13. 02. 2009

G332/69

Teollisuuden Voima Oyj
Olkiluoto
27160 EURAJOKI

3-2/1/748, 28.11.2008, Automaatiotekniikka

OL3 - AUTOMAATION ARKKITEHTUURI

TVO on viitekirjeellään toimittanut Säteilyturvakeskukselle hyväksyttäväksi Olkiluoto 3 laitosyksikön asiakirjan Plant Level I&C Architecture, NLP-G/2008/en/1111; revision B (15.11.2008).

Asiakirjassa havaittujen sisällöllisten ja laadullisten puutteiden takia yksityiskohtainen tarkastus tehdään vasta sellaiselle versiolle, jossa asiakirjan sisällöllistä ja laadullista tasoa on parannettu tämän päätöksen mukaisesti.

STUK edellyttää, että käsittelyn jatkamiseksi asiakirjaa tulee päivittää seuraavien vaatimusten mukaisesti:

1. Automaatioarkkitehtuuritason suunnitteluun vaikuttavat vaatimukset tulee olla dokumentoituna asiakirjassa eksplisiittisesti ja selkeästi siten, että ne ovat suunnitellusta arkkitehtuurista myös verifioitavissa ja jäljitettävissä. Erityistä huomiota tulee kiinnittää luotettavuusteknologisia perusratkaisuja kuten moninkertaistamista, erilaistamista ja erottelua koskeviin vaatimuksiin ja suunnittelupäätöksiin. Esimerkiksi automaatioarkkitehtuurin järjestelmien väliset riippumattomuusvaatimukset on esitettävä asiakirjassa eksplisiittisesti, ts. muodossa " *instanssi A on oltava riippumaton instanssista B"*, jossa instanssilla tarkoitetaan laitteista koostuvaa järjestelmää tai selkeästi määriteltyä järjestelmän osajärjestelmää. Perusratkaisujen taustalla oletetut virhemekanismit tulee olla selkeästi eriteltyinä. Erityisesti käytettäessä vaillinaisia ratkaisuja (esimerkiksi tilanteessa jossa riippumattomuutta ei varmisteta aidolla erottelulla, vaan käytetään järjestelmien välisen vuorovaikutusmekanismin osittaista kaventamista) tulee valittu ratkaisu perustella huolellisesti.

2. Asiakirjan asiasisältö on varmistettava ja asiakirjan laatua on parannettava.
   a) Virheet ja ristiriitaisuudet tulee poistaa. Esimerkiksi:
      - Liitteen 2 taulukon mukaan langoitetun varajärjestelmän suunnittelussa ei tarvitse huomioida seisokkitiloja. Väite poikkeaa aiemmin esitetyistä langoitetun varajärjestelmän suunnitteluperusteista. Langoitetun vara-

järjestelmän suunnittelussa on huomioitava seisokkitilat aihekohtaisen raportin TR64 (rev H) esittämällä tavalla.
- Toimintojen jako eri järjestelmiin tulee esittää yksikäsitteisesti.
- Rajapintojen olemassaolo tulee dokumentoida yksiselitteisesti.

b) Epätäsmällinen kielenkäyttö tulee poistaa ja asiateksti tulee korjata yksiselitteiseksi. Esimerkiksi: termien "adequate", "sufficient" ja "main" käyttöä tulee välttää, teksti purkaa joko yksiselitteiseksi tai viitata yksiselitteiseen määritelmään.

3. Asiakirjassa on kuvattava yleisellä tasolla järjestelmien välisten rajapintojen olemassaolon perusteet. Perusteista tulee käydä ilmi, miksi järjestelmien välillä on olemassa vuorovaikutusta. (Yksityiskohtainen rajapintojen dokumentointi yksityiskohtaisine informaatio/vuorovaikutussisältöineen suoritetaan nk. rajapintadokumentissa, joka on rooliltaan tarkastettua arkkitehtuuriasiakirjaa tarkentava asiakirja.)

Vaatimusten mukaisesti päivitetty asiakirja tulee toimittaa STUKiin hyväksyttäväksi 31.3.2009 mennessä.

Johtaja — Lasse Reiman

Ylitarkastaja — Erik Lönnqvist

LIITE Esittelymuistio G332/69, 12.2.2009

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