STUK

OHJE **YVL 5.5** / 13.9.2002

YDINLAITOSTEN AUTOMAATIOJÄRJESTELMÄT JA -LAITTEET

jatkuu

Tämä ohje on voimassa 1.3.2003 alkaen toistaiseksi. Ohje kumoaa 7.6.1985 annetun ohjeen YVL 5.5.

Kolmas, uudistettu painos
Helsinki 2002
Dark Oy

ISBN 951-712-591-7 (nid.)
ISBN 951-712-592-5 (pdf)
ISBN 951-712-593-3 (html)
ISSN 0783-2397

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

Ydinlaitoksen automaatiojärjestelmien avulla valvotaan, ohjataan ja suojataan laitoksen reaktorin ja järjestelmien toimintaa. Valvontajärjestelmien tehtävänä on tuottaa luotettavaa tietoa ohjaajille ydinreaktorin, laitoksen järjestelmien ja niiden ympäristön tilasta. Automaatiojärjestelmät toimivat joko automaattisesti tai ohjaajien käsin käynnistäminä laitoksen käytön tai turvallisuuden sitä edellyttäessä. Erityisesti suojausautomaation tehtävänä on havaita ydinreaktorin ja järjestelmien epänormaalit toimintatilat ja muodostaa automaattisesti signaalit kyseisessä tilanteessa tarvittavien turvallisuustoimintojen (reaktorin pysäyttäminen, suojarakennuksen toiminta, jälkilämmönpoisto reaktorista jne.) käynnistämiseksi ja ylläpitämiseksi.

Yleiset määräykset ydinvoimalaitosten turvallisuudesta on esitetty valtioneuvoston päätöksessä (395/1991). Tämä päätös sisältää sekä yleisiä määräyksiä kaikista turvallisuusjärjestelmistä että määräyksiä automaatiojärjestelmistä. Nämä määräykset koskevat käyttöhäiriöiden ja onnettomuuksien havaitsemista ja hallintaa (13 §), turvallisuustoimintojen varmistamista (18 §), inhimillisten virheiden välttämistä (19 §), turvallisuusluokitusta (21 §) ja ydinvoimalaitosten valvontaa ja ohjausta (22 §). Ohjeessa YVL 1.0 esitetään yleisiä määräyksiä täsmentäviä vaatimuksia mm. suojausautomaatiosta, tarvittavasta automaatioasteesta ja käsiohjausmahdollisuuksista.

Useat muut YVL-ohjeet koskevat myös automaatiojärjestelmiä ja -laitteita. Ohje YVL 2.0 koskee yleisesti ydinvoimalaitosten järjestelmien suunnittelua ja valvontaa. Ohjeessa YVL 2.7 esitetään vikakriteerejä koskevat vaatimukset. Ohje YVL 2.1 esittää vaatimukset automaatiojärjestelmien turvallisuusluokituksesta, ja ohjeissa YVL 2.2 ja YVL 2.8 esitetään vaatimuksia turvallisuuden tavoitteista ja osoittamisesta. Ohjeessa YVL 1.8 esitetään, miten STUK valvoo ja tarkastaa ydinlaitosten järjestelmien, laitteiden ja rakenteiden muutos-, korjaus- ja kunnossapitotöitä sekä esitetään luvanhaltijan näihin töihin liittyviä velvoitteita. Laitoksella tehtävistä käyttöönottokokeista vaatimukset on esitetty ohjeessa YVL 2.5. Ohjeessa YVL 1.1 selvitetään, kuinka STUK valvoo kokonaisuutena ydinlaitoksen suunnittelua, rakentamista ja käyttöä.

VNp:n (395/1991) 5 §:n mukaisesti *ydinvoimalaitoksen suunnittelua, rakentamista ja käyttöä koskevissa turvallisuuteen vaikuttavissa toiminnoissa on noudatettava kehittyneitä laadunvarmistusohjelmia.* Ohjeessa YVL 1.4 esitetään yleiset periaatteet laadunhallinnasta ja ohjeessa YVL 1.9 vaatimukset käytönaikaisesta laadunhallinnasta. Nykyaikaisen automaatioteknologian luotettavuuden varmistaminen edellyttää, että laadunhallinnassa otetaan huomioon erityisesti käytettävän teknologian erityispiirteet.

Tässä ohjeessa esitetään ydinlaitosten automaatiojärjestelmien ja -laitteiden suunnittelua, toteutusta ja käyttöä koskevat luvanhaltijan velvoitteet sekä Säteilyturvakeskuksen valvontaan ja tarkastukseen liittyvät menettelyt.

2 Automaatiojärjestelmien ja -laitteiden suunnitteluperusteet

2.1 Suojausautomaation toimintojen varmistaminen

Suojausautomaation tehtävänä on havaita automaattisesti ydinreaktorin ja järjestelmien epänormaalit toimintatilat ja muodostaa signaalit kyseisessä tilanteessa tarvittavien turvallisuustoimintojen käynnistämiseksi ja ylläpitämiseksi. Tärkeimpiä turvallisuustoimintoja ovat reaktorin pysäyttäminen, jälkilämmön poisto reaktorista lopulliseen lämpönieluun ja suojarakennuksen toiminta. Suojausautomaatio ulottuu mittauksesta toimilaitteelle. Suojausautomaatiota koskevia vaatimuksia sovelletaan kaikkeen turvallisuusluokkaan 2 kuuluvaan automaatioon.

Ohjeen YVL 1.0 kohdassa 3.4 edellytetään, että *suojausjärjestelmä on suunniteltava siten, että järjestelmä joutuu sen vikautumisen seurauksena laitoksen turvallisuuden kannalta edulliseen*

tilaan. Erilaiset vikatilanteet ja niiden seuraukset tulee analysoida sekä turvallisuuden kannalta edullinen tila tulee perustella.

Ohjeen YVL 1.0 kohdan 3.4 mukaisesti *turvallisuustoiminnot käynnistävän suojausjärjestelmän on toimittava odotettavissa olevissa käyttöhäiriöissä ja oletetuissa onnettomuuksissa myös yksittäisvikautumisen sattuessa, vaikka mikä tahansa turvallisuustoimintoon vaikuttava laite olisi samanaikaisesti pois käytöstä korjauksen tai huollon vuoksi. Reaktorisuojausjärjestelmän suunnittelussa tulee noudattaa lisäksi erilaisuusperiaatetta.*

Ohjeen YVL 2.7 luvun 4 mukaisesti *reaktorin suojausjärjestelmässä tulee mitata vähintään kahta eri prosessisuuretta, jotka ovat molemmat fysikaalisesti häiriötilanteesta tai onnettomuudesta riippuvia ja joiden laukaisurajat voidaan valita siten, että ne saavutetaan riittävän aikaisin. Mikäli tämä ei ole kaikissa suojaustoiminnoissa mahdollista, tulee käyttää eri mittausperiaatteita ko. prosessisuureiden mittaamisessa.*

Ohjeen YVL 1.0 luvun 3.4 mukaisesti *suojausjärjestelmä tulee ensisijaisesti erottaa säätö- ja muista automaatiojärjestelmistä. Mahdollisen suojaus- ja säätö- tai muiden automaatiojärjestelmien keskinäinen riippuvuus ei saa heikentää turvallisuutta.*

Valvomossa tulee olla ohjaajien käytettävissä tieto suojausautomaation tilasta.

Suojausautomaation toiminnot tulee voida testata myös laitoksen käynnin aikana. Näillä testeillä tulee varmistaa, että suunnitteluperusteena olevat toiminnalliset vaatimukset täyttyvät.

Suojausautomaation määräaikaiskokeiden tulee kattaa koko ketju mittauksesta toimilaitteisiin. Määräaikaiskokeiden ajaksi osajärjestelmä tulee saattaa laitoksen turvallisuuden kannalta edulliseen tilaan. Lisäksi kokeiden mahdollisuus tulee ottaa huomioon järjestelmän suunnittelussa.

Suojausautomaatio tulee suunnitella siten, että se valvoo tulo- ja lähtöviestiensä kelvollisuutta ja sisäistä toimintaansa sekä hälyttää tarvittaessa. Suojausautomaatiossa käytettävän itsediagnostiikan tulee olla riittävän kattava ja hyvin testattu. Itsediagnostiikan kattavuutta analysoitaessa tulee tarkastella erikseen laite- ja ohjelmistovikoja.

Suojausautomaation samaa turvallisuustoimintoa suorittavat osajärjestelmät tulee ohjeen YVL 2.0 mukaisesti erottaa fyysisesti toisistaan, ja näiden rinnakkaisten osajärjestelmien tulee olla myös toiminnallisesti erotettu. Suojausautomaatio tulee erottaa muista järjestelmistä käyttäen toiminnallista ja riittävää fyysistä erottelua.

Ohjeen YVL 1.0 luvussa 3.4 todetaan edelleen, että *turvallisuustoimintojen käsikäynnistys tulee toteuttaa mahdollisimman luotettavaa tekniikkaa käyttäen. Yksittäisten laitteiden käsikäynnistyksen lisäksi tulee suojaussignaali tarvittaessa voida laukaista käsin.*

Suojausautomaation tulee valvoa laitoksen toimintasuureita sekä näyttää laitoksen ohjaajille suojaussignaalien käsin laukaisussa tarvittavat toimintasuureet.

Ohjaajien erilaisissa tarvetilanteissa mahdollisesti tekemien suojaussignaalien käsikäynnistysten vaikutukset tulee analysoida. Käsin laukaisun riippuvuus automaattisista toiminnoista tulee minimoida. Lisäksi suojaussignaalin käsin laukaisun tulee olla toiminnallisesti riippumaton valvomon muista järjestelmistä.

Ohjeessa YVL 2.8 esitetään ydinvoimalaitoksen todennäköisyyspohjaisia suunnittelutavoitteita ja numeerisia turvallisuustavoitteita.

2.2 Valvonta, ohjaus ja säätö

Ohjeen YVL 1.0 luku 3.6 edellyttää, että *toimintasuureiden ja järjestelmien pitämiseksi määrättyjen toiminta-arvojen rajoissa on laitoksella oltava luotettavat ohjaus- ja säätöjärjestelmät. Näiden tulee yhdessä ohjaamiensa järjestelmien ja laitteiden kanssa huolehtia siitä, että käyttötilanteissa tai ohjaus- ja säätöjärjestelmien yksittäisen vian sattuessa ei synny tarvetta käynnis-*

tää oletettujen onnettomuuksien varalle suunniteltuja turvallisuusjärjestelmiä.

Ydinvoimalaitoksella tulee olla riittävä automaatio reaktorin ja prosessijärjestelmien valvontaa, ohjausta ja säätöä varten. Tämän ns. käyttöautomaation tehtävänä on pitää prosessin parametrit käyttötilannetta vastaavalla normaalilla toiminta-alueella sekä valvoa järjestelmien ja laitteiden kuntoa.

Käyttöautomaatioon tulee sisältyä riittävät tila- ja hälytystiedot, jotka automaattisesti tai laitoksen ohjaajien avustamana käynnistävät korjaavat ohjaus- ja säätötoimenpiteet, jos laitoksen parametrit joutuvat normaalin toiminta-alueen ulkopuolelle.

Käyttöautomaation hälytysrajat tulee asettaa siten, että ohjaus- ja säätötoimenpiteet voidaan toteuttaa ja saattaa päätökseen niin, että turvallisuustoimintoja käynnistäviä suojausrajoja ei ylitetä.

Käyttöautomaation toiminta tulee varmistaa suojaustoimintoja lievemmillä toiminnoilla siten, että käyttöautomaation yksittäinen vika ei aiheuta reaktorin turvallisuustoimintoja käynnistävien suojausrajojen ylittämistä.

Ohjeen YVL 1.0 luvussa 3.6 edellytetään, että *ydinvoimalaitoksen reaktoria sekä muita rakenteita, järjestelmiä ja laitteita varten on suunniteltava riittävä instrumentointi toimintasuureiden valvomiseksi ja järjestelmien toiminnan ja kunnon seuraamiseksi.*

Ydinreaktorin mittaukset tulee suunnitella siten, että ne antavat riittävän tarkat ja luotettavat lähtötiedot reaktorin suoritusarvojen laskentajärjestelmälle sekä suojaus-, säätö- ja valvontajärjestelmille.

Ainakin seuraavia reaktoriin liittyviä suureita tulee valvoa:

- reaktorin neutroniteho ja terminen teho
- reaktorin paine
- reaktorin pinnankorkeus
- reaktorin pääkiertovirtaus
- lämpötila primääripiirin eri osissa
- paineistimen pinnankorkeus ja paine (painevesireaktori)
- primääripiiriin syötettävät ja ulos laskettavat virtaukset
- höyrystimien pinnankorkeus ja paine (painevesireaktori)
- primääripiirin booripitoisuus (painevesireaktori)
- säätösauvojen asento.

Reaktorin valvonnan suunnittelussa on otettava huomioon seuraavat vaatimukset:

- Reaktorin tehojakauma on määritettävä luotettavasti, ja reaktorin termiset marginaalit on laskettava säännöllisesti.
- Reaktorisydämeen liittyvät virheelliset toimintatilat tulee voida havaita luotettavasti reaktorin instrumentoinnin avulla.
- Reaktoria tulee valvoa mittauksilla tai muulla järjestelyllä siten, että reaktorin sisäosien tai polttoaineen virheellinen sijoitus voidaan havaita luotettavasti.
- Prosessissa mahdollisesti olevien irtoesineiden valvonta tulee järjestää riittävällä tavalla.

Ohjeen YVL 1.0 mukaisesti *mittausjärjestelmien tulee pystyä riittävän tarkasti mittaamaan koko sillä alueella, jolla mitattava suure voi vaihdella käyttötilanteissa ja onnettomuuksissa. Mittaukset tulee suunnitella mahdollisuuksien mukaan siten, että jos mittaus vikautuu tai mittausalue ylittyy, ohjaajat huomaavat sen helposti.*

Ohjeen YVL 1.0 luku 3.6 edellyttää, että *valvontalaitteet tulee suunnitella tallentamaan laitoksen tilaa kuvaavat toimintasuureet ja järjestelmien ohjauskäskyt siten, että laitoksen käyttötapahtumia voidaan jälkikäteen analysoida.*

2.3 Valvomo ja käyttöliittymä

VNp:n (395/1991) 22 § 1 momentin mukaisesti *ydinvoimalaitoksen valvomoissa on oltava käytettävissä laitteet, jotka antavat tiedon laitoksen käyttötilasta ja poikkeamista normaalista käyttötilasta sekä järjestelmät, jotka valvovat laitoksen turvallisuusjärjestelmien tilaa käytön aikana ja niiden toimintaa käyttöhäiriöiden ja onnettomuuksien aikana.*

VNp:n (395/1991) 19 §:n mukaisesti *inhimillisten virheiden välttämiseen, havaitsemiseen ja korjaamiseen on kiinnitettävä erityistä huomiota. Virheiden mahdollisuus on otettava huomioon sekä ydinvoimalaitoksen että sen käyttötoiminnan suunnittelussa siten, että laitos kestää hyvin virheitä ja poikkeamia suunnitelluista käyttötoimenpiteistä.*

Ohjaajien ja automaation työnjako tulee suunnitella häiriö- ja onnettomuustilanteita koskevan ohjaustehtävien analyysin avulla siten, että inhimilliset rajoitukset otetaan huomioon. Valvomo tulee suunnitella siten, että inhimillisten virheiden mahdollisuus minimoidaan. Tämän varmistamiseksi tulee käyttää valvomoergonomian tarjoamia keinoja suunniteltaessa valvomoa ja sen toimintoja.

Hyvään suunnittelukäytäntöön kuuluu, että valvomosuunnitelmasta laaditaan valvomon suunnittelusta riippumaton asiantuntija-arvio.

Valvomon automaatiojärjestelmien ja ydinvoimalaitoksen hallintaan tarvittavan ohjeiston tulee muodostaa kokonaisuus, jonka toimivuus tulee varmistaa laitoskohtaisella simulaattorilla. Valvomon toiminnallisten ja merkittävien ergonomisten muutosten toimivuus tulee varmistaa etukäteen simulaattorilla tehtävin testein. Simulaattoria koskevat vaatimukset on esitetty ohjeessa YVL 1.6.

Ohjeen YVL 1.0 mukaisesti *valvomo tulee suunnitella siten, että sieltä voidaan tehdä laitoksen hallitsemiseksi tarvittavat toimenpiteet käyttötilanteissa ja onnettomuuksissa. Valvomon rakenteet ja turvallisuusjärjestelmät tulee suunnitella siten, että siellä voidaan työskennellä turvallisesti myös onnettomuuksien aikana.*

Edelleen ohjeen YVL 1.0 mukaisesti *valvomon, varaohjauspaikan ja paikallisten ohjauspaikkojen suunnittelussa tulee ottaa huomioon valvomossa työskentelyä koskevat ergonomiset periaatteet, jotka mahdollistavat sen, että ohjaustoimenpiteet voidaan tehdä luotettavasti. Erityistä huomiota on kiinnitettävä ohjaustaulujen, hälytysjärjestelmien ja tietokonepohjaisten näyttöjärjestelmien suunnitteluun siten, että häiriötilanteissa ja onnettomuuksissa ohjaajat voivat saada nopeasti hyvän yleiskuvan laitoksen tilasta ja että laitoksen turvallisuuden kannalta tärkeimmät tiedot tulevat selvästi esiin.*

Ohjeen YVL 1.0 mukaisesti *yleiskuvan ja hälytysinformaation esittämisessä käytettävien järjestelmien suunnittelussa tulee noudattaa mahdollisuuksien mukaan erilaisuusperiaatetta.*

Valvomon näytöt ja hälytykset tulee suunnitella ja toteuttaa siten, että niiden avulla ohjaajat saavat luotettavasti tiedon ohjaajan toimenpiteitä vaativasta laitostapahtumasta. Hälytykset tulee priorisoida tapahtuman turvallisuusmerkityksen mukaan. Hälytysten käsittely ja näyttö valvomon automaatiojärjestelmissä tulee suunnitella siten, että turvallisuudelle tärkeät hälytykset havaitaan mahdollisimman luotettavasti.

Näyttöhierarkian tulee olla looginen, ja tarvittavan prosessi-informaation tulee olla helposti saatavilla. Lisäksi prosessi-informaation esityksessä tulee käyttää loogista merkintäjärjestelmää.

Valvomo on ydinvoimalaitoksen keskeinen tila, jossa on turvallisuusluokiteltuja ja luokittelemattomia järjestelmiä ja laitteita. Valvomon suunnittelussa tulee ottaa huomioon turvallisuusjärjestelmien eri osajärjestelmien välinen fyysinen ja toiminnallinen erottelu sekä eri turvallisuusluokkiin kuuluvien järjestelmien ja laitteiden riittävä fyysinen ja toiminnallinen erottelu.

Valvomon automaatiojärjestelmien sähkönsyöttö tulee varmentaa ohjeen YVL 5.2 mukaisesti.

Valvomon suunnittelussa on otettava huomioon vaatimukset, jotka koskevat paloturvallisuutta, suojausta tulvimista vastaan, valaistusta, ilmastointia, meluntorjuntaa, säteilysuojausta ja kulunvalvontaa.

2.4 Varaohjauspaikat ja paikalliset ohjausjärjestelmät

VNp:n (395/1991) 22 §:n 3 momentin mukaisesti *ydinvoimalaitoksessa on oltava valvomosta riip-*

pumaton varaohjauspaikka ja tarvittavat paikalliset ohjausjärjestelmät, joiden avulla voidaan pysäyttää ja jäähdyttää ydinreaktori ja poistaa ydinreaktorin ja laitosyksiköllä varastoituna olevan käytetyn polttoaineen jälkilämpöä.

Ohjeen YVL 1.0 mukaisesti *varaohjauspaikka tulee suunnitella siten, että sieltä voidaan pysäyttää reaktori ja ohjata laitos vakaaseen sammutustilaan.* Varaohjauspaikasta tulee olla mahdollisuus pysäyttää reaktori sekä käynnistää ja ylläpitää jälkilämmön poistossa tarvittavat toiminnot. Varaohjauspaikka voi olla jaettuna yhteen tai useampaan huonetilaan. Lisäksi varaohjauspaikassa tulee olla varmennetut, riittävät kommunikointivälineet tarvittavaa yhteydenpitoa varten.

Valvomosta tulee voida siirtyä varaohjauspaikkaan turvallisesti ja riittävän nopeasti.

Ohjeen YVL 1.0 mukaisesti *valvomon ulkopuolisen varaohjauspaikan ohjausjärjestelmät on erotettava valvomon ohjausjärjestelmistä siten, että yhden palo-osaston sisältämien laitteiden tuhoutuminen tulipalossa täydellisesti ei vahingoita molempia ohjausjärjestelmiä niin paljon, että turvallisuustoimintoja ei voitaisi toteuttaa.*

Valvomon ja varaohjauspaikan ohjausten keskinäinen riippumattomuus tulee toteuttaa käyttäen fyysistä ja toiminnallista erottelua. Valvomon ja varaohjauspaikan fyysinen erottelu tulee toteuttaa siten, että valvomojärjestelmät sijoitetaan eri palo-osastoihin. Toiminnallisesti valvomon ja varavalvomon ohjausjärjestelmät tulee erottaa toisistaan sähköisesti ja siten, että ydinreaktoria ja jälkilämmön poistoa voidaan ohjata vain jommastakummasta ohjauspaikasta kerrallaan.

Varaohjauspaikkaan sijoitettavien toimintojen ja laitoksen järjestelmien tilatietojen riittävyys tulee analysoida erilaisissa ohjaustilanteissa siltä varalta, että laitosta ei voida ohjata ja valvoa valvomosta. Näiden valittujen ratkaisujen soveltuvuutta tulee tarkastella erilaisissa tilanteissa, joissa valvomon käyttö ei ole enää mahdollista.

2.5 Onnettomuusinstrumentointi

2.5.1 Yleiset vaatimukset

Ohjeen YVL 1.0 mukaisesti *onnettomuuksien seurantaa ja hallintaa varten ydinvoimalaitokseen tulee suunnitella asianmukainen mittaus- ja valvontainstrumentointi, jonka avulla käyttöhenkilökunta saa riittävästi tietoa tilanteen arvioimiseksi sekä vastatoimenpiteiden suunnittelemiseksi ja toteuttamiseksi.*

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

Informaation oletetusta onnettomuustilanteesta on oltava ohjaajien käytettävissä päävalvomossa. Onnettomuusinstrumentoinnin mittaukset tulee olla tunnistettavissa valvomossa siten, että valvomohenkilökunta pystyy helposti erottamaan nämä mittaukset muista mittauksista.

Onnettomuustilanteen prosessi-informaatio tulee tallentaa niin, että sitä voidaan myöhemmin analysoida.

Onnettomuusinstrumentoinnin laitteiden kelpoistusta oletettujen ja vakavien onnettomuuksien ympäristöolosuhteisiin käsitellään luvussa 3.1.

2.5.2 Oletettu onnettomuus

Oletettujen onnettomuuksien seurantaa ja hallintaa varten tarkoitetun onnettomuusinstrumentoinnin tulee sisältää ainakin seuraavantyyppisiä mittauksia:

- mittaukset, joiden perusteella voidaan myöhemmässä vaiheessa käsin käynnistää ne tarvittavat turvallisuustoiminnot, jotka eivät käynnisty automaattisesti alkutapahtuman seurauksena
- mittaukset, joiden avulla valvomohenkilökunta voi todeta turvallisuustoimintojen toteutuvan
- mittaukset, joista saadaan tietoa yksittäisten turvallisuusjärjestelmien ja näihin liittyvien laitteiden toiminnasta

- mittaukset, joiden avulla voidaan valvoa radioaktiivisten aineiden leviämistä estävien peräkkäisten teknisten esteiden eheyttä
- mittaukset, joita käytetään radioaktiivisten aineiden päästöjen arviointiin.

Mittauksia tulee olla riittävästi, jotta voidaan havaita paikalliset onnettomuuden hallinnan kannalta merkitykselliset olosuhteiden muutokset esimerkiksi suojarakennuksessa.

2.5.3 Onnettomuuden hallinnan tukitoiminto

VNp:n (395/1991) 13 §:n 3 momentin mukaisesti *onnettomuuden seurauksien lieventämiseen on varauduttava tehokkain teknisin ja hallinnollisin järjestelyin. Vastatoimenpiteet onnettomuuden saamiseksi hallintaan ja säteilyhaittojen ehkäisemiseksi on suunniteltava ennalta (seurausten lieventäminen).*

Onnettomuuden hallintaa varten tulee ohjaajien toimintaa avustamaan olla muusta automaatiosta saatavan hälytysinformaation lisäksi tukitoiminto, jolla valvotaan ja esitetään tarvittavien turvallisuustoimintojen tila. Tämä tulee toteuttaa erillisellä toiminnolla eli nk. onnettomuuden hallinnan tukitoiminnolla. Informaatio on esitettävä sellaisessa muodossa, että ohjaajat pystyvät selkeästi määrittelemään laitoksen tilan. Informaatio on näyttöteknisesti erotettava muusta valvomoinformaatiosta. Onnettomuuden hallinnan tukitoiminnon tulee olla käytettävissä kaikissa laitoksen käyttötilanteissa ja oletetuissa onnettomuuksissa.

Seisokkitiloja varten tulee olla vastaava tukitoiminto.

2.5.4 Vakava reaktorionnettomuus

Vakavien reaktorionnettomuuksien kulun hallitsemiseksi ja seuraamiseksi ydinvoimalaitos tulee varustaa ohjeen YVL 1.0 luvun 3.6 edellyttämillä valvontalaitteilla.

Vakavien reaktorionnettomuuksien valvontainstrumentoinnin suunnittelua koskevat seuraavat vaatimukset:

- Käytettävien mittausmenetelmien tulee olla sellaiset, että ne soveltuvat vakavien reaktorionnettomuuksien valvontaan.
- Instrumentoinnin tulee olla riippumaton laitosyksikön kaikesta muusta instrumentoinnista.
- Instrumentoinnin käyttöenergian (sähkö, paineilma jne.) syöttöjen tulee olla riippumattomia laitosyksikön muista syöttölähteistä.

Vaatimukset koskevat myös mahdollisia vakavan reaktorionnettomuuden yhteydessä tarvittavia ohjaustoimenpiteitä.

3 Yleiset suunnitteluvaatimukset

3.1 Kelpoistaminen ympäristöolosuhteisiin

Ydinvoimalaitoksen automaatiojärjestelmien ja -laitteiden ympäristöolosuhteet ja -rasitukset kaikissa suunnitelluissa käyttöolosuhteissa sekä varastoinnissa ja kuljetuksissa tulee määritellä sekä laitteet suunnitella siten, että laitteiden toimintakyky säilyy asetettujen vaatimusten mukaisina niiden koko suunnitellun käyttöiän. Turvallisuusluokiteltujen laitteiden kelpoisuus suunnitelluissa ympäristöolosuhteissa ja -rasituksissa tulee osoittaa standardien mukaisin testein. Testien tulee vastata epäedullisimpia mahdollisia paikallisia käyttöolosuhteita.

Onnettomuuksissa tarvittavien automaatiolaitteiden rakenteet ja materiaalit on valittava siten, että laitteiden toimintakyky onnettomuuksissa säilyy asetettujen vaatimusten mukaisena niiden koko suunnitellun käyttöiän.

Oletettujen onnettomuuksien ympäristöolosuhteiden ja prosessin sisäisten olosuhteiden vaikutukset on otettava huomioon muuta kuin sähköistä signaalia kuten hydraulista tai mekaanista signaalia käyttävien mittausten suunnittelussa. Tällaisia mittauksia ovat esimerkiksi impulssiputkia käyttävät mittaukset.

Oletetuissa onnettomuustilanteissa tai niiden jälkeen tarvittavien laitteiden tyyppikokeiden on muodostettava yhtenäinen koesarja, jossa samoihin koekappaleisiin kohdistetaan suunnitellun käyttökohteen suunnitteluperusteena olevat ympäristörasitukset. Ennen onnettomuusolosuhteiden kokeita koekappaleet tulee vanhentaa keinotekoisesti vastaamaan niiden suunniteltua käyttöikää.

Laitteen keinotekoinen vanhentaminen tulee tehdä siten, että se kuvaa riittävällä varmuudella todellista vanhenemista. Vanhentaminen tehdään yleensä siten, että laite vanhennetaan ensin termisesti ja sitten säteilytetään. Seuraavaksi laitteelle tehdään mekaaninen rasituskoe ja lopuksi edellä esitetyt oletettua onnettomuutta kuvaavat kokeet.

Oletettua onnettomuutta jäljittelevän kokeen tulee sisältää onnettomuusolosuhteita vastaava säteilytys ja lämpötilan, paineen ja kosteuden aiheuttamat rasitukset sekä nopeat olosuhteiden muutokset. Kokeessa käytettävän veden tulee koostumukseltaan vastata onnettomuusolosuhteissa kysymykseen tulevaa vettä. Jos laite voi jäädä oletetussa onnettomuudessa veden alle ja jos sen on tällöinkin kyettävä toimimaan, toimintakykyisyys tulee osoittaa myös tässä tilanteessa. Kokeet tulee suunnitella siten, että ne osoittavat riittävällä varmuudella laitteen toimintakykyisyyden onnettomuusolosuhteissa koko laitteen suunnitellun käyttöiän ajan.

Seismiset kokeet tai analyysit tulee tehdä ohjeen YVL 2.6 mukaisesti.

Jos automaatiolaitteen tulee toimia vakavissa reaktorionnettomuuksissa, sen kelpoisuus tähän tulee osoittaa soveltuvalla tavalla. Suojarakennuksessa sijaitsevien automaatiolaitteiden toimintakyvyn säilyminen onnettomuuden aikana mahdollisesti tapahtuvien vetypalojen yhteydessä tulee osoittaa, jos laitteiden toimintaa tarvitaan sellaisissa onnettomuuksissa, joissa vetypalojen esiintyminen on mahdollista.

3.2 Sähkömagneettinen yhteensopivuus

Ydinvoimalaitoksen automaatiojärjestelmät ja laitteet on suojattava luotettavasti sähköisten ja magneettisten häiriökenttien vaikutuksilta sekä erilaisilta verkko- ja radiohäiriöiltä ja tietoliikenteen aiheuttamilta häiriöiltä.

Automaatiolaitteet tulee suunnitella ja asentaa siten, että ne eivät aiheuta haitallisia sähkömagneettisia häiriöitä toimintaympäristöönsä.

Ohjeen YVL 5.2 kohdan 2.1 mukaisesti *maadoitus- ja ukkossuojausjärjestelmät tulee suunnitella siten, että ne suojaavat tehokkaasti ihmisiä, rakennuksia, laitteita sekä sähkö- ja automaatiojärjestelmiä ja -laitteita salamaniskujen aiheuttamilta ylijännitteiltä ja -virroilta sekä mahdollisilta muilta ilmastollisilta sähkömagneettisilta häiriöiltä.*

Myös muita luonnon tai ihmisen aiheuttamia sähkömagneettisia häiriöitä tulee tarkastella. Ydinvoimalaitoksen automaatiojärjestelmien ja -laitteiden sähkömagneettisilta häiriöiltä riittävään suojautumiseen käytettävät menettelyt ja tekniset ratkaisut tulee perustella.

3.3 Paloanalyysit

Ohjeessa YVL 4.3 esitetään ydinlaitosten palontorjunnan suunnittelua ja toteuttamista sekä STUKille toimitettavia, palontorjuntaa käsitteleviä asiakirjoja koskevat vaatimukset. Ohjeen YVL 4.3 kohdan 3.8 mukaisesti *suojarakennuksesta ja valvomosta on tehtävä paloanalyysit. [– –] Valvomon paloanalyysillä tulee osoittaa, että välttämättömien turvallisuustoimintojen ohjaukset voidaan toteuttaa valvomon tai minkä tahansa muun paloteknisen osaston palossa.* Tässä yhteydessä tulee myös selvittää palojen vaikutukset automaatiojärjestelmien kaapeleihin ja tästä aiheutuvien häiriöiden ja vikojen heijastuminen suojaus- ja ohjaustoimintojen toteuttamiseen.

Analyysissä tulee tarkastella sellaisia palotilanteita, jotka voivat vaikuttaa automaatiojärjestelmien tai -laitteiden toimintaan lämmön, savukaasujen tai muiden palon vaikutusten tai sammutustoimenpiteiden ja -aineiden välityksellä.

Järjestelmien, laitteiden ja kaapeleiden mahdolliset vikautumistavat kohonneiden lämpötilojen ja savukaasujen sekä palon sammutustoimenpiteiden vaikutuksesta tulee tunnistaa. Niiden vaikutuksia ohjaussignaalien läpimenoon sekä oikeellisuuteen tulee tarkastella. Suojaustoimintoihin vaikuttavat vikautumistavat tulee tunnistaa. Vian tai häiriön leviämismahdollisuuksia sähkönsyöttö- tai tiedonsiirtoreittien kautta tulee arvioida. Analyysissä tulee tarkastella valvomoon ja varaohjauspaikoille saatavan laitoksen tilaa koskevan informaation saatavuutta ja oikeellisuutta sekä käyttöhenkilökunnan toimintamahdollisuuksia tarvittavien laitoksen turvallisuustoimintojen varmistamiseksi erilaisissa paloista aiheutuvissa häiriö- ja vikatilanteissa.

Analyysiin tulee sisällyttää olennaisimpiin tekijöihin liittyvät epävarmuustarkastelut.

3.4 Tietoturvallisuus

Automaatiojärjestelmän suunnittelussa, käytössä ja ylläpidossa tulee huolehtia tietoturvallisuustekijöiden huomioon ottamisesta. Luvaton pääsy laitoksen häiriöttömän toiminnan kannalta tärkeisiin laitteisiin, ohjelmistoihin tai tietojärjestelmiin tulee estää. Luvaton pääsy turvallisuudelle tärkeiden järjestelmien laitteisiin tulee estää käyttäen fyysisiä, teknisiä ja hallinnollisia turvajärjestelyjä. Asiattomien ohjelmanosien asentaminen tulee estää luotettavasti suunnittelun, valmistuksen, käyttöönoton, määräaikaiskokeiden ja ylläpidon aikana. Luvalliset käynnit järjestelmään ja niiden aikana tehdyt muutokset tulee voida jäljittää.

3.5 Muut vaatimukset

Ohjeen YVL 2.0 kohdan 2.5.3 mukaisesti *samaa turvallisuustoimintoa suorittavat osajärjestelmät, olivatpa ne keskenään samanlaisia tai erilaisia, on erotettava myös toisistaan. Näillä erotteluilla varmistetaan, että ulkoisista vaikutuksista aiheutuvien yhteisvikojen mahdollisuus on hyvin pieni (erotteluperiaate).* Osajärjestelmien automaation tulee olla fyysisesti ja toiminnallisesti erillisiä.

Ohjeen YVL 2.0 kohdan 2.7 mukaisesti *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 apu- tai 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.* Suunnittelussa tulee varmistaa, ettei alempaan turvallisuusluokkaan kuuluvan automaatiojärjestelmän tai -laitteen toiminto tai vika aiheuta virhetoimintoa ylemmän turvallisuusluokan automaatiojärjestelmän toiminnassa.

Automaatiojärjestelmien välinen ja sisäinen tiedonsiirto tulee suunnitella siten, että tiedonsiirrossa tapahtuvat virheet eivät aiheuta virheellisiä toimintoja tai estä turvallisuustoimintojen toteutumista. Tiedonsiirtojärjestelmän tulee täyttää vasteaikavaatimukset laitoksen normaalikäytön, käyttöhäiriöiden tai onnettomuuksien aikana. Turvallisuusluokan 2 ja 3 järjestelmille tämä tulee osoittaa kaikissa mahdollisissa kuormitustilanteissa.

Ohjeen YVL 1.0 kohdan 3.13 mukaisesti *laitteiden tunnistamiseksi tulee suunnitella selkeä merkintäjärjestelmä.* Laitteiden tunnistamisen helpottamiseksi ja inhimillisten virheiden välttämiseksi tulee laitoksen automaatiojärjestelmien laitteet ja kaapelit varustaa kestävästä materiaalista valmistetulla tunnusmerkinnällä, joka on helposti luettavissa tarkastuksen, huollon ja vianhaun yhteydessä.

Ohjelmoitavien järjestelmien versioiden hallitsemiseksi ja inhimillisten virheiden välttämiseksi ohjelma- ja laiteversiot tulee varustaa yksikäsitteisillä tunnisteilla. Luvanhaltijalla tulee

olla käytössä järjestelmät, niiden laitteet ja ohjelmat kattava asianmukainen konfiguraation ja version hallintamenettely.

Järjestelmien ja laitteiden käyttöliittymien suunnittelussa tulee ottaa huomioon inhimilliset tekijät.

Langattoman ohjauksen käyttötarve tulee erityisesti perustella. Langattomalla ohjauksella ohjattava laite tai järjestelmä tulee suunnitella siten, että ohjaustoimenpide on mahdollista vain ohjaukseen tarkoitetulla yhteyssignaalilla ja että järjestelmä tai laite menee yhteyden katketessa riittävän nopeasti turvallisuuden kannalta edulliseen tilaan.

Automaatiojärjestelmien ja laitteiden sähkönsyöttöä koskevia vaatimuksia on esitetty ohjeessa YVL 5.2.

4 Automaatiojärjestelmien suunnittelu ja toteutus

4.1 Yleiset vaatimukset

Ydinvoimalaitoksen automaatiojärjestelmien ja -laitteiden suunnittelussa on noudatettava ennalta ehkäisemisen periaatetta, jonka mukaisesti *käyttöhäiriöiden ja onnettomuuksien ehkäisemiseksi on käytettävä koeteltua tai muutoin huolella tutkittua, korkealaatuista tekniikkaa suunnittelussa, rakentamisessa ja käyttötoiminnassa* [VNp:n (395/1991) 13 § 1 momentti].

Ohjeessa YVL 2.0 esitetään yleisiä vaatimuksia ydinvoimalaitosten järjestelmien ja laitteiden suunnitteluorganisaatiolle, suunnittelun riippumattomalle arvioinnille sekä suunnittelussa käytettävät deterministiset ja todennäköisyyspohjaiset suunnitteluperiaatteet.

Yleinen periaate on, että turvallisuusluokiteltujen automaatiojärjestelmien suunnittelussa ja toteutuksessa käytetään soveltuvia ydinteknisiä ohjeita ja standardeja. Turvallisuusluokan 2 laitteiden suunnittelussa ja toteutuksessa käytetään ydinteknisiin sovellutuksiin tarkoitettuja standardeja ja ohjeita sekä niiden mukaisia laadunhallintamenettelyjä. Turvallisuusluokkien 3 ja 4 laitteiden suunnittelussa käytetään soveltuvia standardeja sekä niiden mukaisia laadunhallintamenettelyjä.

Suunnittelussa ja toteutuksessa käytettävät standardit tulee esittää ja niiden soveltuvuus perustella. Turvallisuusluokkien 2 ja 3 automaatiojärjestelmien ja -laitteiden osalta mahdolliset poikkeamat esitetyistä standardeista tulee arvioida ja perustella.

Automaatiojärjestelmien ja -laitteiden määrittelyä, suunnittelua, toteutusta, ylläpitoa ja laadunhallintaa koskevien vaatimusten tulee olla suhteessa kohteen turvallisuusluokkaan ja -merkitykseen. Asetettaessa vaatimuksia automaatiojärjestelmän tai -laitteen suunnittelulle, toteutukselle ja kelpoistukselle tulee ottaa huomioon myös suunnittelun perusteena olevien toimintojen luotettavuustavoitteet.

Ohjeen YVL 1.4 mukaisesti luvanhaltijalla on kokonaisvastuu siitä, että voimassa olevat määräykset ja YVL-ohjeiden vaatimukset otetaan huomioon eri organisaatioiden laadunhallintajärjestelmissä. Luvanhaltijalla on päävastuu siitä, että asetettuja laatuvaatimuksia noudatetaan ja että riittävä laatutaso saavutetaan. Laatuvaatimusten asianmukainen siirtyminen automaatiojärjestelmien ja -laitteiden suunnitteluun, valmistukseen ja ylläpitoon osallistuvissa organisaatioissa ja niiden alihankinnoissa tulee varmistaa.

4.2 Laadunhallinta

4.2.1 Yleiset vaatimukset

VNp:n (395/1991) 21 §:n toisen momentin mukaisesti *turvallisuuden kannalta tärkeät järjestelmät, rakenteet ja laitteet on suunniteltava, valmistettava ja asennettava sekä niitä on käytettävä siten, että niiden laatutaso ja laatutason todentamiseksi tarvittavat tarkastukset ja testaukset ovat riittävät kohteen turvallisuusmerkityksen huomioon ottaen.*

Tämän varmistamiseksi tulee luvanhaltijalla olla käytössä laadunhallintamenettelyt, joissa on esitetty järjestelmälliset menettelytavat ydinvoimalaitoksen suunnittelun, rakentamisen ja käytön aikana noudatettavista laatuun vaikuttavista toimista.

Ydinvoimalaitoksen automaatiojärjestelmien ja -laitteiden suunnittelussa, valmistuksessa, asennuksessa, käytössä ja ylläpidossa tulee käyttää kehittyneitä suunnittelu-, valmistus- ja muutoksenhallintamenetelmiä, joissa otetaan huomioon käytettävän teknologian erityispiirteet. Korkeatasoinen laadunhallinta on keskeistä erityisesti ohjelmoitavien järjestelmien kelpoisuuden osoittamisessa. Laadunhallintamenettelyillä varmistetaan, että laitokselle hankittavien tuotantoerien rakenne ja ominaisuudet vastaavat kelpoistettujen tuotteiden ominaisuuksia.

4.2.2 Laadunhallintajärjestelmä

Ydinvoimalaitoksen rakentamis- ja käyttövaiheita varten tulee laatia automaatiojärjestelmiä ja -laitteita koskevat yleiset laadunhallinnan vaatimukset, jotka ottavat huomioon kohteen turvallisuusmerkityksen. Rakentamisen aikaisen laadunhallinnan tulee koskea suunnitteluun, valmistukseen, vastaanottoon, asennukseen ja käyttöönottoon osallistuvien osapuolten laadunhallintaa. Käytössä olevien ydinvoimalaitosten laadunhallinnan tulee kattaa vastaavat toiminnot sekä olemassa olevien järjestelmien ja laitteiden käyttö, ylläpito ja muutossuunnittelu. Sen tulee koskea kaikkia toimintaan osallistuvia osapuolia.

Käytönaikaisen laadunhallintajärjestelmän tulee sisältää muun muassa menettelytavat määräaikaishuoltojen ja -testien tekemiselle, testausten arvioimiselle, korjaus- ja muutostöiden tekemiselle, versionhallinnalle, varaosien vaihdolle ja kiireellisten korjausten tekemiselle sekä mittauslaitteiden tarkkuuden varmistamiselle ja ylläpitämiselle. Lisäksi siinä tulee esittää menettelytavat, joilla varmistetaan, että käyttö- ja onnettomuustilanteissa tarvittavien automaatiolaitteiden laatutaso säilyy koko laitoksen käyttöiän ajan.

Yleisten laadunhallintavaatimusten lisäksi tulee laatia laadunvarmistussuunnitelmia yksityiskohtaisine menettelyohjeineen hankinta-, valmistus-, vastaanotto-, asennus-, käyttöönotto- ja ylläpitovaiheita varten.

Automaatiojärjestelmien suunnittelua, toteutusta sekä muutosprojekteja varten tulee olla oma laatusuunnitelma kohdan 4.2.3 mukaisesti.

4.2.3 Automaatiojärjestelmän suunnittelun ja toteutuksen laadunhallinta

Automaatiojärjestelmän suunnittelua ja toteutusta varten tulee laatia laatusuunnitelma, josta ilmenevät käytettävät laadunhallinnan keinot. Laatusuunnitelman tulee kattaa koko järjestelmän suunnittelu ja toteutus sekä käyttöönotto. Laatusuunnitelma tulee laatia soveltuvan standardin mukaisesti. Laatusuunnitelmalla tulee varmistua siitä, että mahdolliset virheet havaitaan ja niiden poistamiseksi tehdään riittävät toimenpiteet sekä luvanhaltijan laadunhallintaa koskevat vaatimukset toteutuvat hankinnassa.

Laatusuunnitelmasta tulee ilmetä suunnitteluun osallistuvien organisaatioiden rajapinnat ja niiden hallinta, vastuut projektin laatutoiminnoista kaikissa osallistuvissa organisaatioissa sekä alihankkijoiden valvonta. Laatusuunnitelmassa tulee esittää menettelyt, joilla varmistutaan dokumentoinnin oikeellisuudesta ja valmiudesta hankkeen eri vaiheiden päättyessä. Lisäksi suunnitelmassa tulee määritellä järjestelmän suunnittelussa ja toteutuksessa noudatettavat version- ja muutosten hallintamenettelyt sekä laatusuunnitelman muutosmenettely.

Laatusuunnitelmassa on määriteltävä asianmukainen välitulosten katselmusmenettely, jolla luvanhaltija arvioi erityisesti toimittajan suunnitteluprosessia. Katselmusten tavoitteena on eliminoida suunnitteluvirheet mahdollisimman aikaisessa vaiheessa sekä varmistaa suunnitteluperusteiden, turvallisuusvaatimusten ja käyttö- ja kunnossapitovaatimusten huomioon ottaminen, teknisen toteutuksen oikeellisuus ja kelpoistusprosessin oikea-aikainen eteneminen.

Järjestelmän suunnittelua koskevissa katselmuksissa tulee käsitellä luvun 4.4 mukaista järjestelmän kelpoistamista.

Turvallisuusluokan 2 automaatiojärjestelmän laatusuunnitelmaan tulee kuulua suunnittelusta ja toteutuksesta riippumaton arviointi, jossa arvioidaan laatusuunnitelman noudattamista sekä riittäviä korjaavia toimenpiteitä mahdollisten puutteiden poistamiseksi. Arvioijilla tulee olla tehtävän edellyttämä, käytännössä hyväksi osoitettu pätevyys laadunhallinnasta turvallisuussovellutuksissa sekä käytettävästä teknologiasta.

Turvallisuusluokkien 2 ja 3 automaatiojärjestelmien ja -laitteiden toimittajilla tulee olla soveltuvan standardin mukainen ja riippumattomasti arvioitu laadunhallintajärjestelmä.

Luvanhaltijan on määriteltävä menettelytavat, joilla automaatiojärjestelmien ja -laitteiden toimittajia arvioidaan, valitaan ja valvotaan. Ennen suunnittelun ja toteutuksen aloittamista on todettava, että toimitukseen osallistuvilla organisaatioilla on edellytykset korkealaatuiseen toimintaan.

4.3 Suunnitteluprosessi

4.3.1 Yleiset vaatimukset

Järjestelmän suunnittelussa tulee pyrkiä yksinkertaisuuteen ja vikasietoisuuteen sekä mahdollisten vikojen havaitsemismahdollisuuteen oikea-aikaisesti. Suunnittelussa ja toteutuksessa tulee käyttää virheitä välttäviä ja virheitä havaitsevia menetelmiä.

Ydinlaitoksen automaatiojärjestelmät ja laitteet tulee suunnitella ja dokumentoida siten, että suunnitteluprosessin eri vaiheissa voidaan varmistua asetettujen vaatimusten siirtymisestä oikein lopulliseen käyttöön otettavaan järjestelmään. Tämän nk. elinkaarimallin mukaisen suunnitteluprosessin ensimmäinen vaihe on vaatimusmäärittely. Suunnitteluprosessin vaiheet tulee esittää kelpoistussuunnitelmassa (luku 4.4).

Jokaisen vaiheen lähtötiedot ja tulosaineisto tulee dokumentoida siten, että ne ovat toimittajasta, luvanhaltijasta ja suunnittelusta riippumattoman henkilön arvioitavissa. Turvallisuusluokan 2 järjestelmien jokainen suunnitteluvaihe tulee todentaa edellisen vaiheen asettamien vaatimusten perusteella. Suunnitteluprosessin on oltava kokonaisuutena läpinäkyvä ja todennettavissa. Vaiheistettu suunnitteluprosessi on esitetty monissa erilaisissa ohjeissa ja standardeissa, kuten tämän ohjeen viitteinä olevissa IAEA:n ohjeissa ja IEC-standardeissa.

4.3.2 Vaatimusmäärittely

Ydinlaitoksen automaatiojärjestelmän ja -laitteen vaatimusmäärittelyn tulee sisältää kaikki merkittävät järjestelmän toiminnalliset, suorituskyky- ja luotettavuusvaatimukset. Lisäksi tulee esittää muut järjestelmän suunnitteluun vaikuttavat vaatimukset kuten ympäristöolosuhteet ja -rasitukset sekä liityntöjä, määräaikaiskokeita, ylläpitoa, tietoturvallisuutta ja käyttöikää koskevat vaatimukset. Turvallisuuden kannalta merkittävien vaatimusten tulee olla yhdenmukaisia laitoksen turvallisuusanalyysissä tehtyjen oletusten kanssa. Järjestelmän rajapinta laitoksen muihin järjestelmiin ja käyttäjiin tulee määritellä selkeästi.

Vaatimusmäärittelyä tulee tarkentaa suunnittelun edetessä. Järjestelmän, laitteen ja ohjelmiston lopullisen vaatimusmäärittelyn tulee olla riittävän yksityiskohtainen ja kattava, jotta toteutus on testattavissa tai todennettavissa kyseisiä vaatimuksia vasten. Vaatimusten tulee olla ristiriidattomia ja yksikäsitteisiä. Vaatimusten toteutuminen tulee olla todennettavissa. Vaatimusmäärittelyä tulee ylläpitää järjestelmän koko suunnittelu-, valmistus- ja käyttöjakson ajan.

Turvallisuusluokkaan 2 tai 3 kuuluvan automaatiojärjestelmän ja -laitteen laitoskohtaisen vaatimusten määrittelyn tulee olla riittävän yksityiskohtainen järjestelmän arviointia sekä järjestelmään valittavien laitteiden kohdan 4.4.7 mukaista soveltuvuusarviointia varten.

Turvallisuusluokan 2 järjestelmän vaatimusmäärittelyn oikeellisuus, täydellisyys ja ristiriidattomuus tulee arvioida riippumattomasti. Arviointiraportissa tulee esittää arvioinnissa tehdyt havainnot sekä perusteltu johtopäätös.

4.3.3 Dokumentointi

Automaatiojärjestelmän ja -laitteen suunnitteluprosessin alussa tulee määritellä dokumentointivaatimukset ja dokumenttien hallintamenettely, jota noudatetaan hankkeen alusta lähtien. Periaatesuunnitteluvaiheessa tulee käyttää toiminnalliseen määrittelyyn selkeätä ja täsmällistä eri alojen asiantuntijoiden ymmärtämää esitystapaa. Toimintakaavioiden tai vastaavan suunnittelumenetelmän mukaisen esitystavan käyttäminen kuuluu hyvään suunnittelukäytäntöön.

Järjestelmää kuvaavan dokumentaation tulee olla rakenteeltaan selkeä ja riittävän kattava. Dokumenttien tietojen tulee olla ajan tasalla ja riittäviä järjestelmälle asetettujen vaatimusten toteutumisen arviointia varten.

Automaatiojärjestelmien ja -laitteiden dokumentointi tulee päivittää muutosten yhteydessä. Luvanhaltijan laadunhallintajärjestelmän dokumentoinnin hallintaa koskevat vaatimukset on esitetty ohjeessa YVL 1.4.

4.3.4 Muutosten hallinta suunnitteluprosessin aikana

Automaatiojärjestelmän ja -laitteen suunnitteluprosessin alussa tulee määritellä asianmukainen muutoksenhallintamenettely, jota noudatetaan koko suunnitteluprosessin ajan.

4.4 Kelpoistaminen

4.4.1 Yleiset vaatimukset

Ydinlaitoksen automaatiojärjestelmät ja niiden laitteet tulee kelpoistaa käyttötarkoitukseensa. Turvallisuusluokan 2 tai 3 automaatiojärjestelmän ja sen laitteiden soveltuvuuden osoittamiseksi aiottuun käyttötarkoitukseen tulee luvanhaltijan laatia erityinen kelpoistussuunnitelma. Kelpoistussuunnitelman tulee sisältää aineistoa neljältä osa-alueelta: suunnittelu- ja valmistusprosessi, testit, analyysit ja käyttökokemukset. Mikäli osoittamiseen tarkoitettua aineistoa on vähän jollakin osa-alueella, puute on kompensoitava laajentamalla toisella osa-alueella esitettyä aineistoa. Kelpoistussuunnitelmassa tulee esittää laadittavat soveltuvuusarviot ja siihen tulee liittää myös tiedot automaatiojärjestelmän tai laitteen aiemmista tyyppihyväksynnöistä, joita halutaan hyödyntää kelpoisuuden osoituksessa.

Osana turvallisuusluokkaan 2 kuuluvan järjestelmän kelpoistusta käytetään riippumattomia asiantuntija-arviointeja. Toteutettavista riippumattomista todentamisista ja arvioinneista tulee laatia suunnitelmat. Arvioinnin toteutus ja tehdyt havainnot sekä perusteltu johtopäätös tulee esittää arviointiraportissa.

Luvanhaltijan tulee arvioida ja esittää perusteltu johtopäätös kelpoistuksen tulosten hyväksyttävyydestä.

Kelpoistussuunnitelma tulee päivittää, mikäli järjestelmän vaatimusmäärittely muuttuu kelpoistukseen vaikuttavalla tavalla tai järjestelmästä saadaan olennaista tietoa, jolla voidaan katsoa olevan vaikutusta kelpoistussuunnitelmaan.

4.4.2 Suunnittelu- ja valmistusprosessi

Kelpoistussuunnitelmassa tulee kuvata järjestelmän suunnittelu- ja valmistusprosessin vaiheistus sekä kunkin vaiheen jälkeen tehtävät tarkastukset ja arvioinnit.

Tarkastusten ja arviointien tekijöiden tulee olla suunnitteluorganisaation teknisiä asiantuntijoita, jotka eivät itse ole osallistuneet suunnitteluun tai toteutukseen. Heidän tulee arvioida ja todentaa kussakin työvaiheessa edellistä vaihetta koskevien vaatimusten täyttyminen. Tarkastukset ja arvioinnit tulee tehdä kaikille turvallisuusluokan 2 ja oleellisille turvallisuusluokan 3 automaatiojärjestelmän suunnittelu- ja valmistusvaiheille lopulliseen tuotteeseen saakka. Tarkastus- ja arviointisuunnitelmat sekä tulokset

tulee dokumentoida siten, että ne ovat ulkopuolisen tahon arvioitavissa tarpeen vaatiessa.

4.4.3 Testit

Testit voidaan jakaa suunnittelu- ja valmistusprosessin aikana tehtäviin testeihin ja toteutetulle automaatiojärjestelmälle ja -laitteille tehtäviin testeihin. Tässä yhteydessä laitteilla tarkoitetaan sekä kenttälaitteita että automaatioteknisiä laitteita.

Suunnittelu- ja valmistusprosessin aikaisia testejä ovat mm. yksikkötestit, integrointitestit ja järjestelmätestit. Ohjelmiston testit jakaantuvat staattisiin ja dynaamisiin testeihin. Suunnittelun ja valmistuksen aikaisilla testeillä varmistutaan siitä, että automaatiojärjestelmä tai -laite täyttää sille asetetut toiminnalliset ja suorituskykyvaatimukset. Nämä testaukset päättyvät tehdaskokeisiin. Tilastollisia testejä voidaan tehdä erityisesti luotettavuustarkastelujen tueksi.

Automaatiojärjestelmän ja siihen kuuluvien laitteiden testeille tulee laatia testiohjelma. Järjestelmän suunnittelusta ja valmistuksesta riippumattomien testaajien tulee tehdä ohjelman mukaiset kokeet. Testaussuunnitelma, testien hyväksymiskriteerit ja testien tulokset tulee dokumentoida siten, että ne voidaan arvioida riippumattomasti.

Testauksilla ja analyyseillä tulee varmistua myös siitä, ettei järjestelmässä tai siihen kuuluvissa laitteissa ole tarkoituksettomia, turvallisuudelle haitallisia toimintoja. Turvallisuusluokan 2 järjestelmän testien riittävyys tulee perustella sekä testien kattavuus tulee analysoida järjestelmän vaatimuksia vasten.

Tehdaskokeiden jälkeen on arvioitava automaatiojärjestelmän tai –laitteen vaatimusten mukaisuus ja virheettömyys, jotta voitaisiin varmistua siitä, että automaatiolaite tai -järjestelmä voidaan siirtää laitospaikalle. Hankkeen aikataulu tulee suunnitella siten, että tehdaskokeiden jälkeen mahdollisesti tarvittava muutossuunnittelu on tehtävissä automaatiojärjestelmän tai -laitteen turvallisuusmerkityksen mukaisin menettelyin.

Toteutettavaan järjestelmään kuuluville laitteille edellytettäviä testejä ovat erityisesti tyyppi- ja ympäristötestit, joissa otetaan huomioon laitteen sovellus (järjestelmä- ja laitosympäristö). Toteutetulle järjestelmälle tehdään muun muassa hyväksymiskokeet ja käyttöönottokokeet laitoksella.

Lopullisessa testauksessa tulee osoittaa, että automaatiojärjestelmä tai -laite vastaa sille asetettuja toiminnallisia ja suorituskykyvaatimuksia. Testauksessa voidaan osittain käyttää hyväksi simulointia. Lopullinen testaus tulee kuitenkin tehdä todellisessa toimintaympäristössä.

Laitoksella tehtävää järjestelmän koekäyttöä koskevat vaatimukset on esitetty ohjeessa YVL 2.5.

Erityisvaatimukset ohjelmoitaville järjestelmille ja laitteille esitetään kohdassa 4.6.5.

4.4.4 Turvallisuuteen liittyvät analyysit

Toiminnallisten ja suorituskykyvaatimusten toteutuminen tulee osoittaa osana järjestelmän ja laitteiden kelpoistusta mukaan lukien tarvittavat analyysit.

Turvallisuusluokan 2 järjestelmille tulee tehdä vikautumistapojen ja -vaikutusten analyysi, yhteisvika-analyysi, käyttökokemusanalyysi ja kvantitatiivinen luotettavuusanalyysi.

Turvallisuusluokan 3 automaatiojärjestelmille tulee tehdä vikautumistapojen ja -vaikutusten analyysi, yhteisvika-analyysi ja käyttökokemusanalyysi ja turvallisuusmerkityksestä riippuen kvantitatiivinen luotettavuusanalyysi.

Turvallisuusluokan 2 ja 3 järjestelmille tulee tehdä turvallisuusarvio, jolla osoitetaan turvallisuusvaatimusten täyttyminen. Laitoskohtainen PSA-malli tulee päivittää vastaamaan muutettua järjestelmää.

Erityisvaatimukset ohjelmoitaville järjestelmille ja laitteille esitetään kohdassa 4.6.

4.4.5 Käyttökokemukset

Aikaisempien käyttökokemusten analyysi tulee tehdä turvallisuusluokkien 2 ja 3 automaatiojärjestelmille sekä turvallisuusluokan 2 laitteille ja turvallisuusluokan 3 keskeiseen onnettomuusinstrumentointiin kuuluville automaatiolaitteille. Käyttökokemusten tulee olla kerätty hyvin määritellyn menetelmän mukaisesti. Keräysprosessin kattavuus ja sen merkitys tietojen luotettavuuteen tulee arvioida. Käyttökokemusten tulee olla edustavia käsiteltävän sovellutuksen kannalta. Käyttökokemusten keruuajan tulee olla riittävän pitkä. Muista laite- ja ohjelmaversioista, kokoonpanoista ja käyttöprofiileista kerättyjen käyttökokemusten hyödyntäminen järjestelmän tai laitteiden kelpoistuksessa tulee perustella.

4.4.6 Tyyppihyväksyntä

Turvallisuusluokan 2 laitteilla ja turvallisuusluokkaan 3 kuuluvalla keskeisellä onnettomuusinstrumentoinnilla (NRC Regulatory Guide 1.97, cat. 1 [1]) tulee olla soveltuvan ydinteknisen standardin mukainen akkreditoidun tai vastaavan pätevyyden omaavan tarkastuslaitoksen myöntämä tyyppihyväksyntä. Tyyppihyväksynnän tulee kattaa laitteen suunnittelun arviointi ja laitteen valmistuksen laadunhallinnan arviointi. Laitteen vaatimustenmukaisuus tulee osoittaa käyttäen testejä ja analyysejä sekä käytännön tyyppikokeita.

Laadunhallinnan arviointiin tulee liittyä laitteen valmistukseen liittyvien asiakirjojen tarkastus sekä tuotteen valmistuksen arviointi. Laadunhallinnan arvioinnin tekijöillä tulee olla käytännössä osoitettu pätevyys laadunhallintajärjestelmien arviointiin sekä turvallisuussovellutuksessa käytettävän laitteen teknisten vaatimusten täyttymisen arviointiin. Laadunhallinnan arvioinnin yhteydessä tulee erityisesti kiinnittää huomiota toimenpiteisiin, joilla varmistutaan, että sarjatuotannossa valmistetut laitteet vastaavat tarkastettua laitetta.

Tyyppihyväksyntäraportissa tulee esittää tarkastuksessa tehdyt havainnot, perusteltu päätös tuotteen hyväksyttävyydestä sekä hyväksynnän voimassaoloon liittyvät ehdot.

Ohjelmoitavalla tekniikalla toteutetun laitteen tyyppihyväksynnän tulee kattaa sekä ohjelmiston että laitteiston arviointi. Ohjelmistoja koskevia lisävaatimuksia on esitetty kohdassa 4.6.

4.4.7 Soveltuvuusarvio

Kaikille turvallisuusluokkien 2 ja 3 laitteille tulee tehdä soveltuvuusarvio. Soveltuvuusarvioinnissa tulee arvioida laitteen toiminnallisia ja suorituskykyominaisuuksia automaatiojärjestelmässä laitteelle määriteltyjä vaatimuksia vasten. Erityisesti tulee tarkastella ympäristöolosuhdetestejä, ohjelmiston arviointia, laitteen käyttökokemuksia sekä laitteiden toiminnan luotettavuutta suhteessa laitteen turvallisuusmerkitykseen.

Soveltuvuusarviossa tulee selvittää toimittajan edellytykset toimittaa kyseistä tuotetta kohdan 4.2 mukaisesti.

Soveltuvuusarvio tulee laatia luvanhaltijan laadunhallintajärjestelmään kuuluvan ohjeen mukaisesti.

4.5 Asennus ja käyttöönotto

Turvallisuusluokkiin 2, 3 ja 4 kuuluville laitteille ja ohjelmille tulee tehdä vastaanottotarkastus. Laitteiden ja ohjelmien vastaanottotarkastuksissa luvanhaltijan tulee varmistaa, että automaatiolaite tai ohjelmisto on suunnitelmien mukainen ja sen laadunvalvonnan tulosaineisto on hyväksyttävä. Lisäksi tulee varmistua, että laite ei ole vaurioitunut kuljetuksen aikana. Vastaanottotarkastukseen mahdollisesti kuuluvat testit tulee tehdä hyväksytysti. Vastaanottotarkastus tulee dokumentoida asianmukaisesti.

Luvanhaltijan tulee tehdä asennetuille turvallisuusluokkiin 2, 3 ja 4 kuuluville laitteille asennustarkastus. Asennustarkastuksessa luvanhaltijan tulee varmistaa, että laitteen vastaanottotarkastus on tehty hyväksytysti ja asennus on asianmukainen. Asennuksille tulee määritellä

asennusaikataulu, asennustapahtumien dokumentoinnissa noudatettavat menettelytavat sekä asennuksen jälkeen tehtävien asennus- ja kytkentätarkastusten sekä toimintakokeiden laajuus.

Luvanhaltijan tulee tehdä asennetuille tai muutetuille turvallisuusluokkiin 2, 3 ja 4 kuuluville järjestelmille käyttöönottotarkastus. Siinä tulee todentaa, että paikoilleen asennettu järjestelmä on hyväksyttyjen suunnitelmien mukainen ja että tämä on varmistettu riittävin tarkastuksin ja kokein. Lisäksi tulee todentaa, että tarkastuksissa havaitut puutteet ja viat on korjattu. Käyttöönottotarkastuksessa tulee myös varmistua siitä, että mahdolliset käyttöönottovaiheessa tehdyt muutokset on toteutettu noudattaen järjestelmän muutostenhallinnalle määriteltyjä menettelyjä.

Käyttöönottotarkastuksissa tulee käsitellä luvanhaltijan laadunhallinnan toteutuminen sekä varmistua siitä, ettei käyttöönotolle ole esteitä. Käyttöönottotarkastuksessa tulee varmistua laitteiden ja järjestelmien asennuspaikan ja ympäristön yhdenmukaisuudesta asetettujen vaatimusten kanssa. Asennustarkastukset ja toimintakokeet tulee olla hyväksyttävästi suoritettu ja koekäytön tulosaineistossa ja käyttöönottoon liittyvissä pöytäkirjoissa ei saa olla puutteita, jotka ovat esteitä käyttöönotolle. Järjestelmää koskevien ohjeiden valmius tulee varmistaa. Käyttöönottotarkastuksessa tulee myös varmistua, että STUKin aikaisempien valvontatoimenpiteiden yhteydessä mahdollisesti esitetyt huomautukset on asianmukaisesti hoidettu.

Luvanhaltijan laadunhallintajärjestelmässä olevista automaatiojärjestelmien ja -laitteiden vastaanoton, asennuksen ja käyttöönoton aikaisista menettelyistä tulee ilmetä toiminnosta vastaavien organisaatioiden tehtävät, työnjako ja vastuualueet sekä dokumentoinnissa noudatettavat menettelyt ja tehtävien tarkastusten laajuus.

Käyttöönottotarkastuksia tekevän organisaatioyksikön tulee täyttää soveltuvin osin ohjeen YVL 1.3 mukaiset tarkastuslaitoksia koskevat vaatimukset.

4.6 Ohjelmoitavan järjestelmän ja laitteen erityisvaatimukset

4.6.1 Perusjärjestelmän ja sovelluksen kelpoistaminen

Ohjelmoitavan järjestelmän kelpoistussuunnitelman tulee sisältää sekä perusjärjestelmän että sovelluksen kelpoistus. Kohdassa 4.4.6 on esitetty yleiset vaatimukset tyyppihyväksynnöille. Nämä vaatimukset koskevat myös perusjärjestelmän ohjelmistoja. Turvallisuusluokkaan 3 kuuluville perusjärjestelmille ja laitteille, joille ei edellytetä kohdan 4.4.6 mukaisesti tyyppihyväksyntää, tulee harkita soveltuvan standardin mukaista ohjelmiston arviointia järjestelmälle tai laitteelle asetetun luotettavuustavoitteen perusteella. Arviointiraportissa tulee esittää tarkastuksessa tehdyt havainnot, mahdollisten korjaavien toimenpiteiden tarve sekä perusteltu päätös ohjelmiston hyväksyttävyydestä aiottuun käyttötarkoitukseen.

Ohjelmoitavan järjestelmän luotettavuuden osoittamiseen käytettäviä tekijöitä ovat erityisesti korkeatasoinen perusjärjestelmän ja sovelluksen suunnitteluprosessi ja toteutukseen osallistuvan henkilöstön pätevyys sekä ohjelmistotuotantoon soveltuvien standardien käyttö. Erilaiset riippumattomat tarkastukset ja vaatimustenmukaisuuden arvioinnit sekä soveltuvat työkalut ovat olennainen osa korkeatasoista ohjelmiston suunnitteluprosessia.

4.6.2 Ohjelmistotyökalut ja suunnittelumenetelmät

Kaikki turvallisuusluokkien 2 ja 3 järjestelmien ja laitteiden suunnittelussa ja toteutuksessa käytettävät ohjelmistotyökalut kuten esimerkiksi kääntäjät, koodigeneraattorit, analysaattorit jne. sekä testaus- ja suunnittelumenetelmät tulee esittää kelpoistussuunnitelmassa.

Turvallisuusluokan 2 järjestelmien ja laitteiden suunnittelussa ja toteutuksessa käytettyjen ohjelmistotyökalujen käyttökokemusten tulee olla kattavasti ja järjestelmällisesti kerättyjä sekä

dokumentoituja. Turvallisuusluokan 3 järjestelmien ja laitteiden suunnittelussa ja toteutuksessa tulee käyttää standardiohjelmistotyökaluja, joiden versionhallinta, ylläpito ja vikatietojen keruu on dokumentoitu asianmukaisesti. Turvallisuusluokan 4 järjestelmien suunnittelussa ja toteutuksessa tulee käyttää standardiohjelmistotyökaluja.

Konfigurointiin ja objektikoodin tuottoon käytettävien työkalujen versionhallinta, ylläpito ja muutossuunnittelu tulee toteuttaa järjestelmän tai laitteen turvallisuusmerkityksen mukaisin menettelyin.

Ohjelmistotyökalujen kelpoistusmenettelyjä määriteltäessä tulee ottaa huomioon mahdollisen työkalusta johtuvan virheen vaikutus turvallisuuteen.

Mahdollisen ohjelmistotyökalun virheen ilmenemisen yhteydessä noudatettavat menettelyt laitokselle asennettujen järjestelmien luotettavan toiminnan varmistamiseksi tulee dokumentoida.

Turvallisuusluokkien 2 ja 3 ohjelmistojen suunnittelussa ja toteutuksessa tulee käyttää koeteltuja korkeatasoisia työkaluja ja testausmenetelmiä. Turvallisuusluokan 2 ohjelmiston suunnitteluun ja toteutukseen käytettävien työkalujen kelpoisuus käyttötarkoitukseensa tulee osoittaa.

4.6.3 Olemassa oleva ohjelmisto ja laitteisto

Olemassa olevaa ohjelmistoa koskevat samat vaatimukset kuin kehitettävää ohjelmistoa. Suunnitteluprosessin dokumentoinnissa ja toteutuksessa mahdollisesti esiintyviä puutteita voidaan korvata analyysien ja testauksen avulla. Korvausmenettelyjen arvioinnissa otetaan huomioon turvallisuusluokan ja -merkityksen mukaiset vaatimukset.

Olemassa olevan ohjelmiston soveltuvuusarviointia varten on analysoitava ohjelmiston rakenne ja toiminnot ja pois jätettävät toiminnot.

Ohjelmiston ja järjestelmän dokumentoinnin tulee olla riittävän kattava laitteen tai ohjelmiston versioiden hallitsemiseksi sekä muutossuunnittelun mahdollistamiseksi laitteen tai ohjelmiston turvallisuusmerkityksen edellyttämillä menettelyillä.

4.6.4 Yhteisvikautumisen välttäminen ja analysointi

Ohjelmistoviat ovat tyypillisesti suunnitteluvirheitä. Tästä seuraa, että sama vika on mahdollinen samanaikaisesti järjestelmän rinnakkaisissa osissa. Suunnitteluvirheisiin liittyvä yhteisvikojen aiheuttama riski tulee saattaa hyväksyttävän alhaiselle tasolle käyttäen erilaisuusperiaatetta tai muuta mahdollista tapaa varmistaa järjestelmän riittävän luotettava toiminta. Yhteisvikautumisen välttämiseen käytettävät menettelyt tulee dokumentoida ja perustella sekä esittää osana ohjeen YVL 2.7 mukaisia analyysejä.

4.6.5 Ohjelmoitavan järjestelmän tai laitteen testaus

Turvallisuusluokiteltujen järjestelmien tai laitteiden testisuunnitelman ja käytettävien menettelyjen tulee olla riittäviä järjestelmän tai laitteen turvallisuusmerkitykseen ja luotettavuustavoitteeseen nähden. Ohjelmisto tulee testata myös asennettavassa laitteistossa.

Turvallisuusluokkien 2 ja 3 järjestelmän lopullisen testauksen tulee kattaa kaikki järjestelmän toiminnot ajoituksineen mukaan lukien itsediagnostiikan toiminnot niiltä osin kuin se on käytännössä mahdollista. Ohjelmiston moduulien testauksen tulee sisältää staattisia ja dynaamisia testejä. Testitapausten tulee sisältää mm. häiriö- ja onnettomuusanalyysien mukaisia transienttitilanteita.

Turvallisuusluokan 2 järjestelmien ja laitteiden testien kattavuus testauksen eri vaiheissa tulee analysoida ja lopullisten testien valinta sekä määrä tulee perustella.

4.6.6 Ohjelmoitavan järjestelmän tai laitteen muut vaatimukset

Julkaisussa ”Common position of European nuclear regulators for the licensing of safety critical software for nuclear reactors”, (European Commission’s Advisory Expert Group, Nuclear Regulators Working Group, 2000) esitetään yksityiskohtaisesti vaatimustasojen välisiä eroja eri turvaluokkaan kuuluvien ohjelmien suunnittelussa ja toteutuksessa sekä ylläpidossa. Julkaisun vaatimukset tulee ottaa soveltuvin osin huomioon automaatiojärjestelmien ja -laitteiden suunnittelussa.

Turvallisuusluokan 2 järjestelmän ja laitteen suunnittelussa tulee pyrkiä yksinkertaisuuteen. Järjestelmän rakenteen tulee minimoida yksittäisen ohjelmavirheen vaikutuksen leviäminen ja mahdollistaa järjestelmälle asetettujen vaatimusten todentaminen. Ohjelman suoritusjaksot tulee määritellä. Tehtävän suorittamisen kannalta tarpeettomat ohjelmiston osat tulee tunnistaa sekä niiden turvallisuusmerkitys tulee analysoida ja ottaa huomioon järjestelmän suunnittelussa.

Ohjelmiston vikautumistavat tulee tunnistaa ja analysoida riittävän pitkälle.

Ohjelmoitavaan järjestelmään ja laitteeseen tulee suunnitella itsediagnostiikka, joka vastaa sen turvallisuusmerkitystä.

Turvallisuusluokan 2 ohjelmoitavien automaatiojärjestelmien ja -laitteiden itsediagnostiikan ja määräaikaiskokeiden kattavuus tulee analysoida. Myös mahdollisten itsediagnostiikan vikojen vaikutus suojausautomaation toimintaan tulee analysoida.

Turvallisuusluokkaan 2 kuuluvan ohjelmoidun järjestelmän vaatimusten jäljitettävyys suunnitteluprosessin eri vaiheissa tulee osoittaa osana järjestelmän kelpoistusta.

5 Vanhenemisen seuranta

Ohjeen YVL 1.0 luvun 3.15 mukaisesti *ydinvoimalaitoksen suunnittelussa tulee arvioida riittäviä turvallisuusmarginaaleja käyttäen kaikkien turvallisuuden kannalta tärkeiden rakenteiden, laitteiden ja materiaalien elinikä ja niiden vanhenemisen vaikutus turvallisuuteen. Lisäksi tulee varautua niiden vanhenemisen seurantaan ja tarvittaessa niiden vaihtamiseen tai korjaamiseen.*

Ohjeen YVL 2.0 luvun 2.2 mukaisesti *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.*

Ydinlaitoksen automaatiojärjestelmien ja -laitteiden vanhenemisen seurantaa varten tulee laatia ohjelma, jonka avulla seurataan laitoksen järjestelmien ja laitteiden jäljellä olevaa käyttöikää ja mahdollista uusintatarvetta. Ohjelman laadinnassa tulee ottaa huomioon erilaisiin komponentteihin liittyvät vanhenemismekanismit ja niiden merkitys. Ohjelman tulee kattaa laitteiden ja järjestelmien vikahistorian keruu- ja analysointimenettelyt mahdollisten vikataajuuksissa tapahtuneiden muutosten havaitsemiseksi ja vaihtotarpeen ennakoimiseksi sekä mahdolliset muut vanhenemisen seuraamiseksi tehtävät analyysit ja testit. Myös muilta laitoksilta ja toimittajilta saatavia vikatietoja tulee mahdollisuuksien mukaan hyödyntää vanhenemisen seurannassa. Seurannan tulee kattaa laitoksen turvallisen käytön kannalta merkittävät laitteet ja järjestelmät niiden turvallisuusluokasta riippumatta. Seurannan kohteeksi esitettyjen järjes-

telmien ja laitteiden valintaperusteet tulee esittää ohjelman yhteydessä. Erityisesti on valvottava onnettomuuksissa tarvittavien laitteiden ja niiden kaapelien sekä asennusten kuntoa. Ydinlaitoksen kaapeleiden vanhenemisen seurantaa koskevat vaatimukset on esitetty ohjeessa YVL 5.2. Vanhenemisen seurantaohjelman kattavuutta ja tehokkuutta tulee arvioida säännöllisesti.

Ydinvoimalaitoksen automaatiojärjestelmien ja -laitteiden vanhenemisen seurantaohjelmassa tulee myös tarkastella järjestelmien ja laitteiden teknologista vanhenemista sekä siitä mahdollisesti johtuvia toimenpidetarpeita.

Vanhenemisen seurannan tulokset tulee esittää vuotuisessa selvityksessä, jossa tulee esittää seurannan kohteiden vikahistorian analysointitulosten sekä muiden mahdollisten analyysien tulosten lisäksi mahdolliset korjaustoimenpiteet ja kehityssuunnitelmat aikatauluineen.

6 Säteilyturvakeskuksen valvonta

6.1 Yleiset valvontaperiaatteet

Ohjeessa YVL 2.0 esitetään järjestelmien ennakkotarkastusta koskevat vaatimukset. Ohjeen mukaan järjestelmien hyväksymiskäsittely tehdään osana alustavan ja lopullisen turvallisuusselosteen käsittelyä.

Ydinvoimalaitoksen käytön aikana muutettavan järjestelmän tai lisättävän järjestelmän ennakkotarkastus tehdään erillisen muutostyötä koskevan periaatesuunnitelman ja ennakkotarkastusaineiston pohjalta. Automaatiojärjestelmien valvonnan yleisperiaatteena on, että turvallisuusluokkiin 2 ja 3 kuuluvista järjestelmistä sekä sellaisista järjestelmistä, jotka STUK vaatii tarkastettavaksi erillisellä päätöksellä, on toimitettava STUKin hyväksyttäväksi periaatesuunnitelmat ja järjestelmäkohtaiset ennakkotarkastusaineistot. Turvallisuusluokan 4 järjestelmistä on toimitettava järjestelmän ennakkotarkastusaineisto tiedoksi STUKiin.

Ohjeen YVL 2.0 kohdan 3.4.1 mukaisesti toimitettavan aineiston laajuus voi vaihdella muutoksen turvallisuusmerkityksen ja laajuuden mukaan.

Lopulliseen turvallisuusselosteeseen on muutostyön yhteydessä tehtävä viipymättä tarvittavat muutokset. Muutostöitä käsitellään ohjeessa YVL 1.8.

Turvallisuusluokkaan 2 kuuluvista automaatiolaitteista sekä turvallisuusluokkaan 3 kuuluvista keskeisistä onnettomuusinstrumentoinnin laitteista on toimitettava automaatiolaitteiden soveltuvuusarvio hyväksyttäväksi. Muiden turvallisuusluokkaan 3 kuluvien laitteiden soveltuvuusarvio toimitetaan tiedoksi STUKiin.

Mekaanisia laitteita ja niiden ennakko- ja rakennetarkastuksia koskevat YVL-ohjeet asettavat vaatimuksia automaatiolaitteille, mikäli näiden mekaanisilla ominaisuuksilla on turvallisuusmerkitystä, esimerkiksi painetta kantavat laitteet.

6.2 Periaatesuunnitelma

Turvallisuusluokkien 2 ja 3 automaatiojärjestelmän periaatesuunnitelman sisältö vastaa pääsääntöisesti alustavan turvallisuusselosteen sisältöä ja sen tulee sisältää seuraavat selvitykset:

- järjestelmän suunnitteluperiaatteet ja -perusteet
- järjestelmän toiminnot, toimintaperiaatteet ja tärkeimmät suunnitteluarvot sekä toimintojen määrittely laitteille
- kuvaus järjestelmän merkityksestä varsinaisen turvallisuustoiminnon toteuttamisessa, jos järjestelmä on turvatoimintoa suorittavan järjestelmän tukijärjestelmä
- järjestelmän sekä sen laitteiden erotteluperiaatteet (osastointi, suojaus) ja alustava sijoittelu laitoksella ohjeen YVL 4.3 kohdan 3.3 mukaisesti
- järjestelmän toimintojen ja laitteiden alustava turvallisuusluokitus
- järjestelmän ympäristöolosuhteet ja -rasitukset ja niistä aiheutuvat suunnitteluvaatimukset

- muista järjestelmistä, mukaan lukien apu- ja tukijärjestelmistä sekä ohjattavasta prosessista aiheutuvat vaatimukset ja riippuvuudet
- järjestelmän rajapinnat mukaan lukien käyttöliittymä sekä liittyminen muihin automaatiojärjestelmiin
- selvitys laadunhallinnan periaatteista sekä suunnitteluun osallistuvien organisaatioiden pätevyydestä
- alustava kelpoistussuunnitelma
- suunnittelijan laatima alustava turvallisuusarvio
- luvanhaltijan ohjeen YVL 2.0 kohdan 2.3 mukainen oma turvallisuusarviointi.

Järjestelmän suunnitteluperusteissa tulee esittää, minkä ohjeiden ja standardien mukaisesti järjestelmä suunnitellaan. Samoin tulee esittää järjestelmän ja sen laitteiden alustava turvallisuusluokitus sekä järjestelmän ympäristöolosuhteet ja niistä aiheutuvat suunnitteluvaatimukset.

Periaatesuunnitteluvaiheen alustavassa kelpoistussuunnitelmassa tulee esittää kohdan 4.4 mukainen suunnitelma kelpoistuksesta sekä aiemmat kelpoistukset, joita halutaan hyödyntää järjestelmän kelpoistusprosessissa. Alustavassa kelpoistussuunnitelmassa tulee esittää aikataulu kelpoistuksen tulosaineiston toimittamisesta STUKiin.

Alustavassa turvallisuusarviossa tulee osoittaa, kuinka järjestelmä täyttää sitä koskevat turvallisuusvaatimukset. Siinä tulee esittää myös alustava arvio järjestelmän muutoksen vaikutuksesta todennäköisyyspohjaisiin turvallisuusanalyyseihin (PSA).

6.3 Järjestelmän ennakkotarkastusaineisto

Turvallisuusluokkien 2 ja 3 automaatiojärjestelmän ennakkotarkastusaineiston sekä soveltuvin osin turvallisuusluokan 4 automaatiojärjestelmän ennakkotarkastusaineiston tulee pääsääntöisesti vastata lopullista turvallisuusselosteen sisältöä ja sen tulee sisältää seuraavat selvitykset:

- järjestelmän yksityiskohtaiset suunnitteluperusteet
- järjestelmän yksityiskohtainen toiminta- ja rakennekuvaus
- järjestelmän ympäristöolosuhteet ja -rasitukset ja niistä aiheutuvat suunnitteluvaatimukset
- turvallisuudelle tärkeiden osajärjestelmien sijoittelu, erottelu, suojaus (palo-osastointi, fyysinen suojaus)
- vaikutukset ydinvoimalaitoksen muihin järjestelmiin ja riippuvuudet muista järjestelmistä sekä vikojen leviämisen estäminen
- todennäköisyyspohjainen tarkastelu järjestelmän vaikutuksesta laitoksen turvallisuuteen
- laatusuunnitelma
- tietoturvallisuussuunnitelma
- kelpoistussuunnitelma
- kelpoistuksen tulosaineisto
- suunnittelijan turvallisuusarvio siitä, miten järjestelmä täyttää sille asetetut turvallisuusvaatimukset
- luvanhaltijan ohjeen YVL 2.0 kohdan 2.3 mukainen oma turvallisuusarviointi
- järjestelmää koskevat turvallisuusteknisten käyttöehtojen vaatimukset
- muut tarvittavat selvitykset.

Järjestelmän ennakkotarkastusaineisto toimitetaan hyväksyttäväksi vaiheittain siten, että kelpoistuksen tulosaineisto ja riippumattomat arvioinnit toimitetaan vasta suunnittelun ja toteutuksen edettyä asianomaisiin vaiheisiin.

Ohjeessa YVL 2.0 annetaan ohjeita siitä, mitä ennakkotarkastusaineistossa tulee esittää järjestelmän suunnitteluperusteiden osalta. Turvallisuusluokkaan 2 ja 3 kuuluvan automaatiojärjestelmän vaatimusmäärittely tulee lähettää tiedoksi STUKiin. Turvallisuusluokan 2 automaatiojärjestelmän vaatimusmäärittelyn oikeellisuutta, täydellisyyttä ja ristiriidattomuutta koskeva arviointiraportti tulee toimittaa tiedoksi STUKiin.

Ohjeessa YVL 2.0 esitetään järjestelmän toimintakuvauksen sisältöä koskevia ohjeita. Järjestelmän toimintakuvauksen tulee sisältää myös oh-

jelmoitavan järjestelmän itsediagnostiikkaa ja tämän kattavuutta kuvaava selvitys.

Järjestelmän rakennetta ja toimintaa selventävinä kaavioina esitetään tarpeen mukaan muun muassa

- säätö-, automatiikka-, lukitus- yms. periaate- ja toimintakaaviot
- yhteenveto mittausten käyttötiedoista (tunnus, tyyppi, mittausalue, suojaus- ja hälytysrajat)
- ohjelmoitavasta järjestelmästä lisäksi ohjelmiston arkkitehtuuri- ja vuokaaviot
- ohjelmistotyökalut ja niiden toimintakuvaus
- sähköisten suojausten toimintakaaviot
- apujännitesyöttöjen periaatekaaviot.

Laatusuunnitelmassa tulee esittää järjestelmän suunnittelua ja toteutusta koskevat laadunhallinnan keinot. Laatusuunnitelmaan liittyvät toiminta- ja menettelyohjeet toimitetaan STUKiin tiedoksi.

Kelpoistussuunnitelmassa tulee esittää tämän ohjeen luvussa 4.4 esitetyt tiedot. Kelpoistuksen tulosaineiston tulee sisältää luvanhaltijan arvio kelpoistuksen toteutumisesta.

Laatusuunnitelman ja kelpoistussuunnitelman tarkastuksessa otetaan huomioon järjestelmän turvallisuusmerkitys ja järjestelmän toimintojen luotettavuustavoitteet.

Tietoturvallisuussuunnitelmaan liittyvät toiminta- ja menettelyohjeet toimitetaan tiedoksi STUKiin.

Turvallisuusluokan 2 ja 3 järjestelmille tulee tehdä turvallisuusarvio, jolla osoitetaan YVL-ohjeiden ja vaatimusmäärittelyn vaatimusten täyttyminen sekä vaikutus PSA:han.

Järjestelmän ennakkotarkastusaineiston yhteydessä on esitettävä periaatetasolla mahdolliset muutokset turvallisuusteknisiin käyttöehtoihin.

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.

6.4 Laitteiden soveltuvuusarvio

STUK tarkastaa luvanhaltijan soveltuvuusarvion seuraavien laitteiden osalta:

- turvallisuusluokkaan 2 kuuluvat automaatiolaitteet
- turvallisuusluokkaan 3 kuuluva keskeinen onnettomuusinstrumentointi (NRC Regulatory Guide 1.97, cat. 1 [1]).

Alustava soveltuvuusarvio toimitetaan STUKiin hyväksyttäväksi, mikäli laitteelle joudutaan tekemään tyyppihyväksyntä osana kelpoistusprosessia. Alustavassa soveltuvuusarviossa tulee esittää tyyppihyväksyntäprosessissa käytettävät standardit ja tyyppihyväksynnän toteuttava organisaatio, josta tulee esittää tiedot akkreditoinnista tai soveltuvin osin ohjeen YVL 1.3 mukaiset tarkastuslaitosta koskevat tiedot.

Soveltuvuusarvion yhteydessä tulee toimittaa tiedoksi seuraavat aineistot:

- laitteen laitos- ja sovelluskohtainen vaatimusmäärittely
- laitteen suunnitteluperusteet
- laitteen toiminta- ja rakennekuvaus sekä piirustukset
- tiedot toimittajasta
- laitteen laatusuunnitelma
- laitteen tyyppihyväksymisraportti.

Turvallisuusluokkaan 3 kuuluvan laitteen soveltuvuusarvio tulee toimittaa tiedoksi ilman edellä mainittuja aineistoja.

Laitteen suunnitteluperusteissa tulee esittää laitteen suunnittelussa, valmistuksessa, testauksessa ja asennuksessa noudatettavat ohjeet ja

standardit. Mahdolliset poikkeamat esitetyistä standardeista ja ohjeista tulee esittää ja perustella luvun 4.1 mukaisesti.

Laitteen toiminta- ja rakennekuvausten sekä piirustusten tulee olla riittäviä tyyppihyväksynnän arvioimiseksi ja soveltuvuusarvion tarkastamiseksi. Laitteen kuvaukseen tulee kuulua myös ohjelmistotyökalujen kuvaukset.

Laitteen toimittajaa koskevassa selvityksessä tulee esittää toimittajan organisaatio, pätevyys sekä toimittajan laadunhallintajärjestelmän arviointitapa ja -tulokset.

6.5 Valmistuksen valvonta, tehdaskokeet

STUK valvoo harkintansa mukaan tarkastuskäynnein ennakkotarkastuksen piiriin kuuluvien automaatiojärjestelmien ja -laitteiden valmistusta. STUKille on varattava tarkastuskäyntien yhteydessä mahdollisuus tutustua mm. valmistajien laadunhallintajärjestelmiin, valmistuksen laadunvalvonnan tulosaineistoon sekä kelpoistussuunnitelmassa esitettyyn aineistoon.

Mahdollisia valmistajilla ja toimittajilla suoritettavia tarkastuksia varten on STUKille toimitettava tiedoksi järjestelmien koestusaikataulut (suorituskyky- ja toiminnalliset kokeet). Niistä tehdaskokeista, joita STUK ilmoittaa seuraavansa, tulee toimittaa tiedoksi tehdaskoeohjelma.

6.6 Asennuksen valvonta

STUK valvoo harkintansa mukaan turvallisuusluokan 2 ja 3 automaatiojärjestelmien ja -laitteiden asennusta.

Asennuksen valvontaa varten STUKille on ennen asennusten alkamista toimitettava tiedoksi turvallisuusluokkiin 2 ja 3 kuuluvien automaatiojärjestelmien ja -laitteiden asennusaikataulu. Tarkastuksen yhteydessä luvanhaltijan tulee esittää STUKille luvanhaltijan tekemien tarkastusten tulokset ja niihin liittyvä tulosaineisto.

Säteilyturvakeskus arvioi tarkastuskäyntiensä yhteydessä, että toteutus kokonaisuudessaan vastaa hyväksytyn ennakkotarkastusaineiston suunnitelmia ja esitettyä laatutasoa.

6.7 Käyttöönoton valvonta

STUK valvoo automaatiojärjestelmien koekäyttöä laitoskokeiden yhteydessä ohjeen YVL 2.5 mukaisesti. STUK seuraa harkintansa mukaan kokeita laitospaikalla. Turvallisuusluokkiin 2 ja 3 kuuluvien automaatiojärjestelmien koekäyttöohjelmat on toimitettava STUKin hyväksyttäväksi ja aikataulut tiedoksi hyvissä ajoin ennen koekäytön aloittamista. Turvallisuusluokkiin 2 ja 3 kuuluvien automaatiojärjestelmien koekäytön tulosraportit tulee toimittaa hyväksyttäväksi STUKille. STUK määrittelee turvallisuusluokan 4 järjestelmän ennakkotarkastuksen yhteydessä, minkä järjestelmän koekäyttöohjelmat ja -aikataulut sekä koekäytön tulosraportit tulee toimittaa STUKille tiedoksi.

STUK määrittelee automaatiojärjestelmien ennakkotarkastuksen yhteydessä mille järjestelmille se tekee järjestelmän käyttöönottotarkastuksen. STUKin järjestelmän käyttöottotarkastusten yhteydessä luvanhaltijan tulee esittää STUKille toteutetut järjestelmämuutokset ja luvanhaltijan luvun 4.5 mukaisesti tekemien tarkastusten tulokset ja niihin liittyvä tulosaineisto.

STUKin järjestelmän käyttöönottotarkastus on suoritettava ennen laitoksen käynnistämistä vuosihuoltoseisokista tai käynnin aikana ennen järjestelmän käyttöönottoa. STUKin järjestelmän käyttöönottotarkastuksen suorittamista on pyydettävä kirjallisesti hyvissä ajoin ennen tarkastusajankohtaa.

Ydinvoimalaitoksen muiden painelaitteiden kuin reaktoripainesäiliön käyttöturvallisuuden vaatimien mittaus- ja säätölaitteiden koekäyttöä ja toimintakokeiden tekemistä käsitellään ohjeessa YVL 3.7.

6.8 Laitteiden laadunhallinnan valvonta

Luvanhaltijan on laadittava kohdan 4.2 mukaiset eri turvallisuusluokkien laitteita koskevat yleiset suunnitelmat laaduntarkastusten järjestämisestä suunnittelu-, valmistus-, vastaanotto-, asennus- ja käyttöönottovaiheessa. Suunnitelmat on toimitettava STUKiin hyväksyttäväksi ennen kutakin edellä mainittua vaihetta.

6.9 Käytönaikainen valvonta

STUK valvoo käytön aikana ydinlaitoksen automaatiojärjestelmiä ja -laitteita tarkastamalla järjestelmien ja yksittäisten laitteiden korjaus- ja muutostöitä sekä arvioimalla luvanhaltijan toimintaa ja menettelytapojen tehokkuutta järjestelmien ja laitteiden luotettavan toiminnan varmistamiseksi. Luvanhaltijan toimintaa arvioidaan määräajoin toistettavissa käytön tarkastusohjelman tarkastuksissa.

Käytön tarkastusohjelman osana STUK valvoo, että turvallisuusluokiteltujen kohteiden osalta

- automaatiojärjestelmien ja -laitteiden vaatimusten määrittely, suunnittelu ja kunnossapito ovat asianmukaisia
- laadunhallinta, laitehankinnat, varaosien hallinta ja vastaanottotarkastukset ovat asianmukaisia
- automaatiojärjestelmien ja -laitteiden toimintakyky ja kunto todetaan määräaikaiskokein
- laitteiden ympäristö- ja käyttöolosuhteita arvioidaan
- laitteiden vanhenemista arvioidaan
- mittauslaitteiden mittaustarkkuuden ylläpito varmistetaan
- laitteiden kunnonvalvontamittaukset, vikatiedot, vikatietojen keruujärjestelmät ja analyysit ovat asianmukaiset
- laitteiden ennakkohuolto, korjaustoiminta ja varaosahuolto toimivat asianmukaisesti
- laitteiden ja järjestelmien konfiguraation- ja versionhallinta on asianmukaista.

Automaatiojärjestelmien ja -laitteiden määräaikaiskoeohjelmat, niissä noudatettavat menettelytavat ja kunnonvalvontaa kuvaavat ohjeet tulee toimittaa tiedoksi STUKille. Koetulokset tulee tallentaa laitospaikalla siten, että myös STUK voi arvioida saatuja tuloksia ja verrata niitä aikaisempiin tuloksiin.

Turvallisuuden kannalta tärkeiden automaatiojärjestelmien ja -laitteiden toimintakuntoisuutta koskevien vaatimuksien hyväksyttävyyden ja määräaikaiskokeiden kattavuuden STUK arvioi ydinlaitoksen turvallisuusteknisten käyttöehtojen tarkastamisen yhteydessä.

STUK seuraa myös säännöllisin välein, että turvallisuusluokiteltujen laitteiden ympäristö- ja käyttöolosuhteita seurataan asianmukaisesti kohteissa tehtävien mittausten avulla ja tarvittaessa ryhdytään toimiin huolto-ohjelmien ja käyttöikäarvioiden sekä kelpoistuksen tarkistamiseksi. STUK tarkastaa mittaustulokset harkitsemassaan laajuudessa laitospaikalla.

STUK valvoo luvanhaltijan automaatiojärjestelmien ja -laitteiden vanhenemisen seurantaohjelman toteutumista ja tuloksia mm. käytön tarkastusohjelman yhteydessä.

Vanhenemisen seurannan tulokset tulee esittää vuotuisessa selvityksessä, joka tulee toimittaa STUKiin tiedoksi.

6.10 Käytönaikaiset järjestelmä- ja laitemuutokset

Ohjeissa YVL 1.8 ja YVL 2.0 esitetään ydinlaitosten muutostöitä koskevia vaatimuksia.

STUK tekee ennakkotarkastuksen turvallisuusluokiteltujen automaatiojärjestelmien ja -laitteiden muutoksille siinä laajuudessa kuin kohdassa 6.1 on esitetty.

Muutostyöt saa aloittaa vasta, kun STUK on hyväksynyt ennakkotarkastusaineiston ja kun päätöksessä mahdollisesti esitetyt työn aloittamista ja valvontaa koskevat vaatimukset on täytetty. Järjestelmien muutettujen osien ja laitteiden koekäyttöohjelmat tulee laatia siten, että ne vastaavat mahdollisimman hyvin vastaavia alkuperäisiä koekäyttöohjelmia.

Turvallisuusluokkaan 4 ja luokkaan EYT kuuluvien järjestelmien muutoksille tulee hakea

STUKin hyväksyntä, mikäli muutokset ovat sellaisia, että ne vaikuttavat ohjeessa YVL 1.0 esitettyjen suunnitteluperusteiden toteutumiseen.

Ennen järjestelmän käyttöönottoa tulee luvanhaltijan hakea hyväksyntä turvallisuusteknisiin käyttöehtoihin tarvittaville muutoksille. Hätä-, häiriö- ja käyttöohjeet tulee ennen järjestelmän käyttöönottoa päivittää vastaamaan muutettua järjestelmää.

Esitys lopulliseen turvallisuusselosteeseen tarvittavista muutoksista on toimitettava viivytyksettä STUKille hyväksyttäväksi järjestelmän käyttöönoton jälkeen.

7 Määritelmiä

Deterministinen suunnitteluperiaate
Järjestelmän suunnittelun perustana käytetään ennalta asetettuja suunnitteluvaatimuksia ja valittua joukkoa alkutapahtumia, joiden vaikutukset laitoksen turvallisuuteen otetaan järjestelmän suunnittelussa huomioon.

Dynaaminen testaus
Järjestelmän tai komponentin arviointia toiminnallisten testien perusteella.

Integrointitestit
Integrointitestissä testataan järjestelmän yksiköiden välisiä liittymiä eli yksiköiden yhteensopivuutta. Ohjelmoitavan järjestelmän integrointitestit varmistavat myös ohjelmiston ja laitteiden yhteensopivuuden.

Itsediagnostiikka
Järjestelmän tai laitteen sisään rakennettu toiminto, joka valvoo järjestelmän tai laitteen virheetöntä toimintaa ja vikautumista ja joka virheen havaittuaan suorittaa ennalta määritellyt toiminnot.

Kelpoistaminen
Kelpoistamisella osoitetaan, että automaatiojärjestelmä tai -laite kykenee kaikissa sen käyttötilanteissa niissä ympäristöolosuhteissa, joihin se on suunniteltu, täyttämään sille asetetut toiminnalliset ja suorituskykyvaatimukset.

Käyttötilanteet
Käyttötilanteilla tarkoitetaan ydinvoimalaitoksen normaaleja käyttötilanteita ja odotettavissa olevia käyttöhäiriöitä.

Laatusuunnitelma
Laatusuunnitelma on tuotteeseen tai projektiin liittyvät laatukäytännöt, resurssit ja toimintasarjat määräävä asiakirja.

Normaalit käyttötilanteet
Normaaleilla käyttötilanteilla tarkoitetaan ydinvoimalaitoksen käyttämistä turvallisuusteknisten käyttöehtojen mukaisesti. Normaaleihin käyttötilanteisiin kuuluvat myös järjestelmien ja laitteiden testaukset, laitosyksikön ylös- ja alasajo, huolto ja polttoaineen vaihto.

Odotettavissa olevat käyttöhäiriöt
Odotettavissa olevalla käyttöhäiriöllä tarkoitetaan sellaista onnettomuutta lievempää poikkeamaa normaaleista käyttötilanteista, jonka esiintymistaajuuden odotusarvo on suurempi kuin kerran sadan käyttövuoden aikana.

Ohjelmistotyökalu
Ohjelmiston kehittämiseen, kääntämiseen, testaamiseen ja analysointiin käytettävä työkalu.

Ohjelmoitava järjestelmä
Ohjelmoitava järjestelmä on automaatiojärjestelmä, jonka toiminnot on pääosin tai kokonaan toteutettu käyttäen mikroprosessoria, ohjelmoitavaa laitetta tai tietokonetta. Järjestelmään kuuluvat kaikki järjestelmän yksiköt kuten sisäinen sähkönsyöttö, anturit ja muut sisääntuloyksiköt, tiedonsiirtoväylät, ulostuloyksiköt ja muut tiedonsiirtokanavat ohjattaviin toimilaitteisiin.

Ohjelmoitava laite
Ohjelmoitava laite on ohjelmoitavan järjestelmän yksi tai useampi yksikkö. Ohjelmoitava laite on järjestelmän yksittäinen määriteltävä ja usein irrotettavissa oleva osa järjestelmää. Ohjelmoitava laite voi olla myös itsenäinen laite, jonka toteutuksessa on käytetty ohjelmoitavaa tekniikkaa.

Olemassa oleva ohjelmisto
Olemassa olevalla ohjelmistolla tarkoitetaan ennen kyseistä hanketta kehitettyä ohjelmistoa tai ohjelmaa. Sen laajuus voi vaihdella yksinkertaisesta ohjelmasta aina laajaan automaatiojärjestelmään saakka.

Oletettu onnettomuus
Oletetulla onnettomuudella tarkoitetaan sellaista ydinvoimalaitoksen turvallisuusjärjestelmien suunnitteluperusteena käytettävää tilannetta, josta ydinvoimalaitoksen edellytetään selviytyvän ilman vakavia polttoainevaurioita ja niin suuria radioaktiivisten aineiden päästöjä, että laitoksen ympäristössä jouduttaisiin turvautumaan laajoihin toimenpiteisiin väestön säteilyaltistuksen rajoittamiseksi.

Onnettomuus
Onnettomuudella tarkoitetaan sellaista poikkeamaa normaaleista käyttötilanteista, joka ei ole odotettavissa oleva käyttöhäiriö. Onnettomuudet jaetaan kahteen luokkaan: oletetut onnettomuudet ja vakavat reaktorionnettomuudet.

Onnettomuusinstrumentointi
Onnettomuuden seurantaa ja hallintaa varten suunniteltu mittaus- ja valvontainstrumentointi, jonka avulla käyttöhenkilökunta saa riittävästi tietoa tilanteen arvioimiseksi sekä vastatoimenpiteiden suunnittelemiseksi ja toteuttamiseksi.

Perusjärjestelmä
Perusjärjestelmällä tarkoitetaan automaatiojärjestelmän sitä osuutta, joka on sovelluksesta riippumaton ja käytetään osana toimivaa järjestelmää.

Riippumaton tarkastus tai arviointi
Riippumatonta tarkastusta ja arviointia voi olla kolmea eri tasoa siten, että tarkastuksen tai arvioinnin tekijä on kohteen suunnittelusta ja toteutuksesta riippumaton henkilö, riippumaton organisaatioyksikkö tai riippumaton organisaatio. Kulloinkin käytettävä riippumattomuus määräytyy suoritettavan tehtävän luonteesta sekä arviointituloksen merkityksestä turvallisuuden varmistamisessa. Yksityiskohtaisempia vaatimuksia eritasoisille riippumattomuuksille on esitetty standardissa SFS-EN 45004 ”Yleiset vaatimukset erityyppisten tarkastuslaitosten toiminnalle”.

Sovellus
Ohjelmoidun järjestelmän sovellus on se osa järjestelmää, joka toteuttaa järjestelmän prosessia ohjaavat toiminnot.

Staattinen testaus
Prosessi, jossa järjestelmää tai komponenttia, arvioidaan sen muodon, rakenteen, sisällön tai dokumentoinnin perusteella. Esimerkkejä staattisesta testauksesta ovat muun muassa ohjelmiston suunnittelun, koodin ja standardinmukaisuuden todentaminen (esim. Faganin menetelmä), ohjaus- ja datavuokaavioiden analysointi, symbolinen ohjelman suoritus sekä formaali koodin todentaminen.

Tarkoitukseton toiminto
Tarkoituksettomalla toiminnolla ymmärretään sellaista toimintoa, joka ei ole järjestelmän tai laitteen varsinaisen toiminnan kannalta tarpeellinen. Toimintoja, joita tehtävän suorittaminen ei vaadi, mutta joiden turvallisuusmerkitys on analysoitu ja otettu huomioon järjestelmän suunnittelussa, ei pidetä tarkoituksettomina.

Toiminnallinen riippumattomuus
Automaatiojärjestelmän toiminnallinen riippumattomuus toteutetaan käyttäen sähköistä ja tiedonsiirrollista riippumattomuutta.

Turvallisuusjärjestelmä
Turvallisuusjärjestelmä on järjestelmä, joka suorittaa jotakin turvallisuustoimintoa.

Turvallisuustoiminto
Turvallisuustoiminnot ovat turvallisuuden kannalta tärkeitä toimintoja, joiden tarkoituksena on ehkäistä häiriöiden ja onnettomuuksien syntyminen tai eteneminen tai lieventää onnettomuuksien seurauksia. Turvallisuustoimintoon kuuluu koko toiminnon toteuttamiseen tarvittava laitteisto: mittaus, logiikka ja toimilaite.

Vakava reaktorionnettomuus

Vakavalla reaktorionnettomuudella tarkoitetaan tilannetta, jossa huomattava osa reaktorissa olevasta polttoaineesta vaurioituu.

Yhteisvika

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

Yksittäisvika

Yksittäisvika tarkoittaa satunnaisvikaa ja sen seurausvaikutuksia, jotka oletetaan tapahtuviksi joko normaalissa käyttötilanteessa tai alkutapahtuman ja sen seurausvaikutusten lisäksi. Tarkempia ohjeita yksittäisvikautumisesta ja siihen varautumiseksi annetaan ohjeessa YVL 2.7.

8 Viitteet

1. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.97, revision 3, May 1983.
2. ”Common position of European nuclear regulators for the licensing of safety critical software for nuclear reactors”, EUR 19265, 2000.
3. IAEA Safety Standards Series, NS-G-1.3, ”Instrumentation and control systems important to safety in nuclear power plants”, Safety Guide, March 2002.
4. IAEA Safety Standards Series No. NS-G-1.1, ”Software for Computer Based Systems Important to Safety in Nuclear Power Plants”, Safety Guide, September 2000.
5. IEC 61513 ”Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems”, First edition 2001-03.
6. IEC 60880 ”Software for computers in the safety systems of nuclear power stations”, First edition 1986.
7. IEC 60880-2 ”Software for computers important to safety for nuclear power plants – Part 2: Software aspects of defence against common cause failure, use of software tools and of pre-developed software”, First edition 2000-12.
8. IEC 60987 ”Programmed digital computers important to safety for nuclear power stations”, First edition 1989-11.
9. IEC 62138 ”Nuclear Power Plants – Instrumentation and Control – Computer-based systems important for safety – Software aspects for I&C systems of class 2 and 3”, Draft 2001.
10. IEC 60780 ”Nuclear Power Plants – Electrical equipment of the safety systems – Qualification”, Second edition 1998-10.