Suomen Automaatioseuran turvallisuusjaosto (ASAF)
Teemasarja
Toiminnallinen turvallisuus - standardisarja IEC 61508

Standardin IEC 61508-2 laitteistovaatimusten soveltaminen

VR Track Oy
Janne Peltonen
Insinöörit-ekonomit talo, Itä-Pasila, 17.10.2011

VR TRACK

Teemat

Standardin IEC 61508-2 rakenne ja uudistukset

Standardin IEC 61508-6 opastus

Arkkitehtuurit ja vaatimustenmukaisuuden reitit

Systemaattiset vikaantumiset

IEC 61508-2 : 2010 yleiskatsaus

- IEC 61508 Ed.2.0 : 2010 – SÄHKÖISTEN / ELEKTRONISTEN / OHJELMOITAVIEN ELEKTRONISTEN TURVALLISUUTEEN LIITTYVIEN JÄRJESTELMIEN TOIMINNALLINEN TURVALLISUUS – *Osa 2: Vaatimukset sähköisille / elektronisille / ohjelmoitaville elektronisille turvallisuuteen liittyville järjestelmille*
  - Kuva 1 – IEC 61508-sarjan kokonaisrakenne
  - Kappale 7 - S/E/OE järjestelmän turvallisuuden elinkaaren vaatimukset

- Velvoittava osa - Sähköisen / elektronisen / ohjelmoitavan elektronisen turvallisuuteen liittyvän järjestelmän vaatimukset
  - Liitteineen noin 90s. (Englanninkielinen teksti)
  - Velvoittavat liitteet A-E ja informatiivinen ASIC-liite F
  - Dokumentointi, toiminnallisen turvallisuuden hallinta ja arviointi - viite osaan IEC 61508-1
  - Ohjelmiston vaatimukset - viite osaan IEC 61508-3

IEC 61508-2 : 2010 uudistukset

- Nimikkeet
  - 7.2 S/E/OE järjestelmän suunnitteluvaatimusten erittely (E/E/PE system design requirements specification - aiemmin E/E/PES safety requirements specification)
  - S/E/OE järjestelmän kelpuutus/integrointi/yms. (aiemmin ilman järjestelmäpainotusta)

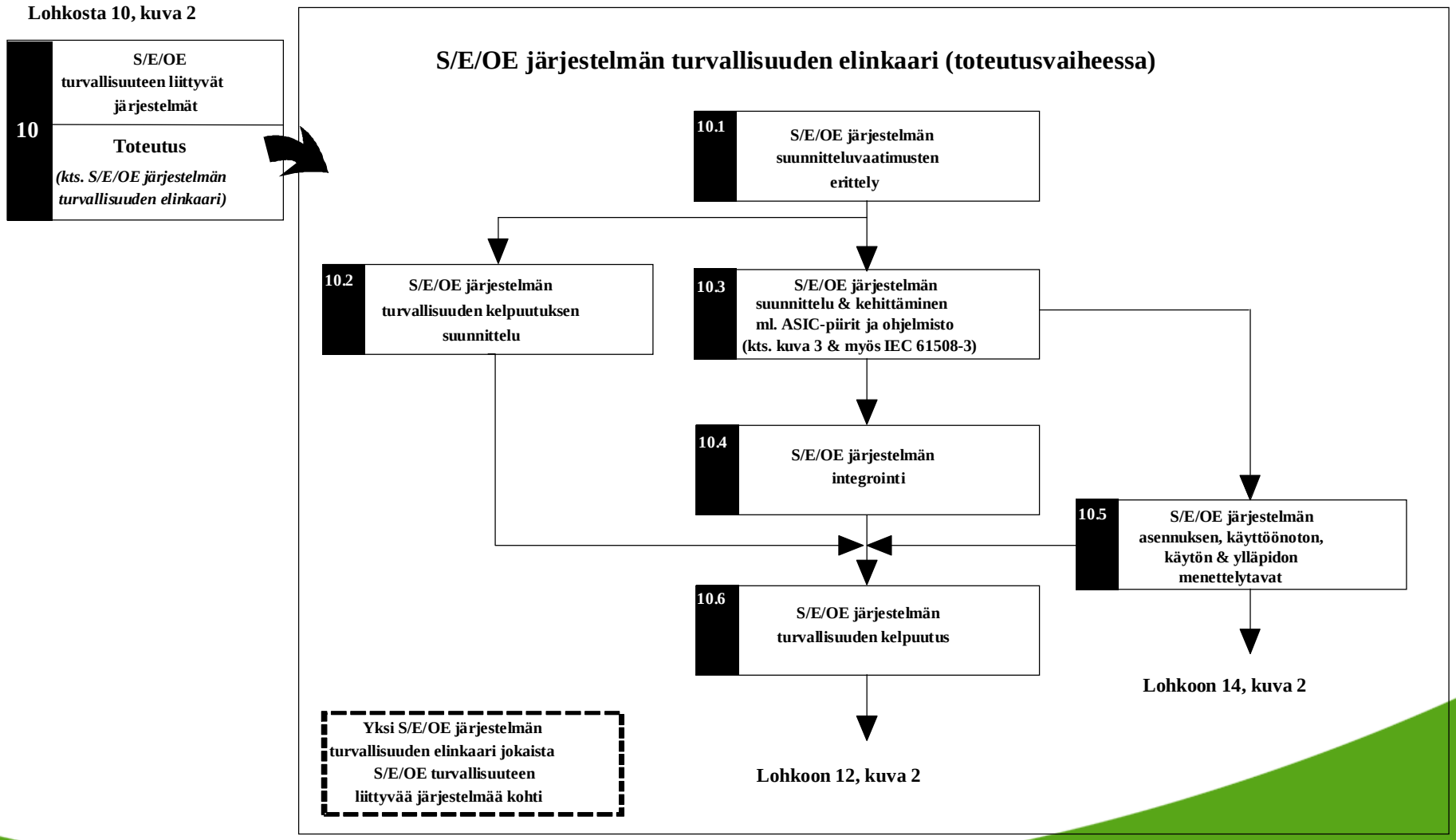
- Uudet liitteet
  - Liite D (velvoittava) Vaatimustenmukaisten tuotteiden turvallisuuskäsikirja
  - Liite E (velvoittava) Erityiset arkkitehtuurivaatimukset piirillä varmennetuille integroiduille piireille (IC-piirit)
  - Liite F (informatiivinen) Tekniikat ja toimenpiteet ASIC-piireille – systemaattisten vikaantumisten välttäminen

- Julkaistaan suomennettuna SFS-standardina 2011

IEC 61508-2 : 2010
Uudet velvoittavat standardiviitteet

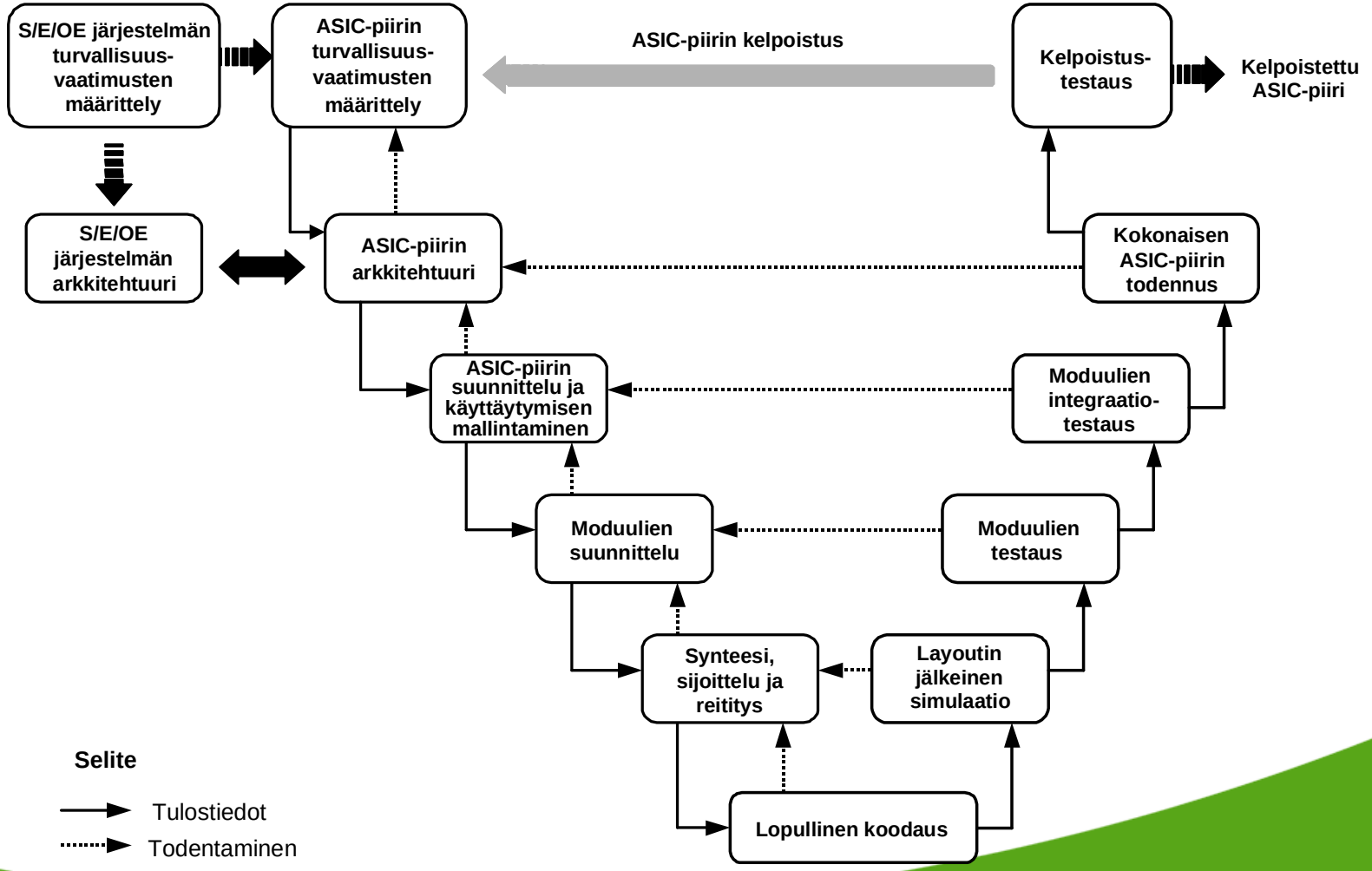
- IEC 60947-5-1, Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices
- IEC/TS 61000-1-2, Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena
- IEC 61326-3-1, Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications
- IEC 61784-3, Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions
- IEC 62280-1, Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems
- IEC 62280-2, Railway applications – Communication, signalling and processing systems – Part 2: Safety-related communication in open transmission systems
- EN 50205, Relays with forcibly guided (mechanically linked) contacts

IEC 61508-2 : 2010
S/E/OE järjestelmän turvallisuuden elinkaari



IEC 61508-2 : 2010 ASIC-kehityksen V-elinkaarimalli

- Uusi ASIC kehityksen V-elinkaarimalli ja liitteet – arkkitehtuuriset rajoitukset sekä tekniikat ja menetelmät



VR TRACK

IEC 61508-2 : 2010
Systemaattinen kyvykkyys (SC)

- Uusi käsite Systematic Capability (SC) - systemaattinen kyvykkyys
  - Käsitteellisesti lähes sama kuin systemaattinen turvallisuuden eheys (Systematic Safety Integrity)
  - SC N viittaa TET N systemaattiseen kyvykkyyteen

- Uudet reitit systemaattisen kyvykkyyden (SC) osoittamiseen
  - Route 1_s: standardin vaatimusten täyttäminen
  - Route 2_s: käytössä koettu (proven-in-use)
  - Route 3_s: vain ennalta kehitetyt ohjelmistot
  - Alaindeksi s viittaa systemaattiseen turvallisuuden eheyteen

IEC 61508-2: 2010
Arkkitehtuuriset rajoitukset

- Vaihtoehtoinen arkkitehtuuristen rajoitusten käsittely
  - Reitti 1_h: HFT ja SFF
  - Reitti 2_h: Minimi HFT ja komponenttien luotettavuusdata määritellyin kriteerein
  - Alaindeksi h viittaa laitteiston turvallisuuden eheyteen

- Reitti 1_h vastaa standardin edellisen version HFT/SFF konseptia sisältäen arkkitehtuuristen rajoitusten taulukot tyypin A ja tyypin B alajärjestelmille

- Reitti 2_h on uusi yksinkertaistettu konsepti sisältäen minimivaatimuksen HFT:lle
  - Reitti 2_h huomioi erityisesti myös tilanteen, jossa varmennuksen lisääminen johtaisi kokonaisturvallisuuden heikkenemiseen
  - Reitti 2_h asettaa täsmennetyt kriteerit käytetylle luotettavuusdatalle
    - tavoitteellinen vikaantumismitta (PFH tai PFD_{avg}) on saavutettava yli 90% luotettavuudella tai järjestelmää on parannettava
    - luotettavuusdata arvioidaan ja se perustuu samanlaisessa sovelluksessa sekä IEC 60300-3-2 tai ISO 14224 mukaisesti kerättyyn käyttö*palautteeseen*

IEC 61508-2 : 2010
Turvallisuuskäsikirja

- ’Turvallisuuskäsikirja vaatimustenmukaisille tuotteille’ vaatimukset
  - määritellään turvallisuuteen liittyvät tiedot, jotka käyttäjän on saatava
  - ennalta kehitettyjen ohjelmistojen osalta IEC 61508-3 esittää lisävaatimuksia
  - jos turvallisuuden arviointi estyy tietojen saatavuuden takia, standardin vaatimuksia ei täytetä!

- Vaatimukset parantavat loppukäyttäjien asemaa
  - kaikkien toimittajien on esitettävä täsmennetyt turvallisuuteen liittyvät tiedot väittäessään tuotteen olevan IEC 61508 vaatimusten mukainen
  - todistamattomat väitteet elementtien osalta eivät auta turvatoiminnon eheyden perustamisessa

- Uusi velvoittava liite D määrittelee tiedot, jotka tulee käsitellä käsikirjassa itse tuotteen ja tuotteen toteuttamien toimintojen osalta

IEC 61508-2: 2010
Turvaväylien lisävaatimukset

- Vikaantumismitta (esim. jäännösvirhetaajuus) arvioitava turvaväylän ollessa osa turvatoimintoa huomioiden kommunikointiprosessin tunnetut virhemekanismit (esim. naamioituminen, korruptoituminen)

- Turvaväyläliikenteen vaatimuksiin esitetään Black Channel / White Channel näkökohdat

- Velvoittavat viitteet turvaväylästandardeihin
  - IEC 61784-3 - Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions
  - IEC 62280-1 Ed. 1.0 Railway applications - Communication, signalling and processing systems - Part 1: Safety-related communication in closed transmission systems
  - IEC 62280-2 Ed. 1.0 - Railway applications - Communication, signalling and processing systems - Part 2: Safety-related communication in open transmission systems

IEC 61508-2 : 2010
Tekniikat ja menetelmät

- Tekniikat ja menetelmät pysyneet pääpiirteissään ennallaan
  - Taulukko A.16 ympäristörasitusten tai -vaikutusten aiheuttamien systemaattisten vikaantumisten ehkäisemiseksi esitetään oikosulku/johdinkatkodiagnostiikkaa ja lepovirtaperiaatetta

- Uudet ASIC tekniikat ja menetelmät liitteessä F
  - Table F.1 Techniques and measures to avoid introducing faults during ASIC's design and development – full and semi-custom digital ASICs
  - Table F.2 Techniques and measures to avoid introducing faults during ASIC design and development: User programmable ICs (FPGA/PLD/CPLD)
  - Yksikään menetelmä tai tekniikka ei ole pakollinen (M)

IEC 61508-2 : 2010
Varmennuksia sisältävät integroidut piirit

- Velvoittavassa liitteessä E esitetään erityiset arkkitehtuuria koskevat vaatimukset integroiduille piireille

- Vaatimukset koskevat integroituja piirejä, jotka käyttävät piirin sisäisiä varmennuksia HFT kasvattamiseksi, esimerkiksi:
  - yksittäinen integroitu piiri korkeintaan TET 3 sovelluksiin
  - vaatimukset koskevat vain digitaalisia integroituja piirejä
  - systemaattinen kyvykkyys ei kasva varmentamalla
  - korkean lämpötilan tai virransyötön aiheuttama yhteisvikaantuminen on huomioitava
  - vaatimuksia piirin fyysiselle rakenteelle ja kytkennöille
  - TET 3 erityisvaatimukset
  - integroidulle piirille arvioitava $\beta_{B\text{-}IC}$-kerroin pisteytystaulukon avulla ($\beta_{B\text{-}IC}$-kerroin parhaimmillaan 25%)
  - yms.

VR TRACK

IEC 61508-2 : 2010
ASIC-piirit

- Informatiivisessa liitteessä F esitetään sovelluskohtaisille integroiduille piireille tekniikat ja menetelmät systemaattisten vikaantumisten välttämiseksi

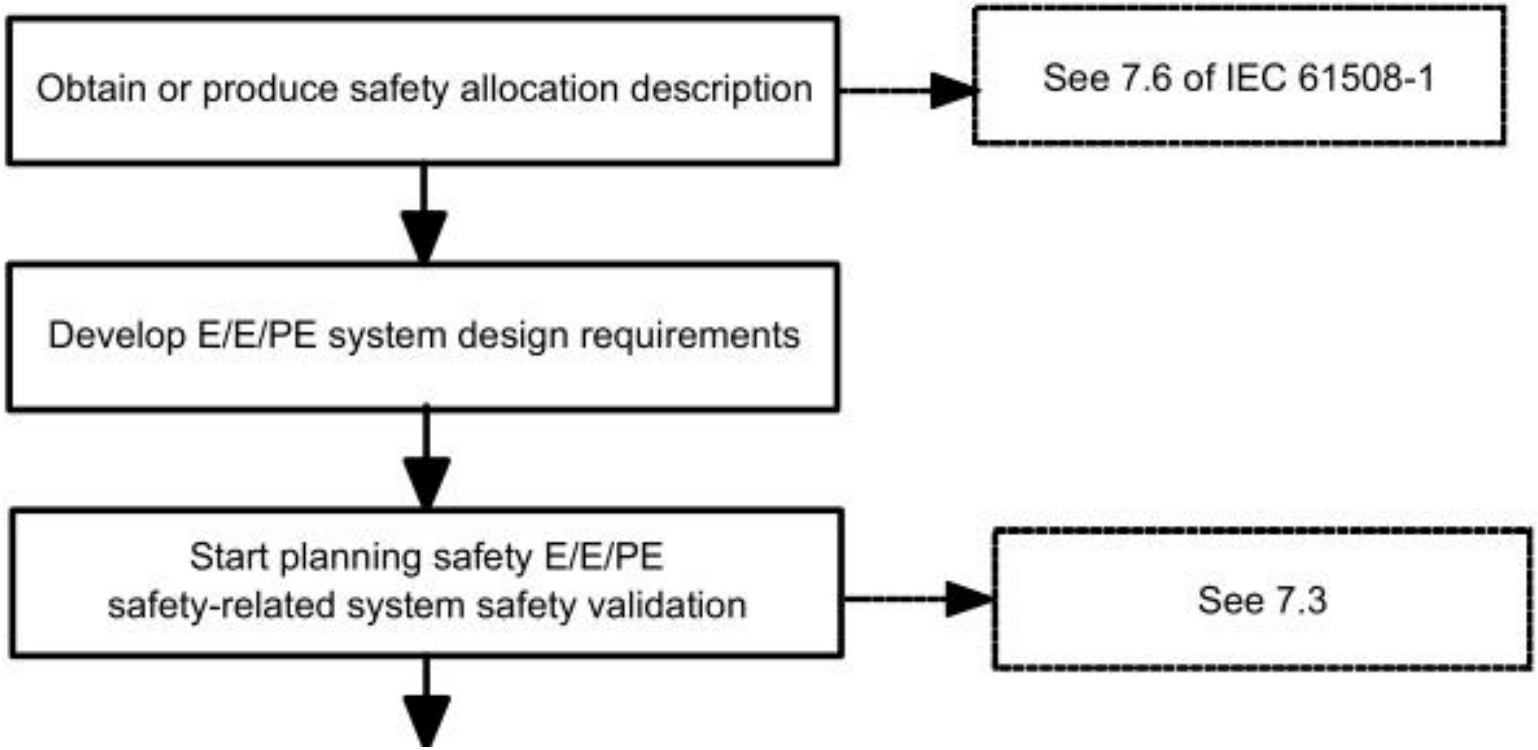
- Suosituksina esitetään esimerkiksi:
  - toiminnalliset simulaatiot järjestelyineen tulisi dokumentoida
  - tulisi käyttää vain käytössä koeteltuja työkaluja, kirjastoja ja valmistusmenettelyjä
  - kaikki toimet ja niiden tulokset tulisi todentaa
  - suunnittelun toteutusprosessin toistettavuuden ja automatisoinnin mahdollistavia menetelmiä tulisi käyttää
  - kolmannen osapuolen kovissa ja pehmeissä ytimissä tulisi käyttää vain kelpuutettuja makrolohkoja
  - yms.

IEC 61508-6 : 2010
Yleiskatsaus

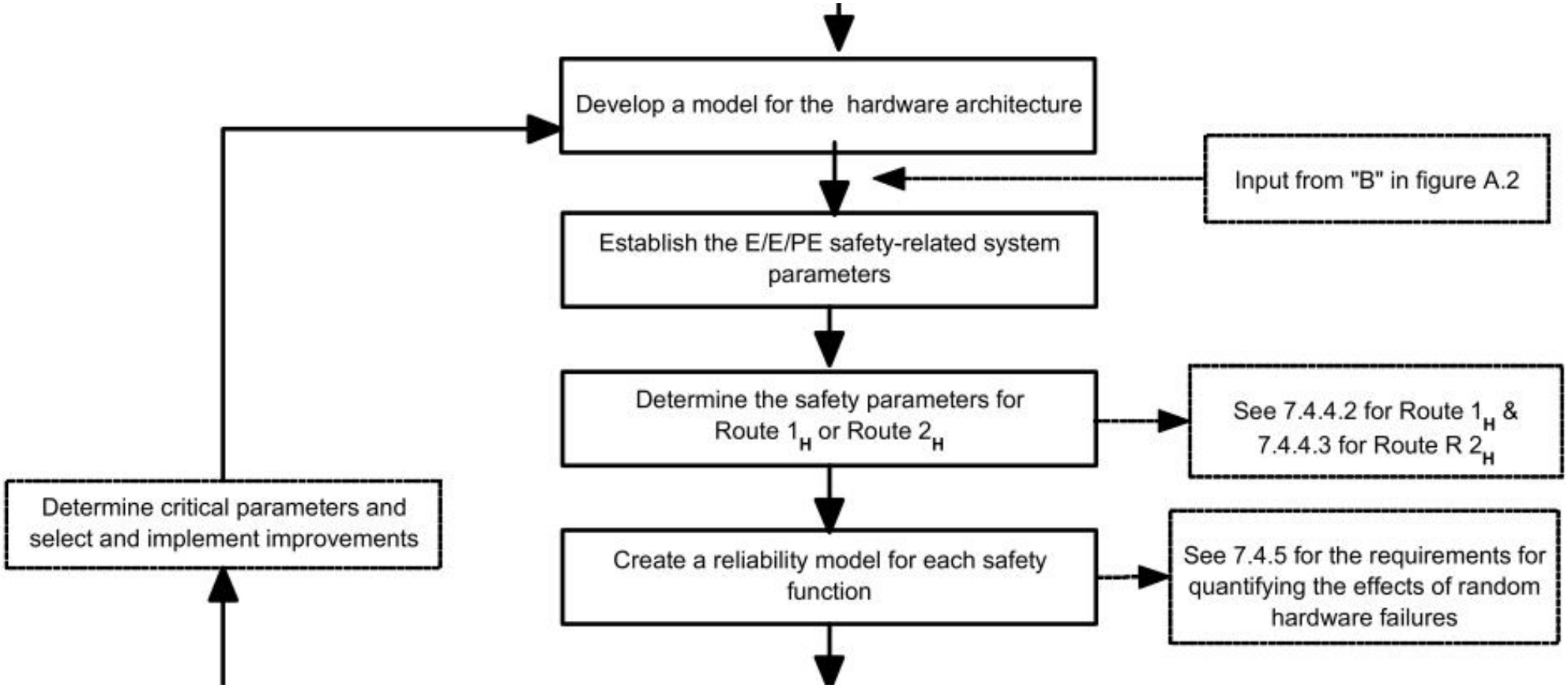
- IEC 61508-6 Ed. 2.0 : Functional safety of electrical / electronic / programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3

- Informatiivinen osa - Soveltamisohjeet sähköisen / elektronisen / ohjelmoitavan elektronisen turvallisuuteen liittyvän järjestelmän toteuttamiseksi IEC 61508 standardin osien 2 ja 3 mukaisesti
  - Liitteineen noin 110s. (Englanninkielinen teksti)
  - Liite A - IEC 61508-2 ja IEC 61508-3 soveltaminen
  - Liite B - esimerkki tekniikasta laitteiston vikaantumisen todennäköisyyden arvioimiseksi
  - Liite C - esimerkki diagnostiikan kattavuuden ja turvallisten vikaantumisten osuuden laskemisesta
  - Liite D - menetelmä yhteisvikaantumisten käsittelemiseksi
  - Liite E – esimerkkejä IEC 61508-3 ohjelmiston turvallisuuden eheyden taulukoiden soveltamisesta

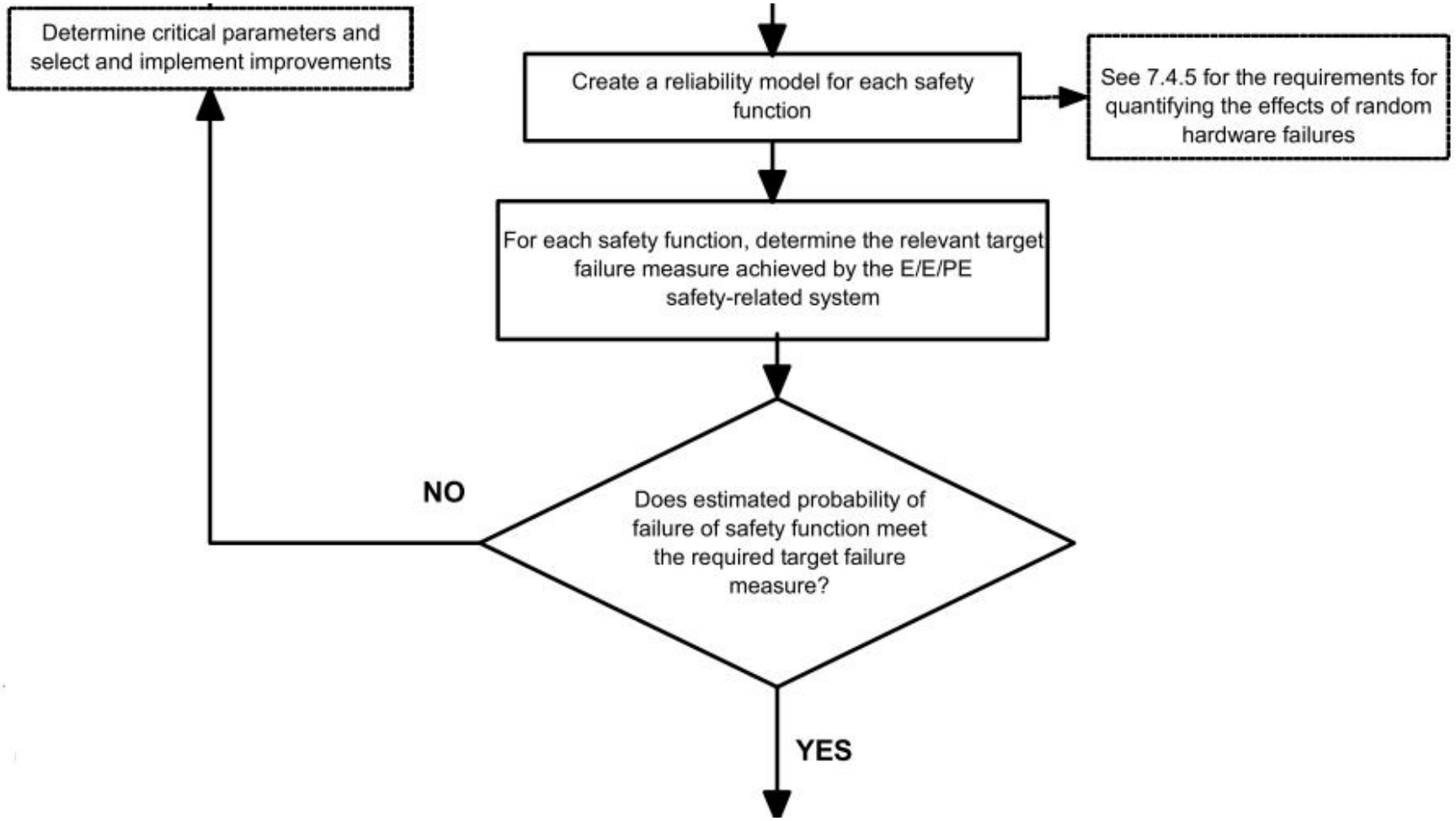
IEC 61508-6 liite A - Vaiheet IEC 61508-2 soveltamisessa



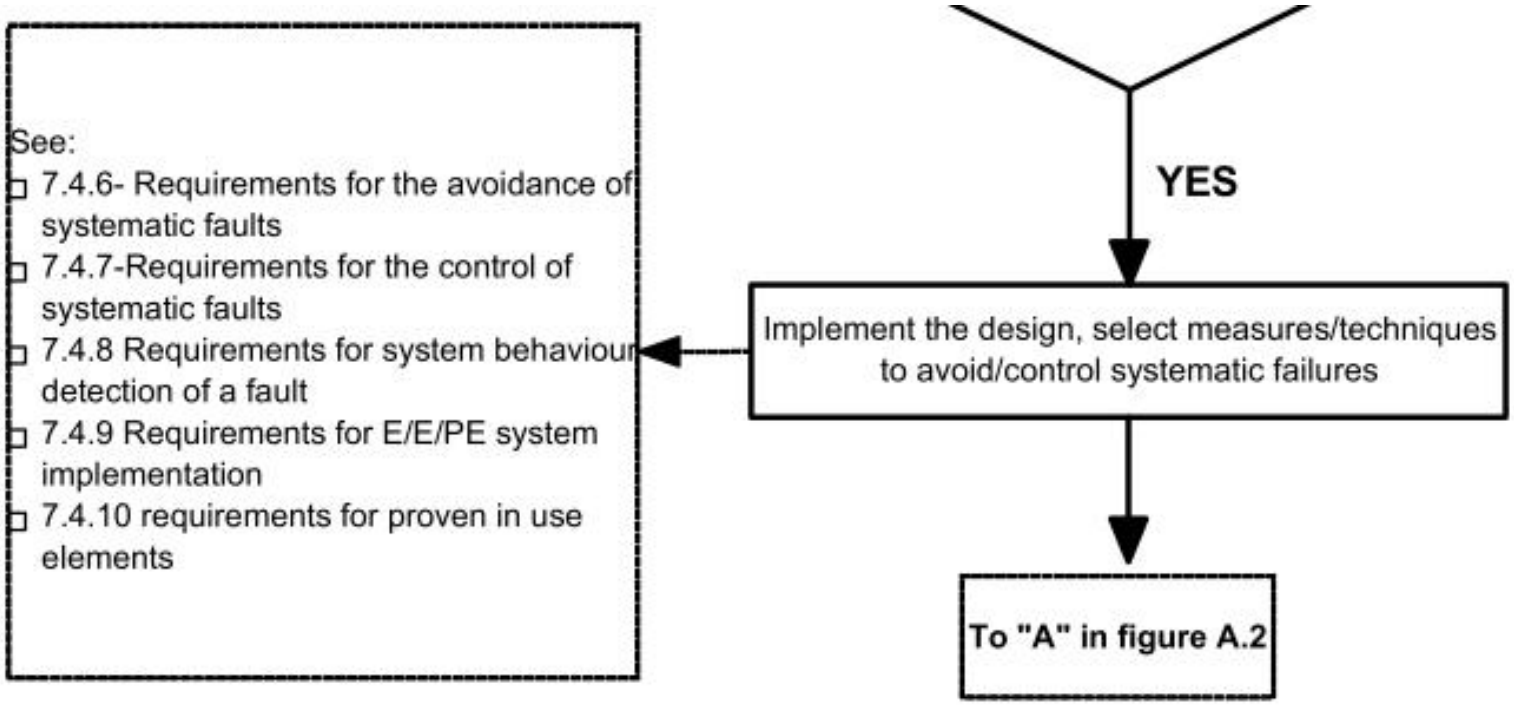
IEC 61508-6 liite A - vaiheet IEC 61508-2 soveltamisessa



IEC 61508-6 liite A - vaiheet IEC 61508-2 soveltamisessa

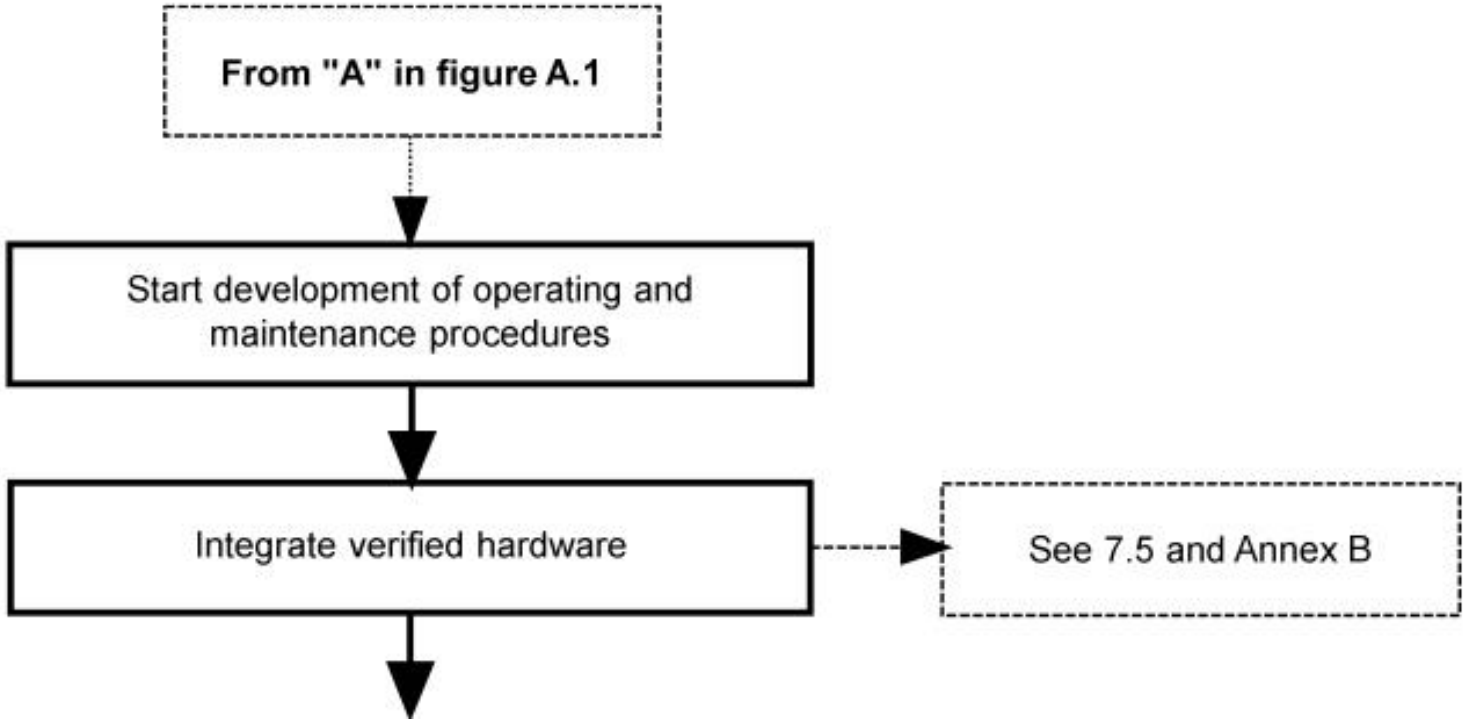


IEC 61508-6 liite A - vaiheet IEC 61508-2 soveltamisessa

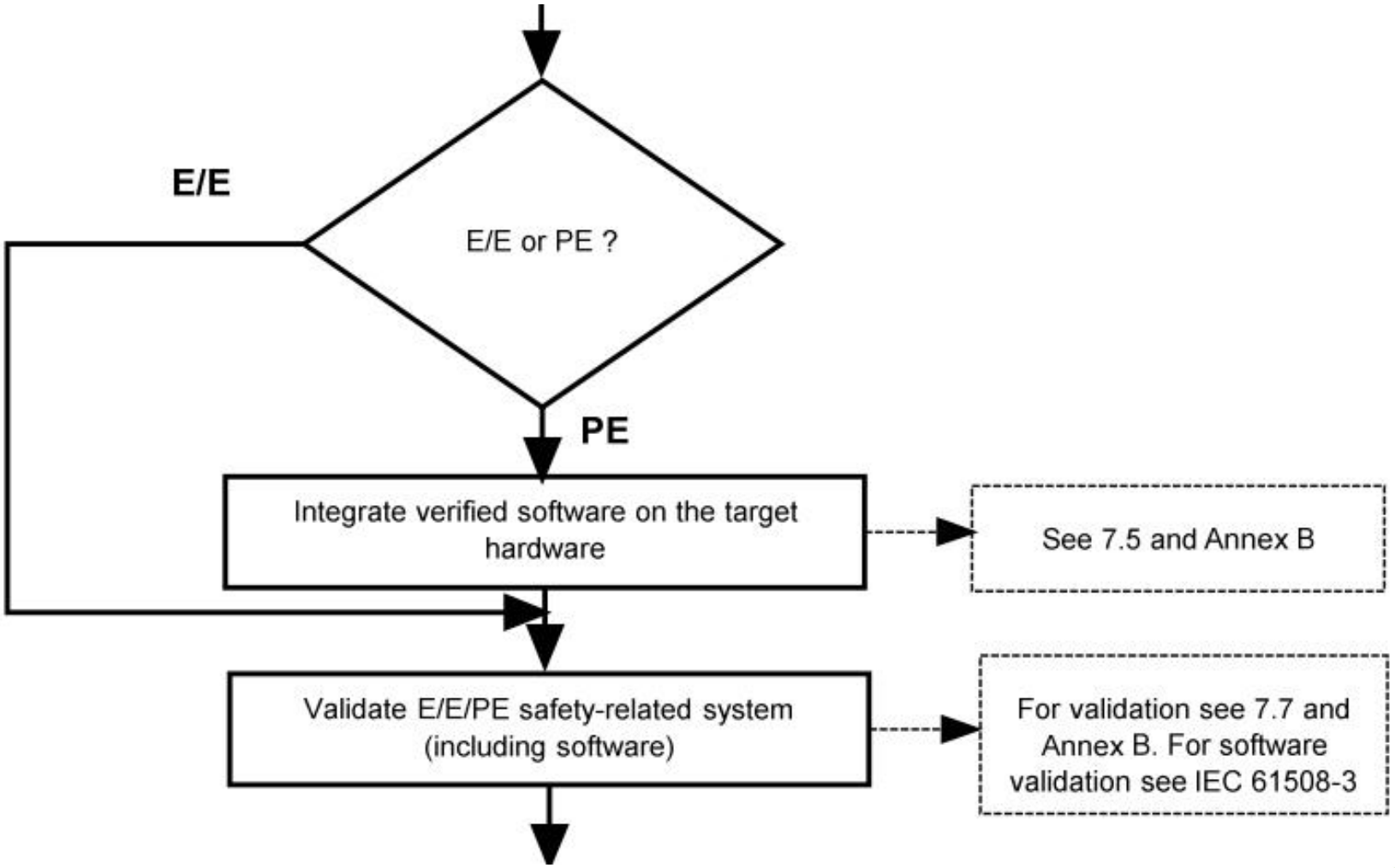


NOTE: For PE safety-related systems, activities for software occur in parallel (see figure A.3).

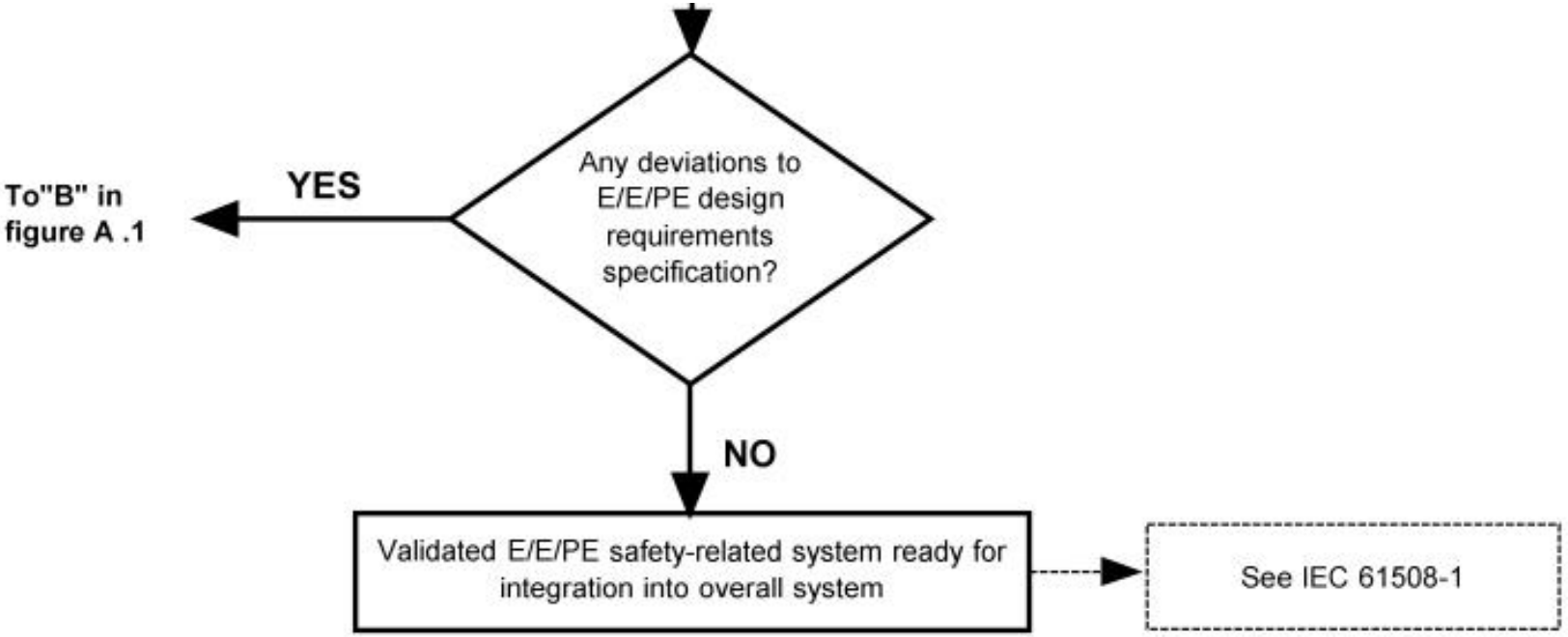
IEC 61508-6 liite A - vaiheet IEC 61508-2 soveltamisessa



IEC 61508-6 liite A - vaiheet IEC 61508-2 soveltamisessa

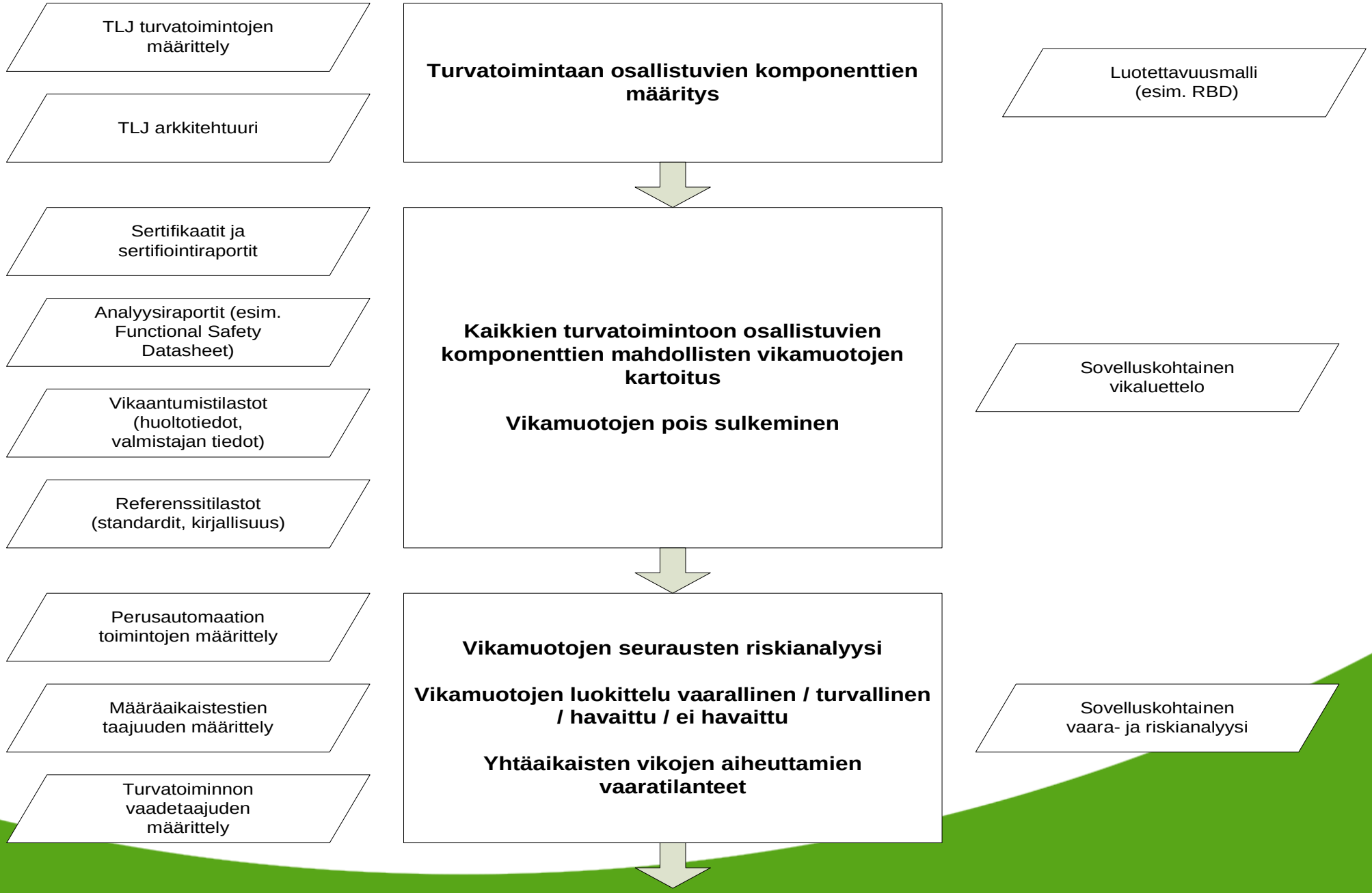


IEC 61508-6 liite A - vaiheet IEC 61508-2 soveltamisessa



NOTE: For PE safety-related systems, activities for software occur in parallel (see figure A.3).

Laitteiston todentamisen vaiheistus - esimerkki



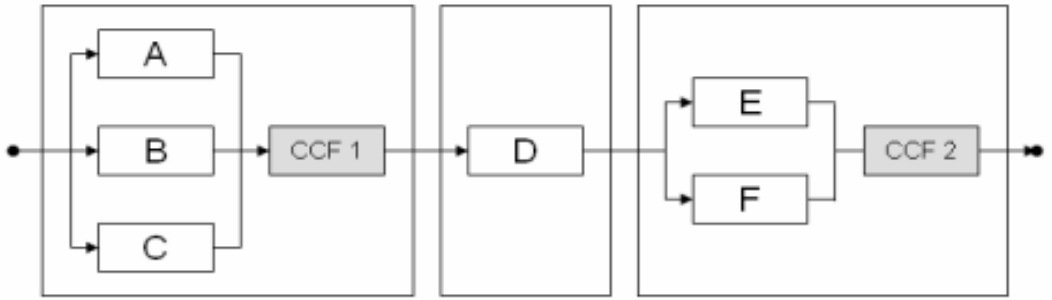
Laitteiston todentamisen vaiheistus - esimerkki

IEC 61508-6
Liite B - esimerkki tekniikasta laitteiston vikaantumisen todennäköisyyden arvioimiseksi

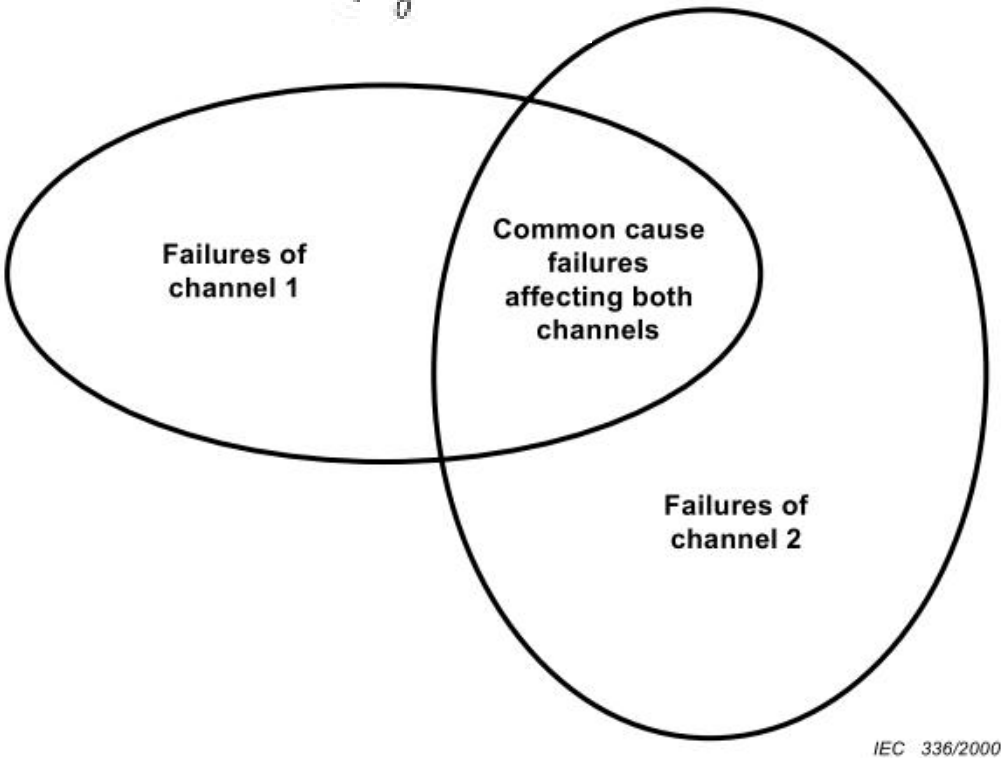
- Painotetaan analyysin tekijän pätevyyttä valittuun tekniikkaan ja täsmennetty analyysien teoreettisia perusteita merkittävästi
- B1 Yleistä
  - staattiset mallit (Boolean) vs. dynaamiset mallit (tilat/siirtymät)
  - analyyttiset laskennat vs. Monte Carlo simuloinnin laskennat
- B2 Huomioitavaa perustodennäköisyyslaskennoissa
- B3 Luotettavuuslohkokaavio-lähestymistapa, vakiovikaantumistaajuuden olettamalla
- B4 Boolean-lähestymistapa
  - Luotettavuuslohkokaavio, vikapuu, tapahtumapuu, syy-seurauskaavio
- B5 Tilat/siirtymät-lähestymistapa
  - Markov-malli, Petri-verkko
- B6 Epävarmuuksien käsittely

IEC 61508-6
Liite B - Huomioitavaa perustodennäköisyyslaskennoissa

- CCF lisätty luotettavuuslohkomalliin
- ’Minimal Cut Set’ käsitteenä
- Yleinen PFH laskentakaava lisätty
- MDT laskentakaava varmennetuille elementeille
- PFH laskentakaava useiden turvakerrosten tapauksessa
- Sarjarakenteiden käsittelyn helppous ja rinnakkaisten rakenteiden käsittelyn vaikeus käsiteltäessä koko järjestelmän vikataajuutta λ



$$PFH(T) = \frac{1}{T}\int_0^T w(t)dt$$



IEC 61508-6
Liite B - Luotettavuuslohkokaavio-lähestymistapa, vakiovikaantumistaajuuden olettamalla

- Esimerkin analyysin perusteena olevat oletukset esitetty ja PFD/PFH taulukot antavat mallitulokset

- PFD_g/PFH_g laskentakaavat 1oo2D järjestelmälle muuttuneet
  - uusi termi K (automaattisten testien onnistumisosuus 1oo2D järjestelmässä)

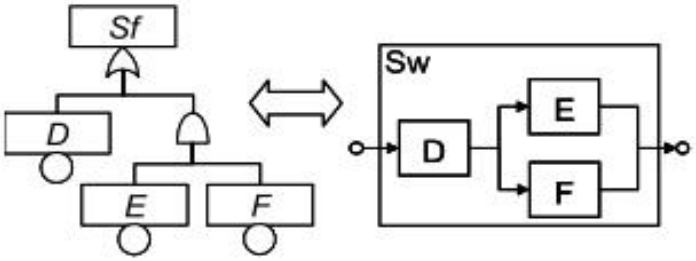
$$PFD_G = 2(1-\beta)\lambda_{DU}((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD})t_{CE}' t_{GE}' + 2(1-K)\lambda_{DD}t_{CE}' + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

$$PFH_G = 2(1-\beta)\lambda_{DU}((1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD})t_{CE}' + 2(1-K)\lambda_{DD} + \beta\lambda_{DU}$$

- Uutena 1oo3 rakenteen laskentakaavat

- 2oo4 rakenteelle ei vieläkään esitetä laskentakaavaa
  - johdettuna kirjallisuudessa (Josef Börcsök / HIMA)

IEC 61508-6
Liite B - Boolean-lähestymistapa



- Luotettavuuslohkokaavion ja vikapuun vastaavuus
- PFD laskentaperusteet luotettavuuslohkokaaviosta ja vikapuusta
- Testien porrastamisen (staggering) käsittely analyysissa
- Boolean tekniikat soveltuvat hyvin elementtien ollessa kohtuullisen itsenäisiä
  - analyysin tekijän tulee osata havaita väärät toteutukset käyttääkseen ohjelmistotyökaluja

IEC 61508-6
Liite B - Tilat/siirtymät-lähestymistapa

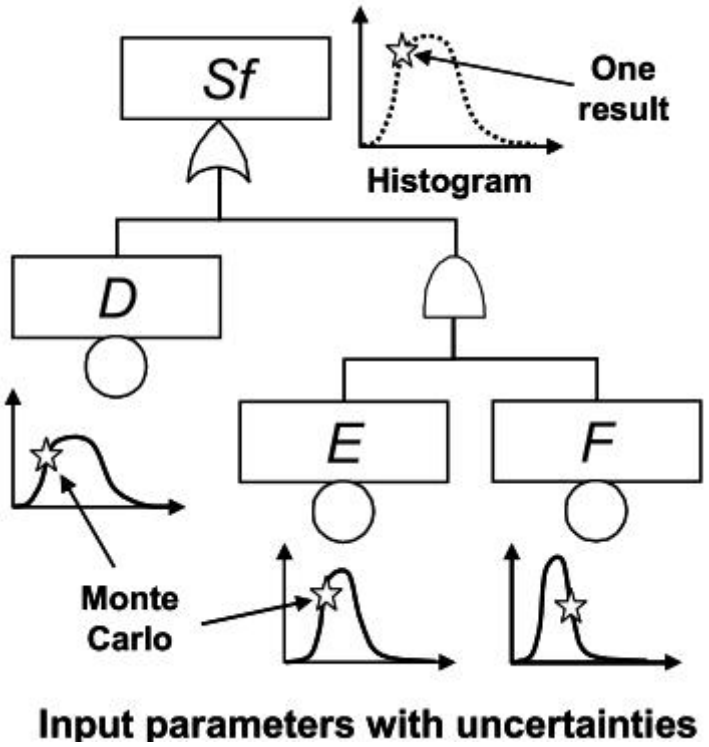
- Markov-mallinnus
  - käsitellään analyyttisesti
  - mallinnusperiaate
  - PFD laskentaperiaatteet
  - PFH laskentaperiaatteet

- Petri-verkko
  - käsitellään Monte-Carlo simulaatiolla
  - mallinnusperiaate
  - simulointiperiaate
  - PFD laskentaperiaatteet
  - PFH laskentaperiaatteet

VR TRACK

IEC 61508-6
Liite B - Epävarmuuden käsittely

- Todennäköisyyslaskentoihin sisältyy olennainen luotettavuusparametrien epävarmuustekijä
- Monte-Carlo analyysia suositellaan tehokkaana tapana epävarmuuksien käsittelyyn



KIITOS!