G332/55

Teollisuuden Voima Oyj
Olkiluoto
27160 EURAJOKI

OL3 - I&C TYÖPAJAKOKOUS ERLANGENISSA 23.-25.4.2008

Säteilyturvakeskus (STUK) on OL3 projektin automaatiosuunnittelun tarkastamisen yhteydessä tehnyt havaintoja, joista turvallisuuden kannalta merkittävimmät koskevat I&C arkkitehtuuritason automaatiosuunnittelua, automaation testausta ja tietoturvallisuussuunnittelua.

Tehtyjen havaintojen perusteella laitostoimittaja järjesti asiaan liittyvän kokouksen Erlangenissa 23 - 25.4.2008. Kokouksessa vahvistettujen havaintojen perusteella STUK on harkinnut tarpeelliseksi asettaa seuraavat vaatimukset:

1. I&C arkkitehtuuritason suunnittelun periaatteet on esitettävä suunnitteluohjeistossa. I&C arkkitehtuuritason kokonaissuunnittelulle on nimettävä selkeästi siitä vastaava organisaatioyksikkö ja yksikön vastuuhenkilö. Selvitys on toimitettava STUKiin tiedoksi 30.9.2008 mennessä.

2. I&C arkkitehtuuritason toteutus tulee kuvata asianmukaisessa asiakirjassa. Asiakirjan tulee sisältää (turvallisuusluokasta 2,3,4,EYT riippumatta) vähintään
   a) yksiselitteinen lista I&C arkkitehtuuriin kuuluvista järjestelmistä järjestelmien yleiskuvauksineen
   b) yksiselitteinen kuvaus I&C arkkitehtuurin ulkoisista rajapinnoista sekä rajapintojen yli kulkevasta informaatiosta sekä informaationkululle ja informaatiokulun rajoituksille asetetuista vaatimuksista
   c) yleiskuvaus I&C arkkitehtuurin järjestelmien välisistä rajapinnoista sekä rajapintojen sisältämistä informaatiosisällöistä. Eri järjestelmien rajapintojen minimointiperiaatteen vuoksi jokaisen rajapinnan olemassaolon peruste eli syy on oltava dokumentoituna selkeästi. (Rajapintojen yksityiskohtainen analyysi kohdentuu erilliseen asiakirjaan, ks. vaatimus n:o 3).

d) lista I&C arkkitehtuuritason osajärjestelmistä ja komponenteista, eli toiminnallisista yksiköistä joita ei ole selkeästi dokumentaatiossa kiinnitetty mihinkään yksittäiseen järjestelmään (esim. laitosväylä komponentteineen), tai jotka on kiinnitetty implisiittisesti useampaan järjestelmään (esim. TXP SU ja PU yksiköt).
e) selkeä kaaviokuva järjestelmien ja arkkitehtuuritason osajärjestelmien/komponenttien sijoittelusta eri turvallisuusluokkiin sekä turvallisuusluokkien välisistä erotuselimistä
f) selkeä kaaviokuva järjestelmien ja arkkitehtuuritason osajärjestelmien/komponenttien fyysisen sijoittelun riippuvuuksista (esim. boorikonsentraation mittausjärjestelmä on fyysisesti osa suojausjärjestelmää)
g) selkeä kaaviokuva OL3 I&C toteutuksen puolustuslinjoista ja järjestelmien sijoittumisesta eri puolustuslinjoihin

Kuvattu asiakirja ja vastine vaatimukselle on toimitettava STUKiin hyväksyttäväksi 30.8.2008 mennessä.

3. I&C arkkitehtuuriin kuuluvien järjestelmien väliset rajapinnat on analysoitava.
   a) Analyysin tulee sisältää kaikki I&C arkkitehtuuriin kuuluvat järjestelmät (ks. vaatimus n:o 2).
   b) Analyysin tulee sisältää signaalitason/informaatiosisältötason tarkastelu järjestelmien välisistä vuorovaikutuksista
   c) Analyysin tulee sisältää rajapinnalle asetetut vaatimukset koskien sekä sähköistä että tiedonsiirron rajoittamista. Tiedonsiirron osalta erityisesti yksisuuntaisuuden tai virheiden leviämisen estoa kuvaavat vaatimukset tulee kuvata.
   d) Analyysin tulee sisältää kuvaus rajapinnan toteutuksesta siten, että kuvauksesta ilmenee rajapinnan luonne kaikilla protokollapinontasoilla (esim. sähköinen/optinen, binääri/analogi/väyläyhteys, ylemmän tason protokollat etc.).
   e) Analyysin tulee sisältää lyhyt kuvaus rajapinnan testauksesta ja testauksessa käytetyistä menetelmistä, sekä viite asianmukaiseen testisuunnitelman testiin jossa rajapintaa testataan.
   f) Analyysissä on erityisesti huomioitava rajapintojen ja automaatioalustojen *implisiittisesti oletettu toiminta* sekä huomioidut virhemekanismit jotka on dokumentoitava selkeästi.

   Kuvattu asiakirja ja vastine vaatimukselle on toimitettava STUKiin hyväksyttäväksi 30.8.2008 mennessä.

4. Luvanhaltijan on selvitettävä Teleperm XS automaatioalustan tyyppihyväksyntäprojektista vastaavan ISTECin
   a) akkreditoinnit eri standardeja vasten
   b) sekä miten ISTECin toiminnan korkea laatu ja riippumattomuus on todennettu niiden teknologian osa-alueiden suhteen, joilta ISTEC ei ole akkreditoitu

Vastine vaatimukseen tulee toimittaa STUKiin tiedoksi 30.9.2008 mennessä. STUK tulee käsittelemään tyyppihyväksyntien sisältöä tyyppihyväksyntöjen ja soveltuvuusarvioiden saavuttua STUKin tarkastettavaksi.

5. Turva-automaatiojärjestelmän SAS
   a) tulee olla yksittäisvikasietoinen, kuten esimerkiksi asiakirja NLP-G/2006/en/1001 *Safety Automation System - Requirements Specification* asian esittää
   b) riippuvuus laitosväylästä ja laitosväylän toiminnasta eri tilanteissa on analysoitava ja dokumentoitava selkeästi
   c) eri toiminnallisiin puolustuslinjoihin kuuluvien toimintojen riippumattomuus on analysoitava ja dokumentoitava selkeästi

   Vastine vaatimukseen tulee toimittaa STUKiin hyväksyttäväksi 30.8.2008 mennessä.

6. Vakavien onnettomuuksien hallintajärjestelmä SA I&C
   a) on oltava erillinen ja riippumaton järjestelmä vakavien onnettomuuksien hallinnan puolustuslinjassa, kuten asiakirja TR105 kappale 2.3.3 asian kuvaa.
   b) on siten oltava myös erillinen ja riippumaton eri puolustuslinjaan kuuluvasta suojausjärjestelmästä PS ja suojausjärjestelmän osajärjestelmistä.

   Vastine vaatimukseen tulee toimittaa STUKiin hyväksyttäväksi 30.8.2008 mennessä.

7. Prosessiautomaatiojärjestelmän PAS ja turva-automaatiojärjestelmän SAS
   a) on toiminnallisesti eri puolustuslinjoissa olevina oltava riippumattomia järjestelmiä, kuten asiakirja TR105 ja PSAR asian kuvaa.
   b) välinen rajapinta on analysoitava ja toiminnalliset sekä fyysiset riippuvuudet tunnistettava ja dokumentoitava selkeästi
   c) yhteisten yksiköiden (esim. PU, SU etc.) toiminta vikatilanteissa sekä toiminta mahdollisena virhelähteenä on analysoitava ja dokumentoitava selkeästi

   Vastine vaatimukseen tulee toimittaa STUKiin hyväksyttäväksi 30.8.2008 mennessä.

8. Vaatimusmäärittelyt
   a) I&C arkkitehtuuritason ja järjestelmätason vaatimusmäärittelyjen tulee olla sillä tasolla, että laitoksen automaatio voidaan 60 vuoden eliniän aikana uusia jopa tilanteessa, jossa nykyisellä laitostoimittajalla ei ole taloudellista intressiä tai teknologista kykyä toimia automaatiouusinnan toteuttajana. Dokumentaation tulee olla sellaista, että automaation uusinta voidaan tarpeentullen suorittaa myös osissa.

b) Turvallisuusluokan 2 järjestelmien, turvallisuusluokan 3 TXS-pohjaisten järjestelmien ja järjestelmän SAS vaatimusmäärittelyille tulee suorittaa jäljitettävyysanalyysi. Analyysit tulee toimittaa STUKiin.

Vastine vaatimukseen tulee toimittaa STUKiin hyväksyttäväksi 30.10.2008 mennessä.

Johtaja Lasse Reiman

Tarkastaja Mika Koskela

LIITTEET Esittelymuistio, 1.7.2008, Mika Koskela

TIEDOKSI LR, PT, KV, TV, HTa, EL, SK, PSu, MTu, KW, RO, MjK

MjK/MjK