



HANHIKIVI 1

Toiminnallisen turvallisuuden arviointi

ASAF teemapäivä: kokonaisturvallisuus
Insinöörit & Ekonomit –talo, Helsinki, 19.4.2018
Janne Peltonen, Fennovoima Oy

FENNOVOIMA

Fennovoima on suomalainen ydinvoimayhtiö,

joka tuottaa ilmastoystävällistä sähköä kotitalouksien ja teollisuuden tarpeisiin.



Omistajat:

- 66 % Voimaosakeyhtiö SF
- 34 % RAOS Voima

Investoinnin suuruus
6,5-7 miljardia euroa,
josta kotimaisen
investoinnin osuus
1,8-2,7 miljardia euroa

Työntekijöitä
nyt n. **350**
vuonna 2024 n. **500**



HANHIKIVI 1

FH1-ydinvoimalaitos
rakennetaan
Pyhäjoelle



Sähkäteho
1200 MW

Kolmannen
sukupolven
painevesireaktori

VVER-1200

Käynnistyy vuonna

2024



Ei aiheuta
kasvihuone-
kaasupäästöjä

Voimalaitoksen
käyttöikä on
vähintään

60 vuotta

FENNOVOIMA

Fennovoima rakentaa uutta
ydinvoimaa tuottaakseen
vakaahintaista sähköä
omistajilleen

Esittäjä

- Janne Peltonen
 - Automaation laadunhallinnan asiantuntija, Fennovoima Oy
 - DI (prosessitekniikka)
 - TÜV FS Eng, CISSP
 - Erikoisosaamisalueet laadun, turvallisuuden ja tietoturvallisuuden hallinta
 - Suomen ensimmäinen sertifioitu turva-insinööri
- Turva-automaatioprojekteissa mukana vuodesta 2001
 - Kattilalaitosten kattilasuojaus- ja poltinohjaus
 - Rautateiden turvalaitokset
 - Kemian teollisuuden hätöpysäytys
 - Koneiden ja kaivosteollisuuden hätöpysäytys
 - Ydinvoimalaitosten suojausjärjestelmät
- Kokemusta kaikkien em. alojen turvallisuusstandardien soveltamisesta

Määritelmiä

SFS-EN 61511-1

toiminnallisen turvallisuuden arviointi

(FSA, functional safety assessment)

todistusaineistoon perustuva selvitys yhden tai useamman turva-automaatiojärjestelmän ja/tai muiden suojauskerrosten saavuttaman toiminnallisen turvallisuuden päättelemiseksi

SFS-EN 61508-1:

8.1 Tavoite

Tämän kohdan vaatimusten tavoite on määrittää tarpeelliset toimet S/E/OE turvallisuuteen liittyvän järjestelmän/järjestelmien tai vaatimusten mukaisten nimikkeiden (esim. elementtien/alajärjestelmien) saavuttaman toiminnallisen turvallisuuden riittävyyden tutkimiseksi ja siitä ratkaisuun pääsemiseksi perustuen tämän standardin asiaankuuluvien kohtien noudattamiseen.

Mistä on kyse?

Homma on nyt valmis. Tarkistin lopuksi vielä kerran, että meni oikein.
En löytänyt mokia, mutta tulikohan nyt kaikki varmasti katsottua ja huomioitua.
Taitaa olla parasta, että pyydän vielä työkaveria tarkistamaan.

No hän tarkisti, mutta luottikohan se nyt kuitenkin liikaa, kun tietää, että olen
ennenkin tehnyt. Kysyin vielä, että mitä asioita hän nyt katsoikaan.
Työkaveri nauroi, että älä stressaa. Kyllähän se tarkastaja käy ne vielä läpi.

Tarkastajan testasi. Eihän siitä virheitä löytynyt, mutta ei hän nyt kyllä mitään
sellaista testannutkaan, mitä ei olisi jo muutenkin testattu.

Näinhän nämä on aina tehty ja viranomaisellekin on paperit kelvannut, mutta
kuka vastaa, jos jotakin kuitenkin jäi huomaamatta?

Turvallisuuteen liittyvä ohjausjärjestelmä

- Toteuttaa turvatoiminnot laitoksen turvallisen käytön varmistamiseksi
 - Tarvitaan sekä automaation että ihmisen toteuttamia turvallisuustoimenpiteitä
 - Varautuminen turvalliseen tilaan pääsemiseksi tulisi olla automaattinen
 - Laitoksen turvallisuus muodostuu prosessisuunnittelun, käyttöautomaation, turva-automaation ja henkilöstön toiminnan kokonaisuutena
- Turvallisuustason vaatimus vastaa riskin suuruutta
 - Muiden riskin vähentämismenetelmien soveltaminen laitossuunnittelussa tulisi olla ensisijainen varautuminen vaaroihin turva-automaatioon nähden
 - Ohjausjärjestelmälle asetettu vaatimustaso tulee perustua vaarojen ja riskien arviointiin, suojauskerroksien analyysiin ja turvatoimintojen määrittelyyn
 - Käyttöautomaatiolla on aina merkitys vaaratilanteiden ehkäisemisessä ja onnettomuustilanteiden hallinnassa
- Toimii vaaratilanteen edellyttämällä tavalla riittävällä varmuudella
 - Instrumentaatio, toimilaitteet ja tukijärjestelmät (ml. apuenergian syötöt) huomioitava
 - Fyysiset ja toiminnalliset rajapinnat muihin järjestelmiin ja laitteistoihin mahdollistavat odottamattomat toiminnot, vikojen leviämisen, tahattoman vaikuttamisen tai tahallisen manipulaation

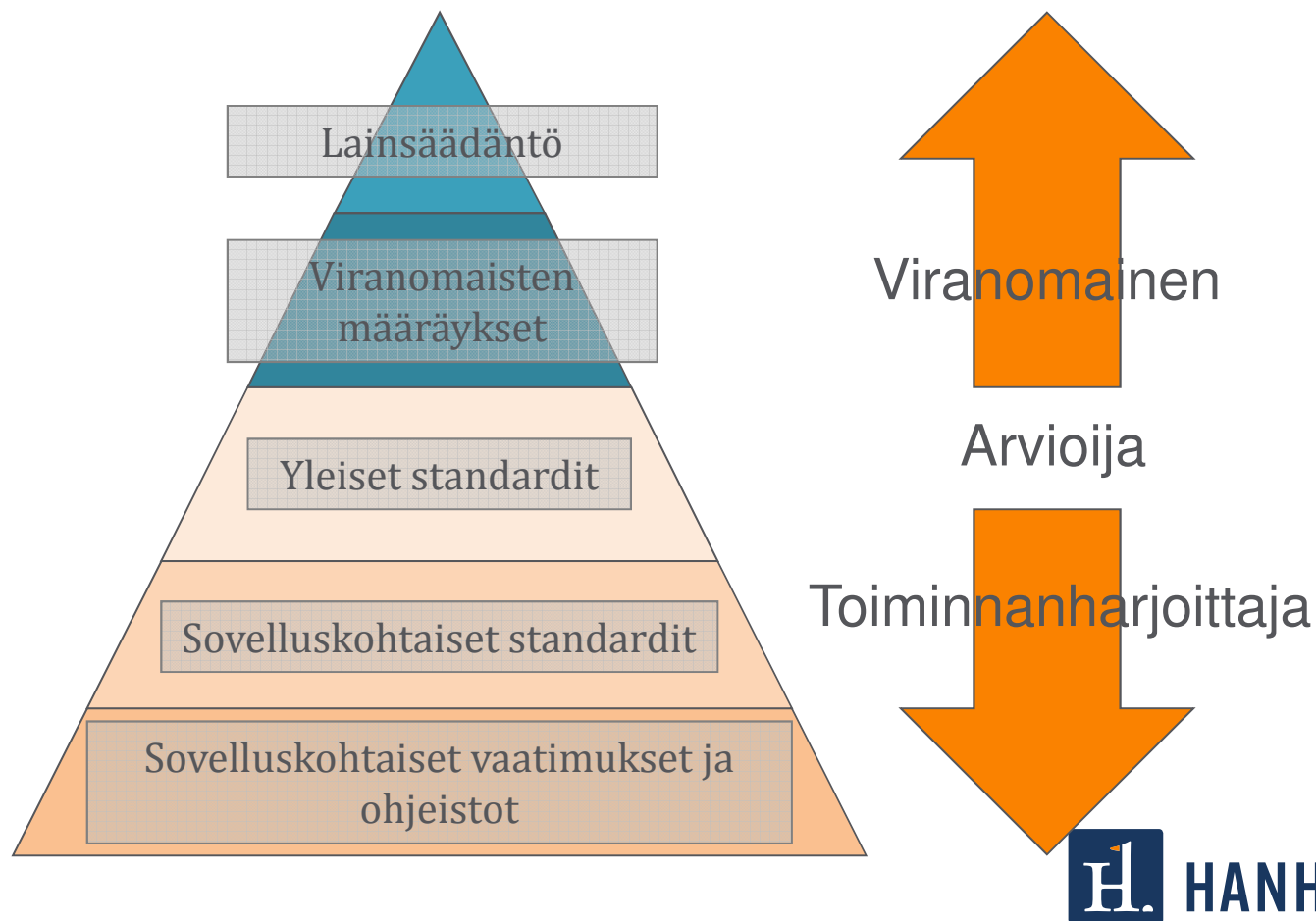
Ohjelmoitava turvallisuuteen liittyvä ohjausjärjestelmä

- Pelkkä laitteiston vikaturvallisuus tai vikasietoisuus ei riitä
 - Tarvitaan sekä ohjelmiston että laitteiston varmennuksia
 - Tuotekohtaiset ja sovelluskohtaiset turvallisuuskriittiset ohjelmistot
- Ohjelmakomponentit ovat turvallisuuden kannalta hankalia
 - Tehokas testaaminen edellyttää tilakäyttäytymisen, sisäisen rakenteen ja rajapintojen käyttötarkoituksen tuntemusta
 - Kerran toimivaksi testattu komponentti saattaa käyttäytyä eri tavalla eri alustalla tai erilaiseen ympäristöön integroituna
 - Ohjelmakomponentti on käyttäjälle usein täysin ”musta laatikko”
- Koko laitteiston ja ohjelmiston kelpuutus tai arviointi on loppukäyttäjälle täysin mahdoton tehtävä
 - Ohjelmointivirheiden peikko on aina taustalla

Turvajärjestelmien hyväksynnät

- Ohjelmoitavat, sähköiset ja elektroniset turvallisuuteen liittyvät laitteet ja järjestelmät hyväksytään kansainvälisten turvallisuusstandardien mukaisesti
- Vaatimustenmukaisuuden tarkastus ja arviointi sekä tyyppitarkastukset järjestelmille ja laitteistoille perustuen turvallisuusstandardeihin
 - IEC 61508, SIL1...SIL4 (kaikki sovellusalat)
 - IEC 61511, SIL1...SIL3 (prosessiteollisuus)
 - EN 62061, SIL1...SIL3 (koneturvallisuus)
 - ISO 13849, PL a...PL e (koneturvallisuus)
 - EN 50495, SIL1...SIL2 (räjähdysvaaralliset tilat)
 - EN 50129, SIL1...SIL4 (rautatiet)
 - IEC 61513/IEC 61226, Category A/B/C (ydinvoima)
- Ohjelmistojen hyväksyntään on erikseen erityiset alastandardit

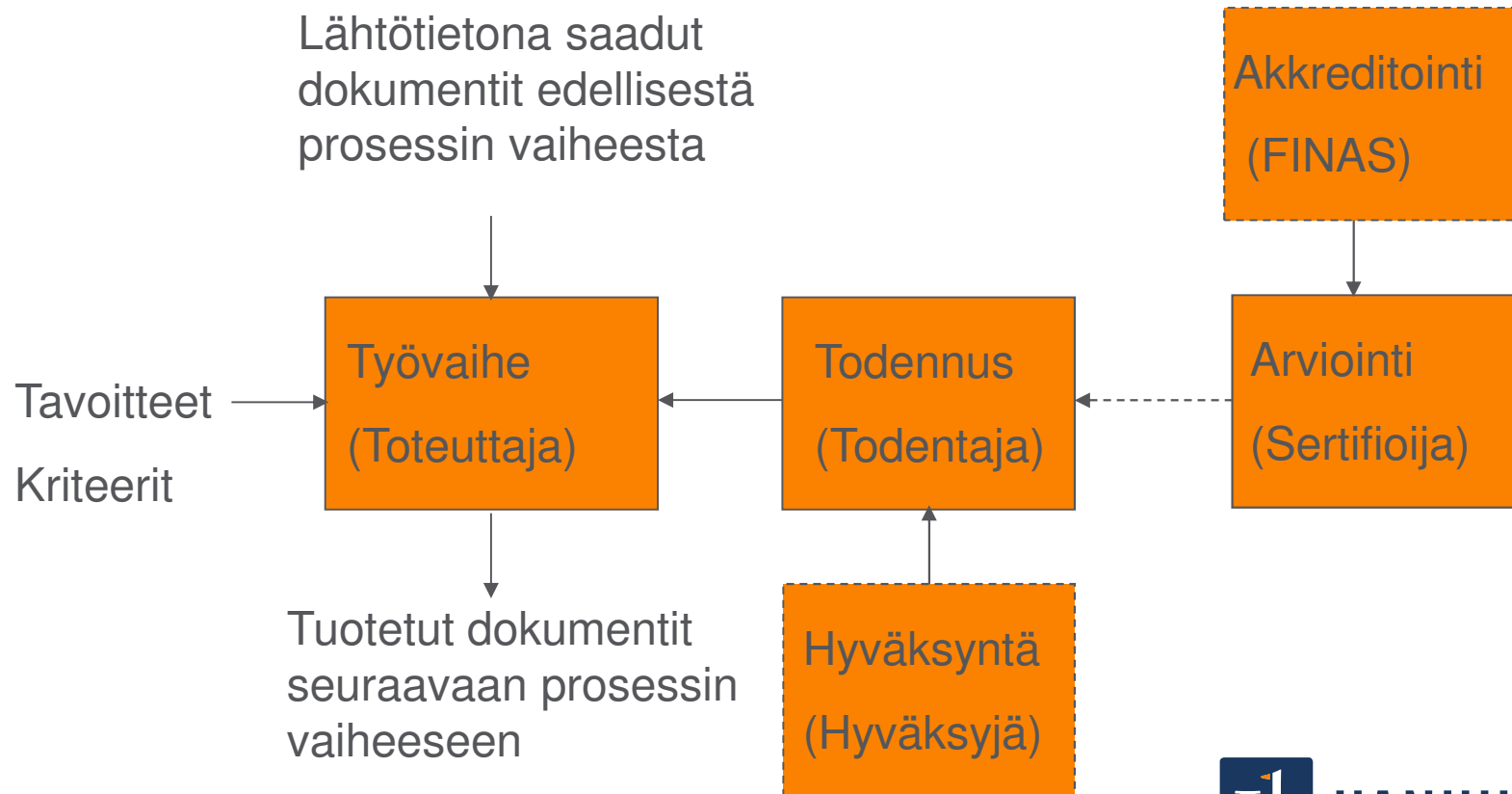
Vaatimusten hallinta



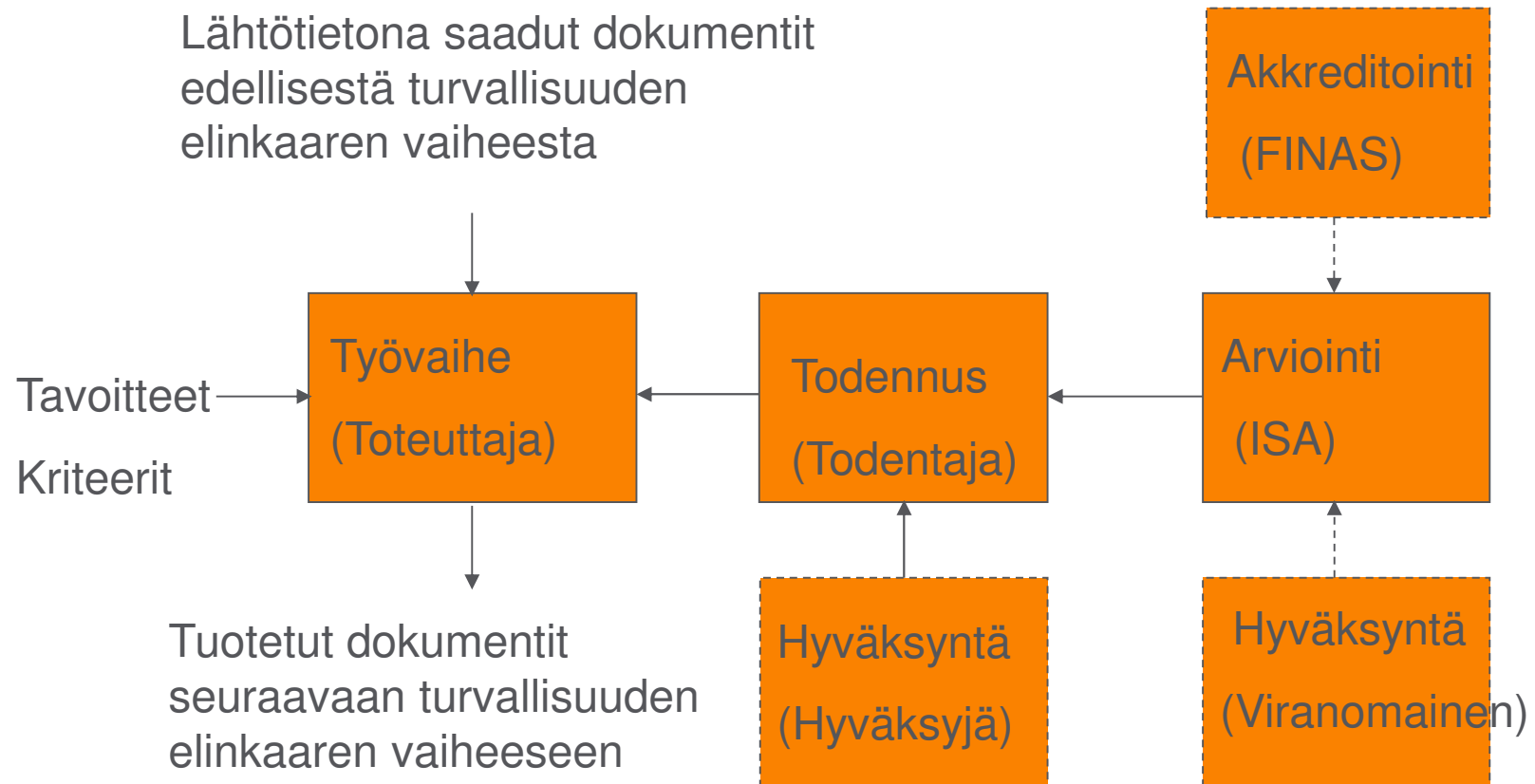
Turvallisuuden elinkaarimalli

- Turvallisuuden elinkaarimallia käytetään monimutkaisten kokonaisuuksien hallitsemiseksi ja vastuiden selkeyttämiseksi
- Turva-automaation määrittely, suunnittelu ja toteutus on jaettava vaiheisiin ja kontrollipisteisiin, joilla varmistetaan hallittu eteneminen
- Toiminnallisen turvallisuuden arviointi pelkästään lopullisia dokumentteja tarkastelemalla on hankalaa, mahdotonta tai kiellettyä
- Toiminnallisen turvallisuuden arviointi pelkästään turvallisuuteen liittyvän ohjausjärjestelmän toimintaa testaamalla ei anna riittävää luottamustasoa
- Eri vastuuorganisaatioiden väliset hallinnalliset ja tekniset rajapinnat on oltava ymmärrettävissä arvioinnin yhteydessä
- Hallintajärjestelmän toimivuus on arvioitava

ISO 9001 laatujärjestelmä



IEC 61508 turvallisuusjärjestelmä



Turvallisuusperustelut

- Turvallisuusperusteluja tarvitaan erilaisissa yhteyksissä
 - Laitteen tai koneen tyyppitarkastuksen yhteydessä teknisen asiakirjan tiedot riskinarvioinnista ja olennaisista terveys- ja turvallisuusvaatimuksista
 - Laitoskohtaisen ohjausjärjestelmän kelpuutus ja turvallisuustason osoittaminen
 - Komponentin, tuotteen tai järjestelmän ennalta tarkastus tai sertifiointi soveltuvaksi turvallisuuskriittiseen käyttöön
 - Laitoksen tai järjestelmän käyttöönottoluvan hakeminen turvallisuutta valvovalta viranomaiselta
- Turvallisuusperusteluissa on osoitettava vaatimustenmukaisuus ja turvallisuusperustelut on oltava ulkopuolisen arvioitavissa

Kattostandardin SFS-EN IEC 61508 toiminnallisen turvallisuuden arviointi

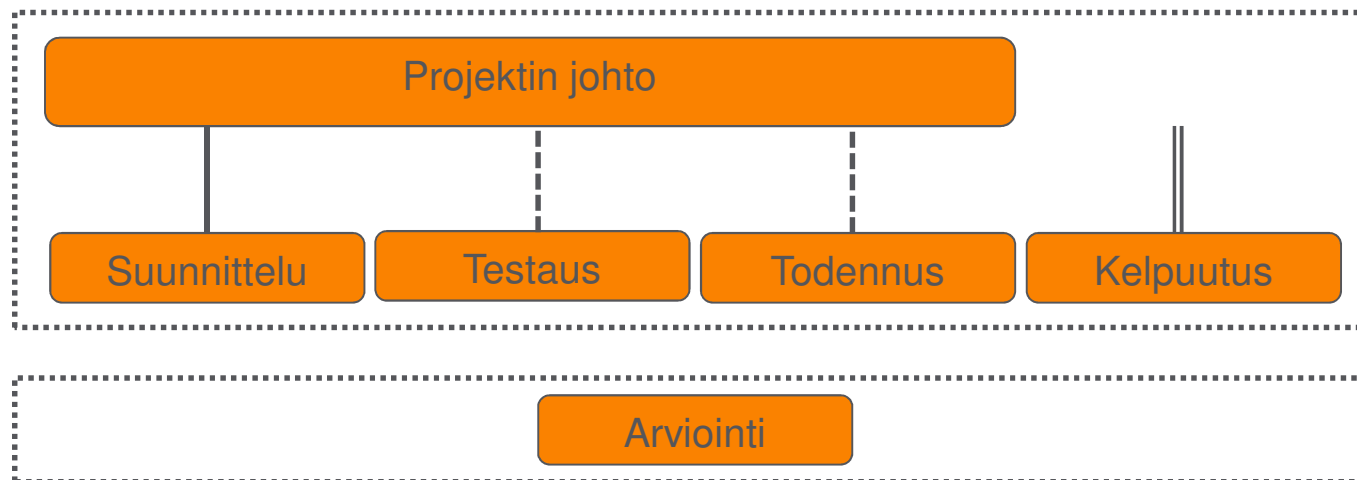
- Riippumattoman turvallisuusarvioijan on tehtäkseen päätelmän tuotteen tai järjestelmän turvallisuudesta huomioitava sekä turvallisuuteen liittyvä järjestelmä että sen kehittämisen ja toteuttamisen prosessit
- Riippumattoman turvallisuusarvioijan tehtäviin kuuluu mm.
 - Turvallisuusvaatimusten erittelyn ja turvallisuuteen liittyvien valmistajan vakuutusten tai aiempien todistusten tarkastus
 - Turvallisuus- ja laatuorganisaation ja niiden turvallisuusprosessien tarkastus (ml. auditoinnit)
 - Teknisen laajuuden tarkastus
 - Toiminnallisen turvallisuuden toteuttamistavan tarkastus

Riippumattomuus ja puolueettomuus

- Turvallisuuteen liittyvien ohjausjärjestelmien ja -laitteiden hyväksyntäprosessit edellyttävät riippumatonta ja puolueetonta tarkastusmenettelyä eturistiriitojen aiheuttamien riskien varalta
 - Riippumattomuuden aste riippuu riskin suuruudesta
 - Toteutusorganisaation ”ulkopuolisuus” ei takaa riippumattomuutta
 - Riittävän riippumattomuuden saavuttamiseen on lukuisia keinoja
- Riippumattomuutta voidaan edellyttää
 - Hyväksyjältä
 - Arvioijalta
 - Kelpoistajalta
 - Todentajalta
- Useilla toimialoilla käytetään ulkopuolista riippumatonta turvallisuusarvioijaa (Independent Safety Assessor, ISA)

Esimerkki – toteutusorganisaatio

- Riippumattomuusvaatimukset kohdistuvat tarkastusorganisaatioihin



— Rajoittamaton työn ohjaus

== Työn ohjaus ei sallittu

---- Määritelty työn ohjaus

..... Organisaatoraja



HANHIKIVI 1

Toimialakohtaiset erot

- Eri toimialoilla turvallisuusarvioinnille asetetaan erilaisia vaatimuksia lainsäädännön ja standardoinnin kautta
- IEC 61508 esittää toiminnallisen turvallisuuden arvioinnin riippumattomuuden vaatimuksen
- IEC 61511 esittää toiminnallisen turvallisuuden arviointiryhmän vaatimuksen
- Tietyillä toimialoilla riippumattoman turvallisuusarvioinnin suorittavalta organisaatiolta edellytetään akkreditointitodistusta osoituksena tehtävän mukaisesta pätevyydestä ja riippumattomuudesta
- Tietyillä toimialoilla riippumattoman arvioinnin, tarkastuksen ja kelpuutuksen tehtävät ja vastuut voivat olla huonosti määritelty, yhdistettyjä tai päällekkäisiä

Turva-automaatiojärjestelmän arvioija (TUKES-opas, turva-automaatio prosessiteollisuudessa, 2007)

- Prosessilaitoksen turva-automaatiojärjestelmän arvioijana voi toimia pätevyyksiensä mukaisesti tarkastuslaitos (ilmoitettu laitos, hyväksytty laitos) tai muu valmistuksesta riippumaton ja pätevä osapuoli.
- Vaatimustenmukaisuuden osoittamiseen liittyvät asiat tulee selvittää hyvissä ajoin, esim. miten ja kuka eri vaiheiden arviointeja tekee.
- Tilaaja tai toiminnanharjoittaja valitsee sovellusalueelle sopivan arvioijan, mutta on suositeltavaa, että valintaa tehtäessä ollaan yhteydessä vaatimustenmukaisuuden arvioinnista vastuussa olevaan tahoon. Siten voidaan välttää resurssitarpeiden päällekkäisyys ja varmennetaan menettelyn asianmukaisuus.

Turva-automaatiojärjestelmän arvioijan edellytykset (TUKES-opas, turva-automaatio prosessiteollisuudessa, 2007)

- Arvioijalta edellytetään:
 - hyvä tekninen ja ammatillinen koulutus, jota tarvitaan käytettävän teknologian arvioimiseen.
 - riittävät tiedot tehtävää koskevista vaatimuksista (esim. säädökset ja standardit) ja riittävä kokemus tällaisten arviointien suorittamiseen
 - vaadittu pätevyys laatia todistuksia ja raportteja, joilla todennetaan arviointien tulokset.

Mietelmiä

Mikä on soveltuva tai riittävä kokemus ”tällaisten arviointien suorittamiseen”?

Kokemus vastaaviin arviointeihin osallistumalla

VAI TARVITAANKO MYÖS

Kokemusta toimialan viranomaisvalvonnasta

Kokemusta toimialan tutkimustoiminnasta

Kokemusta toimialan laitoksien käyttö- ja kunnossapitotoiminnasta

Kokemusta automaatioprojektien hallinnasta

Kokemusta toimialan laitoksien toiminnallisesta suunnittelusta

Kokemusta toimialan laitoksien vaarojen ja riskien analysoinnista

Kokemusta automaatiojärjestelmien suunnittelusta

Kokemusta automaatiojärjestelmien asentamisesta

Kokemusta automaatiojärjestelmien käyttöönotosta

Kokemusta automaatiolaitteistojen tuotekehityksestä

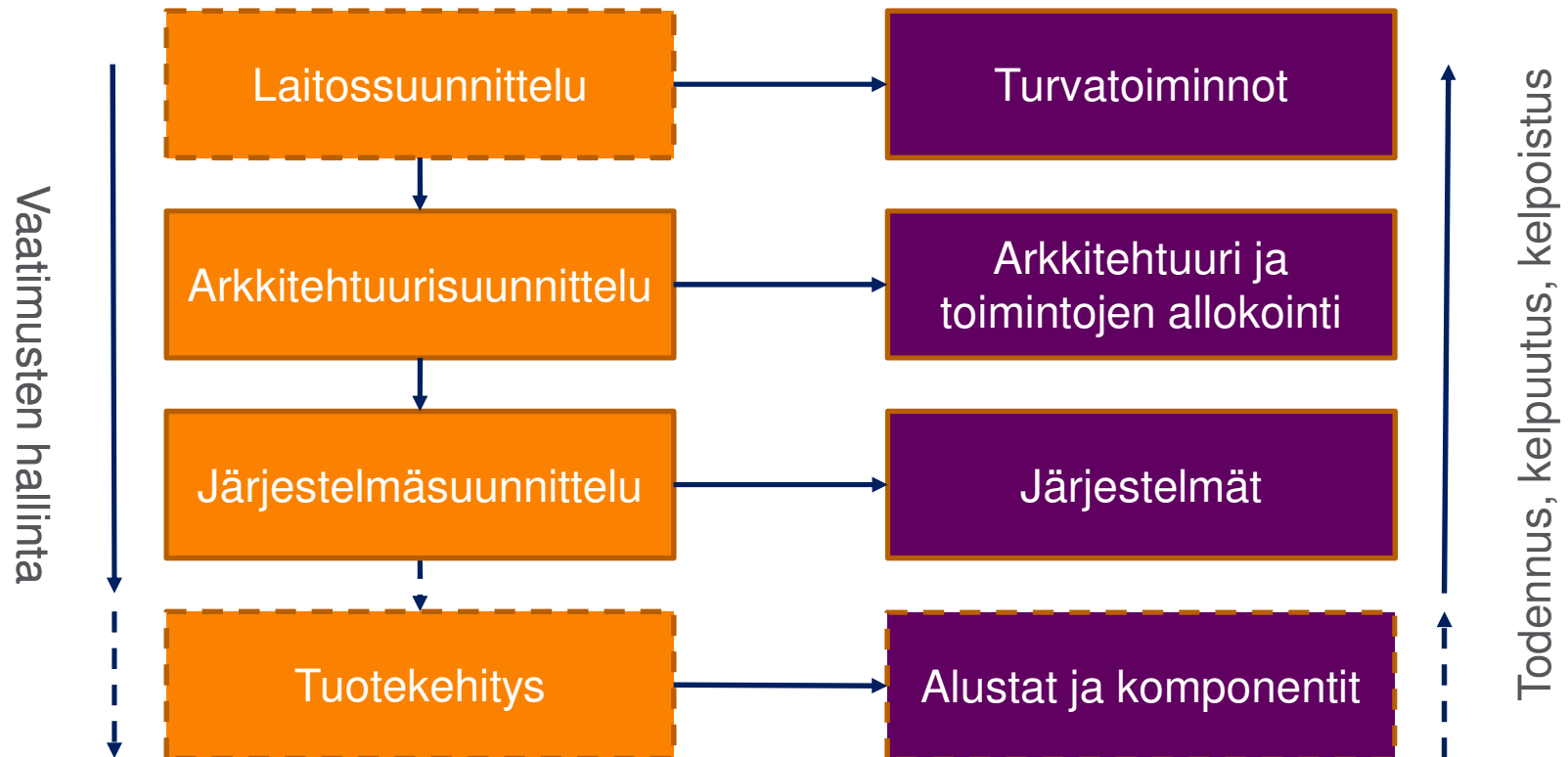
Kokemusta automaatio-ohjelmistojen kehittämisestä

jne.



HANHIKIVI 1

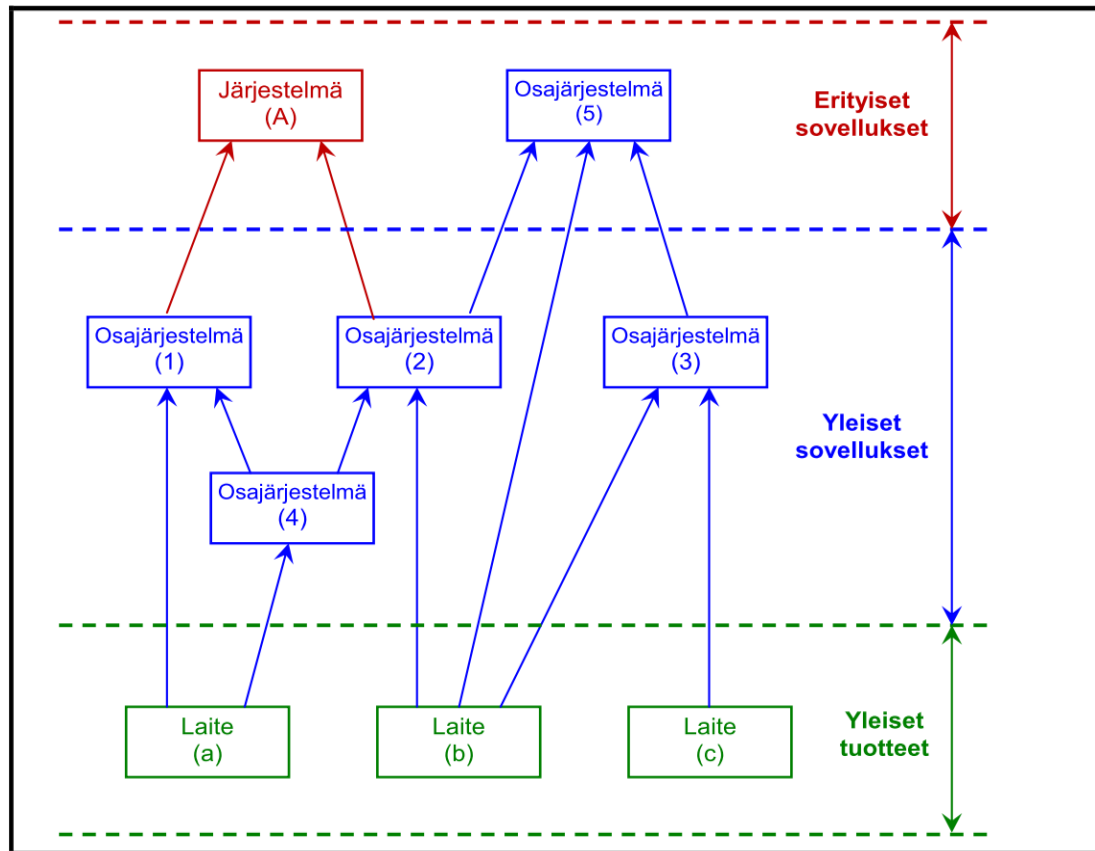
Turva-automaation suunnitteluprosessit ylhäältä alas



Arvioinnin laajuuden erot

- Toiminnallisen turvallisuuden arvioinnin laajuus tulee esittää arviointisuunnitelmassa
- Arvioinnin laajuus voidaan kohdistaa kolmelle eri päätasolle
 - Laitoksen prosessin ohjaus ja tarvittavien turvatoimintojen kohdentaminen eri järjestelmille (vaarojen arviointi ja suojauskerrosten riippumattomuusnäkökohdat)
 - Yksittäisen järjestelmän laitoskohtainen suunnittelu ja sovellusohjelmistot
 - Yleiset laitteistot, komponentit ja ohjelmistot, joita ei muuteta laitoskohtaisesti
- Arviointiraporteista tulee olla ymmärrettävissä, mitä arvioinnin laajuus ei kata

Tuotteistaminen ja hyväksyntä



Kuva:
ERA/GUI/02-
2008/SAF

Päätelmiä

Toiminnallisen turvallisuuden arviointi on luottamustehtävä, johon nimittäminen tulisi edellyttää selkeää suunnitelmaa, osoitettua riippumattomuutta ja pätevyyttä sekä kykyä laadukkaaseen raportointiin.

Toiminnallisen turvallisuuden arviointi on tehokkainta silloin, kun se perustuu vastaavan toteutusorganisaation selkeästi määrittelemään turvallisuuden elinkaarimalliin ja arviointi on vaiheistettu elinkaarimallin mukaisesti.

Toiminnallisen turvallisuuden arviointi on tehottominta silloin, kun vastaava toteutusorganisaatio ei ole toteuttanut vaatimusten hallintaa.

Toiminnallisen turvallisuuden arviointi ei voi käydä läpi kaikkia mahdollisia asioita, vaan arvioinnin tulee perustua laitoksen kokonaisturvallisuuden konseptiin ja vastaavien toteutusorganisaatioiden esittämiin loogisiin turvallisuusperusteluihin ja dokumentoituun näyttöön.



KIITOS!

HANHIKIVI 1