10. 04. 2014

Teollisuuden Voima Oyj
Olkiluoto
27160 EURAJOKI

TVO-STUK-10218, 6.5.2013

OL3 – Automaatioarkkitehtuurin suunnitteluaineiston päivitys

STUK on käsitellyt viitekirjeellä hyväksyttäväksi toimitetut asiakirjat Plant Level I&C Ar-chitecture, NLP-G/2008/en/1111 rev L, Allocation of I&C Functions, NLE-F DC 94 rev I ja I&C Architecture Interface Specification NLE-F DC 191 rev F, joissa esitetään OL3 laitosyksikön automaation arkkitehtuuri, toimintojen allokointi ja automaation rajapintojen määrittely. TVO:n viitekirjeen mukaan toimitettava aineisto muodostaa automaatioarkkitehtuurin laatusuunnitelman mukaisen automaatioarkkitehtuurin perussuunnitteluvaiheen (Phase 2) suunnittelun tulosaineiston. Aineisto koskee turvallisuusluokkia 2,3,4 ja EYT.

Muut viitekirjeellä toimitetut aineistot on käsitelty aiemmin erillisillä päätöksillä:

- Päätös 35/G43C00/2013 kattaa asiakirjat AD-02.02a I&C Decoupling Concept, NGLTC/2005/en/1003 rev H ja Technical Note – Answer to STUK Decision 2/G43C00/2011 NGLTC/2005/en/1003 I&C Decoupling Concept, Rev. F, TEHA task ID 80143; 80145; 80147; 80150; 80152

- Päätös 36/G43C00/2013 koskee asiakirjaa Constraints for Periodic Tests [AD-02.02c], NLE-F DC 39, Rev. F.

- Päätös 38/G43C00/2013 koskee asiakirjaa Concept for Detection of Loss of Computer-based I&C [AD.02.02i] PEL-G/2011/en/1002, Rev. C.

- Päätös 1/G43C00/2014 koskee asiakirjaa Concept for SICS inhibition in case of RSS Switchover [AD.02.02h] NLE-F DC 43, Rev. E.

- Päätös 2/G43C00/2014 koskee asiakirjaa Constraints for Failure Handling and Alarms [AD.02.02b] PELLL-G/2010/en/1009, Rev. D.

- Päätös 4/G43C00/2014 koskee asiakirjaa Concept for Reactor Trip [AD-02.02g] NFLE dc 1096 Rev. H.

STUK on käyttänyt tarkastuksessa tukena viitekirjeellä tiedoksi toimitettuja asiakirjoja TR E1037/2 - I&C CCF Analysis, Functional Part, rev D, I&C Architecture Preliminary Defence-in-Depth and Diversity Analysis [AD-02.04b], PEPR-F DC 131 rev A, Technical Note - Answer to STUK Decisions 10/G43C00/2009, 13/G43C00/2009, 16/G43C00/2009,

2/G43C00/2010 TEHA Task IDs: see page 4 ja Technical note - Answer to STUK Decision 8/G43C00/2011 OVERALL I&C ALLOCATION OF I&C FUNCTIONS TEHA task ID (91688; 91697; 91698; 91699; 91700; 91701). Viitekirjeessä esitetään useiden STUKin aiempien päätösten vaatimusten sulkemista.

- Päätöksen G332/55 vaatimus 2 arkkitehtuurin yksiselitteisestä kuvaamisesta voidaan sulkea.

- Automaatiotoimintojen allokointiraporttia koskevan päätöksen 8/G43C00/2011 kaikki vaatimukset (1-6) voidaan sulkea.

- Automaation arkkitehtuurikuvausta koskevasta päätöksestä 10/G43C00/2009, 13/G43C00/2009, 16/G43C00/2009, 2/G43C00/2010 esitetään suljettavaksi vaatimukset 1, 3-13 ja 16-32. Vaatimukset voidaan sulkea.

- Päätöksen G3263/88 vaatimus 6 TXP-laitealustaan pohjautuvien järjestelmien ja suojausjärjestelmän PS rajapintojen yksisuuntaistamisesta fyysisin, ei ohjelmistoihin perustuvin keinoin suljetaan, ja vaatimus toistetaan tässä päätöksessä tarkennettuna.

Automaation arkkitehtuuriin ja automaatiojärjestelmiin liittyvien suunnitelmien lisäksi luvanhaltijalta edellytetään turvallisuusanalyysejä, joiden tulokset varmentavat esitetyn suunnittelun vaatimustenmukaisuuden ja hyväksyttävyyden. STUK on esittänyt automaation vikaantumisen analysointia koskevia tarkentavia vaatimuksia päätöksellä 5/G43C00/2013. STUK voi arvioida automaation arkkitehtuurin hyväksyttävyyden lopullisesti vasta sitten, kun edellytettyjen vika-analyysien tulokset ja niiden johdosta mahdollisesti tehtävät muutos- ja täydennystarpeet laitosta koskeviin häiriö- ja onnettomuusanalyyseihin ovat selvillä.

STUK hyväksyy vaatimuksin asiakirjat Plant Level I&C Architecture, NLP-G/2008/en/1111 rev L ja I&C Architecture Interface Specification NLE-F DC 191 rev F siinä laajuudessa, kuin on ollut mahdollista automaation vikojen analysoinnin ollessa vielä kesken.

STUK on käsitellyt asiakirjan Allocation of I&C Functions, NLE-F DC 94 rev I tiedoksi tulleena. STUK hyväksyy esitetyt allokaatioperiaatteet, mutta liitettä A ei ole tarkastettu yksityiskohtaisesti.

Tarkastuksen perusteella STUK esittää seuraavat vaatimukset:

1. Vakavien onnettomuuksien hallitsemiseksi tarvittaville automaatiojärjestelmille ja niiden tukijärjestelmille on arkkitehtuuritasolla asetettava todellinen YVL-ohjeiden 1.0, 2,0 ja 5.5 mukainen riippumattomuusvaatimus. Asiaa on käsitelty myös päätöksessä 95/G42301/2012 ja yksityiskohtaisemmin sen esittelymuistiossa.

2. Muiden kuin ehkäisevän puolustuslinjan toimintoihin liittyvät SIC-Siltä tehtävät ohjaukset on voitava toteuttaa ehkäisevän puolustuslinjan automaatiojärjestelmien (SAS, PAS, TGI, RCSL tai PICS) vikatilanteissa.

3. SICS-paneelissa on oltava riittävät hälytykset automaatiojärjestelmien ja pääkäyttöliittymän sekä niiden välisen tiedonsiirron virhetiloista, jotta käyttökäsikirjan ohjeissa on mahdollista asettaa kriteerit SICS/HBS:n käyttöön siirtymiselle.

4. Väyläpohjaisen tekniikan kautta tapahtuva tiedonsiirto muista järjestelmistä tai laitteista suojausjärjestelmään (PS, PS-MSI, RPMS, PI, PS-QDS, PS SU) tulee estää yksisuuntaistamalla rajapinta fyysisin, ei ohjelmistoihin perustuvin keinoin.

5. Automaatiotoimintojen allokointiraportissa on toiminnallisten vaatimusten viitteissä useita vanhentuneita asiakirjojen revisioita, jotka on korjattava vastaamaan ajantasaista suunnittelua.

6. Primääripiirin paineenalennusventtiilien tai paineistimen varoventtiilien virheellinen avautuminen johtaa käytännössä luokan 2 oletettua onnettomuutta vastaavaan tilanteeseen, joten toiminnon ohjaaminen turvallisuusluokkaan 4 kuuluvasta PICS:stä ei ole hyväksyttävää. Venttiileiden ohjaus PICS:n kautta on poistettava.

7. STUK on hyväksynyt suojausjärjestelmän reaktoripikasulun diversifiointikonseptin rajoittumisen käyttöhäiriöihin ja yleisimpiin luokan 1 oletettuihin onnettomuuksiin (DBC3). On kuitenkin selvitettävä, millaisiin onnettomuuksiin reaktoripikasulun ensimmäisen signaalin puuttuminen luokan 1 muissa onnettomuuksissa ja luokan 2 onnettomuuksissa (DBC4) voisi johtaa.

Arkkitehtuurin suunnitteluaineisto on päivitettävä vaatimusten 1–2 ja 4–6 edellyttämällä tavalla. Päivitetylle suunnitteluaineistolle tulee saada STUKin hyväksyntä ennen arkkitehtuurin elinkaaren vaiheen 3 sulkemista.

Vaatimukset 1, 2, 3, 4 ja 6 on otettava huomioon järjestelmätason aineistoissa.

Vaatimuksen 7 edellyttämä selvitys on toimitettava STUKille tiedoksi 30.6.2014 mennessä.

Edellä esitetyistä vaatimuksista huolimatta STUK jatkaa automaatiojärjestelmiä koskevien asiakirjojen tarkastamista. Koska esitetyt vaatimukset voivat kuitenkin vaikuttaa automaatiojärjestelmien teknisiin asiakirjoihin, TVO:n on esitettävä niitä koskevissa saatekirjeissään arvio edellä esitettyjen vaatimusten vaikutuksista toimitettaviin asiakirjoihin.

Osoite/Address • Laippatie 4, 00880 Helsinki
Postiosoite/Postal address • PL/P.O.Box 14, FI-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

Apulaisjohtaja	TV Tapani Virolainen
Toimistopäällikkö	KW Kim Wahlström

Liitteet	Esittelymuistio 7/G43C00/2013, Mika Johansson, 10.4.2014
Jakelu	KiA, TV, ToR, KV, YTO-SAJ, YTO-REA, YTO-RIS, MTu

Osoite/Address • Laippatie 4, 00880 Helsinki
Postiosoite/Postal address • PL/P.O.Box 14, FI-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