STUK

OHJE **YVL 2.0** / 1.7.2002

YDINVOIMALAITOKSEN JÄRJESTELMIEN SUUNNITTELU

Tämä ohje on voimassa 1.12.2002 alkaen toistaiseksi. Ohje kumoaa 14.8.1975 annetun ohjeen YVL 2.3.

Ensimmäinen painos
Helsinki 2002
Dark Oy

ISBN 951-712-586-0 (nid.)
ISBN 951-712-587-9 (pdf)
ISBN 951-712-588-7 (html)
ISSN 0783-2338

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

Säteilyturvakeskus antaa ydinenergian käytön turvallisuutta, turva- ja valmiusjärjestelyjä sekä ydinmateriaalien valvontaa koskevat yksityiskohtaiset määräykset seuraavien lakien ja määräysten nojalla:

- ydinenergialain (990/1987) 55 §:n 2 momentin 3 kohta
- ydinvoimalaitosten turvallisuutta koskevan valtioneuvoston päätöksen (395/1991) 29 §
- ydinvoimalaitosten turvajärjestelyjä koskevan valtioneuvoston päätöksen (396/1991) 13 §
- ydinvoimalaitosten valmiusjärjestelyjä koskevan valtioneuvoston päätöksen (397/1991) 11 §
- ydinvoimalaitosten voimalaitosjätteiden loppusijoituksen turvallisuutta koskevan valtioneuvoston päätöksen (398/1991) 8 §
- käytetyn ydinpolttoaineen loppusijoituksen turvallisuutta koskevan valtioneuvoston päätöksen (478/1999) 30 §.

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 valtioneuvoston päätöksen (395/1991) 27 §:ssä säädetyn periaatteen. Sen mukaan *turvallisuuden edelleen parantamiseksi on toteutettava sellaiset toimenpiteet, joita käyttökokemukset ja turvallisuustutkimukset sekä tieteen ja tekniikan kehitys huomioon ottaen voidaan pitää perusteltuina.*

Jos halutaan poiketa YVL-ohjeessa esitetyistä vaatimuksista, on Säteilyturvakeskukselle esitettävä muu hyväksyttävä menettelytapa tai ratkaisu, jolla saavutetaan YVL-ohjeessa esitetty turvallisuustaso.

1 Yleistä

Tämän ohjeen tarkoituksena on antaa ohjeita ydinvoimalaitoksen järjestelmien, erityisesti turvallisuusluokiteltujen järjestelmien, suunnittelua ja valvontaa varten. Tässä ohjeessa täsmennetään ohjeessa YVL 1.0 annettuja yleisiä suunnitteluvaatimuksia. Täsmennyksiä esitetään myös muissa YVL-ohjeissa. Järjestelmällä tarkoitetaan tiettyä toiminnallista tai rakenteellista kokonaisuutta. Järjestelmä on edelleen jaoteltavissa rakenteiksi ja laitteiksi.

Ydinvoimalaitoksen turvallisuuden varmistamiseksi keskeistä on käyttöhäiriöiden ja onnettomuustilanteiden ehkäisy (VNp 395/1991, 13 §, ennalta ehkäiseminen). Tämä tarkoittaa sitä, että laitoksen järjestelmät, rakenteet ja laitteet suunnitellaan siten, että niiden vikautumisesta tai virhetoiminnoista aiheutuvat häiriöt pysyvät mahdollisimman lievinä eivätkä ne johda onnettomuustilanteisiin. Lisäksi ydinvoimalaitos on varustettava järjestelmillä, joiden avulla häiriö- ja onnettomuustilanteet havaitaan nopeasti ja saadaan hallintaan ennen kuin ne kehittyvät vakavammiksi (VNp 395/1991, 13 §, häiriöiden ja onnettomuustilanteiden hallinta), ja järjestelmillä, joiden avulla onnettomuustilanteiden seurauksia voidaan lieventää ja rajoittaa (VNp 395/1991, 13 §, seurausten lieventäminen).

Käyttöhäiriöiden ja onnettomuustilanteiden hallinta sekä seurausten lieventäminen perustuvat turvallisuustoimintojen ylläpitoon. Ohjeen YVL 1.0 määritelmän mukaan turvallisuusjärjestelmä on järjestelmä, joka suorittaa jotakin turvallisuustoimintoa. Turvallisuustoiminto on turvallisuuden kannalta tärkeä toiminto, jonka tarkoituksena on ehkäistä häiriöiden ja onnettomuuksien syntyminen tai eteneminen tai lieventää onnettomuuksien seurauksia. Ydinvoimalaitoksen järjestelmistä myös muilla kuin turvallisuusjärjestelmillä voi olla turvallisuusmerkitystä. Toisaalta turvallisuusjärjestelmällä voi olla turvallisuustoiminnon lisäksi muita tehtäviä.

Säteilyturvakeskuksen valvontatoimenpiteiden kohdentamisessa keskeistä on järjestelmän toteuttaman toiminnon turvallisuusmerkitys. Ydinvoimalaitoksen järjestelmille, rakenteille ja laitteille tehtävä turvallisuusluokitus vaikuttaa niiden valvontaan. Ydinvoimalaitoksen turvallisuusluokitusta käsitellään ohjeessa YVL 2.1.

2 Järjestelmien suunnittelua koskevia vaatimuksia

2.1 Suunnittelumenetelmät

Järjestelmän suunnittelussa tulee käyttää sekä deterministisiä että todennäköisyyspohjaisia menetelmiä.

Deterministisillä suunnittelumenetelmillä tarkoitetaan menetelmiä, joissa luonnontieteellisen teorian ja kokemusperäisen tiedon perusteella laite tai järjestelmä suunnitellaan toimimaan siten, että se toteuttaa fysikaalisen toiminnon halutulla tavalla ja teknisesti tarkoituksenmukaisesti. Syyn ja seurauksen riippuvuus tunnetaan tarvittavalla tarkkuudella, jolloin järjestelmien ja laitteiden toiminta voidaan suunnitella ja käyttäytyminen ennustaa riittävällä tarkkuudella myös poikkeavien tilanteiden varalta.

Deterministisen menetelmän lähtökohtana ovat järjestelmien suunnitellut käyttötilanteet. Erityisesti turvallisuusjärjestelmien deterministisessä suunnittelussa otetaan ohjeen YVL 1.0 mukaisesti huomioon epätodennäköisiksikin arvioituja alkutapahtumia, joissa kyseistä turvallisuustoimintoa tarvitaan. Turvallisuusjärjestelmän toiminnalliset vaatimukset määritellään näiden alkutapahtumien seurausten ja niiden lieventämistarpeiden mukaan. Alkutapahtumien todennäköisyydet ja seurausvaikutusten vakavuus otetaan huomioon, kun määritellään deterministisiä hyväksymiskriteereitä ohjeen YVL 2.2 mukaisesti.

Todennäköisyyspohjaisilla tarkasteluilla (PSA) arvioidaan eri turvallisuustoimintojen luotettavuutta ja niiden välistä suunnittelun tasapainoa. Laitos on suunniteltava sellaiseksi, että

laskennalliset riskit jakautuvat siten, että mikään yksittäinen laite, järjestelmä, ilmiö tai muu tekijä ei dominoi riskiä ja siten, että vaikeasti hallittavien riskien osuus on mahdollisimman pieni. Tällä tavoin suunniteltu laitos on suunnittelultaan tasapainoinen.

2.2 Yleiset suunnitteluvaatimukset

Suunnittelussa valittujen ratkaisujen ja menetelmien on perustuttava käytännössä hyväksi havaittuun tekniikkaan ja luotettaviin koetuloksiin. Ratkaisuja valittaessa on hyödynnettävä tekniikan kehittyminen (VNp 395/1991, 27§). Uusien innovatiivisten ratkaisujen käyttökelpoisuus on perusteltava huolellisella, kattavalla tutkimuksella ja kokeilla ennen ratkaisujen käyttöönottoa. Perusteknologioita valittaessa suunnittelussa tulee lisäksi ottaa huomioon teknologioiden ja laitteiden elinkaari ja ennakoida niistä seuraavat mahdolliset rajoitukset. Suunnitteluratkaisuissa tulee pyrkiä mahdollisimman suureen riippumattomuuteen yksittäisestä teknologiasta ja varautua jo ennalta sekä laitteiden vaihtotarpeeseen että teknologisten murrosten mahdollisuuteen, jotta laitoksella tarvittavat muutokset voidaan suunnitella hallitusti ja hyvissä ajoin.

Suunnittelussa on tavoiteltava niin korkeaa turvallisuustasoa kuin käytännössä mahdollista (SAHARA-periaate), ks. ohje YVL 1.0, kohta 3.

Kun suunnitellaan yksittäistä järjestelmää, on erityisesti kiinnitettävä huomiota järjestelmän toiminnan tarkoituksenmukaisuuteen ja mahdollisiin haitallisiin sivuvaikutuksiin sekä muiden järjestelmien asettamiin vaatimuksiin ja järjestelmien välisiin riippuvuuksiin ja vuorovaikutuksiin. Järjestelmien ja laitteiden luotettavuutta huonontavia riippuvuuksia ja vuorovaikutuksia tulee välttää.

Järjestelmän virheellinen tai tositilanteessa tapahtuva käynnistyminen ei saa vaarantaa turvallisuustoimintoja eikä aiheuttaa uusia alkutapahtumia. Käynnistymisen mahdollisesti aiheuttamien turvallisuuden kannalta epäedullisten sivu- ja seurausvaikutusten on oltava erittäin vähäisiä.

Ydinvoimalaitoksen järjestelmät on suunniteltava siten, että turvallisuustoiminnon menetys mistä tahansa sisäisestä tai ulkoisesta syystä on erittäin epätodennäköistä. Osajärjestelmän vikautuminen ei saa aiheuttaa saman järjestelmän muiden osajärjestelmien vikautumista eikä samaan turvallisuustoimintoon osallistuvan muun järjestelmän toiminnon menetystä.

Normaalikäytössä tapahtuvat ympäristöolosuhteiden aiheuttamat ja muut ikääntymisilmiöt on otettava huomioon suunnittelussa. Turvallisuusjärjestelmän on säilyttävä käyttökunnossa niissä ympäristöolosuhteissa, joihin se joutuu alkutapahtuman seurauksena.

Suunnitteluperusteita määriteltäessä on otettava huomioon alkutapahtumat seurausvaikutuksineen, laitoksen sisäiset tapahtumat (kuten tulva ja tulipalo) ja ulkoiset ilmiöt (kuten poikkeukselliset sääolosuhteet ja maanjäristykset) sekä ihmisen aiheuttamat ulkoiset tapahtumat (kuten lentokonetörmäys, teollisuusonnettomuus). *Lisäksi on otettava huomioon laitoksen sisäisistä syistä aiheutuneissa onnettomuustilanteissa vallitsevien olosuhteiden ja luonnonilmiöiden vaikutusten mahdollisiksi arvioidut yhdistelmät* (VNp 395/1991, 20 §).

Suunnittelussa tulee ottaa huomioon laitteiden satunnaiset vikautumiset, yhteisvikojen mahdollisuudet ja ihmisen aiheuttamat virhetoiminnot sekä odotettavissa olevien käyttöhäiriöiden ja onnettomuuksien seurausvaikutukset. Järjestelmän ohjaustoimenpiteet ja niissä tarvittavat laitteet tulee suunnitella siten, että järjestelmää käytettäessä inhimillisten virheiden mahdollisuus on erittäin vähäinen.

Järjestelmä on suunniteltava käyttäen koeteltuja ja hyväksi todettuja suunnittelumenetelmiä sekä asiaankuuluvia viranomaismääräyksiä, ohjeita ja standardeja. Järjestelmälle on määriteltävä turvallisuusluokka ohjeen YVL 2.1 mukai-

sesti. Järjestelmä on suunniteltava noudattaen turvallisuusluokkaan liittyviä laatuvaatimuksia.

Käyttökuntoisuuden varmistamiseksi järjestelmä on suunniteltava siten, että sille voidaan tehdä toimintakoe mahdollisimman lähellä niitä käyttötilanteita ja parametrejä, joita varten se on suunniteltu. Järjestelmän käyttökuntoisuuden kannalta tärkeät osat on oltava tarkastettavissa.

Järjestelmän rakenteita, materiaaleja, sijoittelua ja asennuksia suunniteltaessa tulee ottaa huomioon säteilysuojelun ALARA-periaate ja varautuminen huoltoon ja tarkastuksiin.

Ydinturvallisuuden kannalta tärkeät laitososat tulee sijoittaa erilleen pelkästään laitoksen normaalia käyttöä palvelevista laitososista. Lisäksi turvallisuuden kannalta tärkeät osajärjestelmät tulee sijoittaa omiin tiloihin fyysisesti erilleen toisistaan.

Järjestelmän toiminta ja sen vaikutukset laitoksen käyttäytymiseen saattavat riippua laitoksen käyttötilasta. Tämän johdosta on tarpeellista, että järjestelmää suunniteltaessa tarkastellaan laitoksen kaikkia normaaleita käyttötilanteita, kuten tehokäyttöä, ylös- ja alasajoja sekä seisokkitiloja ja näissä yhteyksissä esiintyviä käyttöhäiriöitä ja onnettomuuksia.

2.3 Suunnitteluorganisaatiota koskevia vaatimuksia

VNp 395/1991 4 §:n mukaisesti *ydinvoimalaitosta suunniteltaessa, rakennettaessa ja käytettäessä on ylläpidettävä kehittynyttä turvallisuuskulttuuria, joka perustuu asianomaisten organisaatioiden ylimmän johdon turvallisuutta korostavaan asenteeseen ja henkilöstön motivointiin vastuuntuntoiseen työskentelyyn.* Tämä edellyttää myös suunnittelusta vastaavalta organisaatiolta hyvin järjestettyjä työolosuhteita ja avointa työilmapiiriä. Suunnittelusta vastaavan organisaation on edistettävä valppautta ja aloitteellisuutta, jotta turvallisuutta vaarantavat tekijät voidaan havaita ja poistaa.

VNp 395/1991 5 §:ssä edellytetään, että *ydinvoimalaitoksen suunnittelua, rakentamista ja käyttöä koskevissa turvallisuuteen vaikuttavissa toiminnoissa on noudatettava kehittyneitä laadunvarmistusohjelmia*. Ohjeessa YVL 1.4 esitetään vaatimuksia suunnittelun laadunhallinnalle ja suunnitteluorganisaation laatujärjestelmälle.

Ydinvoimalaitoksen suunnitteluorganisaatiolla tulee olla riittävä kokemus vastaavista tehtävistä ja tarvittava tietämys ottaa kokonaisvaltaisesti huomioon laitoksen toiminta, rakenne ja ominaisuudet.

Suunnitteluorganisaation vastuujaon on oltava selkeä. Erityisesti kun suunnitellaan laajaa kokonaisuutta, suunnittelun tulee edetä koko projektin aikana siten, että eri suunnitteluryhmien välisellä tiedonvaihdolla ja vuorovaikutteisella suunnittelulla päädytään turvallisuuden kannalta mahdollisimman hyvään lopputulokseen.

Suunnitteluprosessiin tulee sisältyä katselmuksia, jotka tulee määritellä suunnitteluorganisaation laatusuunnitelmassa.

Uuden laitoksen suunnittelun tekninen asianmukaisuus tulee osoittaa turvallisuusselosteessa. Selosteen tulee myös sisältää selvitys siitä, miten suunnitteluorganisaatio täyttää sille edellä olevissa kohdissa esitetyt vaatimukset. Luvanhakijan tulee vakuuttautua suunnittelun hyväksyttävyydestä riittävän syvälliseen omaan asiantuntemukseensa perustuvin turvallisuusarvioinnein.

Käytössä olevalla ydinvoimalaitoksella laajaa järjestelmäkokonaisuutta tai järjestelmää koskevaa muutosta varten on laadittava periaatesuunnitelma, joka sisältää alustavassa turvallisuusselosteessa esitettävät asiat, ja jossa lisäksi osoitetaan, että suunnittelu on suoritettu pätevän organisaation toimesta ja suunnittelussa tarvittava tiedonvaihto on toteutunut. Luvanhaltijan on arvioitava periaatesuunnitelman hyväksyttävyyttä katselmuksin, ennen kuin yksityiskohtainen järjestelmäsuunnittelu aloitetaan. Katselmuksia tulee jatkaa suunnitteluprosessin

aikana. Ydinturvallisuuteen merkittävästi vaikuttavien ja laajojen suunnitelmien tai erikoisosaamista vaativien suunnitelmien osalta luvanhaltijan on harkittava, teetetäänkö niille turvallisuusarviointi täysin omasta organisaatiosta riippumattomalla ulkopuolisella arvioijalla. Suunnittelukatselmuksia ja riippumattomia turvallisuusarviointeja tekevillä henkilöillä ja organisaatioilla tulee olla vähintään suunnittelutehtävän edellyttämä, käytännössä hyväksi osoitettu pätevyys. Tehtyjen arviointien jälkeen luvanhakijan tulee vakuuttautua suunnitelman hyväksyttävyydestä riittävän syvälliseen omaan asiantuntemukseensa perustuvin turvallisuusarvioinnein.

2.4 Turvallisuusjärjestelmien suunnitteluvaatimuksia

Turvallisuustoimintojen toteuttamiseen on ensisijaisesti käytettävä järjestelmiä ja laitteita, jotka eivät tarvitse ulkoista käyttövoimaa toimintonsa suorittamiseen ja ohjaamiseen (VNp 395/1991, 18 §). Esimerkkejä tällaisista järjestelmistä ovat hätäjäähdytysjärjestelmissä käytettävät, varastoidun kaasun paineella purkautuvat painevesisäiliöt ja luonnonkierrolla toimiva suojarakennuksen ulkopuolinen ilmajäähdytys.

Toissijaisesti voidaan käyttää järjestelmiä, joissa varsinainen toiminto tai sen ohjaus tai molemmat vaativat ulkoista käyttövoimaa. Esimerkkejä järjestelmistä, joiden varsinainen toiminto tapahtuu luonnonvoimaisesti ja ohjaukseen tarvitaan ulkoista käyttövoimaa, ovat luonnonkierrolla tapahtuva jälkilämmönpoisto primääripiiristä ja painovoiman avulla toimiva reaktorin pikasulkujärjestelmä. Esimerkki järjestelmistä, joissa sekä varsinainen toiminto että sen ohjaus edellyttävät ulkoista käyttövoimaa, ovat pumppuja hyväkseen käyttävät jäähdytysjärjestelmät. Kun ulkoista käyttövoimaa ohjaukseen tai toimintaan tarvitsevat järjestelmät menettävät käyttövoimansa, niiden on asetuttava turvallisuuden kannalta edulliseen tilaan silloin kun se on määriteltävissä.

Deterministisen suunnittelun tavoitteena on varmistaa, että turvallisuustoiminnot toteutuvat kaikissa suunnittelun perusteena käytetyissä tilanteissa. Näitä tilanteita voivat olla normaaliin käyttöön liittyvät tilanteet, odotettavissa olevat käyttöhäiriöt, oletetut onnettomuudet tai vakavat onnettomuudet. Turvallisuusjärjestelmällä saattaa olla yksi tai useampia tehtäviä alkutapahtumien estämisessä tai niiden etenemisen rajoittamisessa ja seurausten lieventämisessä.

Järjestelmän kyky toteuttaa turvallisuustoimintonsa on osoitettava konservatiivisten analyysien tulosten perusteella. Järjestelmän toiminta ja sitä koskevien analyysien riittävä tarkkuus on tarvittaessa osoitettava kokeellisesti. Analyysejä käsitellään ohjeessa YVL 2.2.

2.5 Vikautumisen ottaminen huomioon suunnittelussa

2.5.1 Luotettavuustekniset suunnitteluperiaatteet

Kaikkien järjestelmien, ja erityisesti turvallisuusjärjestelmien, toiminnalta edellytetään hyvää luotettavuutta. Sen vuoksi järjestelmien toiminta tulee varmistaa erilaisissa vikautumistilanteissa. Tähän päästään soveltamalla rinnakkais-, erilaisuus- ja erotteluperiaatteita (VNp 395/1991, 18 §). Vikautumisen ottamista huomioon suunnittelussa on käsitelty ohjeessa YVL 2.7. Vikautumisen ottamista huomioon ydinvoimalaitoksen primääri- ja sekundääripiirin paineenhallinnassa on käsitelty ohjeessa YVL 2.4.

2.5.2 Vikakriteerien täyttyminen

Järjestelmien suunnittelussa käytetään termejä yksittäisvikautuminen ja yhteisvikautuminen. *Yksittäisvialla* tarkoitetaan vikaa, jonka vaikutuksesta yksittäinen laite ei pysty toteuttamaan sille määriteltyä toimintoa ja vian seurausvaikutuksia. Yksittäisviaksi ei katsota vikaa, joka syntyy alkutapahtuman seurausvaikutuksena. *Yhteisvika* tarkoittaa usean samanlaisen laitteen tai rakenteen vikautumista saman yksittäisen tapahtuman tai syyn seurauksena.

Ohjeessa YVL 2.7 on esitetty turvallisuustoiminnot, joiden tulee toteutua, vaikka turvallisuus-

toimintoa toteuttavassa järjestelmässä tai sen osajärjestelmässä esiintyisi yksittäisvika. Ohjeen YVL 2.7 mukaisesti on otettava huomioon, että tärkeimpiä turvallisuustoimintoja toteuttavien järjestelmien suunnittelussa oletetaan yksittäisvian lisäksi myös minkä tahansa laitteen samanaikainen toimintakunnottomuus huollon tai korjaustyön johdosta.

Rinnakkaisperiaatteen mukaan vikautumiseen varaudutaan siten, että samaa toimintoa suorittaa useampi kuin yksi osajärjestelmä. Osajärjestelmät voivat olla keskenään samanlaisia tai erilaisia. Turvallisuustoimintoon saatetaan tarvita useampi kuin yksi osajärjestelmä. Osajärjestelmien vikautumisen huomioonottamisessa noudatetaan ohjeessa YVL 2.7 esitettyjä vaatimuksia.

Lisäämällä samanlaisten rinnakkaisten osajärjestelmien lukumäärää voidaan parantaa järjestelmän kokonaisluotettavuutta, jota kuitenkin rajoittavat mahdolliset yhteisviat. Yhteisvian aiheuttajana voi olla laitteen suunnittelussa, valmistuksessa, käytössä tai kunnossapidossa tapahtunut virhe, jokin ulkoinen tapahtuma tai muu syy, joka vaikuttaa useampaan osajärjestelmään samanaikaisesti.

Jotta yhteisvikojen vaikutuksia voidaan ehkäistä ja lisätä näin järjestelmän luotettavuutta, on turvallisuustoimintojen varmistamisessa käytettävä mahdollisuuksien mukaan eri toimintaperiaatteisiin perustuvia järjestelmiä, osajärjestelmiä tai laitteita (erilaisuusperiaate, VNp 395/1991, 18 §). Esimerkkejä toimintaperiaatteen eroista ovat sähköllä tai pneumatiikalla toimiva ohjausventtiili ja passiivisesti toimiva tai pumpuilla varustettu hätäjäähdytysjärjestelmä. Erilaisuusperiaatetta sovellettaessa tulee kuitenkin huolehtia siitä, että järjestelmän monimutkaisuuden lisääntyminen ei mitätöi erilaisuusperiaatteella saatavaa luotettavuuden lisäystä. Ohjeessa YVL 2.7 on lueteltu ne tärkeimmät turvallisuustoiminnot, joiden varmistamisessa ainakin on käytettävä erilaisuusperiaatetta, ja esitetty miten yksittäisvikautuminen on otettava huomioon erilaisuusperiaatetta sovellettaessa.

2.5.3 Turvallisuudelle tärkeiden järjestelmien erottelu

Pelkästään turvallisuustoimintoa suorittavat järjestelmät on erotettava rakenteellisesti normaalia käyttöä palvelevista laitososista. Samaa turvallisuustoimintoa suorittavat järjestelmät ja osajärjestelmät, olivatpa ne samanlaisia tai erilaisia, on erotettava myös toisistaan. Näillä erotteluilla varmistetaan, että ulkoisista vaikutuksista aiheutuvien yhteisvikojen mahdollisuus on hyvin pieni (erotteluperiaate). Tällaisia ulkoisia vaikutuksia ovat mm. tulvat, tulipalot, missiilit, lentokonetörmäys ja harvinaiset luonnonilmiöt.

Erillisiä osajärjestelmiä voidaan kuitenkin suunnitella siten, että ne voidaan kytkeä poikkeuksellisissa tilanteissa käyttötoimenpitein ristiin. Tämä edellyttää, että ristiinkytkentä parantaa eikä huononna järjestelmäkokonaisuuden luotettavuutta ja että tarkoitukseton ristiinkytkentä on luotettavalla tavalla estetty.

Tulipalojen varalta tehtävälle tilasuunnittelulle ja erottelulle esitetään yksityiskohtaiset suunnitteluvaatimukset ohjeessa YVL 4.3.

Sähkö- ja automaatiojärjestelmien erottelusta esitetään suunnitteluvaatimuksia ohjeissa YVL 5.2 ja YVL 5.5.

2.6 Todennäköisyyspohjainen suunnittelu

Luotettavuusteknisillä menetelmillä on osoitettava, että laitos on suunnittelultaan luotettavuusmielessä tasapainoinen luvussa 2.1 esitetyllä tavalla. Erityisesti on osoitettava, että suunnittelussa on saavutettu oikea tasapaino

- eri turvallisuustoimintojen
- samaa toimintoa suorittavien eri järjestelmien
- pääjärjestelmien ja tukijärjestelmien
- saman järjestelmän osajärjestelmien välillä.

Myös eri alkutapahtumista johtuvien erilaisten riskien (mitattuna sekä sydänvaurion ja/tai ympäristöpäästön taajuudella että vakavuudella)

on jakauduttava alkutapahtumien kesken niin, etteivät mitkään tapahtumaketjut, järjestelmät, osajärjestelmät, rakenteet tai laitteet yksinään aiheuta suhteettoman suurta osuutta kokonaisriskistä.

Ohjeessa YVL 2.8 esitetään todennäköisyyspohjaiset suunnittelutavoitteet ja numeeriset turvallisuustavoitteet.

Luotettavuusteknisiä menetelmiä voidaan käyttää myös eri suunnitteluvaihtoehtojen vertailuun. Esimerkkeinä tästä ovat rinnakkaisten osajärjestelmien lukumäärän ja osajärjestelmäkohtaisen suorituskyvyn optimointi turvallisuuden ja käytettävyyden kannalta sekä osajärjestelmien ristiinkytkentämahdollisuuksien suunnitteleminen siten, että järjestelmäkokonaisuuden toiminnan luotettavuus paranee.

2.7 Muita suunnittelussa huomioon otettavia asioita

Kun järjestelmä liittyy toiseen järjestelmään, on järjestelmien rajapinnat määriteltävä ja järjestelmien väliset liittymät suunniteltava siten, että järjestelmien välinen yhteys ei vaaranna turvallisuustoimintoa suorittavan järjestelmän toimintaa. Lisäksi turvallisuusjärjestelmän ja sen tarvitsemien tukijärjestelmien rajapinnat on mikäli mahdollista suunniteltava siten, että rajapinnan vikautuminen ei vaaranna järjestelmän omaa tai mitään muutakaan turvallisuustoimintoa, ja siten että viat eivät etene rajapinnan yli.

Turvallisuustoiminnon luotettavuus riippuu varsinaisten toimintoa suorittavien järjestelmien lisäksi myös tarvittavien tukijärjestelmien luotettavuudesta. Turvallisuustoimintoon osallistuvien pääjärjestelmien ja niitä palvelevien tukijärjestelmien luotettavuuden on oltava keskenään tasapainossa. Kun analysoidaan apu- ja tukijärjestelmien luotettavuustasoa, voidaan ottaa huomioon mahdollisuudet korjata järjestelmää turvallisuustoiminnon tarvetilanteen aikana edellyttäen, että suunnittelussa on varauduttu korjauksiin (ympäristöolosuhteet, esim. lämpötila, kosteus, säteily).

3 STUKiin toimitettavat asiakirjat

3.1 Suunnitteluvaiheet ja niihin liittyvät asiakirjat

Uutta ydinvoimalaitosta suunniteltaessa tulee toimittaa järjestelmistä tietoa seuraavasti:

- Järjestelmän tai järjestelmäkokonaisuuden suunnitteluperusteet, tekniset perusratkaisut ja sijoittelu laitoksella esitetään alustavassa turvallisuusselosteessa. Alustavan turvallisuusselosteen perusteella on voitava muodostaa kokonaiskuva kunkin turvallisuuteen vaikuttavan järjestelmän teknisistä perusperiaatteista, toteutusratkaisusta ja liittymisestä laitoskokonaisuuteen. Kaikista turvallisuustoiminnoista ja laitoksen pääprosesseista esitetään tiedot siinä laajuudessa, että laitoksen toiminta häiriö- ja onnettomuustilanteissa voidaan arvioida.

- Alustavassa turvallisuusselosteessa tulee myös osoittaa, että suunnittelu on organisoitu kohdan 2.3 mukaisesti.

- Lopullisessa turvallisuusselosteessa esitetään yksityiskohtaisesti järjestelmäkohtaiset tekniset ratkaisut, jotka sisältävät mm. järjestelmien suunnitellut toiminta-arvot, tarvittavat mittaukset ja ohjaukset, järjestelmän analyysit, jne. Lopullisen turvallisuusselosteen ja siihen liittyvien aihekohtaisten raporttien sisällön perusteella tulee voida arvioida, ovatko järjestelmäkokonaisuuden toteutus ja järjestelmän toiminta hyväksyttäviä.

- Järjestelmään kuuluvien laitteiden laitekohtaisissa tarkastusaineistoissa esitetään valittujen laitteiden yksityiskohtaiset tekniset määrittelyt. Niiden perusteella tulee voida arvioida laitteiden hyväksyttävyys suunniteltuihin tehtäviinsä.

3.2 Alustava turvallisuusseloste

Turvallisuusluokkien 1, 2 ja 3 sekä tarvittavilta osin turvallisuusluokan 4 järjestelmien alusta-

van turvallisuusselosteen tulee sisältää seuraavat selvitykset:

- järjestelmän suunnitteluperiaatteet ja -perusteet
- järjestelmän toiminnot, toimintaperiaatteet ja tärkeimmät suunnitteluarvot
- kuvaus järjestelmän merkityksestä varsinaisen turvallisuustoiminnon toteuttamisessa, jos järjestelmä on turvallisuustoimintoa suorittavan järjestelmän tukijärjestelmä
- järjestelmän sekä sen laitteiden erotteluperiaatteet (osastointi, suojaus) ja alustava sijoittelu laitoksella ohjeen YVL 4.3 kohdan 3.3 mukaisesti
- muista järjestelmistä, mukaan lukien apu- ja tukijärjestelmät, aiheutuvat vaatimukset ja riippuvuudet
- luotettavuustavoite sille turvallisuustoiminnolle, jonka toteuttamiseen järjestelmä osallistuu
- selvitys järjestelmän toiminnan osoittamiseksi tehdyistä tai tehtävistä analyyseistä ja kokeista
- suunnittelijan laatima alustava turvallisuusarvio
- luvanhaltijan kohdan 2.3 mukainen oma turvallisuusarviointi.

Luokan EYT järjestelmiä tulee kuvata siinä laajuudessa kuin on tarpeen laitoksen kokonaistoiminnan arvioimiseksi.

Järjestelmän suunnitteluperusteissa tulee esittää, mitä ohjeita ja standardeja käytetään hyväksi järjestelmän suunnittelussa. Samoin tulee esittää järjestelmän ja sen laitteiden alustava turvallisuusluokitus sekä järjestelmän ympäristöolosuhteet ja niistä aiheutuvat suunnitteluvaatimukset.

Ohjeessa YVL 5.5 annetaan ohjeita automaatiojärjestelmien analyyseistä, kokeista, tyyppitesteistä ja kelpoistussuunnitelman laatimisesta. Ohjeessa YVL 7.11 annetaan ohjeita ydinvoimalaitoksen säteilymittausjärjestelmien suunnittelusta ja kelpoistamisesta. Ohjeessa YVL 4.3 annetaan vaatimuksia ydinvoimalaitosten palontorjuntajärjestelyistä.

Alustavassa turvallisuusarviossa tulee esittää, kuinka järjestelmä täyttää sitä koskevat turvallisuusvaatimukset.

3.3 Lopullinen turvallisuusseloste

Järjestelmien lopullisen turvallisuusselosteen turvallisuusluokissa 1, 2 ja 3 ja tarvittavin osin turvallisuusluokassa 4 tulee sisältää seuraavat selvitykset:

- järjestelmän yksityiskohtaiset suunnitteluperusteet
- järjestelmän yksityiskohtainen toimintakuvaus
- sijoitusselvitys, jossa esitetään, miten sijoituksessa on otettu huomioon erityisvaatimukset järjestelmien rakenteiden ja laitteiden sijoittelulle (laitteiden fyysinen erottelu, painelaitteiden edellyttämät sijoitusvaatimukset, säteilyvalvonta- ja ilmastointivyöhykejaot, vuotojen keruu ja valvonta, laitteiden huoltoon ja tarkastukseen varautuminen, luoksepääsy käyttö- ja onnettomuustilanteissa, ergonomia, ALARA-periaate)
- vaikutukset ydinlaitoksen muihin järjestelmiin ja riippuvuudet apu- ja tukijärjestelmistä sekä vikojen leviämisen estäminen
- todennäköisyyspohjainen tarkastelu järjestelmän merkityksestä laitoksen turvallisuuteen tärkeysmittojen avulla (ks. ohje YVL 2.8)
- selvitys analyyseistä, kokeista ja tyyppitesteistä, joilla osoitetaan järjestelmän soveltuvuus aiottuun käyttötarkoitukseen, ja näiden kelpoistuksien tulokset
- suunnittelijan turvallisuusarvio siitä, miten järjestelmä täyttää sille asetetut turvallisuusvaatimukset
- luvanhaltijan kohdan 2.3 mukainen oma turvallisuusarviointi
- järjestelmää koskevat turvallisuusteknisten käyttöehtojen vaatimukset
- muut tarvittavat selvitykset.

Suunnitteluperusteista tulee esittää pääsääntöisesti seuraavat asiat:

- järjestelmän tarkoitus, siihen liittyvät turvallisuustoiminnot sekä järjestelmälle asetettavat turvallisuutta koskevat suunnittelutavoitteet

- järjestelmän suunnitteluperusteille YVL-ohjeissa, standardeissa, normeissa jne. esitetyt vaatimukset, mm. vikakriteeri, erilaisuusperiaatteen toteutuminen ja fyysistä erottelua koskevat vaatimukset
- järjestelmän ympäristöolosuhteet ja niistä aiheutuvat suunnitteluvaatimukset
- selvitys siitä, miten järjestelmän ulkopuoliset onnettomuudet ja muut sen toimintakykyä haittaavat tekijät on otettu huomioon suunnittelussa (tulvat, tulipalot, maanjäristykset, rankat sääolosuhteet, luonnonilmiöiden vaikutukset, missiilit, räjähdykset ja muut ulkoiset uhat)
- järjestelmän ja sen laitteiden turvallisuusluokitus
- järjestelmän luotettavuustavoite ja sen merkitys turvallisuustoiminnon luotettavuuden ja sydänvauriotaajuuden kannalta
- järjestelmän suunnitelluissa käyttötilanteissa esiintyvät, järjestelmän mitoitusperusteena käytettävät parametrit (esim. paine, tilavuusvirtaus, lämpötila, jäähdytysteho, virtaavan aineen koostumus ja säteilytaso) ja näiden perusteella järjestelmän laitteille asetetut toiminta-arvo- ja rakennemateriaalivaatimukset
- järjestelmän toiminnalliseen suunnitteluun liittyvät laskelmat ja perustelut tai viitteet erillisiin selvityksiin, aihekohtaisiin raportteihin, analyyseihin ja muihin asiakirjoihin, joissa nämä asiat esitetään.

Luokan EYT järjestelmiä tulee kuvata siinä laajuudessa kuin on tarpeen laitoksen kokonaistoiminnan arvioimiseksi.

Järjestelmän toimintakuvauksessa on esitettävä järjestelmän toiminta niissä tilanteissa, joita laitoksen suunnittelussa on tarkasteltu kohdan 2.2 mukaisesti. Toimintakuvauksella on osoitettava järjestelmän toiminnan tarkoituksenmukaisuus ja mahdollisten haitallisten sivuvaikutusten vähäisyys.

Toimintakuvaukseen on liitettävä pääsääntöisesti seuraavat selvitykset:

- järjestelmän prosessi- ja instrumentointikaavio (PI-kaavio), josta käyvät ilmi järjestelmän rajat ja yhteydet muihin järjestelmiin sekä toiminnassa keskeiset prosessitekniset parametrit
- ohjausta, säätöä ja instrumentointia koskeva selvitys
- selvitys periaatteista, joiden mukaan järjestelmän toimienergia varmennetaan
- järjestelmän laite- ja mittapisteluettelot.

Järjestelmän toimintakuvauksen tai siihen liittyvien aihekohtaisten raporttien tulee olla niin yksityiskohtaisia, että niiden sisältämillä tiedoilla voidaan analysoida järjestelmää.

Järjestelmän analysoinnilla osoitetaan sitä koskevien suunnitteluperusteiden ja -vaatimusten täyttäminen. Keskeisiä turvallisuusselosteessa tai aihekohtaisissa raporteissa esitettäviä analyysejä ovat mm. järjestelmän fysikaalista toimintaa käsittelevät analyysit, yksittäisvika-analyysi, vika- ja vaikutusanalyysi ja tärkeysmitat. Eri analyysityyppien keskinäinen tärkeysjärjestys vaihtelee tekniikan aloittain.

Automaatiojärjestelmän suunnittelussa noudatettavaa laadunhallintaa, analysointia, kokeita ja tyyppitestejä koskevia vaatimuksia annetaan ohjeessa YVL 5.5.

Järjestelmäkohtaisessa turvallisuusarviossa osoitetaan, että YVL-ohjeiden ja muiden suunnitteluperusteiden vaatimukset on täytetty ja esitetään järjestelmän suunnittelun yhteydessä tehdyt luotettavuustekniset tarkastelut.

Järjestelmää koskevista käytönaikaisista määräaikaistarkastuksista ja -testauksista tulee toimittaa erillinen aineisto.

3.4 Käytössä olevan ydinvoimalaitoksen järjestelmien muutokset

3.4.1 Asiakirjojen yleiset vaatimukset

Ydinvoimalaitoksen käytön aikana muutettavan järjestelmän tai lisättävän järjestelmän ennakkotarkastus tehdään erillisen muutostyötä koskevan periaatesuunnitelman ja ennakkotarkastusaineiston pohjalta. Yleisperiaatteena on, että turvallisuusluokkiin 1, 2 ja 3 kuuluvista järjestelmistä sekä sellaisista järjestelmistä, jotka

STUK vaatii tarkastettavaksi yksityiskohtaisemmissa YVL -ohjeissa tai erillisellä päätöksellä, on toimitettava STUKiin hyväksyttäväksi periaatesuunnitelmat ja järjestelmäkohtaiset ennakkotarkastusaineistot. Turvallisuusluokan 4 järjestelmistä on toimitettava järjestelmän ennakkotarkastusaineisto tiedoksi STUKiin.

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

Lopulliseen turvallisuusselosteeseen on muutostyön yhteydessä tehtävä viipymättä asianmukaiset muutokset. Asiakirjojen muutoksia koskevia vaatimuksia esitetään ohjeessa YVL 1.1. Muutostöitä käsitellään myös ohjeessa YVL 1.8.

3.4.2 Periaatesuunnitelma

Järjestelmän periaatesuunnitelman sisällön tulee vastata pääsääntöisesti alustavan turvallisuusselosteen sisältöä. Sen lisäksi periaatesuunnitelmaan on sisällytettävä seuraavat selvitykset:

- selvitys laadunhallinnan periaatteista, mm. suunnittelukatselmuksista sekä suunnitteluorganisaation pätevyydestä
- selvitys ulkopuolisista riippumattomista turvallisuustarkastuksista, jos sellaisia on tehty (nämä eivät korvaa luvanhaltijan omaa turvallisuusarviota).

Järjestelmämuutosten yhteydessä on periaatesuunnitelmassa tarkasteltava myös sitä, miten järjestelmän muutos vaikuttaa koko laitoksen riskiarvioon.

3.4.3 Järjestelmän ennakkotarkastusaineisto

Järjestelmän ennakkotarkastusaineiston tulee pääsääntöisesti sisältää lopullista turvallisuusselosteen sisältöä vastaavat selvitykset. Sen lisäksi järjestelmän ennakkotarkastusaineiston tulee sisältää

- laatusuunnitelma, jossa esitetään järjestelmän suunnittelua ja toteutusta koskevat laadunhallinnan keinot
- selvitys tehdyistä riippumattomista turvallisuustarkastuksista ja niiden tuloksista, mikäli sellaisia on tarvittu järjestelmän hyväksyttävyyden osoittamiseksi.

Järjestelmän koekäytöstä tulee toimittaa STUKiin hyväksyttäväksi koekäyttöohjelma ohjeen YVL 2.5 mukaisesti.

4 Viitteet

1. IAEA, SS Nro 110, The Safety of Nuclear Installations, 1993.
2. IAEA, 50-C-D, Safety of Nuclear Power Plants: Design, 2000.
3. IAEA, 50-SG-Q10, Quality Assurance in Design, 1996
4. INSAG-10, Defence in Depth in Nuclear Safety, 1996.
5. INSAG-12, Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 rev.1, 1999.
6. IAEA, DS309, The Format and Content of Safety Analysis Reports for Nuclear Power Plants, DRAFT Safety Guide-Version 3.