Teollisuuden Voima Oyj
Olkiluoto
27160 Eurajoki

TVO:n hakemus 3-2/1/798, 25.3.2009

OL3 - AUTOMAATION ARKKITEHTUURIKUVAUKSEN PÄIVITYS

Säteilyturvakeskus (STUK) on käsitellyt Teollisuuden Voima Oyj:n (TVO) rakenteilla olevan ydinvoimalaitosyksikkö Olkiluoto 3 automaation arkkitehtuurikuvausta *Plant Level I&C Architecture*, NLP-G/2008/en/1111 (rev. C, 18.3.2009).

TVO toimitti asiakirjan edellisen revision B viitekirjeellä 3-2/1/748 STUKeen hyväksyttäväksi. Revisiossa B havaittujen puutteiden johdosta STUK esitti selvityspyynnön G332/69, joka sisälsi aineiston päivitysvaateen. Asiakirjan revisio C on TVO:n vastine päätökseen G332/69.

Käsittelyn jatkamiseksi STUK edellyttää, että asiakirjaa, sekä asiakirjan sisältöön välittömästi liittyvää aineistoa päivitetään seuraavien vaatimusten mukaisesti:

1. Automaatioarkkitehtuuritason suunnitteluun vaikuttavat vaatimukset tulee olla dokumentoituna aineistossa eksplisiittisesti ja selkeästi siten, että ne ovat suunnitellusta arkkitehtuurista myös verifioitavissa ja jäljitettävissä. Tämä tarkoittaa mm. sitä, että
   - Vaatimukset tulee nimetä (esimerkiksi numeroimalla) yksiselitteisesti
   - Varsinaiset tekniset suunnitteluvaatimukset on selkeästi erotettava teknisten suunnitteluvaatimusten johtamisessa käytetystä lähdemateriaalista ja esimerkiksi lähteissä esitetyistä yleisluontoisista lähdevaatimuksista
   - Vaatimuksessa tulee viitata yksiselitteisesti vaatimuksen lähteeseen sekä johdettaessa vaatimus ulkopuolisesta lähdemateriaalista että johdettaessa yksityiskohtaisempi suunnitteluvaatimus ylemmän tason yleisestä suunnitteluvaatimuksesta. Yksiselitteinen viittaus voidaan tehdä esimerkiksi numeroituun vaatimukseen, tai lähdemateriaaliin viitatessa lähteen yksilöityyn kohtaan/lauseeseen (paragraph)
   - Erityistä huomiota tulee kiinnittää luotettavuusteknologisia perusratkaisuja kuten moninkertaistamista, erilaistamista ja erottelua koskeviin vaatimuksiin.
   - Erityisesti riippumattomuusvaatimukset tulee esittää sillä yksityiskohtaisuuden tasolla, että ne ovat automaatioarkkitehtuurin

suunnittelusta myös verifioitavissa. Esimerkiksi automaatioarkkitehtuurin järjestelmien väliset riippumattomuusvaatimukset on esitettävä eksplisiittisesti, ts. muodossa "*instanssi A on oltava riippumaton instanssista B*", jossa instanssilla tarkoitetaan laitteista koostuvaa järjestelmää tai selkeästi määriteltyä järjestelmän osajärjestelmää. Mikäli toimintojen välistä riippumattomuutta halutaan käyttää argumenttina, tulee toimintojen väliset riippumattomuusvaatimukset esittää vastaavasti toimintokohtaisesti muodossa "*toiminnon A on oltava riippumaton toiminnosta B*".

Vaatimus 1 on täsmennetty versio STUKen lisäselvityspyynnön G332/69 vaatimuksesta 1.

2. Asiakirjan asiasisältö on varmistettava ja asiakirjan laatua on parannettava. Automaatioarkkitehtuurin suunnittelu on dokumentoitava asiakirjaan asianmukaisella tasolla, jotta laitoksen automaatioarkkitehtuurin turvallisuus ja suunnitteluvaatimusten toteutuminen voidaan dokumentaatiosta myös verifioida. Epätäsmällinen kielenkäyttö on poistettava asiakirjasta. Erityisesti perusratkaisujen taustalla oletettujen virhemekanismien tulee olla selkeästi eriteltyjä. Esimerkiksi, mikäli suunnittelussa käytetään vaillinaisia ratkaisuja (OL3 automaatioarkkitehtuurissa tilanne jossa riippumattomuutta ei varmisteta aidolla erottelulla, vaan käytetään järjestelmien välisen vuorovaikutusmekanismin osittaista kaventamista) tulee valittu ratkaisu perustella huolellisesti.

   Yksityiskohtaisempia esimerkkejä tarkastetun asiakirjan sisältämistä virheistä on esitetty esittelymuistiossa.

Vaatimus 2 on täsmennetty versio STUKen lisäselvityspyynnön G332/69 vaatimuksesta 2.

Hakemuksessaan TVO toteaa, että Olkiluoto 3 automaatioarkkitehtuuri ei täytä ohjeen YVL 5.5 luvun 3.5 kohtaa 2 järjestelmien PAS ja SAS rajapinnan osalta. Edelleen, hakemuksessaan TVO perustelee, että vastaava turvallisuustaso on saavutettavissa hakemuksessa esitetyin perustein. Hakemuksessa perusteita ei ole kuitenkaan esitetty sillä yksityiskohtaisuuden tasolla, että vastaavan turvallisuustason saavuttaminen olisi yksiselitteisesti todettavissa.

3. Mikäli automaatioarkkitehtuurin suunnittelu ei järjestelmien PAS ja SAS rajapinnan osalta täytä riippumattomuusvaatimusta, on poikkeama vaatimuksesta sekä huolellinen perustelu poikkeamalle kirjattava asiakirjan päivitettyyn versioon. Järjestelmien SAS ja PAS välinen riippumattomuusvaatimus on eksplisiittisenä vaati-

muksena dokumentoitava, vaikka suunnittelu ei kyseistä vaatimusta tällä hetkellä täyttäisikään.

Lisäksi

4. Poikkeaman merkitys ja seuraukset laitoksen turvallisuudelle on analysoitava sekä osoitettava, että vastaava turvallisuustaso voidaan saavuttaa vaikka järjestelmien SAS ja PAS välistä riippumattomuutta ei yksiselitteisesti voisi todeta. Analyysin ohessa on esitettävä myös, mitä alemman turvallisuusluokan järjestelmän PAS laadunvarmennusta parantavia toimenpiteitä (esimerkiksi lisätestaus) on suunniteltu vastaavan turvallisuustason saavuttamisen varmentamiseksi.

Lisäselvityspyynnössä G332/69 on esitetty vaatimus automaatiojärjestelmien välisten rajapintojen perustelujen dokumentoinnista. STUK toteaa, että tarkastetussa asiakirjassa ei ole esitetty rajapintojen perusteluita riittävällä tarkkuudella. TVO on esittänyt että tarkempi kuvaus perusteista esitetään automaation arkkitehtuuridokumentaatioon kuuluvassa, myöhemmin toimitettavassa yksityiskohtaisemmassa rajapintakuvauksessa. STUK hyväksyy TVO:n esityksen rajapintojen perustelun sisällyttämisestä rajapintakuvaukseen, mutta huomauttaa, että STUK ei ole toistaiseksi saanut käyttöönsä kyseistä rajapintakuvausta, eikä tämän takia pysty toistaiseksi arvioimaan rajapintojen hyväksyttävyyttä tai mahdollisia rajapintoihin kohdistuvia arkkitehtuurin muutostarpeita.

Vaatimusten 1-3 perusteella päivitetty aineisto tulee toimittaa STUKeen hyväksyttäväksi 31.7.2009 mennessä. Vaatimuksessa 4 esitetty analyysi toimenpidesuunnitelmineen tulee toimittaa STUKeen erillisenä asiakirjana hyväksyttäväksi 31.7.2009 mennessä.

KV

Ryhmäpäällikkö Keijo Valtonen

MjK

Tarkastaja Mika Koskela

Liitteet Esittelymuistio Mika Koskela, 18.6.2009.

Tiedoksi LR, MlJ, PT, KV, NL, MTu, KW, PSu, EL, MKn, HTa, MjK

MjK/MjK