STUK

18. 03. 2009

G3263/88, G3263/86
G3263/83, G3263/80
G3263/75, G3263/65
G3263/60

Teollisuuden Voima Oyj
Olkiluoto
27160 Eurajoki

1. 3-2/JR/95, 30.5.2008
2. 3-2/JR/76, 18.12.2007
3. 3-2/JR/93, 13.5.2008
4. 3-2/JR/102, 29.8.2008
5. 3-2/JR/87, 9.4.2008
6. 3-2JR/71, 26.11.2007
7. G3263/21, G3263/30, 21.11.2007
8. 3-2/JR/58, 23.8.2007
9. G3263/8, 28.5.2007

OLKILUOTO 3 - REAKTORIN SUOJAUSJÄRJESTELMÄ (PS)

Säteilyturvakeskus (STUK) on käsitellyt viitteenä olevia Olkiluoto 3 ydinvoimalaitosyksikön reaktorin suojausjärjestelmää (Protection System, PS) koskevia Teollisuuden Voima Oyj:n (TVO) toimittamia asiakirjoja.

STUK esittää tarkastuksen perusteella seuraavat vaatimukset:

1. Suojausjärjestelmän PS vaatimusmäärittelyn käsittelyn jatkamiseksi vaatimusmäärittelyä ja suunnitteluvaatimusten laatua tulee parantaa ja korjata asianmukaiselle tasolle muun muassa seuraavilta osin:
   a) Suunnitteluvaatimusten tulee olla kattavat ja ne tulee kuvata yhtenäisenä asiakirjana tai asiakirjoina. Suunnitteluvaatimusten tulee sisältää suunnitteluperusteista (YVL-ohjeet, standardit, sopimus) ja konseptisuunnittelutason asiakirjoista johdetut yksikäsitteiset ja ristiriidattomat vaatimukset, joiden perusteella järjestelmä on toteutettavissa.
   b) Yksittäisten vaatimusten tulee olla verifioitavissa testaamalla tai analysoimalla. Vaatimukset tulee kuvata niin, että ne ovat kolmannen osapuolen arvioitavissa. Vaatimusten tulee olla jäljitettävät suunnitteluprosessin eri vaiheissa ja jäljitettävyys tulee osoittaa osana järjestelmän kelpoistusta.
   c) Päätöksen G332/69 (Plant Level I&C Architecture NLP-G/2008/en/1111; revision B) vaikutukset järjestelmään PS ja sen vaatimusmäärittelyyn tulee ottaa huomioon.
   d) Tulee harkita päivitetyn vaatimusmäärittelyn uutta riippumatonta arviota.

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) 7598 8500, +358 9 7598 8500

Viitteellä 1 tiedoksi toimitettu asiakirja NFLE DC 1096, rev.E täydentää kuvausta NGLEE/2005/en/1003 "System Description for the Control Rod Drive Power Supply System" ja asiakirja käsitellään erillään tästä PSn päätöksestä.

2. STUK on viitekirjeellä 2 toimitettujen toiminnallisten kaavioiden ja viitekirjeellä 3 toimitetun vika- ja vaikutusanalyysin tarkastuksessa havainnut, ettei reaktorisuojausjärjestelmä täytä N+2 vikakriteeriä kaikkien käynnistämiensä turvallisuustoimintojen osalta. Esittelymuistion kohdassa 2 on esimerkkejä suojausautomaation divisioonan menetykseen vaikuttavista vikamekanismeista ja sisäisistä tapahtumista.

   Suojausjärjestelmän PS tulee täyttää N+2 vikakriteeri seuraavasti: Suojausjärjestelmä on toteutettava siten, että se pystyy toteuttamaan tehtävänsä, vaikka mikä tahansa järjestelmän yksittäinen laite olisi käyttökunnoton ja vaikka mikä tahansa toinen saman järjestelmän tai sen toiminnan kannalta välttämättömän tuki- tai apujärjestelmän laite olisi samanaikaisesti poissa käytöstä tarvitsemansa korjauksen tai huollon vuoksi.

   Ohjelmistopohjaisessa automaatiotekniikassa on erityisesti otettava huomioon laitteen toiminnallisuuteen vaikuttavat ohjelmistot ja niiden vaikutus yllä esitetyn vaatimuksen täyttymiseen.

3. Toiminnalliset kaaviot (NFLE DC 1018) tulee korjata ottaen huomioon edellä esitetty vaatimus 2. Kaavioiden päivityksessä tulee lisäksi ottaa huomioon alla esitetyt vaatimukset a, b ja c:
   a) Toiminnalliset kaaviot eivät kaikkien toimintojen osalta vastaa toiminnallisia vaatimuksia (OL3 Functional requirements on P/S protection I&C functions NFPSR DC 1014 rev K ja OL 3 Functional requirements for the protection system - Core related NFPSC DC 1003 rev F). Ristiriitaisuudet (esimerkkejä esittelymuistiossa) tulee korjata.
   b) Toiminnallisissa kaavoissa on esitetty tietoja (esim. laskentaa ja viiveitä, esimerkkejä esittelymuistiossa), joita ei ole kuvattu toiminnallisissa vaatimuksissa. Säteilyturvakeskukselle tulee toimittaa selvitys siitä, mitä muuta kuin viiteluettelon dokumentteja on käytetty lähtötietoina kaavioiden laadinnassa.
   c) Suojaustoiminnon loppuunsaattamisen suunnitteluperusteen täyttävä ratkaisu tulee esittää päivitetyissä kaavioissa.

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) 7598 8500
+358 9 7598 8500

4. Vika- ja vaikutusanalyysi (NLE-F DC 10) tulee korjata vastaamaan edellä esitettyä vaatimusta 2. Sen lisäksi analyysin kattavuutta ja läpinäkyvyyttä suojausjärjestelmän PSn toteutukseen tulee parantaa siten, että tarkastelu sisältää myös

   a) kaikki laitteet ja komponentit, jotka ovat osallisena suojaustoiminnon toteutumisessa yksittäisohjaus- ja priorisointimoduuli (PAC) mukaan lukien päätöksen G3263/17 mukaisesti,

   b) suojaustoiminnon toteutumiseen vaikuttavien laitteiden ja komponenttien passiiviset viat edellä olevan vaatimuksen a) toimintoketjun laajuudessa,

   c) suojausjärjestelmälle PS tarkoitetut asiakirjan NFLE DC 1167 mukaiset keskusyksikön eri toimintatilat (käynnistys, testaus, diagnoosi, parametrointi) ja kaikissa toimintatiloissa tulee osoittaa N+2 vikakriteerin täyttyminen,

   d) kaikki suojausjärjestelmän PS tarvitsemat apujärjestelmät ja niiden vikaantumisen sekä vikojen korjauksen tai huollon vaikutukset PSn suojaustoimintojen toteutumiseen.

5. Reaktorisuojausjärjestelmälle PS mahdollisten huolto- ja korjaustoimenpiteiden vaikutuksista tulee toimittaa STUKiin tiedoksi seuraavat selvitykset:

   a) Kaikissa järjestelmän PS keskusyksiköiden eri toimintatiloissa (testaus, diagnosointi etc.), joissa edellytetään turvallisuusluokan 2 toimintojen käytettävyys, tehtäväksi tarkoitetut korjaus- tai huoltotoimenpiteet on esitettävä spesifisesti laitoksen OL3 järjestelmälle PS. Toimenpiteiden kohteet tulee tunnistaa tasolle, jolla toimenpiteillä ei enää ole vaikutusta järjestelmän PS turvallisuusluokan 2 toiminnon toteutumiseen. STUK on käsitellyt keskusyksikön toimintatiloja käsittelevän asiakirjan NFLE DC 1167 tiedoksi tulleena.

   b) On selvitettävä, miten jäähdytyksen menetyksen jälkeinen hidas lämpötilannousu ja siitä pitkällä aikaviiveellä mahdollisesti aiheutuvat virhetoiminnot on tunnistettu ja otettu huomioon järjestelmän PS vika- ja vaikutusanalyysissä.

   c) On esitettävä ne riippumattomuus- ja erotteluvaatimukset suojausjärjestelmän PS divisioonan sisällä ja yksittäisessä elektroniikkakaapissa, joita noudattaen on tarkoitus tehdä tarvittavia korjaus- tai huoltotoimenpiteitä heikentämättä laitoksen turvallisuutta.

6. Asiakirjassa NLE-F 08.1181 kuvataan validointilogiikan ratkaisumalli, jolla rajoitetaan vain ajallisesti mahdolliset haitalliset ohjaukset turvallisuusluokan 4 käyttöliittymäjärjestelmästä PICS turvallisuusluokan 2 reaktorisuojausjärjestelmään PS. Esitetty ratkaisu ei estä deterministisesti virheiden leviämistä alemmasta turvallisuusluokasta turvallisuusluokkaan 2. STUK ei hyväksy tällaista ratkaisua. STUK edellyttää, että vuorovaikutus TXP-laitealustan järjestelmistä reaktorisuojausjärjestelmään PS tulee estää yksisuuntaistamalla rajapinta fyysisin, ei ohjelmistoihin perustuvin keinoin.

7. STUK edellyttää, että reaktorisuojausjärjestelmälle PS tehdään asianmukaisen vaatimusmäärittelyn valmistuttua uudelleensuunnittelukierto järjestelmän turvallisuuden ja hyväksyttävyyden varmistamiseksi. Suunnittelukierron aikana järjestelmän dokumentaatio on saatettava asianmukaiselle laatutasolle siten, että dokumentaatio (esimerkiksi järjestelmäkuvaukset, toiminnalliset kaaviot, analyysit jne.) on virheetöntä, ristiriidatonta ja vastaa vaatimusmäärittelyä. STUKiin toimitettavan dokumentaation on yksiselitteisesti kytkeydyttävä järjestelmän PS jäädytettyyn suunnitteluversioon.

Päivitetty Olkiluoto 3 ydinvoimalaitosyksikön reaktorisuojausjärjestelmän vaatimusmäärittely tulee toimittaa STUKiin hyväksyttäväksi 30.4.2009 mennessä ja muu järjestelmän päivitetty dokumentaatio 30.5.2009 mennessä.

Johtaja Lasse Reiman

Ylitarkastaja Erik Lönnqvist

LIITE Esittelymuistio 16.03.2009, G3263/88, G3263/86, G3263/83, G3263/80 G3263/75, G3263/65, G3263/60

TIEDOKSI LR, MlJ, PT, KV, KW, MTu, AJu, IN, MaL, PSu, MjK, HTa, MKn, EL

EL/EL

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) 7598 8500
+358 9 7598 8500