ASAF Teemapäivä 3
Ydinvoimalaitosten automaatio

Viranomaisvalvonta ydinlaitosten automaatioprojekteissa

12.12.2011; Mika Koskela

STUK

Säteilyturvakeskus lyhyesti

- Pääjohtajana Jukka Laaksonen (1.2.2012 lähtien Tero Varjoranta)
- Henkilöstö ~ 350. Neljä isompaa osastoa, kolme pienempää yksikköä ja tukitoiminnot:
  - Ydinvoimalaitosten valvonta (YTO) ~ 110 henkilöä
  - Ydinjätteiden ja -materiaalien valvonta (YMO) ~ 30 henkilöä
  - Säteilyn käytön turvallisuus (STO) ~ 40 henkilöä
  - Tutkimus ja ympäristövalvonta (TKO) ~ 85 henkilöä
  - Tiedotus (4), Valmius (4), Asiakaspalvelut (7)
  - Tukitoiminnot (tietohallinto, talous- ja henkilöstöhallinto etc.) ~45
- YTO jakaantuu edelleen kolmeen ryhmään
  - Ydinlaitokset ja järjestelmät (YLJÄ)
  - Rakenteet ja laitteet (RALA)
  - Projektit ja käyttöturvallisuus (PROK)
- Sähkö- ja automaatiojärjestelmät toimisto osa YLJÄä
  - Toimistossa 12 henkilöä, päällikkönä Kim Wahlström

Ydinvoimalaitosten valvonnan säädöspohja

- Laki säteilyturvakeskuksesta (1983/1069), 1§:
  - *Säteilyn vahingollisten vaikutusten estämistä ja rajoittamista, säteilyn ja ydinenergian käytön turvallisuusvalvontaa sekä näihin liittyvää tutkimusta, koulutusta ja tiedottamista varten on sosiaali- ja terveysministeriön alainen säteilyturvakeskus.*
- Toiminnan runkona toimii Ydinenergialaki (1987/990)
- Ydinenergialakia täsmentävät Ydinenergia-asetus (1988/161) ja Valtioneuvoston asetukset
  - Ydinenergialain 7q §: *Valtioneuvoston asetuksella säädetään… yleiset turvallisuusmääräykset* => Nämä valtioneuvoston asetukset ovat osa lainsäädäntöä, joihin STUK pykälän mukaisesti esittää ehdotuksensa
  - Turvallisuusjärjestelmien kannalta keskeisin VNA 2008/733 ydinlaitosten turvallisuudesta
- Yksityiskohtaiset vaatimukset on esitetty YVL- ohjeissa
  - Ydinenergialain 7r §: *Säteilyturvakeskuksen tehtävänä on asettaa tämän lain mukaisen turvallisuustason toteuttamista koskevat yksityiskohtaiset turvallisuusvaatimukset.* (*… ja julkaista ne Säteilyturvakeskuksen määräyskokoelmassa*.)

Kansainväliset sidokset

- Edellä esitetyn säädöspohjan lisäksi ydinenergiaan liittyvään toimintaan vaikuttavat useat lait ja kansainväliset sopimukset. Turvallisuusjärjestelmien ja näihin liittyvien laitteiden kannalta edellä esitetyt ovat kuitenkin keskeisimmät.
- Erona esimerkiksi koneturvallisuusmaailmaan verrattuna on ohjaavan direktiivin luonne
  - direktiivi 2009/71/EURATOM on kirjoitettu erittäin yleisellä tasolla verrattuna esimerkiksi koneturvallisuusdirektiiviin 2006/42/EY
  - IEC TC45(a) standardeja on vahvistettu ja vahvistetaan EN- standardeiksi (harmonisoidut standardit)
- IAEA:n jäsenenä Suomi on sitoutunut toteuttamaan IAEA:n vaatimustason. Käytännössä IAEA- vaatimukset on sisällytetty YVL-ohjeiden vaatimuksiin.
- Lisäksi alalla voi törmätä muihin viitteisiin, esim. WENRAan (Western European Nuclear Regulators' Association)

Demonstraatiovelvollisuus

- Keskeistä säädöspohjaa:
  - Ydinenergialain 7f § (23.5.2008/342) mukaisesti luvanhaltija vastaa siitä että ydinlaitos rakennetaan ja sitä käytetään turvallisuusvaatimusten mukaisesti
  - Ydinenergialain 7e§ mukaisesti *Ydinlaitoksen turvallisuutta koskevien vaatimusten täyttyminen on osoitettava luotettavasti.*
  - VNA 2008/733 3§ mukaisesti *Jollei turvallisuusvaatimusten täyttyminen ole suoraan todettavissa ydinvoimalaitoksen suunnitteluratkaisusta, niiden täyttyminen on osoitettava*.
- Käytännön toiminnan kannalta tämä merkitsee seuraavaa:
  - Luvanhaltijan on demonstroitava järjestelmiensä/laitteidensa turvallisuus turvallisuutta valvovalle Säteilyturvakeskukselle
  - Jotta luvanhaltija pystyy demonstroimaan turvallisuuden, luvanhaltijalla on oltava riittävän yksityiskohtainen tieto teknisistä ratkaisuista
  - Etenkin ohjelmistopohjaisissa ratkaisuissa tämä tarkoittaa järjestelmätasolla sovellusohjelman ja tämän kehitysprosessin läpinäkyvyyttä, laitetasolla laitteen toimintaperiaatteen ja kehitysprosessin läpinäkyvyyttä
  - Tarve teknisen informaation luovuttamiselle tulee turhan usein yllätyksenä (kustannukset, toimitussopimusten sisältö)

Kelpoistaminen (qualification)

- Laitteiden ja järjestelmien puitteissa vuosikymmenien mittaan vakiintunut ”kelpoistaminen” aiheuttaa monesti hämmennystä. Verifioinnilla, validoinnilla ja kelpoistuksella on kuitenkin selkeä roolinsa, kun kurkistaa (varsin huonojen) virallisten määritelmien taakse miettimään terminologian taustalla olevaa ajatusmaailmaa
  - **kelpoistaminen** (**qualification**): *process of determining whether a system or component is suitable for operational use*. [IEC 61513 (2001), 3.45]
  - **qualification process**: *process to demonstrate the ability to fulfil specified requirements* [ISO 9000(2005), 3.8.6]
  - **verification** (**verifiointi, todentaminen**): *confirmation, through the provision of objective evidence, that specified requirements have been fulfilled* [ISO 9000(2005), 3.8.4]
  - **validation** (**validointi**, **kelpuutus**): *confirmation, through the provision of objective evidence (3.8.1), that the requirements (3.1.2) for a specific intended use or application have been fulfilled*
- Pelkkiin määritelmiin tuijottamalla nämä eivät aukea.

Kelpoistaminen (qualification) [2]

- Kuitenkin, jos katsotaan yhteisiä ja erilaisia piirteitä, niin huomataan:
  - Kaikki kolme ovat tavalla tai toisella vaatimuksenmukaisuuden arviointia: **tuotetta arvioidaan vaatimuksia vastaan**. Vaatimukset voivat olla joko eksplisiittisiä (verifioinnissa speksi), tai käyttötarkoitukseen liittyviä, implisiittisiä (validoinnin ”intented use”), joka sisältää myös mahdollisuuden vaatimusmäärittelyjen virheellisyyteen (huomaa linkki ohjelmistotekniikan määrittelyihin esim. wikissä!). Kelpoistaminen tapahtuu avointa, kolmannen osapuolen vaatimussettiä vastaan (esim. harmonisoitu standardi.)
- Toisaalta, kaikki tarkastelut liittyvät päätöksentekotilanteisiin
  - Verifiointi liittyy tuotteen työvaiheen (tai useamman) tulosten arviointiin työvaiheen syötettä (vaatimusmäärittely, speksi) vastaan, eli speksinmukaisuuteen. Tämä on toimittajan päätöksentekoprosessien kenttää.
  - Validointi liittyy tuotteen käyttötarpeen mukaisuuteen. Tämä on tuotteen tilaajan päätöksentekoprosessien kenttää.
  - Kelpoistus liittyy kriittisiksi katsottuihin tuotteisiin, joihin liittyvää päätöksentekoa on haluttu korostaa vaatimalla (käytännössä yhteiskunnallisella mandaatilla) tilaaja-toimittajaprosessista riippumattomien vaatimusten täyttämistä. Päätöksentekoprosessi on yhteiskunnalla, joka on voinut tehdä tästä eksplisiittisen (viranomaisvalvonta) tai implisiittisen (itsevalvonta, tarkastuslaitostoiminta).

Dokumentaation merkitys ja ”uhratut anturit”

- Edellä esitettyjen periaatteiden mukaisesti turvallisuus on siis osoitettava. Osoittaminen perustuu kelpoistusevidenssiin.
- Joissakin tapauksissa ongelmana on evidenssin saatavuus. Tämä johtuu pääasiassa kahdesta seikasta:
  - valmistaja ei halua antaa informaatiota hyväksyntäkäsittelyä varten
  - valmistajalla ei ole informaatiota annettavaksi hyväksyntäkäsittelyä varten (useimmin kehitysprosessin dokumentoimattomuus)
  - on selvää, että mikäli päätöksenteon tueksi ei ole objektiivista materiaalia, laitetta ei voi viranomaismielessä hyväksyä
  - käytännössä; joskus voi olla että ihan OK laitetta ei hyväksytä. ”Oikeusmurhaa” ei voi kuitenkaan estää, jos ”OK”:ta ei voi objektiivisesti todeta

YVL- ohjeisto

- Voimassaoleva YVL- ohjeisto koostuu 69 ohjeesta
  - SA- laitteiden ja järjestelmien kannalta keskeisimpiä
    YVL 5.5 *Ydinlaitosten automaatiojärjestelmät ja -laitteet*
    YVL 5.2 *Ydinlaitosten sähköjärjestelmät ja -laitteet*
  - YVL 1.4 *Ydinlaitosten johtamisjärjestelmät* sisältää yleisiä johtamisjärjestelmiin ja laatuun liittyviä vaatimuksia
- Ohjeiston uudistaminen on parasta aikaa käynnissä
  - kokonaisremontin tavoitteina yksittäisten ohjeiden lukumäärän pienentäminen (putoaa 41:teen) , rakenteen selkeyttäminen ja sisällön ajanmukaistaminen
  - SA- laitteiden ja järjestelmien kannalta keskeisimpiä tulevat olemaan
    B.1 Ydinlaitoksen turvallisuusjärjestelmien suunnittelu
    E.7 Ydinlaitoksen sähkö- ja automaatiolaitteet
    E.1 Tarkastus- ja testauslaitokset sekä sertifiointielimet
    A.3 Ydinlaitoksen johtamisjärjestelmät

YVL- ohjeiden ja standardien suhde

- Sähkö ja automaatiotekniikan YVL- ohjeet esittävät hyväksyntään vaadittavat minimivaatimukset. Järjestelmän tai laitteen tekniseen kehitykseen nämä eivät kuitenkaan ole riittävät, vaan tarvitaan yksityiskohtaisemmat suunnitteluvaatimukset esittävä standardipohja.
- Ydinenergialiiketoiminnan kansainvälisyydestä johtuen luvanhaltijalle (ja sitä kautta toimittajille) annetaan mahdollisuus valita soveltamansa standardit, joiden riittävyys arvioidaan
- Käytännössä em. TC45(a) standardit (etenkin EN- vahvistetut) luovat noudatettavan standardipohjan
- Sovelluskohteesta riippuen näitä täydennetään kehitystyössä/tarkastusreferensseinä usein vakiintuneilla yleisstandardeilla
  - Esim. ISO 10005 (laatusuunnitelmat), ISO 10007 (konfiguraationhallinta), ISO 27000 (tietoturvallisuus)

Turvallisuusluokitus

- Ydinlaitoksissa turvallisuusmerkityksen kategorisointi on toteutettu turvallisuusluokittelulla.
- Suomalainen turvallisuusluokittelu sisältää neljä turvallisuusluokkaa (1,2,3,4) ja luokan EYT (ei ydinteknisesti turvallisuusluokiteltu).
- Turvallisuuden kannalta merkittävin on TL1, johon kuuluvat mm. reaktoripaineastia ja primääripiirin keskeiset komponentit. Tässä luokassa ei ole aktiivisia turvatoimintoja (eikä näin ollen automaatiotakaan)
- TL2 kuuluu mm. reaktorin suojaustoiminnot toteuttava suojausjärjestelmä (automaatiota)
- TL3 kuuluu mm. erilaisia vähemmän kriittisiä turvallisuustoimintoja, toiminnot laitoksen ajamiseksi turvalliseen tilaan (=kylmäksi)
- TL2 ja TL3 järjestelmien lisäksi järjestelmien automaatiolaitteet tulee kelpoistaa. Luokkaan TL4 kuuluu järjestelmiä, joilla on turvallisuuden kannalta sekundääristä merkitystä, mutta joiden laitteita ei valvota

Keskeisimmät standardit

- IEC 61513: Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems
  - Järjestelmäkehitystä (ja automaatioarkkitehtuuria) koskevat yleiset vaatimukset
- IEC 60880: Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions
  - Cat A vaatimukset katsotaan riittäviksi turvallisuusluokkaan 2
- IEC 62138: Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category B or C functions
  - Cat B vaatimukset katsotaan riittäviksi turvallisuusluokkaan 3
- IEC 60987: Nuclear Power Plants - Instrumentation and control important to safety - Hardware design requirement for computer based systems
  - Cat A/B => TL2 ja TL3 laitteet/laitteistot

IEC 61508 rooli ydinlaitoksilla

- Kuten edellä todettiin, ydinlaitoksilla turvallisuusmerkityksen arviointi tapahtuu turvallisuusluokitteluprosessissa. Tämä on tietyssä mielessä analoginen prosessi IEC 61508 turvallisuustoiminnon eheysvaatimuksen löytämiseksi.
- Ero on se, että ydinlaitoksen turvallisuusluokittelu perustuu vakiintuneisiin (ja yleistasolla IAEA:n vahvistamiin) deterministisiin luokitusperiaatteisiin, ei todennäköisyyspohjaiseen riskiarviointiin.
  - Todennäköisyyspohjaisia menetelmiä (Probabilistic Risk Assessment, PRA) käytetään kokonaissuunnittelun arviointiin.
- Edellisestä johtuen suoraa relaatiota turvallisuusluokkien ja eheystasojen välillä ei varsinaisesti ole
  - Kaikesta huolimatta SIL- sertifikaatit ovat merkittävä kelpoistusevidenssi
- Reduntanttisuus ja diversiteetti arvioidaan osana laitoksen kokonaisarkkitehtuuria; vastaavaa mekanismia esim. yksittäisen mittauksen laatutason tiputtamiselle moninkertaistamisella ei ole.