksi sekä ohjata laitos tarvittaessa hallittuun tilaan.
3. **Onnettomuustilanteiden hallinta:** Kolmannella tasolla on varauduttava onnettomuuksiin sellaisin luotettavin järjestelmin, jotka käynnistyvät automaattisesti onnettomuustilanteen syntyessä, suojaavat radioaktiivisten aineiden leviämistä pidättäviä esteitä ja estävät vakavien polttoainevaurioiden syntymisen oletetuissa onnettomuuksissa ja oletettujen onnettomuuksien laajennuksissa sekä estävät onnettomuuden kehittymisen vakavaksi onnettomuudeksi. Kolmas taso on jaettava kahteen osaan: tasoihin 3a ja 3b.
   a. Tasolla 3a tavoitteena on hallita yksittäisistä alkutapahtumista ja niiden seurausvaikutuksista johtuvia oletettuja onnettomuuksia (luokka 1 ja luokka 2) radioaktiivisten aineiden päästöjen rajoittamiseksi.
   b. Tasolla 3b tavoitteena on hallita oletettujen onnettomuuksien laajennuksia, joilla tarkoitetaan
   – odotettavissa olevia käyttöhäiriöitä ja luokan 1 oletettuja onnettomuuksia, joiden yhteydessä ilmenee yhteisvika ao. tapahtuman hallintaan suunnitellussa järjestelmässä
   – todennäköisyysperusteisen riskianalyysin perusteella valittuja vikayhdistelmiä
   – epätodennäköisiä mutta kuitenkin mahdolliseksi oletettuja harvinaisia ulkoisia tapahtumia, esimerkiksi harvinaisia sääilmiöitä tai suuren lentokoneen törmäystä.
4. **Päästön rajoittaminen vakavissa onnettomuuksissa:** Tasolla 4 tavoitteena on lieventää vakavan reaktorionnettomuuden seurauksia siten, että varmistetaan suojarakennuksen eheys ja tiiviys niin, että vakaville onnettomuuksille asetetut päästön raja-arvot eivät ylity.
5. **Seurausten lieventäminen:** Tasolla 5 on varauduttava huolehtimaan väestöön kohdistuvien säteilyvaikutusten rajoittamisesta valmiusjärjestelyin tilanteessa, jossa laitokselta pääsee huomattavia määriä radioaktiivisia aineita ympäristöön.

422. Suunnittelutavoitteena on pidettävä sitä, että radioaktiivisten aineiden päästö ei aiheuta laitoksen ympäristön asukkaille suurempaa säteilyannosta kuin valtioneuvoston asetuksen (717/2013) 8–10 §:issä ja ohjeessa YVL C.3 on esitetty.

423. Tapahtumat, jotka voivat johtaa onnettomuuden aikaisessa vaiheessa tapahtuvaan väestön suojautumistoimenpiteitä edellyttävään päästöön on käytännössä eliminoitava.

424. Käytännössä eliminoitavat tapahtumat on tunnistettava ja analysoitava käyttäen menetelmiä, jotka perustuvat deterministisiin analyyseihin täydennettynä todennäköisyysperusteisilla riskianalyyseilla ja asiantuntija-arvioilla. Käytännössä eliminoinnissa ei voida tukeutua yksinomaan todennäköisyysperusteiseen raja-arvoon. Vaikka tapahtuman todennäköisyys analyysin perusteella osoittautuisi hyvin pieneksi, riskin pienentämiseksi on tehtävä kaikki ne toimenpiteet, jotka käytännöllisin toimin on mahdollista. Käytännössä eliminoitavia tapahtumia ovat esimerkiksi

1. kriittisyysonnettomuuteen tai vakavaan reaktorionnettomuuteen johtava nopea hallitsematon reaktiivisuuden kasvu
2. reaktorisydämen paljastumiseen johtava jäähdytteen menetys seisokin aikana
3. suojarakennuksen eheyttä uhkaava kuormitus vakavan reaktorionnettomuuden aikana

(esimerkiksi reaktoripainesäiliön rikkoutuminen korkeassa paineessa, vetyräjähdys, höyryräjähdys, sulaneen reaktorisydämen suora vaikutus suojarakennuksen pohjaan tai seinämään, suojarakennuksen hallitsematon paineen nousu)

4. käytetyn ydinpolttoaineen vakavaan vaurioitumiseen johtava jäähdytyksen menetys ydinpolttoainevarastossa.

4.3.1 Syvyyssuuntaisen puolustuksen tasojen riippumattomuus

425. Valtioneuvoston asetuksen (717/2013) 12 §:n mukaan *syvyyssuuntaisen puolustusperiaatteen puolustustasojen on oltava toisistaan niin riippumattomia kuin käytännöllisin toimenpitein on mahdollista saavuttaa*. Yhden puolustustason menetys ei saa heikentää muiden puolustustasojen toimintaa.

426. Riippumattomuuden on perustuttava toiminnallisen erottelun, erilaisuusperiaatteen sekä fyysisen erottelun riittävään soveltamiseen puolustustasojen välillä.

427. Riippuvuus turvallisuustoimintoja syvyyssuuntaisen puolustuksen eri tasoilla tukevista järjestelmistä on otettava huomioon. Riippuvuus ei saa tarpeettomasti heikentää syvyyssuuntaisen puolustuksen luotettavuutta.

428. Jokaisessa oletetussa alkutapahtumassa tarvittavat järjestelmät, rakenteet ja laitteet on tunnistettava ja on osoitettava deterministisin analyysein, että syvyyssuuntaisen puolustuksen yhden tason toteuttamiseen tarvittavat järjestelmät, rakenteet ja laitteet ovat riittävässä määrin riippumattomia muista tasoista. Saavutetun riippumattomuuden riittävyyttä tulee arvioida myös todennäköisyysperusteisin analyysein.

429. Syvyyssuuntaisen turvallisuusperiaatteen mukaan eri puolustustasojen toteuttamiseen tarvittavat järjestelmät on erotettava toisistaan toiminnallisesti siten, että yhdellä tasolla sattuva toimintahäiriö tai vikaantuminen ei etene muille tasoille.

430. Syvyyssuuntaisen puolustuksen eri tasoilla käytettävät järjestelmät ja laitteet on erotettava saman turvallisuuslohkon sisällä toisistaan etäisyydellä tai suojaavilla rakenteilla, jos on olemassa ilmeinen mahdollisuus seurausvikoihin, jotka aiheutuvat toisella tasolla olevan järjestelmän tai laitteen vikaantumisesta.

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.

4.3.2 Syvyyssuuntaisen puolustuksen yksittäisten tasojen vahvuus

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.

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.

434. Turvallisuustoimintoja toteuttavan järjestelmän moninkertaisuusperiaatetta toteuttavat osat on sijoitettava eri turvallisuuslohkoihin.

435. Turvallisuustoimintoja toteuttavan järjestelmän yhden osajärjestelmän vikaantuminen ei saa aiheuttaa toisen saman järjestelmän moninkertaisuusperiaatetta toteuttavan osajärjestelmän eikä estää minkään samaan turvalli-

suustoimintoon osallistuvaa muuta järjestelmää toteuttamasta turvallisuustoimintoaan.

436. Minkään turvallisuuslohkon ja sen sisältämien laitteiden menettäminen ei saa johtaa minkään turvallisuustoiminnon menetykseen.

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. Turvallisuusjärjestelmien moninkertaisuusperiaatetta toteuttavia osia sisältävien turvallisuuslohkojen erotteluun liittyvät yksityiskohtaiset vaatimukset on esitetty ohjeessa YVL B.7.

438. Järjestelmän moninkertaisuusperiaatetta toteuttavien osien erotteluvaatimus koskee myös kaikkia turvallisuustoiminnon toteuttamiseen tarvittavien järjestelmien tukijärjestelmiä sekä kaikkia turvallisuustoimintoa ohjaavia automaatiojärjestelmiä toiminnon käynnistystarpeen osoittavasta mittauksesta aina turvallisuustoiminnon toteuttaville laitteille asti.

439. Jos turvallisuusjärjestelmän moninkertaisuusperiaatetta toteuttavat osat on kytketty toisiinsa sähkönjakelua tai ohjauskäskyjen välittämistä varten, ratkaisun turvallisuusedut verrattuna sellaiseen ratkaisuun, jossa tällaista kytkentää ei ole, on perusteltava.

440. Eri turvallisuusluokkiin kuuluvat järjestelmät ja laitteet on erotettava toisistaan toiminnallisesti siten, että alemman turvallisuusluokan järjestelmän, rakenteen tai laitteen toimintatapa tai vikaantuminen ei aiheuta ylemmässä turvallisuusluokassa olevan järjestelmän, rakenteen tai laitteen vikaantumista eikä toiminnan menetystä.

441. Sähkömagneettinen yhteensopivuus on otettava huomioon sähkölaitteiden ja kaapelien sijoittelussa.

442. Vikakriteeriä on sovellettava turvallisuusjärjestelmästä ja kaikista turvallisuustoiminnon toteuttamiseen tarvittavista tukijärjestelmistä koostuvaan järjestelmäkokonaisuuteen. Tällaisia tukijärjestelmiä ovat esim. laitteiden jäähdytys ja sähkön syöttö sekä näitä toimintoja ohjaavat järjestelmät. Vikakriteerinä on käytettävä joko (N+2)- tai (N+1)-vikakriteeriä siten, kuin tässä ohjeessa esitetään.

443. Ohjeissa YVL B.7 ja YVL B.8 annetaan tarkempia määräyksiä siitä, miten järjestelmät ja laitteet on eroteltava fyysisesti toisistaan yhden turvallisuuslohkon sisällä.

4.3.3 Hallitun tilan saavuttamiseksi ja ylläpitämiseksi tarvittavia järjestelmiä koskevat erityisvaatimukset

444. Reaktorin on täytettävä tapahtumille asetetut hyväksymiskriteerit suunnitteluperusteluokissa DBC1, DBC2, DBC3, DBC4 ja DEC. Radiologisia vaikutuksia koskevat hyväksymiskriteerit kussakin tapahtumaluokassa on esitetty ydinvoimalaitosten turvallisuuteen liittyvän valtioneuvoston asetuksen (717/2013) 8 §:ssä, 9 §:ssä ja 10 §:ssä sekä ohjeessa YVL C.3. Polttoainevaurioita koskevat hyväksymiskriteerit on esitetty ohjeessa YVL B.4 ja ylipainesuojausta koskevat hyväksymiskriteerit ohjeessa YVL B.3. Analyysivaatimukset kriteerien täyttymisen osoittamiseksi on esitetty ohjeessa YVL B.3.

445. Reaktorissa on oltava kiinteitä neutroniabsorbaattoreita käyttävä pikasulkujärjestelmä, joka yksinään tai yhdessä jäähdytteenmenetystilanteiden varalta suunniteltujen järjestelmien lisäämän reaktiivisuusmyrkyn kanssa pystyy pysäyttämään reaktorin hallittuun tilaan ja pitämään sen pitkäaikaisesti alikriittisenä minkä tahansa odotettavissa olevan käyttöhäiriön tai oletetun onnettomuuden jälkeen siten, että polttoaineen eheydelle, radiologisille vaikutuksille ja primääripiirin paineelle ao. suunnitteluperusteluokassa DBC2, DBC3 tai DBC4 asetetut raja-arvot eivät ylity. Neutroniabsorbaattoreiden työntämisessä reaktorisydämeen tulee käyttää hyväksi painovoimaa, puristettuun kaasuun varastoitunutta energiaa tai muuta sellaista käyttövoimaa, joka ei edellytä ulkoista voimanlähdettä työntämisen aikana. Sammutuksen tulee onnistua, vaikka jotakin yhdessä työnnettävistä

neutroniabsorbaattoreista ei pystyttäisi työntämään reaktoriin. Pikasulun käynnistävän reaktorin suojausjärjestelmän on täytettävä (N+2)-vikakriteeri.

446. Reaktorissa on oltava kiinteisiin neutroniabsorbaattoreihin perustuvan pikasulkujärjestelmän lisäksi erilaisuusperiaatetta toteuttava sammutusjärjestelmä, joka pystyy pysäyttämään reaktorin hallittuun tilaan ja pitämään sen pitkäaikaisesti alikriittisenä minkä tahansa odotettavissa olevan käyttöhäiriön tai luokan 1 oletetun onnettomuuden alkutapahtuman (lukuun ottamatta luokan 1 oletettuihin onnettomuuksiin sisältyviä jäähdytteenmenetysonnettomuuksia) jälkeen siten, että polttoaineen eheydelle, radiologisille vaikutuksille ja ylipainesuojaukselle suunnitteluperusteluokassa DEC asetetut raja-arvot eivät ylity. Erilaisuusperiaatetta toteuttavan sammutusjärjestelmän on täytettävä (N+1)-vikakriteeri.

447. Vikayhdistelmän sisältävissä tapahtumissa (DEC B) ja harvinaisissa ulkoisissa tapahtumissa (DEC C) on oltava mahdollista pysäyttää reaktori ja pitää se alikriittisenä hallitussa tilassa siten, että polttoaineen eheydelle, radiologisille vaikutuksille ja ylipainesuojaukselle suunnitteluperusteluokassa DEC asetetut raja-arvot eivät ylity.

448. Jälkilämmön poisto reaktorista ja suojarakennuksesta on voitava toteuttaa odotettavissa olevissa käyttöhäiriöissä tai oletetuissa onnettomuuksissa yhdellä tai usealla (N+2)-vikakriteerin ja 72 tunnin omavaraisuusehdon yhdessä täyttävällä järjestelmällä siten, että polttoaineen eheydelle, radiologisille vaikutuksille ja ylipainesuojaukselle ao. suunnitteluperusteluokassa DBC2, DBC3 tai DBC4 asetetut raja-arvot eivät ylity. Jos jälkilämmönpoistojärjestelmissä tai niiden tukijärjestelmissä on sellaisia passiivisia laitteita, joiden vikaantumisen todennäköisyys odotettavissa olevissa käyttöhäiriöissä tai oletetuissa onnettomuuksissa on hyvin pieni, näihin laitteisiin voidaan soveltaa (N+1)-vikakriteeriä (N+2)-vikakriteerin sijasta.

449. Ydinvoimalaitoksessa on oltava vaatimuksen 448 täyttävän jälkilämmönpoistojärjestelmän tai -järjestelmien lisäksi erilaisuusperiaatetta toteuttava järjestelmä, joka pystyy poistamaan jälkilämmön reaktorista ja suojarakennuksesta minkä tahansa odotettavissa olevan käyttöhäiriön tai luokan 1 oletetun onnettomuuden alkutapahtuman jälkeen siten, että polttoaineen eheydelle, radiologisille vaikutuksille ja ylipainesuojaukselle suunnitteluperusteluokassa DEC asetetut raja-arvot eivät ylity. Erilaisuusperiaatetta toteuttavan jälkilämmönpoistojärjestelmän on täytettävä (N+1)-vikakriteeri ja 72 tunnin omavaraisuusehto. Jos erilaisuusperiaatetta toteuttava järjestelmä pystyy poistamaan jälkilämmön siten, että polttoaineen eheydelle, radiologisille vaikutuksille ja ylipainesuojaukselle ao. suunnitteluperusteluokassa DBC2, DBC3 tai DBC4 asetetut raja-arvot eivät ylity, järjestelmä voidaan lukea niihin järjestelmiin, jotka yhdessä täyttävät vaatimuksessa 448 annetun (N+2)-vikakriteerin.

450. Jälkilämmön poisto reaktorista suojarakennuksen ulkopuolelle ja reaktiivisuuden hallinta on voitava toteuttaa vikayhdistelmän sisältävissä tapahtumissa (DEC B) ja harvinaisissa ulkoisissa tapahtumissa (DEC C) siten, että polttoaineen eheydelle, radiologisille vaikutuksille ja ylipainesuojaukselle suunnitteluperusteluokassa DEC asetetut raja-arvot eivät ylity.

Jälkilämmön poisto ja reaktiivisuuden hallinta harvinaisissa ulkoisissa tapahtumissa (DEC C) on pystyttävä toteuttamaan siten, että se ei tukeudu sähkötehon syöttöön siirrettävistä lähteistä, ja se on pystyttävä varmistamaan vähintään kahdeksan tunnin ajan ilman materiaalitäydennyksiä tai tasavirta-akkujen uudelleenlataamista. Laitosalueella on lisäksi oltava riittävät vesi- ja polttoainevarastot sekä mahdollisuus tasavirta-akkujen uudelleenlataamiseen siten, että jälkilämpö pystytään poistamaan 72 tunnin ajan.

451. Laitoksen sisäisen sähköjakeluverkon menetyksen varalta on oltava järjestelyt jälkilämmön poistamiseksi reaktorista suojarakennuksen ulkopuolelle ja reaktiivisuuden hallitsemiseksi siten, että.

1. tilanteessa tarvittavien järjestelmien on oltava ilman ulkoista käyttövoimaa toimivia tai itsenäiseen käyttövoimaan perustuvia;

2. laitosalueella on oltava riittävät vesi- ja polttoainevarastot sekä mahdollisuus tasavirta-akkujen uudelleenlataamiseen siten, että em. järjestelyt pystytään toteuttamaan 72 tunnin ajan.

Näihin järjestelyihin tarvittaviin järjestelmiin ei tarvitse soveltaa yksittäisvikakriteeriä ja niihin liittyvät suojarakennuksen eristysventtiilit toimilaitteineen ja kaapeleineen sekä putkilinjat reaktoriin ja höyrystimiin voivat olla yhteisiä muuhun tarkoitukseen käytettävän järjestelmän kanssa. Tasasähköjärjestelmät voidaan riittävää sähköistä erottelua hyödyntämällä katsoa käyttökuntoisiksi.

Tähän tilanteeseen sovelletaan suunnitteluperusteluokan DEC polttoainevauriokriteereitä ja annosrajoja. Yhtäaikaista tällaista tilannetta ja siitä riippumatonta alkutapahtumaa, harvinaista ulkoista tapahtumaa (DEC C) tai muuta monimutkaista vikayhdistelmää (DEC B) ei tarvitse olettaa suunnittelussa.

452. Ydinvoimalaitoksella on oltava sellaiset järjestelyt, joilla varmistetaan polttoainevarastoissa olevan polttoaineen riittävä jäähdytys harvinaisissa ulkoisissa tapahtumissa vaatimuksen 450 mukaisesti. Näiden järjestelyjen on mahdollistettava veden pinnankorkeuden valvonta käytettyä polttoainetta sisältävissä polttoaineen säilytysaltaissa vähintään kahdeksan tunnin ajan ilman tasavirta-akkujen uudelleenlataamista. Polttoaine on lisäksi pystyttävä pitämään luotettavasti veden alla laitoksen sisäisen sähkönjakelujärjestelmän menetyksen tapauksessa vaatimuksen 451 mukaisesti. Laitosalueella on oltava riittävät vesi- ja polttoainevarastot sekä mahdollisuus tasavirta-akkujen uudelleenlataamiseen siten, että järjestelyt pystytään toteuttamaan 72 tunnin ajan.

453. Mikäli reaktoria ei odotettavissa olevan käyttöhäiriön, oletetun onnettomuuden tai oletetun onnettomuuden laajennuksen seurauksena saateta suoraan turvalliseen tilaan, se on pystyttävä pitämään hallitussa tilassa niin pitkään, että edellytykset turvalliseen tilaan siirtymiseksi voidaan varmistaa. Reaktorin hallitusta turvalliseen tilaan jäähdyttämiseksi tarvittavien järjestelmien korjauksen ja huollon mahdollistamiseksi on tehtävä tarvittavat järjestelyt.

4.3.4 Turvallisen tilan saavuttamiseksi ja ylläpitämiseksi tarvittavia järjestelmiä koskevat erityisvaatimukset

454. Kiinteitä neutroniabsorbaattoreita käyttävän, vaatimuksen 446 vaatimukset täyttävän reaktorin sammutusjärjestelmän tai (N+1)-vikakriteerin täyttävän erilaisuusperiaatetta toteuttavan reaktorin sammutusjärjestelmän on pystyttävä pitämään reaktori alikriittisenä sen kaikissa mahdollisissa lämpötiloissa.

455. Reaktorin jäähdytys hallitusta tilasta turvalliseen tilaan ja sen pitkäaikainen pitäminen turvallisessa tilassa on odotettavissa olevien käyttöhäiriöiden, oletettujen onnettomuuksien ja oletettujen onnettomuuksien laajennusten jälkeen voitava toteuttaa jälkilämmönpoistojärjestelmillä, jotka täyttävät (N+1)-vikakriteerin. Turvallisen tilan ylläpitämiseksi tarvittavien järjestelmien korjauksen ja huollon mahdollistamiseksi on tehtävä tarvittavat järjestelyt.

4.3.5 Muut moninkertaisuutta koskevat vaatimukset

456. Seuraavien turvallisuuteen vaikuttavia toimintoja toteuttavien järjestelmien on täytettävä (N+1)-vikakriteeri:

1. kaikki järjestelmät niiltä osin, kuin niiden vikaantuminen voisi suoraan johtaa tilanteeseen, joka edellyttää vaatimuksessa 432 vaadittujen oletettujen onnettomuuksien hallintaan suunniteltujen järjestelmien käyttämistä
2. polttoaineen käsittelyyn käytettävät järjestelmät niiltä osin, kuin ne voisivat vikaantuessaan aiheuttaa polttoaineen vaurioitumisen
3. kiinteät säteilymittausjärjestelmät ja -laitteet, joiden tehtävänä on reaktorihallin ulkoisen säteilynopeuden jatkuvatoiminen mittaaminen, työntekijöiden säteilyannosten rajoittaminen automaattisen ohjaustoiminnon avulla, päästöjen aktiivisuusvalvonta sekä onnettomuuksien seuranta ja hallinta
4. järjestelmät, joilla varmistetaan käytetyn polttoaineen jäähdytys
5. ohjaajan odotettavissa olevien käyttöhäiriöiden ja onnettomuuksien valvontaan ja hallintaan tarvitsemat mittausjärjestelmät, ellei

järjestelmään muista syistä sovelleta ylempää vikakriteeriä
6. vakavien reaktorionnettomuuksien hallintaan suunniteltujen järjestelmien aktiiviset laitteet
7. reaktorisuojarakennuksen ulkopuolella olevat järjestelmät, joiden tarkoituksena on estää radioaktiivista ainetta sisältävien laitteiden tai rakenteiden rikkoutumisesta johtuva radioaktiivisten aineiden leviäminen
8. järjestelmät, jotka tarvitaan valvomon työskentelyolosuhteiden pitämiseen turvallisena
9. järjestelmät, jotka tarvitaan huonetilojen jäähdyttämiseen tai lämmittämiseen siten, että turvallisuustoimintoihin vaikuttavilla sähkö- ja automaatio-järjestelmien laitteilla on niiden vaatimat toimintaolosuhteet; jos jonkin huonetilan jäähdytyksen tai lämmityksen menetys voi johtaa useamman kuin yhden moninkertaisuusperiaatetta toteuttavan sähkö- tai automaatiojärjestelmän osan turvallisuustoiminnon menettämiseen, yksittäisvikakriteerin on täytyttävä kyseisessä huonetilassa
10. suojarakennuksen eristämiseen tarvittavat järjestelmät. Eristystoiminnon on täytettävä (N+1)-vikakriteeri riippumatta eristystoiminnon toteuttamisessa tarvittavien automaatiojärjestelmien tai muiden tukijärjestelmien mahdollisista kunnossapito-/korjaustoimenpiteistä. Suojarakennuksen eristystoimintoa koskevat yksityiskohtaiset vaatimukset on esitetty ohjeessa YVL B.6.

457. Moninkertaisuusperiaatteen soveltamista koskevat järjestelmäkohtaiset vaatimukset on annettu tämän ohjeen luvussa 5 sekä ohjeissa YVL B.4 (Ydinpolttoaine ja reaktori), YVL B.5 (Ydinvoimalaitoksen primääripiiri) ja YVL B.6 (Ydinvoimalaitoksen suojarakennus).

4.4 Inhimillisten virheiden välttäminen

458. Valtioneuvoston asetuksen (717/2013) 6 §:n mukaan *inhimillisten virheiden välttämiseen, havaitsemiseen ja korjaamiseen on kiinnitettävä erityistä huomiota laitoksen koko elinkaaren ajan. Virheiden mahdollisuus on otettava huomioon ydinvoimalaitoksen ja sen käyttöja kunnossapitotoiminnan suunnittelussa siten, että inhimilliset virheet ja niiden aiheuttamat poikkeamat laitoksen normaalista toiminnasta eivät vaaranna laitoksen turvallisuutta. Inhimillisistä virheistä aiheutuvien yhteisvikojen mahdollisuutta on pyrittävä pienentämään. Inhimillisten virheiden vaikutuksia on rajoitettava käyttäen toiminnallista syvyyssuuntaista turvallisuusperiaatetta.*

459. Turvallisuudelle tärkeiden järjestelmien ja laitteiden manuaalisen ohjauksen, testausten, tarkastusten ja kunnossapitotöiden suunnittelun on perustuttava tehtävä- ja luotettavuusanalyysiin. Analyysin tuloksia käytetään järjestelmien suunnittelun perusteena siten, että varmistetaan hyvät edellytykset luotettavalle toiminnalle, virheiden välttämiselle mahdollisuuksien mukaan sekä mahdollisten virheiden nopealle havaitsemiselle.

460. Turvallisuudelle tärkeiden järjestelmien ohjauksessa ja koestuksessa tarvittavan informaation esitys, ohjeistus sekä käytettävät ohjauslaitteet on suunniteltava siten, että inhimilliset virheiden mahdollisuus järjestelmää käytettäessä ja koestettaessa pyritään välttämään.

461. Kunnossapitotöiden suorittamisessa tarvittavan informaation esitys, ohjeistus sekä käytettävät työvälineet on suunniteltava siten, että inhimilliset virheiden mahdollisuus järjestelmän kunnossapidon aikana pyritään välttämään. Lisäksi on kiinnitettävä huomiota fyysiseen työympäristöön ja laitteiden luoksepäästävyyteen.

462. Huonetilojen, järjestelmien ja niihin liittyvien laitteiden, rakenteiden ja kaapeleiden tunnistaminen toisiinsa liittyviksi suunnittelun, käytön, koestuksen, kunnossapidon ja korjausten yhteydessä on tehtävä helpoksi yksiselitteisen tunnusjärjestelmän avulla.

5 Ydinvoimalaitoksen erityisjärjestelmien suunnittelu

5.1 Reaktorin jäähdytys- ja jälkilämmönpoistojärjestelmät

5101. Ydinvoimalaitokseen on suunniteltava sellaiset järjestelmät, jotka käyttö- ja onnettomuustilanteissa jäähdyttävät reaktoria ja siirtävät reaktorissa syntyvän jälkilämmön lopulliseen lämpönieluun. Järjestelmät on suunniteltava siten, että luvussa 4 esitetyt turvallisuussuunnittelun vaatimukset täyttyvät.

5102. Laitoksen suunnittelussa on varattava jälkilämmön poistoa varten toissijainen lopullinen lämpönielu ensisijaisen lopullisen lämpönielun käytön estyessä. Toissijaisen lopullisen lämpönielun on täytettävä 72 tunnin omavaraisuusehto.

5103. Reaktorin jäähdytysjärjestelmä ja sen tuki-, säätö- ja suojausjärjestelmät on suunniteltava siten, että reaktorin primääripiirin suunnitteluarvot eivät ylity käyttötilanteissa.

5104. Reaktorin jäähdytysjärjestelmä on suunniteltava siten, että

1. riski reaktorin jäähdytteen menetykselle aktiivisen polttoaineen yläpään tasoa alempana esiintyvien vuotojen seurauksena on kaikissa käyttötilanteissa erittäin pieni
2. primääripiiriin seisokin aikana kohdistuvat kunnossapitotoimenpiteet eivät aiheuta olennaista reaktorin jäähdytteen menetyksen riskiä.

5105. Reaktorin jäähdytteen tilavuudensäätöjärjestelmä on suunniteltava siten, että jäähdytteen tilavuus primääripiirissä voidaan pitää normaalin jäähdytyksen edellyttämissä rajoissa, vaikka jossakin tilavuuden säätöön vaikuttavassa laitteessa tai säätöjärjestelmässä sattuisi yksittäisvika.

5106. 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 tarkasti.

5107. Reaktorin jäähdytteen puhdistamiseksi on suunniteltava sellainen järjestelmä, joka käyttötilanteissa poistaa jäähdytteestä radioaktiivisia aineita ja muita epäpuhtauksia.

5108. Primääripiirin ja siihen välittömästi liittyvien järjestelmien jäähdytevuotojen hallitsemiseksi on suunniteltava reaktorisydämen hätäjäähdytysjärjestelmä, joka korvaa menetetyn jäähdytteen tai muuten huolehtii reaktorin tehokkaasta jäähdytyksestä siten, että polttoaineeseen liittyviä suunnittelurajoja ei ylitetä.

5109. Hätäjäähdytysjärjestelmän kapasiteetin on pystyttävä kompensoimaan erikokoiset vuodot siten, että suurin vuoto vastaa primääripiirin suurimman putken täydellistä, äkillistä katkeamista.

5110. Reaktorisydämen hätäjäähdytyksen toimivuus ja tehokkuus oletetuissa vuototilanteissa on varmistettava primääripiirin muotoilulla sekä reaktorisydämen hätäjäähdytysyhteiden sopivalla sijoituksella.

5111. Reaktorisydämen hätäjäähdytysjärjestelmä on suunniteltava siten, että se voi poistaa reaktorissa syntyvän jälkilämmön niin kauan, kuin se on tarpeen. Tätä varten on järjestettävä mahdollisuus kierrättää vuotovesi takaisin reaktoriin. Suunnittelussa on otettava huomioon kierrätyksen jatkumista uhkaavat tai reaktorin jäähdytystä heikentävät veteen mahdollisesti sekoittuvat kiinteät tai kemialliset epäpuhtaudet. Jäähdytyskierto on varustettava epäpuhtauksien varalta suodatinrakenteilla, joiden suunniteltu toiminta ja riittävä suorituskyky varmistetaan kokein. Nämä kokeet on tehtävä kemiallisesti edustavissa olosuhteissa käyttäen suojarakennuksen sisäpuolelle sijoitettavia, edustavasti vanhennettuja eriste- ja pinnoitemateriaaleja. Suodatinrakenteiden suunnittelussa on otettava huomioon seuraavat seikat:

1. Suodattimien läpi kulkeutuvien epäpuhtauksien määrä on niin vähäinen, että niistä ei ole haittaa jäähdytettä kierrättävien pumppujen toiminnalle tai reaktorin jäähdytykselle.

2. Suodatinrakenteisiin kertyvien epäpuhtauksien aiheuttama painehäviö ei estä jäähdytyskierron suunniteltua toimintaa.
3. Suodatinrakenteet voidaan puhdistaa käänteisellä jäähdytevirtauksella tai kaasupuhalluksella, mikäli painehäviö niiden yli osoittaa vaaraa suodattimien liiallisesta tukkeutumisesta.

5.2 Automaatiojärjestelmät

5.2.1 Yleiset vaatimukset

5201. Ydinvoimalaitoksen automaatiosuunnittelu on tehtävä siten, että automaatiojärjestelmät täyttävät tämän ohjeen luvussa 4 esitetyt turvallisuussuunnittelun vaatimukset .

5202. Automaatioarkkitehtuurin suunnittelussa on noudatettava samaa perusteellisuutta kuin turvallisuusluokaltaan korkeimman automaatioarkkitehtuuriin liittyvän järjestelmän suunnittelussa. Suunnittelu on suoritettava siten, että tämän ohjeen luvussa 3 esitetyt suunnittelun hallintaa koskevat vaatimukset täyttyvät.

5203. Ydinvoimalaitoksen automaatioarkkitehtuurin suunnittelussa on automaatioarkkitehtuurille määriteltävä toiminnalliset ja ei-toiminnalliset vaatimukset, joihin tulee myös sisältyä

1. tehtäväanalyysin perusteella johdetut vaatimukset
2. laitossuunnittelun asettamat rajoitukset ja vaatimukset automaation toiminnallisuudelle ja vikaantumiskäyttäytymiselle
3. vaatimukset järjestelmien ja muiden eroteltavien kokonaisuuksien väliselle riippumattomuudelle, erottelulle ja suunnittelussa huomioon otettaville yhteyksille
4. vaatimukset koskien kunkin automaatiojärjestelmän odotettua käyttöikää, riippumattomuutta yksittäisestä teknologiasta sekä laitoksen ja automaatiojärjestelmien integrointia sellaisella tavalla, joka helpottaa laitteiden ja järjestelmien vaihtamista myös mahdollisia teknologisia murroksia ajatellen.

5204. Ydinvoimalaitoksen automaatioarkkitehtuurin suunnittelu on dokumentoitava siten, että automaatioarkkitehtuurin ja laitoksen suunnitteluun osallistumaton ulkopuolinen taho voi varmistaa automaatioarkkitehtuurin suunnitteluperusteiden ja -vaatimusten asianmukaisuuden, suunnittelun oikeellisuuden, asianmukaiset perusteet keskeisimmille suunnittelupäätöksille sekä automaation vikaantumiskäyttäytymisen.

5205. Automaatiojärjestelmien suunnittelussa käytettyjen tietoteknisten työkalujen ja testausmenetelmien (esimerkiksi laskentaohjelmistot, ohjelmistojen kääntäjät ja testaustyökalut) turvallisuusmerkitys suunnitellulle lopputuotteelle on arvioitava. Turvallisuusluokiteltujen järjestelmien suunnittelussa ja toteutuksessa käytettävät työkalut on nimettävä. Mikäli työkalun tai testausmenetelmän laadulla on suora merkitys lopputuotteen oikeaan toimintaan tai vikataajuuteen, se on kelpoistettava käyttötarkoitukseensa. Yksityiskohtaiset vaatimukset työkalujen kelpoistuksesta annetaan ohjeessa YVL E.7. Kelpoistus on työkalulle versiokohtainen.

5206. Langattomaan tiedonsiirtoon perustuvia ratkaisuja ei saa käyttää turvallisuustoiminnoissa.

5.2.2 Käyttöliittymät

5207. Ohjaajien ja automaation työnjako on suunniteltava häiriö- ja onnettomuustilanteiden hallintaan liittyvän tehtäväanalyysin avulla siten, että inhimilliset rajoitukset otetaan huomioon. Tehtäväanalyysiä on käytettävä automaatioarkkitehtuurin ja automaation käyttöliittymien suunnittelussa.

5208. Ohjaajalle jäävän harkinta-ajan pituuden riittävyyttä on arvioitava laitokselle tehtäviä odotettavissa olevia käyttöhäiriöitä ja onnettomuuksia sekä niiden yhteydessä vaadittavia ohjaajien toimenpiteitä koskevien analyysien perusteella. Harkinta-aikojen pituus ja niiden perustelut on dokumentoitava tehtäväanalyysiin.

5209. Ohjaajien on voitava käynnistää tarvittavat turvallisuustoimintoja toteuttavat järjestelmät ja automaatiotoiminnot valvomosta käsin, jos se ohjaajien tilannearvion mukaan on turvallisuuden varmistamiseksi tarpeellista.

5210. Ohjaajilla on oltava valvomossa käytettävissään selkeästi esitetyt ja luotettavat tiedot automaation tilasta.

5211. Ohjaajilla on onnettomuuksien hallintatilanteita varten oltava käytössään havainnollinen koottu esitys turvallisuustoimintojen tilasta ja onnettomuuksien hallinnan kannalta keskeisien laitossuureiden arvoista. Informaatio on esitettävä sellaisessa muodossa, että ohjaajat saavat selkeän kuvan laitoksen tilasta.

5212. Automaatiojärjestelmien käyttöliittymiä on käsiteltävä kelpoistuksessa ja vikaantumistarkasteluissa käyttöliittymään liittyvän järjestelmän osana. Eri järjestelmien käyttöliittymien keskittäminen esimerkiksi valvomoergonomian takia ei saa heikentää tässä ohjeessa esitettyjä erotteluvaatimuksia.

5.2.3 Instrumentointi

5213. Turvallisuusautomaatioon liittyvät mittaukset on suunniteltava siten, että ne antavat tarkat ja luotettavat lähtötiedot turvallisuusluokitelluille automaatiojärjestelmille. Lähtötiedot on oltava jäljitettävissä laitoksen ja laitoksen järjestelmien suunnitteluvaatimuksiin.

5214. Ydinvoimalaitoksella on oltava hallittuun tilaan ohjaamiseen ja siinä pitämiseen tarvittava onnettomuusinstrumentointi, joilla todetaan turvallisuustoimintojen toteutuminen onnettomuustilanteissa. Tähän onnettomuusinstrumentointiin kuuluu koko tiedonvälitysketjun laitteet anturista näyttölaitteeseen.

5215. Ydinreaktorin valvontainstrumentointi on suunniteltava siten, että se antaa riittävän tarkat ja luotettavat lähtötiedot reaktorin tehojakauman ja termisten marginaalien määrittämiseksi. Nämä reaktorin suureet on laskettava automaattisesti niin usein, kuin reaktorin toimintaolosuhteiden ylläpitämiseksi on tarpeen.

5216. Reaktorin instrumentoinnilla on saatava riittävä tieto reaktorisydämeen liittyvien epätavallisten tai ennakoimattomien toimintatilojen tunnistamiseksi mukaan lukien tieto polttoaineen tai reaktorin sisäosien virheellisestä sijoituksesta.

5217. Painevesilaitoksen primääripiirissä on oltava irtoesineiden havaitsemisen mahdollistava valvontainstrumentointi.

5218. Suojarakennuksessa on oltava onnettomuuksien seurantaa ja hallintaa varten mittaus- ja valvontainstrumentointi, jolla saadaan riittävä tieto suojarakennuksen tilasta ja jonka avulla voidaan suunnitella ja toteuttaa tarvittavat vastatoimenpiteet.

5219. Suojarakennuksessa on oltava vakavien reaktorionnettomuuksien valvomiseksi mittaus- ja valvontainstrumentointi, jolla saadaan riittävä tieto mahdollisten vakavien reaktorionnettomuuksien kulusta ja suojarakennuksen eheyttä mahdollisesti uhkaavista seikoista.

5220. Mittausjärjestelmien on pystyttävä mittaamaan koko sillä alueella, jolla mitattava suure voi vaihdella käyttötilanteissa tai onnettomuuksissa.

5221. Mittaukset on suunniteltava mahdollisuuksien mukaan siten, että jos mittaus vikaantuu tai mittausalue ylittyy, ohjaajat huomaavat sen helposti.

5222. Valvontalaitteet on suunniteltava tallentamaan laitoksen tilaa kuvaavat toimintasuureet ja järjestelmien ohjauskäskyt siten, että laitoksen käyttötapahtumia ja onnettomuuksia voidaan jälkikäteen analysoida.

5.2.4 Käyttöautomaatio

5223. Ydinvoimalaitoksella on oltava normaaleja käyttötilanteita varten luotettavat järjestelmät reaktorin ja laitoksen järjestelmien toiminnan valvontaa, ohjausta ja säätöä varten. Näitä järjestelmiä kutsutaan käyttöautomaatioksi.

5224. Käyttöautomaation on pidettävä prosessin parametrit normaalia käyttöä vastaavalla toiminta-alueella sekä valvottava laitoksen järjestelmien, rakenteiden ja laitteiden kuntoa.

5225. Käyttöautomaatio on suunniteltava siten, että käyttöautomaation yksittäisen vian sattuessa ei synny tarvetta käynnistää oletettujen onnettomuuksien hallintaa varten suunniteltuja turvallisuusjärjestelmiä.

5226. Käyttöautomaatioon liittyvissä järjestelmissä on oltava riittävät mittaus- ja tilatiedot, jotka

automaattisesti tai laitoksen ohjaajien avustamana käynnistävät korjaavat ohjaus- ja säätötoimenpiteet, jos laitoksen parametrit joutuvat normaalin toiminta-alueen ulkopuolelle.

5227. Käyttöautomaation toiminta- ja hälytysrajat on asetettava siten, että ohjaus- ja säätötoimenpiteet voidaan käynnistää oikea-aikaisesti ja saattaa päätökseen ylittämättä niitä raja-arvoja, joiden mukaisesti turvallisuusluokiteltu automaatio käynnistää turvallisuustoimintoja.

5.2.5 Suojausautomaatio

5228. Ydinvoimalaitoksella on oltava automaatiojärjestelmät, jotka tarpeen mukaan käynnistävät suojaustoimintojen toteuttamiseksi tarvittavat järjestelmät ja ohjaavat näiden järjestelmien toimintaa onnettomuuden estämiseksi tai sen seurausten lieventämiseksi. Näiden suojausautomaatiojärjestelmien on kyettävä pitämään laitos hallitussa tilassa niin kauan, että ydinvoimalaitoksen ohjaajille jää riittävästi harkinta-aikaa oikeiden toimenpiteiden tekemiseksi. Suojausautomaatio käsittää koko toimintoketjut laitoksen tilan seurannasta ohjattaviin toimilaitteisiin saakka.

5229. Suojausautomaation turvallisuustoiminnon on käynnistyttävä vähintään kahdesta eri prosessisuureesta, jotka ovat molemmat fysikaalisesti odotettavissa olevasta käyttöhäiriöstä tai onnettomuudesta riippuvia ja joiden laukaisurajat voidaan asettaa siten, että ne saavutetaan riittävän aikaisin.

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.

5231. Suojausautomaatio on suunniteltava siten, että ohjaajien valvomossa tekemä toimenpide tai jonkin muun järjestelmän toiminta ei voi estää tai pysäyttää suojausjärjestelmän käynnistämää turvallisuustoimintoa, ennen kuin suojaustoiminto on saatettu loppuun tai ennen kuin laitossuureet ovat sellaiset, että suojaustarve on poistunut.

5232. Suojaustoiminnot on pystyttävä koestamaan myös laitoksen käytön aikana. Koestusmahdollisuus on suunniteltava siten, että koestettavan osan jälkeinen suojausautomaation osa voidaan kaikkien kokeiden aikana saattaa laitoksen turvallisuuden kannalta edulliseen tilaan.

5233. Suojausautomaation suunnittelussa on huomioitava määräaikaiset suojaustoimintojen koestukset. Suojausautomaation määräaikaiskokeiden on kyseessä olevan käynnistyksen tyypin mukaan katettava koko ketju mittauksesta toimilaitteisiin tai suojausautomaation lähtösignaaleihin saakka. Vaatimukset, jotka liittyvät määräajoin tapahtuvan koestuksen kattavuuteen ja koestuslaajuuteen on määriteltävä.

5234. Suojausautomaatiossa käytettävän itsediagnostiikan riittävä kattavuus on osoitettava analyysein. Myös itsediagnostiikan vikaantumisen vaikutus suojausautomaation toimintaan on analysoitava.

5235. Suojausautomaatio on suunniteltava siten, että se valvoo tulo- ja lähtöviestiensä kelvollisuutta ja sisäistä toimintaansa sekä hälyttää tarvittaessa.

5.2.6 Automaation erottelu ja vikojen leviämisen estäminen

5236. Automaatiosuunnittelussa on otettava huomioon satunnaiset vikaantumiset (esimerkiksi laiteviat), systemaattiset virheet ja vikaantumiset (esimerkiksi ohjelmistoviat) sekä niiden seurauksena syntyvät passiiviset ja aktiiviset viat.

5237. Automaation vikaantumisen seurauksia on rajoitettava käyttäen turvallisuussuunnittelun keinoja, joita ovat syvyyssuuntaisuus, moninkertaisuus, erilaisuus ja erottelu.

5238. Ydinvoimalaitosta ohjaavat automaatiojärjestelmät on suunniteltava sellaisiksi, että niiden vikaantuminen ei estä alkutapahtuman hallintaa.

5239. Ydinvoimalaitoksen automaatiojärjestelmässä esiintyvä yksittäisvika ei saa aiheuttaa käyttöhäiriötä pahempaa alkutapahtumaa.

5240. Automaatiojärjestelmien vikaantuessa niiden on täytettävä seuraavat vaatimukset.

1. Turvallisuustoimintoja ohjaavat automaatiojärjestelmät on suunniteltava siten, että ne joutuvat vikaantumisen seurauksena laitoksen turvallisuuden kannalta edulliseen tilaan.
2. Alemman turvallisuusluokan automaatiojärjestelmien vikaantuminen ei saa estää suojausjärjestelmää toteuttamasta turvallisuustoimintoja.
3. Luokan EYT automaatiojärjestelmät eivät saa vikaantuessaan aiheuttaa käyttöhäiriötä pahempaa alkutapahtumaa eikä estää onnettomuuksia varten suunniteltujen turvallisuustoimintojen toteutumista.
   a. Onnettomuustilanteissa niiden vikaantuminen ei saa olennaisesti huonontaa laitoksen tilaa (tapahtuma pysyy saman tapahtumaluokan sisällä).
   b. Odotettavissa olevan käyttöhäiriön yhteydessä niiden aktiivinen vikaantuminen ei saa johtaa luokan 1 onnettomuutta pahempiin seuraamuksiin.
4. Turvallisuusluokan 3 käyttöautomaation vikaantuminen ei saa estää onnettomuuksia varten suunniteltujen turvallisuustoimintojen toteutumista eikä onnettomuuden yhteydessä olennaisesti huonontaa laitoksen tilaa.
5. Turvallisuusluokan 3 automaation (muun kuin käyttöautomaation) vikaantuminen alkutapahtumana ei saa johtaa luokan 1 onnettomuutta pahempiin seurauksiin.
6. Turvallisuusluokan 3 automaation (muun kuin käyttöautomaation) vika odotettavissa olevaan käyttöhäiriöön tai luokan 1 onnettomuuteen yhdistettynä ei saa johtaa luokan 2 onnettomuutta pahempiin seurauksiin.
7. Käyttöhäiriöiden ja luokan 1 oletettujen onnettomuuksien yhteydessä tapahtuvaa suojausjärjestelmän yhteisvikaa käsitellään DEC A tapahtumana.
8. Vakavien reaktorionnettomuuksien hallintaan käytettävän instrumentoinnin ja ohjausjärjestelmien on oltava riippumattomia laitoksen muista automaatiojärjestelmistä. Muiden automaatiojärjestelmien vikaantuminen ei saa häiritä vakavien onnettomuuksien hallintatoimenpiteitä.

5241. Automaation suorittamien ohjausten ja toimintojen vikaantumisten ja virheiden vaikutukset on analysoitava toiminnallisina kokonaisuuksina. Toiminnalliset kokonaisuudet voivat olla järjestelmän sisäisiä rakenteita ja ne voivat ylittää järjestelmien väliset rajapinnat. Analyysiin valitut toiminnalliset kokonaisuudet on perusteltava. Analyysissä on otettava huomioon automaation kaikki vikaantumistavat. Analyysilla on osoitettava, että automaatiojärjestelmät täyttävät kohdissa 5238, 5239 ja 5240 esitetyt vaatimukset.

5242. Järjestelmien väliset rajapinnat on määriteltävä osana automaatioarkkitehtuurin suunnittelua.

5243. Turvallisuusautomaation tiedonsiirtojärjestelmien on täytettävä vasteaikaa koskevat vaatimukset laitoksen normaalikäytön, odotettavissa olevien käyttöhäiriöiden ja onnettomuuksien aikana. Tämä on osoitettava pahimmissa mahdollisissa kuormitustilanteissa.

5244. Suojausjärjestelmä on erotettava toiminnallisesti muista automaatiojärjestelmistä siten, että informaatiovirta suojausjärjestelmästä muihin automaatiojärjestelmiin on toteutettu yksisuuntaisesti käyttäen fyysisesti yhdensuuntaistavaa erotuslaitetta.

5245. Automaatioarkkitehtuurin rajapinta automaatioarkkitehtuurista hallinnollisiin tietojärjestelmiin on toteutettava yhdensuuntaistamalla tiedonsiirto siten, että tiedonsiirto on estetty automaatioarkkitehtuuria käyttäen fyysisesti yhdensuuntaistavaa erotinta.

5246. Kyberturvallisuus on huomioitava automaatio- ja sähköjärjestelmien suunnittelussa, ja turvallisuuteen liittyvät vastatoimet on suunniteltava laitosturvallisuuteen perustuvien riskiarvioiden pohjalta. Esimerkiksi luvaton pääsy ohjelmistoa sisältäviin järjestelmiin ja laitteisiin on estettävä riittävien fyysisten, teknisten ja hallinnollisten turvajärjestelyjen avulla, asiattomien laitteiden ja ohjelmien asentaminen on estettävä luotettavasti ja ohjelmistoihin tehdyt muutokset on voitava havaita ja jäljittää. (Muutoksiksi luetaan varsinaisten ohjelmistopäivityksien lisäk-

si esimerkiksi konfigurointi ja parametrointi). Yksityiskohtaiset tietoturvallisuuteen liittyvät vaatimukset annetaan ohjeessa YVL A.12.

5.2.7 Automaatiojärjestelmien testaus

5247. Automaatioarkkitehtuurin ja automaatiojärjestelmien testausta varten on laadittava testaussuunnitelmat.

5248. Testaussuunnitelmat ja -tulokset on dokumentoitava siten, että ne voidaan arvioida riippumattomasti.

5249. Testaussuunnitelmassa on määriteltävä yksiselitteisesti testauksen hyväksymiskriteerit. Testauksen kattavuus on määriteltävä yksiselitteisesti. Automaatiojärjestelmien testauksen kattavuus on määriteltävä automaatiokaaviotasolla esimerkiksi rakenteellisia kattavuusmittoja hyväksikäyttäen.

5250. Testauksen suunnittelussa, suorittamisessa ja tulosten arvioinnissa on hyödynnettävä suunnittelusta ja valmistuksesta riippumatonta testaajaa. Suoritettujen testien tulokset on analysoitava, ja suoritettujen testien riittävyys on perusteltava.

5251. Testauksessa ja toiminnallisissa analyyseissä tulee huomioida järjestelmän tai järjestelmään kuuluvien laitteiden käytettävän toiminnallisuuden lisäksi myös järjestelmän tai laitteiden mahdollisesti sisältämä toiminnallisuus, jota ei järjestelmässä suoraan käytetä. Käyttämättömien toimintojen vikaantumisvaikutukset on kartoitettava. Testauksessa ja toiminnallisissa analyyseissä on huomioitava dokumentoimattoman toiminnallisuuden olemassaolon mahdollisuus.

5252. Tehdastestien on katettava kaikki järjestelmän toiminnot ja ajoitukset, vikaantumiskäyttäytyminen sekä mahdollisuuksien mukaan itsediagnostiikkatoiminnot. Järjestelmän vaatimustenmukaisuutta osoittavissa testeissä ja varsinaisissa kelpuutustesteissä on käytettävä simulaattoreita testauksen apuvälineinä. Muutostöissä simulaattoritestauksen tarve on arvioitava muutostyön laajuuden perusteella.

5253. Ohjelmisto on kattavasti testattava asennettavassa laitteistossa.

5254. Tehdastestit on suoritettava testausta varten suunnitellussa tehdastestiympäristössä.

5255. Tehdastestien jälkeen mahdollisesti tarvittava muutossuunnittelu on suoritettava määriteltyjä konfiguraationhallinta- ja regressiotestausmenettelyjä käyttäen.

5256. Turvallisuusluokan 2 ja 3 automaatiojärjestelmiä koskevat tehdastestit on suoritettava STUKin hyväksymien suunnitteluasiakirjojen mukaiselle kokoonpanolle.

5257. Ennen turvallisuusluokan 2 tai 3 automaatiojärjestelmän purkamista tehdastestikentältä luvanhaltijan on toimitettava STUKille hyväksyttäväksi luvanhaltijan selvitys järjestelmän vaatimustenmukaisuudesta tehdaskenttätestien päättymishetkellä, ja luvanhaltijan selvitykselle on saatava STUKin hyväksyntä.

5.3 Valvomot

5.3.1 Yleistä

5301. Valvomoa ja varavalvomoa on suunnittelussa ja STUKin valvonnassa käsiteltävä toiminnallisena kokonaisuutena kuten turvallisuusluokan 3 järjestelmää. Yksittäisten valvomojärjestelmien luokituksessa noudatetaan yleisiä luokitusperiaatteita.

5302. Inhimilliset ja organisatoriset tekijät on otettava riittävässä laajuudessa huomioon alusta asti valvomotoimintoja ja valvomoon vaikuttavia muutoshankkeita suunniteltaessa.

5303. Uudishankkeissa ja laajemmissa valvomomuutoksissa valvomotoimintojen suunnittelua ja toteutusta on ohjattava HFE-ohjelmalla (Human Factors Engineering), johon on sisällytettävä mm. seuraavat osa-alueet:

1. käyttökokemusten hyödyntäminen
2. toimintojen allokointi ja tehtäväanalyysit
3. henkilöstö- ja koulutussuunnittelu
4. käyttöliittymän suunnittelu
5. ohjeistokehitys

6. inhimillisiin tekijöihin liittyvä todentamis- ja kelpuutussuunnitelma ja sen toteutus
7. inhimillisen luotettavuuden arviointi
8. asennus ja käyttöönotto sekä valvomon toimivuuden arviointi ja seuranta.

Valvomotoimintojen ja ydinvoimalaitoksen hallintaan tarvittavan ohjeiston on muodostettava kokonaisuus, jonka toimivuus on varmistettava laitossimulaattorilla. Valvomon toiminnallisten ja merkittävien ergonomisten muutosten toimivuus on varmistettava etukäteen simulaattorilla tehtävin testein.

5304. Ohjaus- ja säätöjärjestelmien sekä suojausautomaation moninkertaisuusperiaatetta toteuttavat osat on erotettava toisistaan toiminnallisesti valvomon sisällä.

5305. Valvomo ja valmiuskeskus on suojattava siten, että työskentely niissä on mahdollista ilman suojavarusteita normaalin käytön sekä onnettomuuksien ja uhkatilanteiden aikana. Paloturvallisuus, suojaus tulvimista vastaan, valaistus, ilmastointi, meluntorjunta, säteilysuojaus ja kulunvalvonta on otettava huomioon.

5306. Valvomo ja varavalvomo on erotettava toisistaan fyysisesti siten, että todennäköisyys molempien vahingoittumiselle saman sisäisen tai ulkoisen tapahtuman seurauksena on erittäin pieni.

5.3.2 Valvomo

5307. Valtioneuvoston asetuksen (717/2013) 19 §:n mukaan *ydinvoimalaitoksen valvomossa on oltava laitteet, jotka antavat tiedon ydinreaktorin tilasta ja ilmaisevat, jos se poikkeaa normaalista.*

5308. Valvomosta on voitava tehdä laitoksen hallitsemiseksi tarvittavat toimenpiteet käyttötilanteissa ja onnettomuuksien aikana.

5309. Ohjaajien toimintaa avustamassa onnettomuuksien hallintaa varten on oltava hälytysjärjestelmien lisäksi tukitoiminto, jolla esitetään kattavat yhteenvetotiedot turvallisuustoimintojen tilasta. Onnettomuuden hallinnan tukitoiminto on näyttöteknisesti erotettava muusta valvomoinformaatiosta. Myös seisokkitilojen hallintaa varten on oltava erilliset näytöt, joissa esitetään yhteenvetotiedot turvallisuustoimintojen tilasta.

5310. Odotettavissa olevien käyttöhäiriöiden ja onnettomuuksien havaitsemiseksi, tunnistamiseksi ja hallitsemiseksi tarvittavat hälytykset on priorisoitava tapahtuman turvallisuusmerkityksen mukaan. Hälytykset on suunniteltava siten, että nämä havaitaan mahdollisimman luotettavasti.

5311. Keskeisen onnettomuusinstrumentoinnin mittaus- ja tilatietojen näytöt on pystyttävä tunnistamaan helposti.

5312. Valvomosta on pystyttävä seuraamaan ulkoisen voimansiirtoverkon tilaa.

5313. Päävalvomosta ja muista tarvittavista valvonta- ja ohjauspaikoista on esitettävä valvomon kelpoistussuunnitelma rakentamislupaa haettaessa.

5.3.3 Varavalvomo

5314. Valtioneuvoston asetuksen (717/2013) 19 §:n mukaan *ydinvoimalaitoksessa on oltava valvomosta riippumaton varavalvomo ja tarvittavat paikalliset ohjausjärjestelmät ydinreaktorin pysäyttämiseen ja jäähdyttämiseen sekä reaktorin ja laitoksella varastoituna olevan käytetyn polttoaineen jälkilämmön poistamiseen.*

5315. Varavalvomo on suunniteltava siten, että sieltä voidaan ohjata laitos hallittuun tilaan valvomon menetyksen ja tähän mahdollisesti liittyvien käyttöhäiriöiden yhteydessä. Siirtymisessä hallitusta tilasta turvalliseen tilaan voidaan käyttää hyväksi myös paikallisia ohjauksia. Varavalvomon suunnittelua koskevia vaatimuksia esitetään ohjeessa YVL A.11.

5316. Valvomosta on voitava siirtyä turvallisesti varavalvomoon.

5317. Valvomon ja varavalvomon ohjausten keskinäinen riippumattomuus on toteutettava käyttäen fyysistä ja toiminnallista erottelua. Minkään palo-osaston tuhoutuminen ei saa aiheuttaa sekä valvomon että varavalvomon ohjausten menettämistä.

5318. Valvomon ja varavalvomon ohjausjärjestelmien välinen hierarkia on määriteltävä siten, että laitosta voidaan ohjata vain yhdestä ohjauspaikasta kerrallaan.

5.4 Sähköjärjestelmät

5401. Valtioneuvoston asetuksen (717/2013) 14 §:n mukaan *ydinvoimalaitoksella on oltava häiriö- ja onnettomuustilanteiden varalta ulkoinen ja sisäinen sähkötehon syöttöjärjestelmä. Turvallisuustoiminnoissa tarvittava sähköteho on voitava syöttää kumpaa tahansa järjestelmää käyttämällä.*

5402. Laitokseen on suunniteltava järjestelmät, jotka mahdollistavat sähkötehon syötön päägeneraattorilta laitoksen turvallisuuden kannalta tärkeille järjestelmille, jos yhteys ulkoiseen siirtoverkkoon katkeaa. Tämän sähkötehon syötön suunnittelussa on huomioitava ohjeen YVL E.7 kohdassa 5.5 esitetyt vaatimukset.

5403. Laitosyksikön ulkoinen ja sisäinen sähkötehon syöttöjärjestelmät on suunniteltava siten, että kummankin kapasiteetti yksin on riittävä turvallisuustoimintojen toteuttamiseen luvussa 4 edellytettyjen suunnitteluvaatimusten mukaisesti.

5404. Laitoksen ulkoiset ja sisäiset sähkötehon syöttölähteet on suunniteltava siten, että yksittäisen syöttölähteen menetyksestä seuraava tai samasta syystä aiheutuva jäljelle jääneiden syöttölähteiden menetys on erittäin epätodennäköistä.

5405. Turvallisuusluokiteltujen sähköjärjestelmien moninkertaisuusperiaatetta toteuttavien osien välisiä ristiin kytkentöjä on vältettävä, ellei voida osoittaa, että ne parantavat järjestelmän luotettavuutta.

5406. Turvallisuusluokiteltujen sähköjärjestelmien moninkertaisuusperiaatetta toteuttavien osien väliset ristiin kytkennät on suunniteltava siten, että tarkoitukseton kytkeytyminen on estetty luotettavalla tavalla ja inhimilliset virheet niiden käyttöönoton ja käytön yhteydessä ovat epätodennäköisiä.

5407. Yhden moninkertaisuusperiaatetta toteuttavan sähköjärjestelmän osan vian leviäminen ristiin kytkennän kautta toiseen osaan on estettävä luotettavasti.

5408. Ulkoisen verkon aiheuttamat laitospaikkakohtaiset ja laitoksen sähkölaitteiden tai vikojen aiheuttamat taajuus- ja jännitevaihtelut on analysoitava ja otettava huomioon sähköjärjestelmien ja kuluttajien vaatimusmäärittelyissä sekä suunnittelussa. Tämän sähkötehon syötön suunnittelussa on huomioitava ohjeen YVL E.7 kohdassa 5.5 esitetyt vaatimukset.

5409. Ulkoisen verkon laitospaikkakohtaiset, laitoksen sähkölaitteiden tai vikojen aiheuttamat taajuus- ja jännitevaihtelut eivät saa vaarantaa turvallisuustoimintoja normaalikäytön, odotettavissa olevien käyttöhäiriöiden tai onnettomuuksien aikana.

5410. Sähköjärjestelmät on suunniteltava siten, että laitoksen käyttötoimenpiteet sekä sähköjärjestelmien ja -laitteiden määräaikaistarkastukset, -huollot ja -testit sekä korjaukset voidaan tehdä laitoksen tai henkilöstön turvallisuutta vaarantamatta.

5411. Sähköjärjestelmien käyttökunnottomuusaika määräaikaistarkastusten, huoltojen, testien sekä korjausten yhteydessä on pidettävä niin pienenä, kuin käytännössä on mahdollista.

5412. Sähköjärjestelmien määräaikaistarkastukset ja -testit on suunniteltava niin kattaviksi, että turvallisuusluokiteltujen sähköjärjestelmien ja -laitteiden toimintakyvyn heikkeneminen voidaan havaita nopeasti, ennen kuin hyväksymisrajat alitetaan.

5413. Säännöllisin testauksin ja tarkastuksin on varmistuttava siitä, että varavoiman syöttöön liittyvät laitteet ja muut sähköjärjestelmien osat, joita ei käytetä laitoksen normaalin käynnin aikana, ovat jatkuvasti toimintavalmiit.

5414. Ohjelmistopohjaista tai ohjelmoitavaa tekniikka käytettäessä myös niihin liittyvien luvun 5.2 vaatimusten on täytyttävä.

5415. Vakavien reaktorionnettomuuksien hallintajärjestelmän käyttöenergian (sähkö, paineilma jne.) syöttöjen on oltava riippumattomia laitosyksikön muista syöttölähteistä ja käyttöenergianjakelujärjestelmistä.

5416. Ydinvoimalaitosten sähköjärjestelmien ja -laitteiden suunnittelussa, asennuksessa ja käytössä on otettava huomioon Suomessa voimassa olevat sähkölaitteistojen turvallisuutta ja sähkötyöturvallisuutta koskevat turvallisuusstandardit ja sähköturvallisuutta valvovien viranomaisten antamat muut ohjeet (esim. standardisarja SFS 6000: Pienjännitesähköasennukset, standardi SFS 6001: Suurjännitesähköasennukset ja standardi SFS 6002: Sähkötyöturvallisuus).

5.4.1 Yhteydet ulkoiseen voimansiirtoverkkoon

5417. Sähkötehon syöttöä varten on ulkopuolisesta verkosta kuhunkin laitoksen sisäisen sähkönjakelujärjestelmän moninkertaisuusperiaatetta toteuttavaan osaan oltava kaksi erillistä, toisistaan riippumatonta verkkoyhteyttä.

5418. Kumpikin näistä riippumattomista verkkoyhteyksistä on suunniteltava siten, että molempien yhteyksien samanaikainen ja samasta syystä tapahtuva vikaantuminen on epätodennäköistä.

5419. Laitoksen kumpikin riippumaton verkkoyhteys on voitava ottaa käyttöön riittävän nopeasti laitoksen päägeneraattorin verkosta irtautumisen jälkeen.

5420. Laitoksen yhteydet ulkoiseen voimansiirtoverkkoon voivat perustellusta syystä olla yhteiset usealle laitosyksikölle. Tällöin kunkin yhteyden kapasiteetin yksin on oltava riittävä turvallisuustoimintojen samanaikaiseen toteuttamiseen kaikilla laitosyksiköillä.

5421. Verkkoyhteyksien mahdollisten oikosulkujen aiheuttamiin laitevaurioihin ja tulipaloihin on kiinnitettävä huomiota, jotta yksittäinen vika kytkinkentillä tai johtokaduilla ei todennäköisesti johda kummankin verkkoyhteyden menetykseen.

5422. Laitos on varustettava luotettavalla syötönvaihtoautomatiikalla, joka huolehtii automaattisesti sähkönsyötön vaihdosta ulkoisten verkkoyhteyksien välillä.

5423. Laitoksen verkkoyhteyksien syötönvaihtoautomatiikka on suunniteltava siten, että syötönvaihto ei käynnistä laitosyksikön oletettujen onnettomuuksien hallitsemiseksi suunniteltuja turvallisuusjärjestelmiä.

5424. Laitoksen verkkoyhteyksien syötönvaihto on tarvittaessa voitava tehdä myös manuaalisesti ohjaamalla valvomosta tai valvomon menetystilanteessa varavalvomosta käsin.

5.4.2 Omakäyttösähköjärjestelmät

5425. Laitosyksikön omakäyttösähköjärjestelmät on mitoitettava sähköteknisesti siten, että niiden kautta voidaan syöttää riittävä sähköteho laitoksen turvallisuustoimintojen toteuttamiseksi kaikissa laitostiloissa.

5.4.3 Varmennetut vaihtosähköjärjestelmät

5426. Turvallisuudelle tärkeiden vaihtosähkölaitteiden sähkönsyöttö on varmennettava käyttämällä laitosalueen sisällä olevaa varatehon syöttöjärjestelmää ulkoisen sähkötehon syötön varajärjestelmänä.

5427. Sisäisen varatehon syöttöjärjestelmän on täytettävä 72 tunnin omavaraisuusehto.

5428. Sisäisen varatehon syöttöjärjestelmän on käynnistyttävä ja kytkeydyttävä automaattisesti varmistamaan turvallisuustoimintojen katkoton sähkötehon saanti toiminta-aikavaatimusten mukaisesti.

5429. Sisäinen varatehon syöttöjärjestelmä tulee voida ottaa käyttöön myös manuaalisesti valvomosta ja varavalvomosta käsin.

5430. Sähkönsyöttö on voitava palauttaa sisäiseltä varatehon syöttöjärjestelmältä takaisin normaalille ulkoiselle sähkötehon syötölle valvomosta ja varavalvomosta käsin manuaalisesti ohjaten, mikäli normaali ulkoinen sähkötehon syöttö on käytettävissä.

5431. Sisäinen varatehon syöttöjärjestelmä on mitoitettava siten, että se kykenee luotettavasti käynnistymään, kytkeytymään, ottamaan vastaan kuormitukset ja syöttämään sähkötehoa vaativimpienkin kuormitustilanteiden (esim. käynnistystilanteiden tai sähkötehon alajakelussa tapahtuvien oikosulkujen) aikana.

5432. Sisäisen varatehon syöttöjärjestelmän tuottaman vaihtosähkön laatu on pystyttävä ylläpitämään koko ajan siten, että syötettävien laitteiden toimintakyky ei vaarannu.

5433. Ydinvoimalaitosten varatehoa tuottavia laitteita koskevat tarkemmat vaatimukset on esitetty ohjeessa YVL E.10.

5434. Sisäinen varatehon syöttöjärjestelmä on varustettava kattavasti hälyttävillä kunnonvalvontajärjestelmillä, joiden avulla järjestelmien toiminnan estävät tai toimintakyvyn vaarantavat viat voidaan nopeasti havaita ja paikallistaa.

5435. Sisäisen varatehon syöttöjärjestelmän moninkertaisuusperiaatetta toteuttavat osat on voitava erottaa turvallisesti muista sähköjärjestelmistä tai järjestelmän osista toimintakyvyn testausta, huoltoa ja korjausta varten.

5436. Ydinvoimalaitoksen suunnittelussa on otettava huomioon se mahdollisuus, että laitoksen ulkoinen sähkötehon syöttö ja sisäinen varatehon syöttö menetetään yhtä aikaa (täydellinen vaihtosähkön menetys).

5437. Täydellisen vaihtosähkön menetyksen varalle laitoksella on oltava käytettävissä riippumattomat vaihtosähkön syöttölähteet, jotka ovat riippumattomat käyttötilanteita ja oletettuja onnettomuuksia varten suunnitelluista sähkötehon syöttölähteistä.

5438. Riippumattoman vaihtosähkön syöttölähteen on täytettävä 72 tunnin omavaraisuusehto.

5439. Riippumaton vaihtosähkön syöttölähde on voitava ottaa käyttöön riittävän nopeasti minimoiden samalla inhimillisten virheiden mahdollisuus.

5440. Riippumattoman vaihtosähkön syöttölähteen tehon tulee riittää laitosyksikön pitämiseen hallitussa tilassa sekä käyttöhäiriöissä että luokan 1 oletetuissa onnettomuuksissa.

5.4.4 Katkottoman sähkönsyötön järjestelmät

5441. Katkotonta sähkönsyöttöä edellyttävien turvallisuudelle tärkeiden laitteiden toiminnan varmistamiseksi niiden sähkötehon syöttö on varmennettava luotettavilla akustovarmennetuilla järjestelmillä, jotka varmistavat katkottoman sähkötehon saannin silloin, kun vaihtosähkötehon syötössä esiintyy häiriö.

5442. Akustot, latauslaitteet ja mahdolliset muuttajat on mitoitettava siten, että katkottoman sähkönsyötön järjestelmien toimintakyky voidaan niiden avulla varmistaa vaatimusmäärittelyssä järjestelmäkohtaisesti asetettujen toiminta-aikavaatimusten mukaisesti.

5443. Turvallisuudelle tärkeitä kuormia syöttävät akustot on mitoitettava kahden tunnun purkausajalle suurimmalla mahdollisella kuormituksella.

5444. Vakavien onnettomuuksien hallintajärjestelmien akustot on mitoitettava 24 tunnin purkausajalle suurimmalla mahdollisella kuormituksella.

5445. Mahdollisten polttomoottorin käynnistysakustojen ja muiden erikoisakustojen mitoitusperusteet on perusteltava tapauskohtaisesti.

5446. Katkottoman sähkönsyötön järjestelmiin liittyvien akustojen latauslaitteiden on kyettävä samanaikaisesti sekä syöttämään sähköä kuluttajille että lataamaan akustoja.

5447. Katkottoman sähkönsyötön järjestelmiin liittyvien akustojen latauslaitteet on mitoitettava siten, että niiden toimintakyky ei vaarannu vaativimmissakaan kuormitustilanteissa (esim. tyhjentyneiden akustojen lataaminen ja kuormien yhtäaikainen syöttäminen sähkökatkon jälkeen) ja käyttöolosuhteissa.

5448. Katkottoman sähkönsyötön laitteiden on kyettävä syöttämään tarvittava tasavirta myös ilman akustoa.

5449. Katkottoman sähkönsyötön toimiessa ilman akustoa on sähkön laadun oltava sellainen, ettei se aiheuta toimintahäiriöitä kuormituksena oleville laitteille,

5450. Katkottoman sähkönsyötön laitteet on suunniteltava siten, että syöttävän vaihtosähköverkon mahdollisten häiriöiden välittyminen loppukuluttajille on estetty luotettavasti.

5451. Turvallisuusluokitellut katkottoman sähkösyötön järjestelmät on varustettava kattavilla, hälyttävillä kunnonvalvontalaitteilla, joiden avulla järjestelmien toiminnan estävät tai toimintakyvyn vaarantavat viat voidaan nopeasti havaita ja paikallistaa.

5.4.5 Laitosyksiköiden väliset syöttöyhteydet

5452. Ydinvoimalaitosyksiköiden sähkönsyöttöjärjestelmät on suunniteltava siten, että samalla laitospaikalla olevalta laitosyksiköltä voidaan tarvittaessa syöttää sähkötehoa toiselle laitosyksikölle siten, että viimeksi mainittu yksikkö voidaan pitää hallitussa tilassa sähkötehon menetyksen yhteydessä.

5453. Laitosyksiköiden välinen syöttöyhteys on suunniteltava siten, että sähköhäiriön leviäminen sen kautta laitosyksiköltä toiselle ja yhteyden suunnittelematon käyttöönotto tai kytkeytyminen on epätodennäköistä.

5454. Laitosyksiköiden välinen syöttöyhteys on voitava tarvittaessa ottaa käyttöön riittävän nopeasti ja luotettavasti minimoiden samalla inhimillisten virheiden mahdollisuus.

5.4.6 Sähkö- ja automaatiojärjestelmien sähkömagneettinen yhteensopivuus (EMC)

5455. Ydinvoimalaitoksen turvallisuusluokitellut sähkö- ja automaatiojärjestelmät, -laitteet sekä niiden kaapeloinnit ja asennukset on suojattava luotettavasti sähkömagneettisten häiriökenttien vaikutuksilta.

5456. Sähkölaitteet sekä niiden kaapeloinnit on suunniteltava ja asennettava siten, että ne eivät myöskään itse aiheuta haitallisia sähkömagneettisia häiriöitä toimintaympäristöönsä.

5457. Sähkö- ja automaatiojärjestelmien, -laitteiden sekä kaapeloinnin suunnittelussa on otettava huomioon mm. seuraavat sähkömagneettiset häiriötyypit:

1. säteilevät radiotaajuiset häiriöt (häiriön päästö ja sieto)
2. johtuvat radiotaajuiset häiriöt (kaapelien kautta syntyvä päästö ja sieto)
3. staattisen sähkön purkauksen sieto (ElectroStatic Discharge, ESD).

5458. Turvallisuusluokitelluille sähkö- ja automaatiojärjestelmille sekä -laitteille on määriteltävä yksityiskohtaiset EMC-vaatimukset vaatimusmäärittelyssä.

5459. EMC-vaatimusten peruslähtökohtana voivat olla teollisuusympäristöä koskevat yleiset kansainväliset EMC-standardit. Näiden vaatimuksia on tarvittaessa täydennettävä ottamalla huomioon laitteiden sijoituspaikoilla mahdollisesti vallitsevat vaativammat EMC-olosuhteet.

5460. EMC-vaatimuksissa on otettava huomioon laitteiden altistuminen käyttöympäristössä mahdollisesti esiintyville toistuville nopeille (esimerkiksi induktiivisten kuormien poiskytkentä ja releiden kytkentävärähtelyt) ja suurenergisille (esimerkiksi erilaiset kytkentätransientit ja salama) transienttihäiriöille.

5461. EMC-vaatimuksissa on otettava huomioon ihmisen toiminnan aiheuttamat sähkömagneettiset häiriöt, esimerkiksi ydinvoimalaitoksessa käytettävien langattomien tiedonsiirto- ja puhelinjärjestelmien sekä korjaus-, huolto- ja mittauslaitteiden häiriönpäästöt.

5462. Ydinvoimalaitokselle on luotava EMC-vaatimusmäärittelyn ja kelpoistuksen tueksi radiotaajuustaulukko.

5463. Radiotaajuustaulukossa on lueteltava ydinvoimalaitoksella sallitut radiotaajuudet sekä suurimmat sallitut kenttävoimakkuudet.

5464. Radiotaajuustaulukossa on suotavaa ilmoittaa myös suurimmat sallitut lähetystehot jollekin määrätylle laitetyypille (esimerkiksi matkapuhelin tai viranomaisverkon puhelin). Tällöin

on myös ilmoitettava, mihin laskentaolettamuksiin ko. lähetysteho perustuu.

5465. Kunkin ydinvoimalaitosyksikön sähkö ja automaatiojärjestelmien sekä -laitteiden EMC-olosuhteiden kartoittamiseksi on tehtävä yksikkökohtainen analyysi, jonka perusteella arvioidaan asetettujen EMC-vaatimusten riittävyyttä.

5466. Käytössä olevan ydinvoimalaitoksen sähkö tai automaatiojärjestelmiä uusittaessa on kiinnitettävä erityistä huomiota uusien järjestelmien sijoituspaikoissa vallitseviin EMC-olosuhteisiin ja laitteiden EMC-ominaisuuksiin yhteensopivuusongelmien välttämiseksi.

5.4.7 Maadoitus- ja ukkossuojausjärjestelmät

5467. Maadoitus- ja ukkossuojausjärjestelmät on suunniteltava, asennettava ja ylläpidettävä siten, että ne suojaavat tehokkaasti ihmisiä, rakennuksia, laitteita ja sähkö- ja automaatiojärjestelmiä salamaniskujen aiheuttamilta ylijännitteiltä ja virroilta sekä mahdollisilta muilta ilmastollisilta sähkömagneettisilta häiriöiltä.

5468. Ydinvoimalaitoksen maadoitus- ja ylijännitesuojausjärjestelmät on suunniteltava siten, että ne estävät tehokkaasti vahingollisten sisäisistä ja ulkoisista syistä aiheutuvien ylijännitteiden esiintymisen sähkö- ja automaatiojärjestelmissä.

5469. Maadoitusta ja ylijännitesuojausta suunniteltaessa sähkö- ja automaatiojärjestelmät on käsiteltävä kokonaisuutena, koska järjestelmän yhdenkin osan puutteellinen suojaus saattaa altistaa muita järjestelmiä häiriöille.

5.4.8 Sähköjärjestelmien ja -laitteiden suojaus

5470. Sähköjärjestelmät on varustettava luotettavilla suojalaitteilla, jotka häiriö- ja vikatilanteissa erottavat (selektiivisesti) käytöstä ainoastaan vioittuneen laitteen tai sähköverkon osan kaikissa suunnitelluissa sähköverkon kytkentätilanteissa.

5471. Vikavirrat on katkaistava riittävän nopeasti, jotta niistä ei aiheudu vaaraa ja jotta häiriöt jäävät mahdollisimman pieniksi.

5472. Laitoksen turvallisuusluokitellut suuritehoiset kytkinlaitokset on varustettava luotettavalla valokaarisuojauksella tai muulla asianmukaisella suojauksella, jonka avulla voidaan minimoida mahdollisten valokaarivikojen aiheuttamat kojeistovauriot ja varmentaa sekä laitoksen että käyttö- ja kunnossapitohenkilöstön turvallisuus.

5473. Suojalaitteiden toiminta on ilmaistava riittävin hälytyksin, jotta mahdolliset sähköviat voidaan havaita, paikallistaa ja korjata nopeasti.

5474. Sähkönjakeluverkkoa ja suojalaitteiden toimintaa on valvottava riittävällä häiriötallennuslaitteistolla, jotta mahdolliset sähköhäiriöt voidaan havaita, paikallistaa ja korjata nopeasti.

5475. Turvallisuusluokiteltujen sähköjärjestelmien suojalaitteiden toiminta on voitava testata koko suojausketjussa.

5476. Ydinvoimalaitoksen sähköjärjestelmien suojalaitteet on testattava säännöllisesti suojauksen toimintakyvyn varmistamiseksi.

5477. Ydinvoimalaitoksen sähköjärjestelmien suojauslaitteiden testauksen yhteydessä on varmistettava suojauksen toiminnan testauksen lisäksi, että suojaus ei suurimmalla kuluttajien kuormituksella laukaise turvallisuusluokiteltuja sähkölaitteita.

5478. Suojalaitteen jollekin turvallisuustoiminnolle mahdollisesti aiheuttaman eston turvallisuusmerkitys on arvioitava ja tarvittaessa suunniteltava suojalaitteen ohitus edellyttäen, että toimenpiteellä ei vaaranneta turvallisuusluokitellun sähkönsyötön toimintakykyä.

5479. Testaustoiminnan ajaksi mahdollisesti käyttöön otettavat suojalaitteet on kartoitettava ja suunniteltava siten, että niiden käyttö ei vaaranna järjestelmän toimintakykyä todellisessa tarvetilanteessa.

5.5 Ilmanvaihto ja ilmastointijärjestelmät

5.5.1 Yleiset vaatimukset

5501. Sellaisia laitoksen tiloja varten, joiden ilmatilaan voi vapautua radioaktiivisia aineita, on suunniteltava ilmanvaihto- ja suodatusjärjestelmät, joiden tehtävä on

- vähentää laitostilojen ilman sisältämien radioaktiivisten aineiden pitoisuuksia
- estää radioaktiivisten aineiden leviäminen muihin laitostiloihin
- rajoittaa radioaktiivisten aineiden pääsyä ympäristöön.

5502. Ilmanvaihto- ja ilmastointijärjestelmien on ylläpidettävä ja turvattava ydinvoimalaitoksen tiloissa sellaiset ympäristöolosuhteet, että laitoksen turvallisuuden kannalta merkittävät laitteet ja rakenteet pysyvät kunnossa ja toimivat moitteettomasti.

5503. Turvallisuudelle tärkeitä järjestelmiä sisältävien huonetilojen ilmanvaihdon, lämmityksen ja jäähdytyksen menetyksen seurausvaikutuksia on arvioitava ja tilojen lämpötilakäyttäytymistä laitoksen häiriötilanteissa on analysoitava.

5504. Analyysien perusteella on arvioitava, onko tarpeen soveltaa erilaisuusperiaatetta tärkeiden tilojen lämmityksessä tai jäähdytyksessä (esimerkiksi ilma ja merivesi).

5505. Huonetilat, joihin on sijoitettu lämpöä tuottavia laitteita ja joissa lämpötilalle on asetettu oikean toiminnan varmistamiseksi yläraja, on varustettava luotettavilla jäähdytysjärjestelmillä.

5506. Ilmanvaihto- ja ilmastointijärjestelmien avulla on ylläpidettävä laitoksen käyttöä ja kunnossapitoa varten henkilökunnalle asianmukaisia työskentelyolosuhteita siten, että huoneilman puhtaus, lämpötila ja kosteus täyttävät annetut työsuojelumääräykset.

5507. Kukin laitoksen turvallisuuslohko, lukuun ottamatta usean turvallisuuslohkon osia sisältäviä suojarakennuksen ja valvomon tiloja, on varustettava muiden turvallisuuslohkojen ilmanvaihto- ja ilmastointijärjestelmistä riippumattomalla ilmanvaihto- ja ilmastointijärjestelmällä tilojen lämmityksen, jäähdytyksen, paloturvallisuuden ja muiden vaadittujen ympäristöolosuhteiden ylläpitämiseksi.

5508. Ilmanvaihto- ja ilmastointijärjestelmien on täytettävä tehtävänsä normaalikäytön, odotettavissa olevien käyttöhäiriöiden ja onnettomuuksien aikana. Onnettomuustilanteiden aikana tai niiden jälkeen käytettäväksi suunniteltujen ilmanvaihto- ja ilmastointijärjestelmien suunnitteluperusteena on käytettävä onnettomuustilanteiden olosuhteita. Ilmanvaihto- ja ilmastointijärjestelmän laitteiden on säilyttävä toimintakuntoisina niissä onnettomuus- ja häiriötilanteissa, joiden hallitsemiseksi ne on suunniteltu.

5509. Huonetiloille, joissa on turvallisuudelle tärkeitä laitteita, on tehtävä olosuhdemääritys. Olosuhdemäärityksen on katettava ilmanvaihto- ja ilmastointijärjestelmän suunnittelun kannalta keskeiset tekijät, kuten lämpötilat, kosteustaso, säteilytaso, lämpökuormat, paine-erot sekä tiiviys- ja eristysvaatimukset. Huoneiden olosuhdemäärityksen perusteella on esitettävä eri tilojen alustavat ilmanvaihtokertoimet.

5510. Ympäristöministeriön ja sisäasiainministeriön antamia määräyksiä ja ohjeita (RakMK) ilmanvaihtojärjestelmien suunnittelusta, käytöstä ja niihin liittyvistä paloteknisistä suunnitteluperusteista on noudatettava.

5511. Valvomo, varavalvomo, valmiuskeskus, väestönsuoja ja muut tilat, joita tarvitaan onnettomuustilanteissa, on varustettava tuloilman sulku- ja suodatuslaitteilla sekä radioaktiivisten ja myrkyllisten aineiden pitoisuuksia havainnoivilla mittalaitteilla. Suunnittelussa on otettava huomioon laitospaikan ja sen ympäristön vaaralliset aineiden varastointi ja kuljetus, uhkatilanteet ja onnettomuudet.

5.5.2 Alue- ja vyöhykejako

5512. Ydinvoimalaitoksen rakennukset ja niiden huonetilat on jaettava vyöhykkeisiin, joiden välillä on valittava sellaiset etukäteen määritellyt ja tarkistettavissa olevat paine-erot, että ilmavirtausten suunnat ovat säteilyturvallisuuden

kannalta puhtaammilta alueilta vähemmän puhtaiden alueiden suuntaan.

5513. Vyöhykejakoa suunniteltaessa on otettava huomioon
- laitoksen järjestelmistä ja laitteista vuototilanteissa vapautuvat radioaktiivisten aineiden määrät ja esiintymismuodot
- tilojen luoksepäästävyys käyttö- ja onnettomuustilanteiden aikana.

5514. Ilmavirtaukset on mitoitettava siten, että laitostilojen sisäilman radioaktiivisten aineiden pitoisuudet voidaan pitää riittävän pieninä niissä laitostiloissa, joissa työskennellään. Mitoituksessa on otettava huomioon tarvittavat oleskeluajat.

5515. Valvonta-alueeseen ja puhtaaseen alueeseen kuuluvien tilojen ilmanvaihtojärjestelmien on oltava täysin erillisiä toisistaan. Poikkeuksena ovat valvonta-alueen ja puhtaan alueen rajalla olevat, henkilöliikenteeseen käytettävät tilat. Laitoksen säteilyolosuhteisiin perustuva ydinlaitosten käytön aikainen alue- ja vyöhykejako on esitetty ohjeessa YVL C.1.

5516. Valvonta-alueeseen kuuluvien tilojen ilmanvaihtojärjestelmien suunnitelmissa on esitettävä, miten estetään radioaktiivisten aineiden pääsy ympäristöön palotilanteissa.

5.5.3 Tuloilma

5517. Laitoksen turvallisuusluokiteltuja järjestelmiä sisältävien rakennusten tuloilmakeskukset ja tuloilmajärjestelmät on suunniteltava ja sijoitettava siten, että savun leviäminen niihin on palotilanteessa epätodennäköistä. Mikäli savua kulkeutuu palotilanteessa tuloilmakeskuksiin, savun leviäminen laitoksen tiloihin on voitava estää esimerkiksi pysäyttämällä tuloilmajärjestelmä.

5518. Laitoksen turvallisuusluokiteltuja osajärjestelmiä sisältävien rakennusten tuloilmakeskukset ja tuloilmajärjestelmät on lisäksi suunniteltava ja sijoitettava siten, että mahdollisten palavien, myrkyllisten tai muuten vaarallisten aineiden leviäminen niihin on epätodennäköistä. Haitallisten aineiden leviäminen laitoksen tiloihin on voitava havaita sekä estää esimerkiksi pysäyttämällä tuloilmajärjestelmä.

5519. Tuloilmajärjestelmät on varustettava suodatuslaittein, joilla ehkäistään ulkoilman epäpuhtauksien kertyminen laitostiloihin.

5520. Tuloilman saanti on varmistettava sellaisissa tilanteissa, joissa lumi tai jää voi vaikuttaa haitallisesti.

5.5.4 Poistoilma

5521. Valvonta-alueen poistoilma on ohjattava hallitusti ilmanvaihtokanavia käyttäen poistoilmapiipun kautta ympäristöön. Ennen poistoilmapiippua valvonta-alueelta tulevassa turvallisuusluokiteltujen järjestelmien tilojen poistoilmanvaihdossa voi näiden tilojen ulkopuolella olla yhteisiä kanavia, jos ne on varustettu riittävällä savu- ja paloerottelulla.

5522. Asetettaessa vaatimuksia kanavien tiiveydelle on huomioitava radioaktiivisten aineiden määrä poistoilmassa, kanavien paine-erot ympäristöönsä nähden sekä ne huonetilat, joiden kautta ilmanvaihtokanava kulkee.

5523. Ilmanvaihtokanavien ja laitteiden materiaalien sekä niiden pinnoitteiden ja geometristen muotojen suunnittelussa on otettava huomioon pintojen puhdistettavuus mahdollisesta radioaktiivisesta kontaminaatiosta.

5524. Laitostiloihin vapautuneet palavat, myrkylliset tai muuten vaaralliset kaasut ja höyryt on poistettava ilmanvaihdon avulla.

5525. Jos laitostilojen poistoilma sisältää tai saattaa sisältää ympäristön kannalta merkittäviä määriä radioaktiivisia aineita (kaasumaisia, aerosoli- tai partikkelimuodossa), on poistoilma suodatettava riittävän tehokkaasti.

5526. Mikäli poistoilmavirtojen rajoittaminen on tarpeen päästöjen pienentämiseksi onnettomuustilanteessa, on tarvittaessa varauduttava järjestämään näiden tilojen ilmansuodatus ja -jäähdytys tilakohtaisin laittein.

5527. Suodattimien mahdollinen palaminen on otettava huomioon suunnittelussa. Palavat suodattimet on voitava eristää muusta ilmanvaihtojärjestelmästä.

5.5.5 Pinnoitteet

5528. Suojarakennuksen sisäpuolisten rakenteiden pinnoitteita koskevat vaatimukset on esitetty ohjeessa YVL E.6. Vaatimukset on otettava huomioon myös ilmanvaihto- ja ilmastointijärjestelmien suunnittelussa lukuun ottamatta sellaisia yksittäisiä laitteita, joiden pinnoitettu pinta-ala voidaan katsoa niin vähäiseksi, että siitä onnettomuustilanteessa mahdollisesti irtoava pinnoite ei aiheuta virtausteiden tukkeutumista.

6 STUKille toimitettavat asiakirjat

6.1 Uuden ydinvoimalaitoksen suunnittelu ja rakentaminen

601. Uutta ydinvoimalaitosta ja sen järjestelmiä sekä näiden suunnittelua koskevat asiakirjat toimitetaan STUKille sellaisessa muodossa ja sellaisella aikataululla, että niiden perusteella voidaan tehdä kuhunkin lupaprosessiin liittyvä turvallisuusarvio. Asiakirjat voidaan toimittaa luvanhakijan esittämän suunnitelman mukaisina, tarkastuksen kannalta loogisessa järjestyksessä ja soveltuvina kokonaisuuksina yhdessä tai useammassa erässä ennen lupahakemuksen jättämistä ja pääsääntöisesti lupahakemuksen jättämisen yhteydessä. Jos jotkin asiakirjat toimitetaan poikkeuksellisesti lupahakemuksen käsittelyn aikana, ne on toimitettava siten, että kaikki tarvittava tieto on saatavilla hyvissä ajoin ennen kyseistä lupaa koskevan lausunnon arvioitua antamisajankohtaa.

6.1.1 Periaatepäätöstä haettaessa toimitettavat asiakirjat

602. Ydinenergia-asetuksen (161/1988) 24 §:n mukaan periaatepäätöshakemukseen on liitettävä *kunkin ydinlaitoshankkeen osalta*
a) pääpiirteinen kuvaus suunnitellun ydinlaitoksen teknisistä toimintaperiaatteista
b) selvitys noudatettavista turvallisuusperiaatteista.

603. Periaatepäätöshakemukseen liitettävien tietojen on annettava STUKille riittävät perusteet kutakin laitoshanketta koskevan alustavan turvallisuusarvion valmisteluun. Niihin tulee sisällyttää yleisellä tasolla ainakin seuraavat tiedot:

1. yleiskuvaus laitoksen ja sen järjestelmien suunnittelussa käytettävistä turvallisuusperiaatteista ja suunnitteluperusteista
2. selvitys järjestelmäsuunnittelussa ja valmistuksessa käytettävistä keskeisistä standardisarjoista
3. yleiskuvaus ydinvoimalaitoksesta ja sen tärkeimmistä turvallisuusluokitelluista järjestelmistä (reaktori, primääripiiri, suojarakennus sekä niiden eheyttä ylläpitävät turvallisuustoimintoja toteuttavat järjestelmät tukijärjestelmineen)
4. yleiskuvaus siitä, miten seuraavat turvallisuusnäkökohdat on otettu huomioon laitoksen yleissuunnittelussa sekä keskeisten turvallisuusluokiteltujen järjestelmien suunnittelussa:
   a. syvyyssuuntaisen puolustusperiaatteen ja puolustustasojen välisen riippumattomuuden toteutuminen laitoksen yleissuunnittelussa
   b. moninkertaisuusperiaatteen, fyysisen ja toiminnallisen erottelun periaatteen sekä erilaisuusperiaatteen huomioon ottaminen laitoksen eri käyttötilanteissa turvallisuustoimintoja toteuttavissa järjestelmissä
   c. järjestelmien ja niihin liittyvien rakenteiden ja laitteiden alustava sijoittelu
   d. sisäisiltä ja ulkoisilta uhilta suojautumisen periaatteet
   e. alustavat suunnitelmat lentokonetörmäykseltä suojautumiseksi
   f. yhteenveto standardilaitosta varten tehdyistä turvallisuusanalyyseistä ja niiden tärkeimmistä tuloksista, mukaan lukien vakavien reaktorionnettomuuksien arvioidut ympäristöseuraukset
5. viitteet niihin laitoksiin, joita on käytetty suunnittelussa esikuvana, ja yhteenveto tärkeimmistä muutoksista ja niiden syistä
6. laitoksen ja sen järjestelmien suunnitteluun liittyvät tärkeimmät organisaatiot ja tiedot siitä, miten ne täyttävät tämän ohjeen koh-

dassa 3 suunnitteluorganisaatiolle asetetut vaatimukset
7. luvanhakijan oma arvio siitä, miten laitos toteuttaa olennaisimmat suunnitteluun vaikuttavat suomalaiset turvallisuusvaatimukset.

6.1.2 Rakentamislupavaiheessa toimitettavat asiakirjat

604. Ydinenergia-asetuksen (161/1988) 32 §:n mukaan *rakentamislupahakemukseen on liitettävä… 5) pääpiirteinen selvitys teknisistä toimintaperiaatteista ja ratkaisuista sekä muista järjestelyistä, joilla ydinlaitoksen turvallisuus varmistetaan 6) selvitys turvallisuusperiaatteista, jota hakija aikoo noudattaa, sekä arvio periaatteiden toteutumisesta. […]*

605. Ydinenergia-asetuksen (161/1988) 35 §:n mukaan rakentamislupaa haettaessa on lisäksi toimitettava STUKille seuraavat laitoksen ja sen järjestelmien suunnittelua koskevat asiakirjat: *1) alustava turvallisuusseloste, jonka tulee sisältää ainakin ydinlaitoksen yleiset suunnittelu- ja turvallisuusperiaatteet,…, selvitys ydinlaitoksen käytöstä, selvitys ydinlaitoksen käyttäytymisestä onnettomuustilanteissa*
2) suunnitteluvaiheen todennäköisyysperusteinen riskianalyysi
3) ehdotus luokitusasiakirjaksi, jossa esitetään ydinlaitoksen turvallisuuden kannalta tärkeiden rakenteiden, järjestelmien ja laitteiden luokittelu niiden turvallisuusmerkityksen perusteella. […]

Alustava turvallisuusseloste

606. Rakentamislupahakemukseen liitettävien tietojen on annettava STUKille riittävät perusteet turvallisuusarvion valmisteluun. Turvallisuustoiminnoista ja niitä toteuttavista järjestelmistä on esitettävä sellaiset tiedot, joiden perusteella laitoksen toiminta odotettavissa olevissa käyttöhäiriöissä ja onnettomuuksissa kaikissa käyttötilanteissa voidaan analysoida ja todennäköisyysperusteinen riskianalyysi tarkastaa. Tiedot voidaan esittää tarvittavalla tarkkuudella alustavassa turvallisuusselosteessa tai vaihtoehtoisesti voidaan esittää yhteenvetotiedot alustavassa turvallisuusselosteessa ja yksityiskohdat sitä täydentävissä erillisissä aihekohtaisissa raporteissa.

607. Laitoksen yleissuunnittelusta on esitettävä seuraavat tiedot:
1. kuvaus laitoksen ja sen järjestelmien suunnittelussa käytetyistä turvallisuusperiaatteista ja suunnitteluperusteista
2. selvitys järjestelmäsuunnittelussa ja valmistuksessa käytettävistä keskeisistä standardisarjoista
3. kuvaus ydinvoimalaitoksesta ja sen turvallisuusluokitelluista järjestelmistä; järjestelmien yleisarkkitehtuuri
4. selvitys laitoksen käyttöperiaatteista
5. kuvaus siitä, miten seuraavat seikat on otettu huomioon laitoksen yleissuunnittelussa ja turvallisuusluokiteltujen järjestelmien suunnittelussa:
   a. syvyyssuuntaisen puolustusperiaatteen ja puolustustasojen välisen riippumattomuuden toteutuminen laitoksen yleissuunnittelussa
   b. moninkertaisuusperiaatteen, fyysisen ja toiminnallisen erottelun periaatteen sekä erilaisuusperiaatteen toteutuminen laitoksen kaikissa niissä turvallisuustoimintoja toteuttavissa järjestelmissä, joita tarvitaan laitoksen eri käyttötilanteissa
   c. järjestelmien ja niihin liittyvien rakenteiden ja laitteiden sijoittelu
   d. sisäisiltä ja ulkoisilta uhilta suojautuminen
   e. suunnitelmat lentokonetörmäykseltä suojautumiseksi
   f. inhimillisten virheiden välttämiseen liittyvät periaatteet
   g. yhteenveto determinististen ja todennäköisyysperusteisten turvallisuusanalyysien tuloksista, mukaan lukien vakavien reaktorionnettomuuksien arvioidut ympäristöseuraukset
6. laitoksen ja sen järjestelmien suunnitteluun liittyvät tärkeimmät organisaatiot sekä selvitys siitä, miten ne täyttävät tämän ohjeen kohdassa 3 suunnitteluorganisaatioille asetetut vaatimukset
7. hankkeen toteutukseen osallistuvat keskeiset organisaatiot ja niiden laadunhallintasuunnitelmat

8. luvanhakijan oma arvio siitä, miten laitos ja osallistuvat organisaatiot täyttävät suomalaiset turvallisuus- ja laatuvaatimukset.

608. Alustavan turvallisuusselosteen on annettava kokonaiskuva laitostason suunnitteluperiaatteista sekä kunkin turvallisuusluokitellun järjestelmän teknisestä toteutuksesta ja liittymisestä laitoskokonaisuuteen. Rakentamislupaa haettaessa järjestelmien suunnittelun on oltava niin pitkälle kiinnitetty, että tietoja laitoksen sijoitussuunnittelusta, järjestelmien pääosien sijoittelusta tai kappaleessa 609 mainituista järjestelmistä ei ole tarvetta olennaisesti muuttaa yksityiskohtaisessa suunnittelussa ja että vaatimusmäärittelyt laitteiden ja rakenteiden hankintaa varten voidaan tehdä.

609. Turvallisuusluokkiin 1, 2 ja 3 kuuluvista järjestelmistä on esitettävä ainakin seuraavat tiedot:

1. kuvaus järjestelmästä sekä sen toiminnoista ja rajapinnoista muihin järjestelmiin; annettava vähintään liitteessä 1 esitetyt tiedot
2. järjestelmän ja siihen liittyvien laitteiden ja rakenteiden suunnitteluperusteet ja -vaatimukset:
   a. turvallisuustoiminnot ja niihin liittyvät suoritusvaatimukset osana syvyyssuuntaista puolustusta laitoksen eri käyttötilanteissa
   b. ympäristöolosuhteet ja niistä aiheutuvat suunnitteluvaatimukset
   c. järjestelmään kohdistuvat sisäiset ja ulkoiset uhat
   d. järjestelmän sekä siihen sisältyvien rakenteiden ja laitteiden turvallisuusluokitus
   e. vikakriteerit sekä fyysisen ja toiminnallisen erottelun periaatteet ja erilaisuusperiaate yhteisvikojen välttämiseksi
   f. selvitys järjestelmän sekä sen rakenteiden ja laitteiden kelpuuttamiseksi tehdyistä tai suunnitelluista analyyseistä, kokeista ja tyyppitesteistä
   g. vaatimukset kunnossapidolle, tarkastuksille ja testauksille laitoksen eri käyttötiloissa
   h. rakennemateriaaleja koskevat vaatimukset
   i. järjestelmän suunnittelussa huomioon otetut säteilyturvallisuusvaatimukset
   j. suunnittelussa käytettävät standardit ja ohjeet
3. järjestelmän toiminta ja käyttö laitoksen eri käyttötilanteissa:
   a. normaalit käyttötilanteet
   b. järjestelmän vikatilanteet
   c. laitoksen odotettavissa olevat käyttöhäiriöt ja onnettomuustilanteet
4. järjestelmän ja sen laitteiden fyysisessä erottelussa käytettävät menetelmät (osastointi, etäisyyserottelu, suojaus) sekä laitteiden alustava sijoittelu laitoksella
5. toiminnallinen erottelu: vuorovaikutus muiden järjestelmien kanssa, riippuvuudet tukijärjestelmistä sekä vikojen leviämisen estäminen
6. yhteenveto järjestelmän vikasietoisuusanalyysin tuloksista
7. selvitys siitä, miten inhimillisten virheiden välttäminen on otettu huomioon suunnittelussa
8. luvanhaltijan tekemä suunnittelijasta riippumaton turvallisuusarvio.

610. Luokkaan EYT/STUK luokitelluista järjestelmistä on esitettävä soveltuvin osin kappaleessa 609 mainitut tiedot, jos

1. järjestelmällä on laitoskohtaista riskimerkitystä sen vioittumisen aiheuttamien alkutapahtumien seurauksena
2. järjestelmä suojaa turvallisuustoimintoja toteuttavia järjestelmiä sisäisiltä tai ulkoisilta uhkilta, kuten palontorjuntajärjestelmät
3. järjestelmällä valvotaan laitoksella, työvälineissä, työntekijöissä tai ympäristössä (esim. ympäristön säteilyvalvontaverkko) esiintyvää säteilyä, pintakontaminaatiota tai radioaktiivisuutta, mutta järjestelmä ei kuulu turvallisuusluokkaan 3.
4. järjestelmä tarvitaan laitoksen saattamiseksi hallittuun tilaan suunnitteluperusteluokan DEC kuuluvan vikayhdistemän sisältävässä tapahtumassa (DEC B) tai harvinaisessa ulkoisessa tapahtumassa (DEC C)

611. Muita luokan EYT järjestelmiä on kuvattava siinä laajuudessa, kuin on tarpeen laitoksen kokonaistoiminnan arvioimiseksi.

612. Laitoksen ja sen järjestelmien kyky toteuttaa niille määritellyt turvallisuustoiminnot on osoitettava alustavassa turvallisuusselosteessa esitettävillä odotettavissa olevien käyttöhäiriöiden ja onnettomuuksien deterministisillä analyyseillä. Sisäisten ja ulkoisten uhkien analyysit sekä primääripiirin ja suojarakennuksen rakenneanalyysien keskeiset tulokset on niin ikään esitettävä alustavassa turvallisuusselosteessa.

Suunnitteluvaiheen todennäköisyysperusteinen riskianalyysi

613. Alustava todennäköisyysperusteinen riskianalyysi on tehtävä käyttäen niitä tietoja, jotka järjestelmistä esitetään alustavassa turvallisuusselosteessa. Mahdollisesti vielä puuttuvista yksityiskohdista laitosmallissa on käytettävä luotettavuusarvioita, joiden oikeellisuus varmennetaan lopullisten suunnitelmien valmistuttua. Näitä luotettavuusarvioita on käytettävä myös lähtökohtana asetettaessa puuttuvien yksityiskohtien suunnittelua ohjaavia tavoitteita. Todennäköisyysperusteista riskianalyysiä ja siihen liittyviä asiakirjoja koskevat vaatimukset on esitetty ohjeessa YVL A.7.

Ehdotus luokitusasiakirjaksi

614. Järjestelmien ja niihin sisältyvien laitteiden ja rakenteiden turvallisuusluokitus tulee esittää sekä järjestelmäkuvauksissa että kootusti erillisessä luokitusasiakirjassa. Järjestelmien turvallisuusluokitusta ja luokitusasiakirjaa koskevat vaatimukset on esitetty ohjeessa YVL B.2.

6.1.3 Käyttölupavaiheessa toimitettavat asiakirjat

615. Ydinenergia-asetuksen (161/1988) 34 §:n mukaan *käyttölupahakemukseen on liitettävä*

3. *pääpiirteinen selvitys teknisistä toimintaperiaatteista ja ratkaisuista sekä muista järjestelyistä, joilla turvallisuus on varmistettu*
4. *selvitys noudatetuista turvallisuusperiaatteista sekä arvio periaatteiden toteutumisesta.*

616. Ydinenergia-asetuksen (161/1988) 36 §:n mukaan *käyttölupaa haettaessa on lisäksi toimitettava STUKille seuraavat laitoksen ja sen järjestelmien suunnittelua koskevat asiakirjat:*
1)*lopullinen turvallisuusseloste*
2) todennäköisyysperusteinen riskianalyys
3) luokitusasiakirja, jossa esitetään ydinlaitoksen turvallisuuden kannalta tärkeiden rakenteiden, järjestelmien ja laitteiden luokittelu niiden turvallisuusmerkityksen perusteella. […]

Lopullinen turvallisuusseloste

617. Lopullisen turvallisuusselosteen on kuvattava valmiiksi rakennettu laitos sellaisena, kuin se on ennen ydinpolttoaineen latausta reaktoriin. Turvallisuusselosteen on annettava kokonaiskuva koko laitoksen sekä kunkin laitokseen sisältyvän järjestelmän suunnittelussa käytetyistä periaatteista.

618. Laitoksen yleissuunnittelusta on esitettävä seuraavat tiedot:

1. kuvaus laitoksen ja sen järjestelmien suunnittelussa käytetyistä turvallisuusperiaatteista ja suunnitteluperusteista
2. selvitys järjestelmäsuunnittelussa ja valmistuksessa noudatetuista keskeisistä standardisarjoista
3. kuvaus ydinvoimalaitoksesta ja sen turvallisuusluokitelluista järjestelmistä; järjestelmien yleisarkkitehtuuri
4. selvitys laitoksen käyttöperiaatteista
5. kuvaus siitä, miten seuraavat turvallisuusnäkökohdat on otettu huomioon laitoksen yleissuunnittelussa ja turvallisuusluokiteltujen järjestelmien suunnittelussa:
   a. syvyyssuuntaisen puolustusperiaatteen ja puolustustasojen välisen riippumattomuuden toteutuminen laitoksen yleissuunnittelussa
   b. moninkertaisuusperiaatteen, fyysisen ja toiminnallisen erottelun periaatteen sekä erilaisuusperiaatteen toteutuminen laitoksen kaikissa niissä turvallisuustoimintoja toteuttavissa järjestelmissä, joita tarvitaan laitoksen eri käyttötilanteissa
   c. järjestelmien ja niihin liittyvien rakenteiden ja laitteiden sijoittelu
   d. sisäisiltä ja ulkoisilta uhilta suojautuminen
   e. lentokonetörmäykseltä suojautuminen
   f. inhimillisten virheiden välttämiseen liittyvät periaatteet

   g. yhteenveto deterministisen ja todennäköisyysperusteisten turvallisuusanalyysien tuloksista, mukaan lukien vakavien reaktorionnettomuuksien arvioidut ympäristöseuraukset
6. laitoksen ja sen järjestelmien suunnitteluun liittyvät tärkeimmät organisaatiot sekä selvitys siitä, miten ne täyttävät tämän ohjeen kohdassa 3 suunnitteluorganisaatiolle asetetut vaatimukset
7. hankkeen toteutukseen osallistuvat keskeiset organisaatiot sekä selvitys niiden laadunhallintaohjelmista
8. luvanhakijan oma arvio siitä, miten laitos ja osallistuvat organisaatiot täyttävät suomalaiset turvallisuus- ja laatuvaatimukset.

619. Kunkin turvallisuusluokitellun järjestelmän tekninen toteutus ja liittyminen laitoskokonaisuuteen on kuvattava yksityiskohtaisesti täydentäen alustavan turvallisuusselosteen järjestelmäkuvauksia laitteiden teknisillä tiedoilla ja muulla vastaavalla tiedolla, joka on täsmentynyt rakentamisvaiheen aikana. Järjestelmiä koskevat tiedot voidaan esittää tarvittavalla tarkkuudella lopullisessa turvallisuusselosteessa tai vaihtoehtoisesti voidaan esittää yhteenvetotiedot turvallisuusselosteessa ja yksityiskohdat sitä täydentävissä erillisissä aihekohtaisissa raporteissa. Kunkin järjestelmän järjestelmäkuvaus tulee toimittaa STUKin tarkastettavaksi niin pian, kuin kyseisen järjestelmän suunnittelu on kaikilta osiltaan valmis ja yksityiskohtaiset tiedot järjestelmän rakenteiden ja laitteiden suunnitteluperusteista ovat käytettävissä. Vastaavasti järjestelmien suorituskyvyn osoittavat deterministiset analyysit odotettavissa olevista käyttöhäiriöistä ja onnettomuuksista tulee toimittaa siinä vaiheessa, kun kaikki häiriön tai onnettomuuden kulkuun vaikuttavat järjestelmät on suunniteltu. Lopullinen turvallisuusseloste on kooste näistä aiemmin toimitetuista osista, ellei STUK ole tekemänsä tarkastuksen perusteella osoittanut tarvetta muutoksille.

620. Turvallisuusluokkiin 1, 2 ja 3 kuuluvista järjestelmistä on lopullisessa turvallisuusselosteessa esitettävä, sen lisäksi mitä edellä vaatimuksessa 609 ja ohjeen liitteessä edellytetään alustavan turvallisuusselosteen sisällöstä, ainakin seuraavat tiedot:
1. tarkennettu kuvaus toteutetusta järjestelmästä; kuvausta tulee erityisesti täydentää kokoonpano- ja osaluetteloilla sekä järjestelmiin kuuluvien rakenteiden ja laitteiden suunnitteluperusteilla
2. sijoitusselvitys, jossa esitetään, miten sijoituksessa on otettu huomioon vaatimukset järjestelmien rakenteiden ja laitteiden sijoittelulle, suojaamiselle ja laitteisiin kohdistuville käytön aikaisille toimenpiteille:
   – laitteiden fyysinen erottelu (osastointi, etäisyyserottelu, suojaus)
   – painelaitteiden edellyttämät sijoitusvaatimukset
   – säteilyvalvonta- ja ilmastointivyöhykejaot
   – vuotojen keruu ja valvonta
   – laitteiden kunnossapitoon, tarkastuksiin ja testaukseen varautuminen, luoksepäästävyys käyttö- ja onnettomuustilanteissa
   – ergonomia
3. selvitys toteutuneesta toiminnallisesta erottelusta: vuorovaikutus muiden järjestelmien kanssa, riippuvuudet tukijärjestelmistä sekä vikojen leviämisen estäminen
4. järjestelmän vikasietoisuusanalyysin tulokset
5. selvitys järjestelmän sekä sen rakenteiden ja laitteiden kelpuuttamiseksi tehdyistä analyyseistä, kokeista ja tyyppitesteistä.

621. Luokkaan EYT/STUK luokitelluista järjestelmistä on esitettävä soveltuvin osin kappaleessa 620 mainitut tiedot, jos
1. järjestelmällä on laitoskohtaista riskimerkitystä sen vioittumisen aiheuttamien alkutapahtumien seurauksena
2. järjestelmä suojaa turvallisuustoimintoja toteuttavia järjestelmiä sisäisiltä tai ulkoisilta uhkilta, kuten palontorjuntajärjestelmät

3. järjestelmällä valvotaan laitoksella, työvälineissä, työntekijöissä tai ympäristössä (esimerkiksi ympäristön säteilyvalvontaverkko) esiintyvää säteilyä, pintakontaminaatiota tai radioaktiivisuutta, mutta järjestelmä ei kuulu turvallisuusluokkaan 3.
4. järjestelmä tarvitaan laitoksen saatttamiseksi hallittuun tilaan suunnitteluperusteluokan DEC kuuluvan vikayhdistemän sisältävässä tapahtumassa (DEC B) tai harvinaisessa ulkoisessa tapahtumassa (DEC C)

622. Muita luokan EYT järjestelmiä on kuvattava siinä laajuudessa, kuin on tarpeen laitoksen kokonaistoiminnan arvioimiseksi.

623. Järjestelmien kyky toteuttaa niille määritellyt turvallisuustoiminnot kaikissa käyttötilanteissa sekä syvyyssuuntaisen puolustusperiaatteen huomioon ottaminen vaatimusten mukaisella tavalla on osoitettava lopullisessa turvallisuusselosteessa esitettävillä odotettavissa olevien käyttöhäiriöiden ja onnettomuuksien deterministisillä analyyseillä. Sisäisten ja ulkoisten uhkien analyysit sekä primääripiirin ja suojarakennuksen rakenneanalyysien keskeiset tulokset on niin ikään esitettävä lopullisessa turvallisuusselosteessa.

Todennäköisyysperusteinen riskianalyysi

624. Todennäköisyysperusteinen riskianalyysi on tehtävä käyttäen niitä tietoja, jotka järjestelmistä esitetään lopullisessa turvallisuusselosteessa. Todennäköisyysperusteista riskianalyysiä ja siihen liittyviä asiakirjoja koskevat vaatimukset on esitetty ohjeessa YVL A.7.

Luokitusasiakirja

625. Järjestelmien ja niihin sisältyvien laitteiden ja rakenteiden turvallisuusluokitus tulee esittää sekä järjestelmäkuvauksissa että kootusti erillisessä luokitusasiakirjassa. Asiakirjaa on ylläpidettävä jatkuvasti ajantasaisena laitoksen rakentamisen ja käytön aikana. Järjestelmien turvallisuusluokitusta ja luokitusasiakirjaa koskevat vaatimukset on esitetty ohjeessa YVL B.2.

6.2 Järjestelmämuutokset

6.2.1 Asiakirjojen yleiset vaatimukset

626. Järjestelmäkuvaukset on päivitettävä ydinvoimalaitoksen rakentamisen ja käytön aikana tehtävien muutosten yhteydessä.

627. Ydinvoimalaitoksen käytön aikana muutettavista turvallisuusluokkiin 1, 2 ja 3 kuuluvista järjestelmistä on toimitettava STUKiin hyväksyttäväksi periaatesuunnitelmat ja järjestelmäkohtaiset ennakkotarkastusaineistot ennen laitteiden ja rakenteiden tarkemman suunnittelun aloittamista. Periaatesuunnitelman hyväksynnän jälkeen STUKille on toimitettava järjestelmän ennakkotarkastusaineisto, jonka hyväksyminen on edellytys rakenteiden ja laitteiden rakennesuunnitelmien hyväksymiselle. Muutokset lopulliseen turvallisuusselosteeseen toimitetaan hyväksytyn järjestelmän ennakkotarkastusaineiston mukaisena. Kohdassa 621 määritellyistä luokan EYT/STUK järjestelmistä on toimitettava järjestelmän ennakkotarkastusaineisto tiedoksi STUKiin.

628. Jos järjestelmään tehtävä muutos on niin vähäinen, että se ei muuta järjestelmän suunnitteluperustetta, toimintaperiaatetta tai tehtävää, muutoksesta ei tarvitse toimittaa periaatesuunnitelmaa. Järjestelmämuutoksen ennakkotarkastusaineiston laajuuteen ja yksityiskohtaisuuteen vaikuttaa muutoksen turvallisuusmerkitys.

629. Ydinvoimalaitoksen käytön aikana lopullinen turvallisuusseloste on päivitettävä säännöllisesti ottaen huomioon laitoksella tehtävät muutokset. Lopullista turvallisuusselostetta ja aihekohtaisia raportteja tulee tarvittaessa täydentää käyttöönotossa saatujen tulosten perusteella.

6.2.2 Periaatesuunnitelma

630. Järjestelmän periaatesuunnitelman sisällön on vastattava alustavan turvallisuusselosteen sisältöä. Periaatesuunnitelmaan tulee lisäksi sisältyä selvitys laadunhallinnan periaatteista, mm. suunnittelukatselmuksista sekä suunnitteluorganisaation pätevyydestä.

631. Järjestelmämuutosten yhteydessä periaatesuunnitelmassa on osoitettava todennäköisyysperusteisella riskianalyysillä, että järjestelmän muutos ei heikennä laitoksen kokonaisturvallisuutta.

6.2.3 Järjestelmän ennakkotarkastusaineisto

632. Järjestelmän ennakkotarkastusaineiston on pääsääntöisesti sisällettävä lopullista turvallisuusselosteen sisältöä vastaavat selvitykset.

7 Turvallisuussuunnittelun viranomaisvalvonta

7.1 Periaatepäätöshakemuksen käsittely

701. STUK tarkastaa periaatepäätöstä koskevaan hakemukseen liitetyt tiedot kustakin laitoshankkeesta ja pyytää tarvittaessa sellaiset lisätiedot, joita se pitää tarpeellisina alustavan turvallisuusarvion laadintaa varten. Hakemukseen liitetyistä asiakirjoista ei tehdä erikseen hyväksymispäätöksiä, mutta luvanhakijan pyynnöstä STUK voi ilmoittaa alustavan kantansa turvallisuusperiaatteiden soveltamisesta tai tietyistä teknisistä ratkaisuista.

702. STUK laatii tarkastuksen perusteella alustavan turvallisuusarvion. Laitoksen turvallisuussuunnittelusta alustavassa turvallisuusarviossa tuodaan esille

1. laitoksen suunnitteluperiaatteissa tai niiden soveltamisessa järjestelmäsuunnitteluun mahdollisesti havaitut seikat, jotka saattaisivat muodostua rakentamisluvan myöntämisen esteeksi
2. arvio tarpeista parantaa laitoksen rakennetta suomalaisten turvallisuusvaatimusten täyttämiseksi
3. suunnitteluratkaisut, joita STUK pitää tarpeellisena selvittää tai perustella tarkemmin, jos hanke etenee.

Ohjeessa YVL A.1 on esitetty periaatepäätöstä varten tarvittavia asiakirjoja koskevia lisävaatimuksia.

7.2 Rakentamislupahakemuksen käsittely

703. STUK tekee kullekin rakentamislupahakemuksen jättämisen yhteydessä STUKille toimitettavalle asiakirjalle aluksi yleisarvion, jossa todetaan toimitettujen tietojen riittävyys ja asianmukaisuus ja päätetään asiakirjan ottamisesta tarkempaan käsittelyyn. Merkittäviä täydennyksiä tai korjauksia vaativaa asiakirjaa ei käsitellä tarkemmin. Tällöin STUK keskeyttää asiakirjan käsittelyn, ilmoittaa asiasta luvanhaltijalle tai -hakijalle ja edellyttää lähettäjää täydentämään hakemusaineistoaan määräajassa.

704. Laitossuunnittelun osalta STUK tarkastaa ja arvioi laitoksen suunnitteluperusteet, vaatimusmäärittelyt, turvallisuusvaatimusten täyttymisen osoittavat analyysit, syvyyssuuntaisen puolustusperiaatteen toteutumisen suunnittelussa sekä moninkertaisuusperiaatteen, fyysisen ja toiminnallisen erottelun periaatteiden ja erilaisuusperiaatteen toteutumisen turvallisuustoimintojen suunnittelussa ja toteutuksessa.

705. STUK tarkastaa alustavassa turvallisuusselosteessa järjestelmistä esitetyt tiedot johdonmukaisina yhden tai useamman järjestelmän sisältävinä kokonaisuuksina. Mikäli järjestelmän suorituskykyä on tarpeen perustella deterministisillä häiriö- ja onnettomuusanalyyseillä, analyysit tarkastetaan yhdessä järjestelmien suunnittelutietojen kanssa.

706. Rinnan alustavan turvallisuusselosteen kanssa STUK tarkastaa todennäköisyysperusteisen riskianalyysin ja käyttää myös tämän tarkastuksen havaintoja perusteena laitoksen ja kunkin järjestelmän turvallisuutta arvioidessaan.

707. Rakentamislupaa varten toimitettua alustavaa turvallisuusselostetta ja siihen liittyvää suunnitteluaineistoa tarkastaessaan STUK varmistaa, että laitoksen ja sen järjestelmien suunnittelua voidaan käyttää rakenteiden ja laitteiden suunnitteluperusteena.

708. Sen jälkeen kun STUK on tarkastanut kaikki osat alustavasta turvallisuusselosteesta ja siihen liittyvät aihekohtaiset raportit eikä niiden suhteen ole lisäkysymyksiä tai huomautuksia, STUK tekee koko asiakirjaa koskevan hyväksymispäätöksen. Tämä päätös on edellytys STUKin myönteiselle lausunnolle rakentamislupahakemuksesta.

709. STUK tekee erillisen päätöksen suunnitteluvaiheen todennäköisyysperusteisesta riskianalyysistä todettuaan, että analyysi osoittaa laitoksen täyttävän riittävällä varmuudella STUKin asettamat kvantitatiiviset tavoitteet reaktorisydämen vakavan vaurion ja suuren radioaktiivisten aineiden päästön todennäköisyydelle. Myös tämä päätös on edellytys STUKin myönteiselle lausunnolle rakentamislupahakemuksesta.

710. Järjestelmien, rakenteiden ja laitteiden turvallisuusluokitusta koskeva asiakirja tulee olla kokonaisuudessaan STUKin hyväksymä, ennen kuin STUK antaa rakentamislupahakemusta koskevan myönteisen lausunnon.

7.3 Käyttölupahakemuksen käsittely

711. Rinnan lopullisen turvallisuusselosteen kanssa STUK tarkastaa todennäköisyysperusteisen riskianalyysin ja käyttää myös tämän tarkastuksen havaintoja perusteena laitoksen ja sen kunkin järjestelmän suunnittelua arvioidessaan.

712. Sen jälkeen kun STUK on tarkastanut kaikki osat lopullisesta turvallisuusselosteesta eikä niiden suhteen ole lisäkysymyksiä tai huomautuksia, STUK tekee koko asiakirjaa koskevan hyväksymispäätöksen. Tämä päätös on edellytys STUKin myönteiselle lausunnolle käyttölupahakemuksesta.

713. STUK hyväksyy todennäköisyysperusteisen riskianalyysin sen jälkeen, kun laitos on kaikilta osin suunniteltu valmiiksi ja riskianalyysissä käytetty laitosmalli on päivitetty vastaamaan valmiin laitoksen rakennetta. Käyttölupaa koskevan STUKin myönteisen lausunnon edellytys on, että analyysi osoittaa laitoksen täyttävän riittävällä varmuudella STUKin asettamat kvantitatiiviset tavoitteet reaktorisydämen vakavan vaurion ja suuren radioaktiivisten päästön todennäköisyydelle.

714. Turvallisuusluokituksen täydennykset hyväksytään järjestelmien suunnittelun tarkastuksen yhteydessä. Käyttölupaa koskevan STUKin myönteisen lausunnon edellytys on, että turvallisuusluokitus on ajantasainen ja että turvallisuusluokitusasiakirja on kokonaisuudessaan STUKin hyväksymä.

7.4 Järjestelmämuutokset ydinvoimalaitoksilla

715. Kun laitoksen järjestelmiin tehdään muutoksia, järjestelmiä otetaan pois käytöstä tai laitokselle asennetaan kokonaan uusia järjestelmiä, STUKin tulee tarkastaa periaatesuunnitelmat ja järjestelmän ennakkotarkastusaineistot ja hyväksyä ne ennen kyseisten muutostöiden aloittamista.

Määritelmät

Aktiivinen vikaantuminen
Aktiivisella vikaantumisella tarkoitetaan muita kuin passiivisia vikaantumistapoja (esimerkiksi virhetoimintoja).

Alkutapahtuma
Alkutapahtumalla tarkoitetaan yksilöityä tapahtumaa, joka johtaa odotettavissa oleviin käyttöhäiriöihin tai onnettomuustilanteisiin.

Erilaisuusperiaate
Erilaisuusperiaateella tarkoitetaan toimintojen varmistamista eri toimintaperiaatetta käyttävillä tai muuten keskenään erilaisilla järjestelmillä tai laitteilla, joista kukin erikseen pystyy toteuttamaan toiminnon. (VNA 717/2013)

Erotteluperiaate
Erotteluperiaateella tarkoitetaan fyysistä ja toiminnallista erottelua (VNA 717/2013).

Fyysinen erottelu
Fyysisellä erottelulla tarkoitetaan järjestelmien tai komponenttien erottamista toisistaan riittävillä esteillä, etäisyydellä tai sijoittelulla tai niiden yhdistelmillä. (VNA 717/2013)

Hallittu tila
Hallittu tilalla tarkoitetaan tilaa, jossa reaktori on sammutettu ja sen jälkilämmön poisto on turvattu. (VNA 717/2013)

Ilmanvaihto

Ilmanvaihdolla tarkoitetaan huoneilman laadun ylläpitämistä ja parantamista huoneen ilmaa vaihtamalla; joissakin ydinvoimalaitoksen tiloissa käytetään ilmastointijärjestelmiä myös radioaktiivisten aineiden leviämisen rajoittamiseen.

Ilmastointijärjestelmät

Ilmastointijärjestelmillä tarkoitetaan huoneilman puhtauden, lämpötilan, kosteuden ja ilman liikkeen hallintaan tulo tai kierrätysilmaa käsittelemällä suunniteltuja järjestelmiä.

Järjestelmä

Järjestelmällä tarkoitetaan laitteista ja rakenteista muodostuvaa kokonaisuutta, joka suorittaa määritetyn toiminnon.

Katselmointi

Katselmoinilla tarkoitetaan toimintoa, joka suoritetaan asetettujen tavoitteiden saavuttamiseksi tarvittavien toimenpiteiden sopivuuden, asianmukaisuuden ja vaikuttavuuden arvioimiseksi.

Kelpoistus

Kelpoistuksella tarkoitetaan prosessia, jonka perusteella osoitetaan kyky täyttää määritellyt vaatimukset (vastaa ISO 9000:n pätevöintiprosessia).

Kelpuutus

Kelpuutuksella tarkoitetaan objektiiviseen näyttöön perustuvaa varmistumista siitä, että tiettyä käyttöä tai soveltamista koskevat vaatimukset on täytetty.

Kriittisyys

Kriittisyydellä tarkoitetaan tilaa, jossa fissiossa syntyvien, ketjureaktiota ylläpitävien neutronien tuotto ja hävikki ovat tasapainossa niin, että ketjureaktio jatkuu tasaisena. (VNA 717/2013)

Kriittisyysonnettomuus

Kriittisyysonnettomuudella tarkoitetaan onnettomuutta, jonka aiheuttaa hallitsematon fissioiden ketjureaktio. (VNA 717/2013)

Käyttötilanne

Käyttötilanteilla tarkoitetaan normaalia käyttöä (DBC 1) ja odotettavissa olevia käyttöhäiriöitä (DBC 2).

Moninkertaisuus

Moninkertaisuudella tarkoitetaan vaihtoehtoisten (keskenään identtisten tai erilaisten) rakenteiden, järjestelmien tai järjestelmien osien käyttöä siten, että mikä tahansa niistä pystyy suorittamaan vaaditun tehtävän riippumatta siitä, missä toimintatilassa mikä tahansa toinen niistä on tai minkä tahansa toisen niistä vikaantuessa.

Normaalit omakäyttösähköjärjestelmät

Normaaleilla omakäyttösähköjärjestelmillä tarkoitetaan omakäyttösähköjärjestelmiä, joiden toimintaa ei ole varmennettu turvallisuusluokiteltujen laitosalueen sisällä olevien varatehon syöttöjärjestelmien avulla.

Odotettavissa oleva käyttöhäiriö (DBC 2)

Odotettavissa olevalla käyttöhäiriöllä (DBC 2) tarkoitetaan sellaista poikkeamaa normaaleista käyttötilanteista, jonka voidaan odottaa esiintyvän yhden tai useamman kerran sadan käyttövuoden aikana. (VNA 717/2013)

Oletettu onnettomuus

Oletetulla onnettomuudella tarkoitetaan sellaista poikkeamaa normaaleista käyttötilanteista, jonka voidaan olettaa esiintyvän harvemmin kuin kerran sadassa käyttövuodessa, pois lukien oletetun onnettomuuden laajennukset, ja josta ydinvoimalaitoksen edellytetään selviytyvän ilman vakavia polttoainevaurioita, vaikka yksittäisiä turvallisuuden kannalta tärkeiden järjestelmien laitteita olisi käyttökunnottomina huoltotöiden tai vikojen johdosta; oletetut onnettomuudet jaetaan niiden alkutapahtumataajuuden perusteella kahteen luokkaan: a) luokan 1 oletetut onnettomuudet (DBC 3), joiden voidaan olettaa esiintyvän harvemmin kuin kerran sadassa käyttövuodessa mutta vähintään kerran tuhannessa käyttövuodessa. b) luokan 2 oletetut onnettomuudet (DBC 4), joiden voidaan olettaa esiintyvän harvemmin kuin kerran tuhannessa käyttövuodessa.

Oletetun onnettomuuden laajennus (DEC)

Oletetun onnettomuuden laajennuksella (DEC) tarkoitetaan:

a. onnettomuutta, jossa odotettavissa olevaan käyttöhäiriöön tai luokan 1 oletettuun onnettomuuteen liittyy turvallisuustoiminnon toteuttamiseen tarvittavassa järjestelmässä esiintyvä yhteisvika (DEC A);
b. onnettomuutta, jonka aiheuttaa todennäköisyysperusteisen riskianalyysin perusteella merkittäväksi tunnistettu vikayhdistelmä (DEC B); tai
c. onnettomuutta, jonka aiheuttaa harvinainen ulkoinen tapahtuma, ja josta laitoksen edellytetään selviytyvän ilman vakavia polttoainevaurioita (DEC C).

Omakäyttösähköjärjestelmät

Omakäyttösähköjärjestelmällä tarkoitetaan Järjestelmiä, joiden tehtävänä on syöttää tarvittava sähköteho laitosyksikön käyttölaitteille ja automaatiojärjestelmille

Omavaraisuusehto

72 tunnin omavaraisuusehdolla tarkoitetaan, että järjestelmän, johon ehtoa sovelletaan, pitää pystyä suorittamaan tehtävänsä vähintään 72 tunnin ajan siten, että ensimmäisen 24 tunnin aikana ei tarvita minkäänlaisia materiaalitäydennyksiä (esim. järjestelmän vesi- tai polttoainesäiliön täyttöä) ja että seuraavan 48 tunnin aikana laitosalueella on valmiudet ja materiaalivarannot järjestelmää varten tarvittavien materiaalitäydennysten järjestämiseksi, vaikka kaikki laitoksen kiinteät aktiiviset järjestelmät olisivat käyttökunnottomina.

Onnettomuus

Onnettomuudella tarkoitetaan oletettuja onnettomuuksia, oletettujen onnettomuuksien laajennuksia ja vakavia onnettomuuksia. (VNA 717/2013)

Passiivinen vikaantuminen

Passiivisella vikaantumisella tarkoitetaan vikaantumistapaa, jota voidaan käsitellä suorituskyvyn puutteena (esimerkiksi laitteen tai toimintakyvyn kokonainen tai osittainen puuttuminen).

Perustason konfiguraatio

Perustason konfiguraatio: tuotteen tiettynä ajankohtana muodollisesti vahvistettu konfiguraatio, joka toimii jatkotoimenpiteiden viitekohtana (ISO 10007).

Satunnainen vikaantuminen

Satunnaisella vikaantumisella tarkoitetaan vikaantumista jonka tapahtumista ei voida ennustaa muutoin kuin tilastollisilla tai todennäköisyysmenetelmillä.

Seurausvika

Seurausvialla tarkoitetaan vikaa, joka aiheutuu jonkin toisen järjestelmän, laitteen tai rakenteen viasta tai laitoksen sisäisestä tai ulkoisesta tapahtumasta.

Sisäiset tapahtumat

Sisäisillä tapahtumilla tarkoitetaan ydinvoimalaitoksen sisällä esiintyviä tapahtumia, jotka voivat vaikuttaa haitallisesti laitoksen turvallisuuteen tai käyttöön.

Suojausautomaatio

Suojausautomaatiolla tarkoitetaan automaatiojärjestelmiä, jotka tarpeen mukaan käynnistävät turvallisuustoimintojen toteuttamiseksi tarvittavat järjestelmät ja ohjaavat näiden järjestelmien toimintaa onnettomuuden estämiseksi tai lieventämiseksi. Suojausautomaatio käsittää koko toimintoketjut laitoksen tilan seurannasta ohjattaviin toimilaitteisiin saakka.

Suunnitteluorganisaatio

Suunnitteluorganisaatiolla tarkoitetaan suunnittelutoimintaan, myös suunnittelun muutoksiin, osallistuvaa organisaatiota.

Systemaattinen vikaantuminen

Systemaattisella vikaantumisella tarkoitetaan vikaantumista, joka ei ole satunnainen vikaantuminen.

Todennäköisyysperusteinen riskianalyysi (PRA)

Todennäköisyysperusteisella riskianalyysillä (PRA) tarkoitetaan kvantitatiivista arviota ydinvoimalaitoksen turvallisuuteen vaikut-

tavista uhkista, tapahtumaketjujen todennäköisyyksistä ja haittavaikutuksista. (VNA 717/2013)

Todentaminen

Todentamisella tarkoitetaan objektiiviseen näyttöön perustuvaa varmistumista siitä, että määritellyt vaatimukset on täytetty.

Toiminnallinen erottelu

Toiminnallisella erottelulla tarkoitetaan järjestelmien erottamista toisistaan siten, että yhden järjestelmän toiminta tai vika ei vaikuta haitallisesti toiseen järjestelmään; toiminnallinen erottelu sisältää myös sähköisen erottelun ja järjestelmien välisen informaation käsittelyn erottelun. (VNA 717/2013)

Tukijärjestelmä

Tukijärjestelmällä tarkoitetaan järjestelmää, joka tarvitaan käynnistämään, ohjaamaan, jäähdyttämään tai käyttämään turvallisuustoimintoa suorittavaa järjestelmää tai muuten ylläpitämään sen toimintaedellytyksiä.

Turvallinen tila

Turvallisella tilalla tarkoitetaan tilaa, jossa reaktori on sammutettu ja paineeton ja sen jälkilämmön poisto on turvattu. (VNA 717/2013)

Turvallisuusjärjestelmä

Turvallisuusjärjestelmällä tarkoitetaan järjestelmää, joka on suunniteltu toteuttamaan turvallisuustoimintoja.

Turvallisuuslohkot

Turvallisuuslohkolla tarkoitetaan sellaisia fyysisesti toisistaan eroteltuja tiloja ja niiden sisältämiä laitteita ja rakenteita, joihin sijoitetaan kunkin turvallisuusjärjestelmän yksi moninkertaisuusperiaatetta toteuttava osa.

Turvallisuusluokiteltu järjestelmä/ rakenne/laite

Turvallisuusluokitellulla järjestelmällä, rakenteella ja laitella tarkoitetaan järjestelmää, rakennetta tai laitetta, joka on luokiteltu niiden turvallisuusmerkityksen mukaan eri turvallisuusluokkiin.

Turvallisuustoiminnot

Turvallisuustoiminnoilla tarkoitetaan turvallisuuden kannalta tärkeitä toimintoja, joiden tarkoituksena on hallita häiriötilanteita tai ehkäistä onnettomuustilanteiden syntyminen tai eteneminen tai lieventää onnettomuustilanteiden seurauksia. (VNA 717/2013)

Ulkoiset tapahtumat

Ulkoisilla tapahtumilla tarkoitetaan ydinvoimalaitoksen ympäristössä esiintyviä poikkeuksellisia tilanteita tai tapahtumia, jotka voivat vaikuttaa haitallisesti laitoksen turvallisuuteen tai käyttöön.

Vakava reaktorionnettomuus

Vakavalla reaktorionnettomuudella tarkoitetaan onnettomuutta, jossa huomattava osa reaktorissa olevasta polttoaineesta menettää alkuperäisen rakenteensa. (VNA 717/2013)

(N+1)-vikakriteeri

(N+1) vikakriteeri tarkoittaa, että turvallisuustoiminto on pystyttävä toteuttamaan, vaikka mikä tahansa toimintoa varten suunniteltu yksittäinen laite vikaantuisi.

(N+2)-vikakriteeri

(N+2)-vikakriteerillä tarkoitetaan, että turvallisuustoiminto on pystyttävä toteuttamaan, vaikka mikä tahansa toimintoa varten suunniteltu yksittäinen laite vikaantuisi ja mikä tahansa toinen rinnakkaisen järjestelmän laite tai osa – tai sen toiminnan kannalta välttämättömän tukijärjestelmän laite – olisi samanaikaisesti poissa käytöstä korjauksen tai huollon vuoksi.

Vuosiannos

Vuosiannoksella tarkoitetaan ulkoisesta säteilystä vuoden ajanjaksona saatavan efektiivisen annoksen ja samana ajanjaksona kehoon joutuvista radioaktiivisista aineista saatavan efektiivisen annoksen kertymän summaa. (VNA 717/2013)

Yhteisvika

Yhteisvialla tarkoitetaan kahden tai useamman rakenteen, järjestelmän tai laitteen vikaantumista saman yksittäisen tapahtuman tai syyn vaikutuksesta.

Yksittäisvika

Yksittäisvialla tarkoitetaan yksittäistä vikaa, jonka seurauksena järjestelmä, laite tai rakenne ei pysty toteuttamaan sille määriteltyä toimintoa.

Viitteet

1. Ydinenergialaki (990/1987).
2. Ydinenergia-asetus (161/1988).
3. Valtioneuvoston asetus (717/2013) ydinvoimalaitoksen turvallisuudesta.
4. Valtioneuvoston asetus (734/2008) ydinenergian käytön turvajärjestelyistä.
5. Valtioneuvoston asetus (716/2013) ydinvoimalaitoksen valmiusjärjestelyistä.
6. Valtioneuvoston asetus (736/2008) ydinjätteiden loppusijoituksen turvallisuudesta.
7. IAEA, Fundamental Safety Principles, Series No. SF-1, November 07, 2006.
8. IAEA, The Management System for Facilities and Activities Safety Requirements,Series No. GS-R-3, July 21, 2006.
9. IAEA, Safety Assessment for Facilities and Activities General Safety Requirements Part 4 Series, No. GSR Part 4, May 19, 2009.
10. IAEA, Safety of Nuclear Power Plants: Design, Series No. SSR-2/1, February 20, 2012.
11. IAEA, Format and Content of the Safety Analysis Report for Nuclear Power Plants Safety Guide, Series No. GS-G-4.1, April 27, 2004.
12. IAEA, Software for Computer Based Systems Important to Safety in Nuclear Power Plants Safety Guide, Series No. NS-G-1.1, November 14, 2000.
13. IAEA, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants Safety Guide, Series No. NS-G-1.3, March 29, 2002.
14. IAEA, Design of Fuel Handling and Storage Systems in Nuclear Power Plants Safety Guide, Series No. NS-G-1.4, August 08, 2003.
15. IAEA, Deterministic Safety Analysis for Nuclear Power Plants Specific Safety Guide, Series No. SSG-2, January 05, 2010.
16. IAEA, Ageing Management for Nuclear Power Plants Safety Guide, Series No. NS-G-2.12, February 06, 2009.
17. IAEA, Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants Safety Guide, Series No. NS-G-1.9, September 23, 2004.
18. IAEA, Design of Emergency Power Systems for Nuclear Power Plants Safety Guide, Series No. NS-G-1.8, September 01, 2004.
19. IAEA, Modifications to Nuclear Power Plants Safety Guide, Series No. NS-G-2.3, October 23, 2001.
20. IAEA, Periodic Safety Review of Nuclear Power Plants Safety Guide, Series No. NS-G-2.10, March 09, 2003.
21. WENRA reference requirements, Appendix E, 6.1.

Liite Järjestelmäkuvauksia koskevat yksityiskohtaiset vaatimukset

A01. Järjestelmien kuvauksiin on sisällytettävä ainakin

1. sanallinen kuvaus järjestelmästä sekä kuvausta täydentävät kuvat, kaaviot, luettelot ja taulukot
2. prosessijärjestelmät: järjestelmän pääosat ja tärkeimmät laitteet, liitynnät muihin järjestelmiin, prosessi- ja instrumenttikaaviot, pääosien 3D-kaavio/tietokonemalli, järjestelmän toiminnan vaatimat tukijärjestelmät (esim. jäähdytys, käyttövoima), järjestelmän toimintojen valvonta, ohjaus ja säätö, toimintaparametrit eri käyttötilanteissa (esim. paineet, lämpötilat, tilavuusvirtaukset, jäähdytystehot) sekä järjestelmän toimintaan liittyvät suojaustoiminnot ja -rajat
3. automaatiojärjestelmät: automaatiojärjestelmien arkkitehtuurikokonaisuus, mukaan lukien järjestelmien rajapinnat, järjestelmien väliset yhteydet ja vuorovaikutus sekä yhteydet ulkoiseen ympäristöön, automaatiojärjestelmien antamien käskyjen priorisointi, ohjelmoitavien järjestelmien laitealustat ja tiedot niiden kelpoistuksesta
4. sähköjärjestelmät: kaikkien sähköjärjestelmien muodostaman kokonaisuuden esittävä pääkaavio, kunkin järjestelmän rakenne ja toimintaparametrit (esim. jännitetasot), järjestelmien valvonta, ohjaus ja säätö, kytkimien asennot suunnitelluissa käyttötilanteissa ja automaattiset kytkentätoimet käyttöhäiriöiden sattuessa
5. rakennukset: pääpiirustukset, rakenteiden materiaalit mukaan lukien pinnoitukset ja teräs- tai vastaavat verhoilut, turvallisuustoimintoja toteuttavien laitteiden ja tärkeimpien sähköntuotantoprosessin laitteiden sijoittelu rakennuksiin, rakennusten suunnittelussa huomioon otettavat kuormitukset ja kuormitusyhdistelmät; menetelmät laitteiden kiinnittämiseksi rakenteisiin, suojarakennuksen sulut ja läpiviennit.