Teollisuusautomaation standardit
Osio 4

Osio 1:	SESKOn Komitea SK 65: Teollisuusprosessien ohjaus
Osio 2:	Toiminnallinen turvallisuus: periaatteet
Osio 3:	Toiminnallinen turvallisuus: standardisarja IEC 61508
Osio 4:	**Koneiden ohjausjärjestelmät: standardi IEC 62061**
Osio 5:	Riskin arviointi ja turvallisuuden eheyden tason SIL määrittäminen: standardit IEC 61508-5 ja IEC 62061
Osio 6:	Koneiden ohjausjärjestelmien suunnittelutyökalu SISTEMA
Osio 7:	Hätäpysäytys: standardit ISO 13850 ja IEC 60947-5-5
Osio 8:	Turvaväylät ja niiden valinta: tekninen raportti IEC/TR 62513
Osio 9:	Logiikat: standardi IEC 61131-1 ja 61131-3
Osio 10:	Turvallisuuteen liittyvän elektroniikan asennus- ja muutostyöt

matti.sundquist@sundcon.fi

Koneiden ohjausjärjestelmät: standardi IEC 62061

Matti Sundquist
Sundcon Oy

Standardin IEC 62061 tarkoitus #1

- IEC 62061 on ”kattostandardin” IEC 61508 sovellusstandardi.
- Standardin tarkoituksena on
  - auttaa koneiden ja niiden sähköisen/elektronisen ohjausjärjestelmien suunnittelijoita, kone- ja laitetoimittaja ja vaatimustenmukaisuuden arviointilaitoksia suunnittelemaan ja arvioimaan turvallisuuteen liittyviä ohjausjärjestelmiä
  - esittää riskin arviointimenetelmä ja sen tulosten perusteella määrittää tarvittava turvallisuuden eheystason SIL jokaiselle turvatoiminnolle.

Standardin IEC 62061 tarkoitus #2

- Standardin tarkoituksena on lisäksi
  - esittää ohjeita sähköisen/elektronisen ohjausjärjestelmän suunnitteluun
  - yhdistää standardin SFS-ISO EN 13849-1 mukaisesti suunniteltuja ohjausjärjestelmän osia yhdeksi kokonaisuudeksi
  - esittää ohjausjärjestelmälle asetettujen vaatimusten todentamisen ja kelpuutuksen vaatimukset ja ohjeet.

Konedirektiivin toiminnalliset vaatimukset koneiden hallintajärjestelmille

- Toiminnalliset vaatimukset:
  - toimintatavan valinta (mm. turvatoiminnot automaattisesti valinnan mukana)
  - hallintalaitteet (mm. ergonomiset vaatimukset)
  - käynnistystoiminto (mm. odottamattoman käynnistyksen estämisen toimenpiteet)
  - pysäytystoiminto (mm. turvalliseen tilaan saattaminen)
  - ohjelmistojen toiminnot (mm. oikeellisuus).

Konedirektiivin vaatimukset koneiden hallintajärjestelmän laitteistolle

- Laitteiden toiminnalliset vaatimukset:
  - turvallisuus ja luotettavuus (mm. suurin sallittu vaarallisten vikaantumisten taajuus)
  - energiansyötön häiriöt (mm. tehonsyötön valvonta)
  - ohjauspiirin häiriöt (mm. ohjausjärjestelmän luotettavuus, diagnostiikka).

Ohjausjärjestelmien erot: koneet vs. prosessit

- Kone tai laite: tavallisesti tiheiden tai jatkuvien vaateiden toimintamuoto. Seuraukset työtapaturmia.
- Prosessit: tavallisesti harvojen vaateiden toimintamuoto. Seuraukset voivat olla suuronnettomuuksia.

Rajana on vaade kerran vuodessa (kerran 10^4 tunnissa) eli koneet kuuluvat pääsääntöisesti tiheiden tai jatkuvien vaateiden toimintatapaan.

Turvallisuuden eheys SIL (Safety Integrity Level)

Todennäköisyys sille, että turvallisuuteen liittyvä järjestelmä toteuttaa hyväksyttävästi vaadittavat turvatoiminnat kaikissa määritellyissä olosuhteissa ja määriteltynä ajanjaksona.

”Turvallisuuden luotettavuus”

Turvallisuuden eheyden tasot

- Konesovelluksissa käytetään tavallisesti tiheiden vaateiden tai jatkuvan toiminnan toimintatapa.
- Vaarallisen vikaantumisen todennäköisyys tuntia kohden PFH (Probability of Failure per Hour):

SIL = 4	10^{-9} ... 10^{-8}	(ei tavallisesti konesovelluksissa)
SIL = 3	10^{-8} ... 10^{-7}	
SIL = 2	10^{-7} ... 10^{-6}	
SIL = 1	10^{-6} ... 10^{-5}	

Standardi IEC 62061

- Standardi esittää järjestelmällisen menetelmän riskin vähentämiseksi vaaditulle tasolle.
- Jokaiselle turvatoiminnolle arvioidaan riskin arvioinnin perusteella turvallisuuden eheyden tasot.
- Turvatoiminto toteutetaan sarjamuotoon kehitetyillä toimilohkoilla.

Ohjausjärjestelmästandardien soveltamisalat

SFS-EN ISO 13849-1:

Yksinkertaistettu menetelmä, joka perustuu parametrien likiarvoihin ja valmiiksi laskettuihin tyypillisiin arkkitehtuurimalleihin. Menetelmä ei sovellu puhtaasti elektronisten ohjausjärjestelmien suunnitteluun.

IEC 62061:

Vikatarkastelu perustuu turvatoiminnon vikaantumisen todennäköisyyden määrälliseen (laskennalliseen) arviointiin. Menetelmä soveltuu kompleksisten (elektronisten) ohjausjärjestelmien suunnitteluun.

Standardien SFS-EN ISO 13849-1 ja IEC 62061 soveltamisalojen vertailu

- Jos turvatoimintoja toteuttavissa ohjausjärjestelmissä käytetään elektronisia osia standardia SFS-EN ISO 13849-1 voidaan soveltaa jos
  - vaadittu riskin vähentäminen on pieni tai ohjausjärjestelmän osuus riskin vähentämisessä on pieni tai
  - turvatoiminnalla on kiinteästi langoitettu varmistus tai divergenssi (kanavien erillisyys, ks. sivu 26) on viety pitkälle tai
  - käytetään vain sertifioituja osia (alajärjestelmiä), (ks. osio 3 sivut 15 ja 16).

Standardin IEC 62061 sisältö

- Vaatimusten määrittely turvallisuuteen liittyville ohjausjärjestelmän osille
- Turvallisuuden eheyden tasojen SIL määrittäminen riskin arvioinnin avulla
- Turvallisuuteen liittyvien ohjausjärjestelmien suunnittelu
- Käyttäjän tarvitsemat tiedot turvallisuudesta ja kunnossapidosta
- Kelpuutus
- Vaatimukset järjestelmän turvallisuuden ylläpidolle jälkikäteen tehtävien muutosten yhteydessä.

Turvallisuuteen liittyvän järjestelmän osia

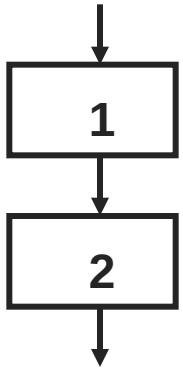
- Turvatoimintoja toteuttavia laitteita ja ohjelmistoja:
  - antureita
  - ohjelmoitavia elektronisia laitteita
  - toimilaitteita
  - sulautettuja ohjelmistoja
  - sovellusohjelmistoja
  - jne.

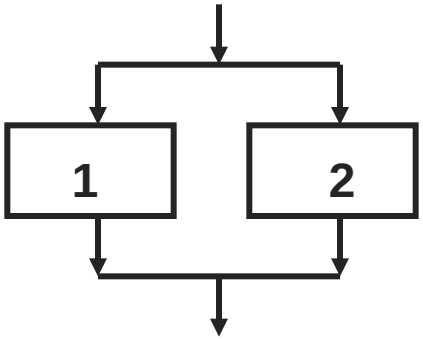
Vaatimusmäärittely

- Vaatimukset laitteiden turvallisuuden eheydelle
  - satunnaisten vaarallisten vikaantumisten taajuus
  - ohjausjärjestelmän arkkitehtuurin (rakenteen) tuomat rajoitukset luotettavuudelle
- Vaatimukset järjestelmän turvallisuuden eheydelle
  - vikaantumisten välttäminen
  - järjestelmän vikojen hallinta
- Vaatimukset järjestelmän toiminnalle tunnistettaessa vikaantuminen
- Vaatimukset turvallisuuteen liittyvän järjestelmän ohjelmiston suunnitteluun ja kehittämiseen.

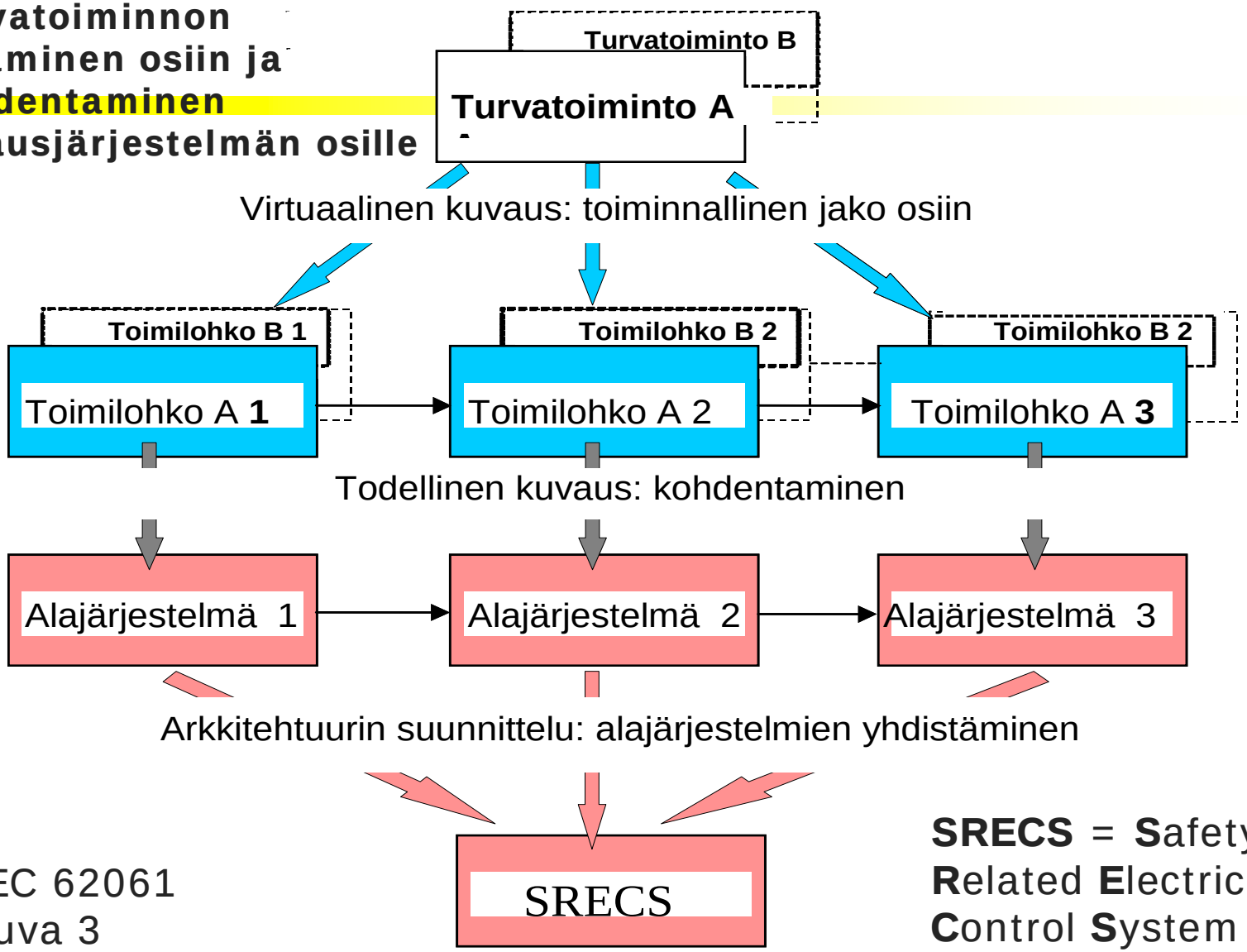
Sarjamuotoinen vs. rinnakkainen rakenne

- Sarjamuotoisessa rakenteessa komponentit ovat peräkkäin siten, että yhdenkin komponentin tai kanavan vikaantuminen aiheuttaa koko ohjattavan toiminnon vikaantumisen (”ketjun heikoin lenkki”).
- Rinnakkaisessa rakenteessa toisen komponentin vikaantuessa toinen komponentti voi toteuttaa ohjaustoiminnon.





Turvatoiminnon jakaminen osiin ja kohdentaminen ohjausjärjestelmän osille

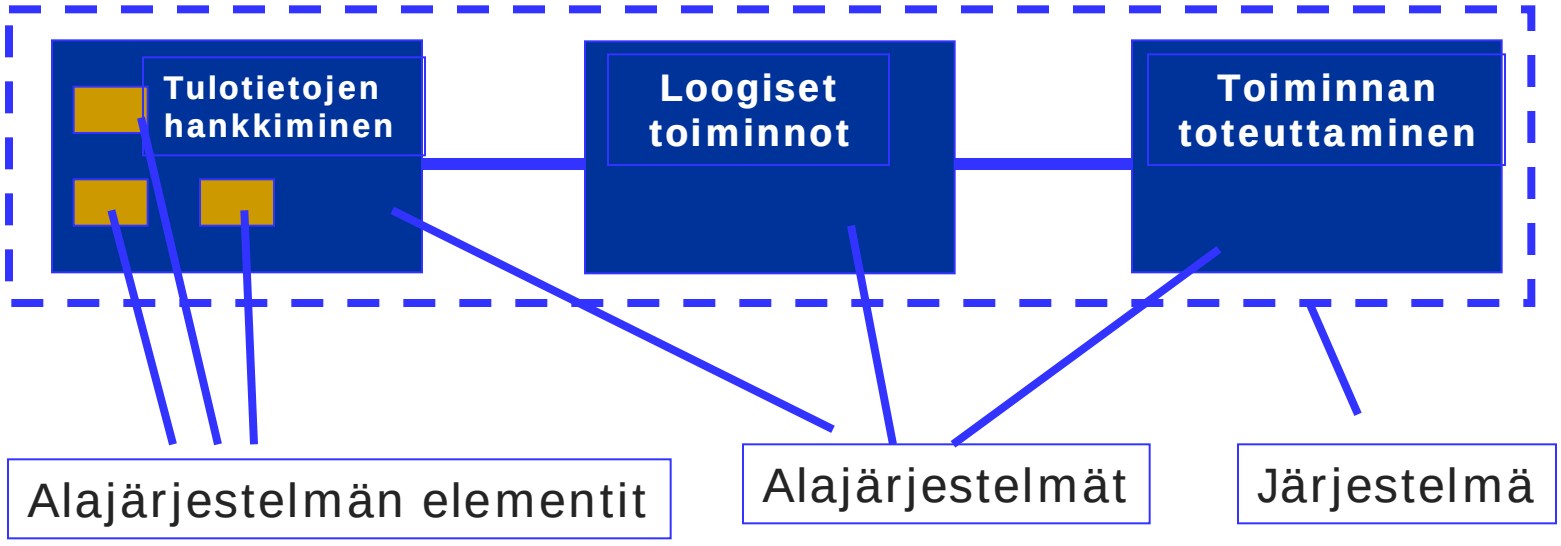


IEC 62061
kuva 3

SRECS = **S**afety **R**elated **E**lectric **C**ontrol **S**ystem

Arkkitehtuuri (rakenne)

- Turvatoiminnon toteuttava järjestelmä koostuu sarjamuotoisesta alajärjestelmien kokoonpanosta.
- Alajärjestelmä puolestaan koostuu elementeistä, jotka voivat olla myös rinnakkaisia.



Suurin vikataajuus

Turvatoiminnon vikataajuus saadaan laskemalla yhteen kaikkien alajärjestelmien vaarallisten satunnaisvikojen esiintymistodennäköisyydet (tuntia kohden, PFH). Jokaista vikataajuutta vastaa jokin SIL-taso (katso taulukko saivulla 9).

$$PFH_D = PFH_{D1} + \ldots + PFH_{Dn} + P_{TE}$$

Turvallisuuden eheyden SIL yläraja

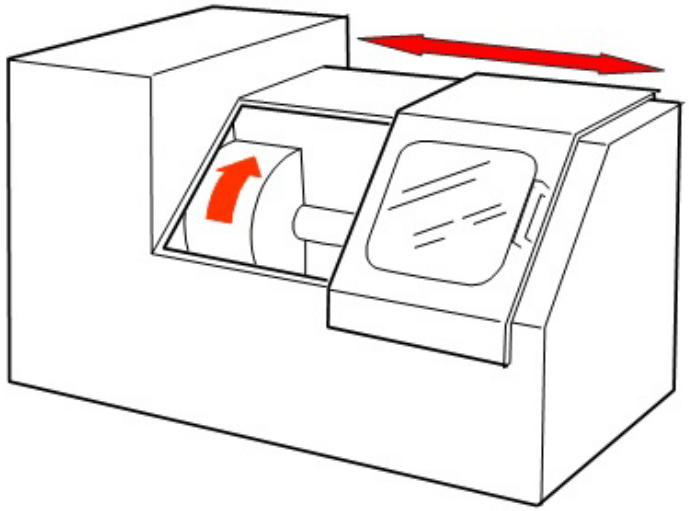
- Jokaisen turvatoiminnon eheystason SIL arviointi perustuu jokaisen alajärjestelmän turvallisuuden eheyden tason arviointiin.
- Turvatoiminnolle esitettävän turvallisuuden eheystason yläraja (SIL Claim Limit, SILCL) arkkitehtuurin rajoitusten johdosta on enintään alajärjestelmälle esitettävän pienimmän turvallisuuden eheystason suuruinen:

$$SIL_{koko} \leq (SIL_{alajärjestelmä})_{alin}$$

Arkkitehtuurin (rakenteen) aiheuttamat turvallisuuden eheyden SIL rajoitukset

- Arkkitehtuurin (rakenteen) rajoituksilla osoitetaan korkein turvallisuuden eheyden taso (SIL Claim Limit, SILCL), joka voidaan hyväksyä kyseiselle alajärjestelmälle.
- Nämä rajoitukset perustuvat siihen, että pelkällä komponenttien luotettavuudella ei voida saavuttaa korkeaa luotettavuustasoa, vaan tarvitaan redundanttisia (kahdennettuja tai useampikanavaisia) rakenteita.
- Rajoitukset esitetään taulukossa alajärjestelmän diagnostiikan (SFF) ja vikasietoisuuden avulla.

Esimerkki alajärjestelmien yhdistämisestä ja diagnostiikasta



Riskin arvioinnin perusteella (ks. osio 5) on päädytty käsivahinkovaaran osalta turvallisuuden eheyden tasolle SIL 2. Turvallisuustoimenpiteenä on asennettu työstötilan suojus, joka on kytketty koneen toimintaan.

Toiminnan jakaminen toimilohkoiksi

Turvallisuuteen liittyvän ohjaustoiminnon turvallisuusvaatimusten spesifikaatio (toiminta - eheys)

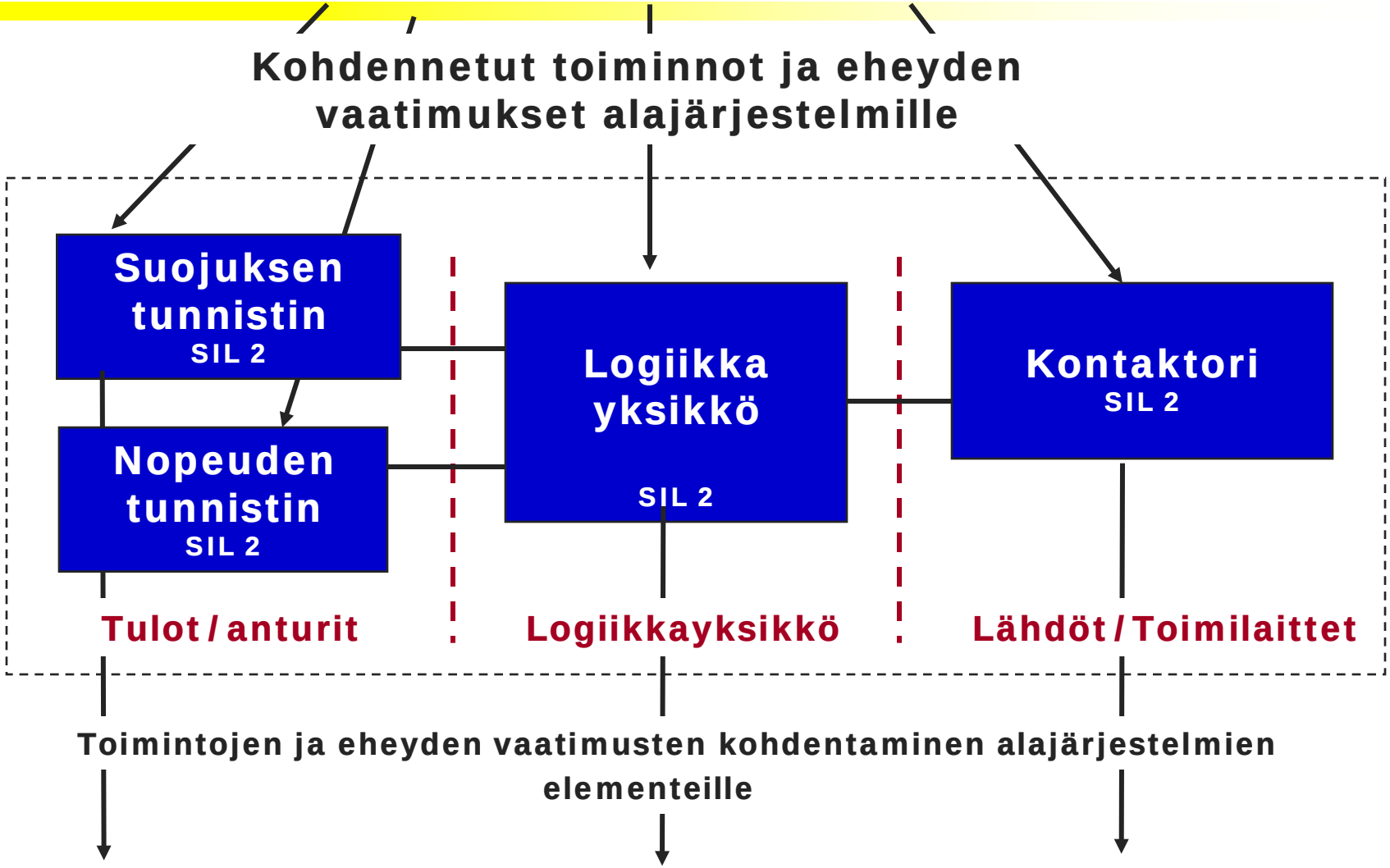
Esimerkki turvallisuuteen liittyvästä ohjaustoiminnosta:
jos suojuksen ovi on auki, akselin pyörimisnopeus ei saa ylittää määritettyä arvoa.
Riskin arviointi:
Vaadittava turvallisuuden eheys = SIL 2.

Ehdotus ohjausjärjestelmän luonnokseksi toiminnallisten ja eheyden vaatimusten (SIL2) mukaisesti

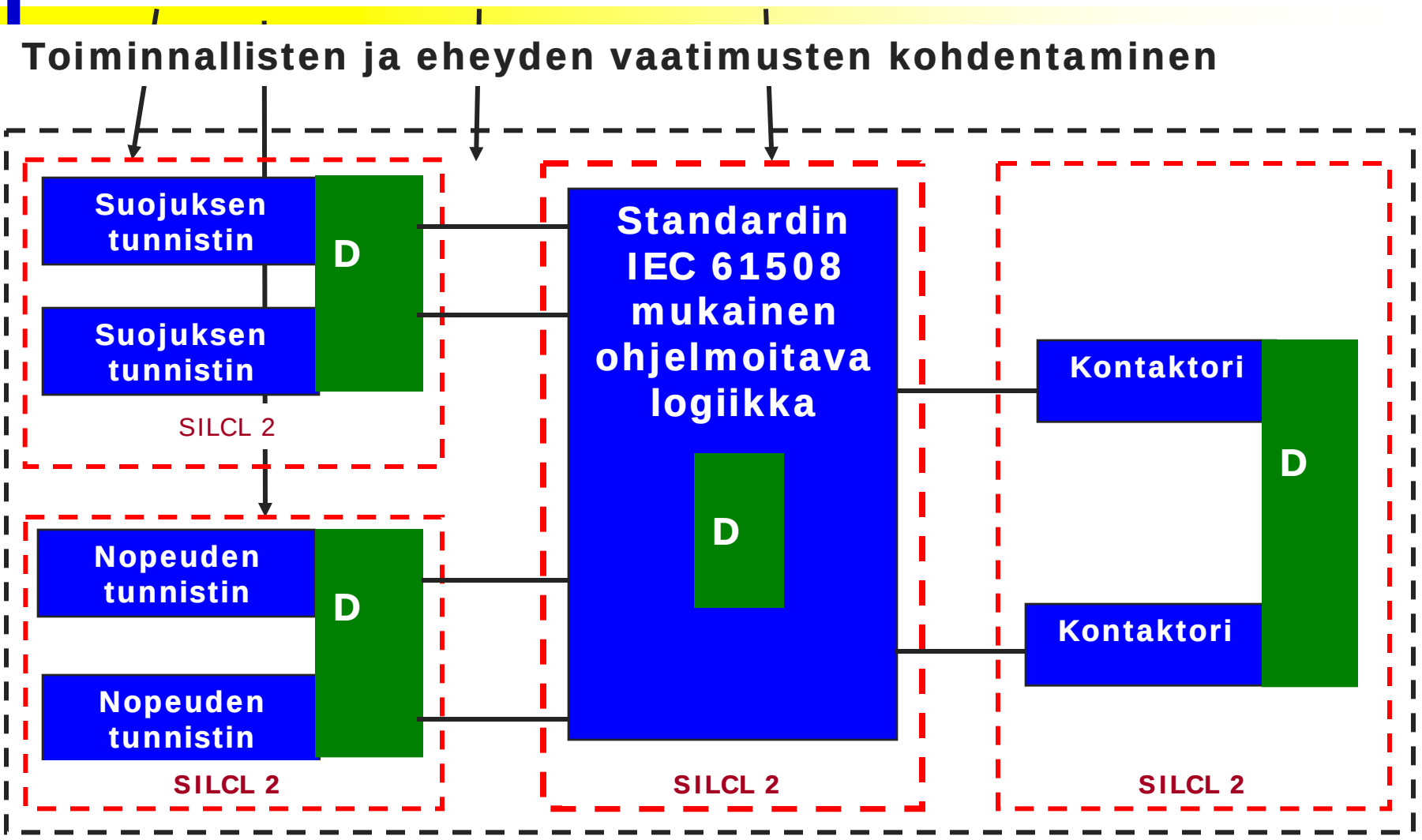
Järjestetään suojuksen aseman tunnistus ja akselin pyörimis-nopeuden tunnistus. Tunnistuksen lähtötiedot käsitellään logiikkayksikössä, siten, että
- käyttömoottori pysäytetään aina kun akselin pyörimisnopeus on liian suuri ja
- aina kun suojuksen ovi ei ole suljettuna, moottorin energiansyöttö on katkaistuna.

Kohdennetaan kaikille alajärjestelmille

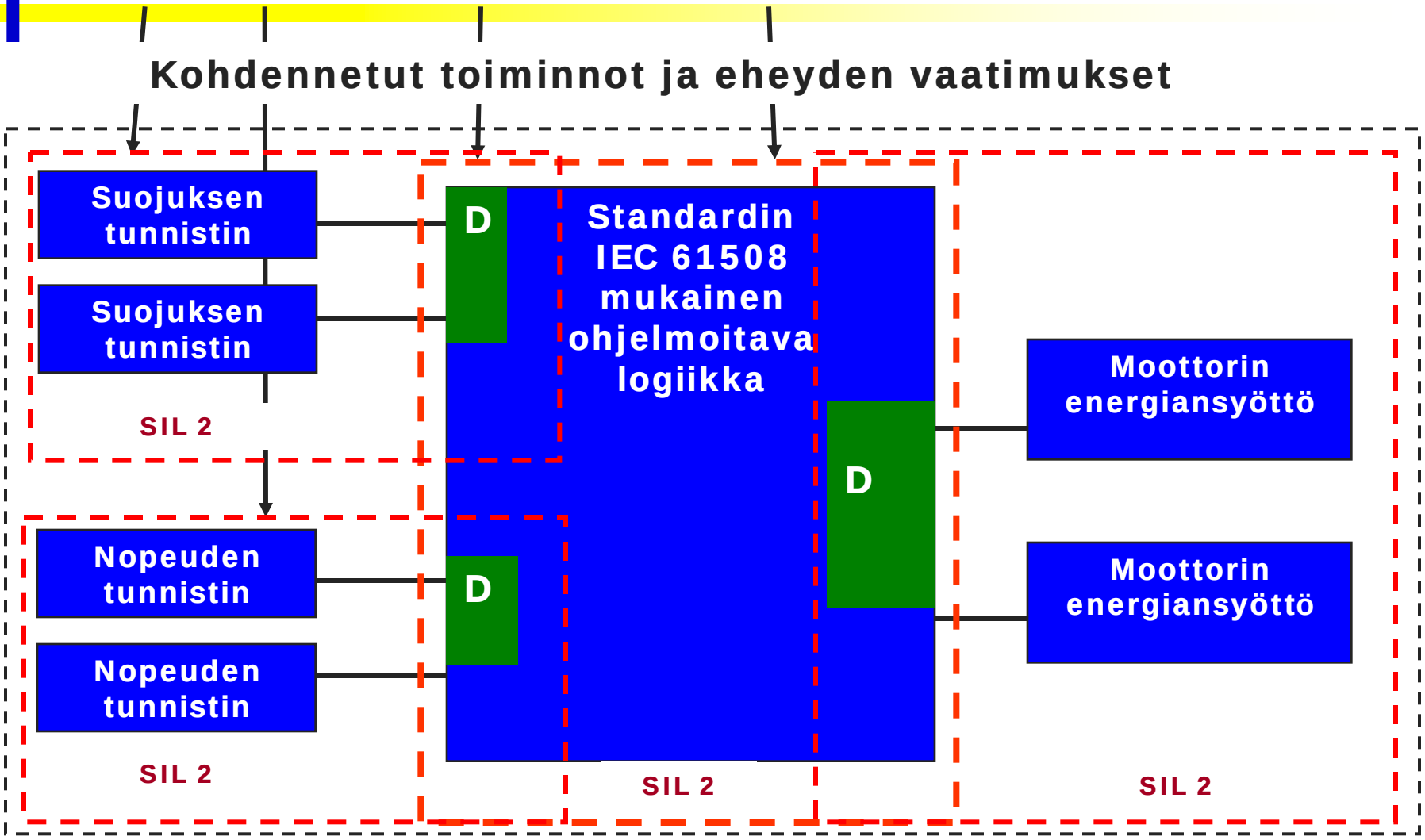
Esimerkki alajärjestelmistä



Diagnostiikkatoiminnot

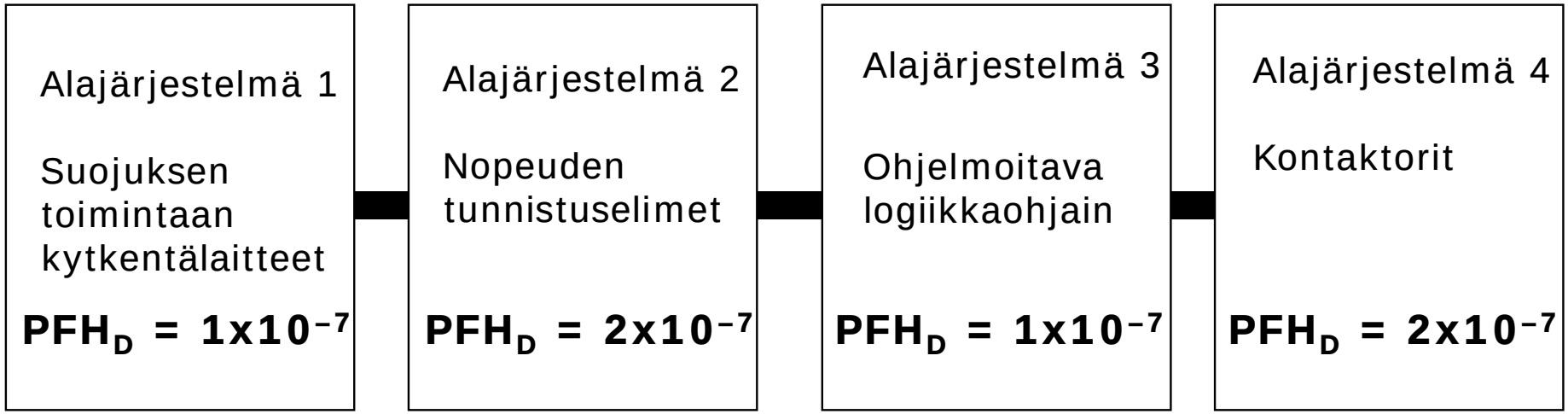


Diagnostiikkatoiminnot



Ohjausjärjestelmän vaarallisen vikaantumisen todennäköisyyden arviointi

Esimerkki: vaatimus SIL 2 => $PFH_D = 10^{-7}...10^{-6}$



$PFH_{koko} = (1 \times 10^{-7}) + (2 \times 10^{-7}) + (1 \times 10^{-7}) + (2 \times 10^{-7}) = 6 \times 10^{-7}$

=> SIL 2 (ks. sivu 9)

Yhteisviat

Yhteisviat (β-tekijä):

- Katso osio 6 sivut 27 ja 28 (myös standardi IEC 62061 liite F)
- β-tekijä ilmaisee kuinka suuri osa [%] yhden kanavan vioista vaikuttaa toisiinkin kanaviin (ilman diagnostiikkaa)

Systemaattisten virheiden välttäminen #1

- Suunnittelun ja toteutuksen aikana:
  - ohjausjärjestelmän suunnittelu toiminnallisen turvallisuuden hallintasuunnitelman mukaisesti
  - valmistajan antamia tietoja ja ohjeita on noudatettava ja omaksuttava hyvä insinöörikäytäntö
  - valittava sopivat alajärjestelmät ja varmistettava alajärjestelmien toiminnalliset ominaisuudet ja varsinkin yhteensopivuus
  - huolehdittava ohjausjärjestelmän sähköteknisistä ominaisuuksista standardin IEC 60204-1 ”*Koneturvallisuus. Koneiden sähkölaitteistot*” mukaisesti.

Systemaattisten virheiden välttäminen #2

- Vaatimukset suunnitteluvirheiden hallintaan:
  - turvallisen vikaantumisen periaatteen käyttäminen esim. siten, että komponentin vikaantuminen johtaa koneen vaarallisen liikkeen pysähtymiseen tai energian syötön katkeaminen johtaa järjestelmä turvalliseen tilaan
  - vaarallisiin vikaantumisiin reagoivien toimintojen on toteuduttava ennen kuin vaaratilanne ehtii syntyä
  - varmistettava, että komponenteilla ei ole dokumentoimattomia toimintoja

Systemaattisten virheiden välttäminen #3

- Alajärjestelmien vikaantumisen hallinta:
  - vikaantumisten paljastaminen ohjausjärjestelmän käytönaikaisella valvonnalla
  - tietoliikenteen häiriöiden hallinta (ks. osio 10)
  - ympäristötekijät (lämpötila, kosteus, tärinä, EMC jne).
  - ylijänniteen- ja alijännitten sekä jännitteen vaihteluiden ja keskeytysten hallinta (ks. IEC 60204-1)

Systemaattisten virheiden välttäminen #4

- laitteiston divergenssi (komponenttien tai kanavien erillisyys: esim. eri toimintaperiaate, eri valmistajat, eri ohjelmistot jne.)
- pakkotoimiset kytkimet (esim. ohjauskappaleen suora sähkömekaaninen ohjaus koskettimien aukaisuun)
- ylimitoitus (esim. 50 % nimellisarvon yläpuolelle)

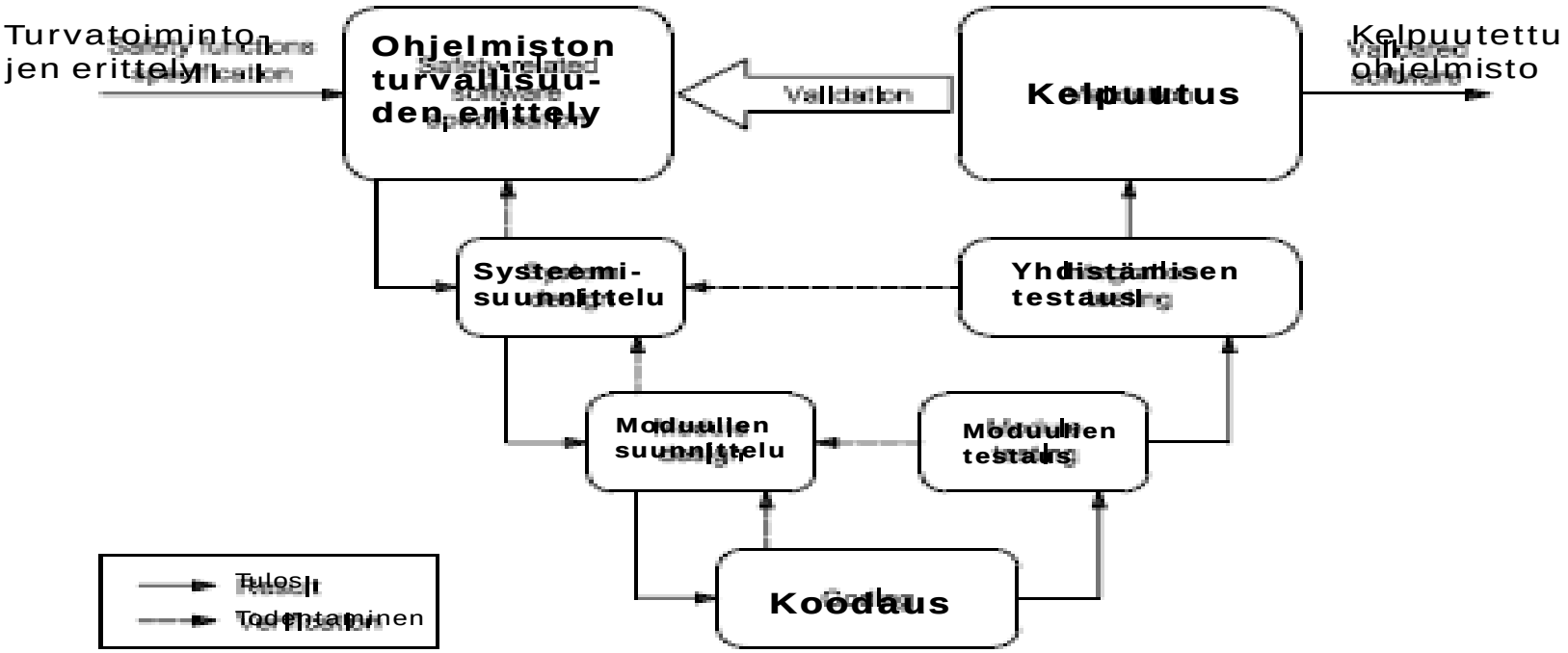
Systemaattisten virheiden välttäminen #5

- Systemaattisen turvallisuuden eheyden tarkistaminen: Sovellettava vähintään yhtä seuraavista menetelmistä riippuen turvatoimintojen turvallisuuden eheystasosta:
  - ohjausjärjestelmän laiteosuuden suunnittelun tarkistaminen vertaamalla eritelmää laitteisiin
  - tietokoneavusteisten suunnittelumenetelmien käyttäminen, jolla mahdollistetaan simulointi tai analyysi
  - toimintojen kattava simulointi.

Ohjelmistokehitys #1

- Vikojen välttäminen (puolustuksellinen suunnittelu):
  - V-malli: toiminnat, todentaminen ja kelpuutus (ks. seuraava sivu)
  - ohjelmiston rakenteen hallinta
  - kattava dokumentointi ja versionhallinta
  - soveltuvat toimenpiteet muutosten jälkeen.

Ohjelmistokehitys #2



NOTE Annex J gives more detailed recommendations for lifecycle activities.

ISO 13849-1:2006

120107 matti.sundquist

Ohjelmistokehitys #3

- Vaatimukset ohjelmiston arkkitehtuurille
- Vaatimukset työmenetelmille, käyttäjälle annettaville tiedoille ja sovelluskielille
- Vaatimukset sovellusohjelmiston suunnitteluun
- Vaatimukset koodaukselle
- Vaatimukset sovellusmoduulien testaukselle
- Vaatimukset sovellusohjelmiston kokoonpanon testaukselle.

Kelpuutus

- Kaikki turvallisuusvaatimusten määrittelyssä esitettävät ohjaustoiminnat on kelpuutettava.
- Standardissa esitetään yleisluontoisia vaatimuksia
  - kelpuutussuunnitelmalle
  - testauslaitteistolle
  - dokumentoinnille.

Kelpuutuksen testaukset

- Testauksia ohjausjärjestelmän turvallisuuden eheystasosta ja monimutkaisuudesta riippuen:
  - ympäristöolosuhteiden vaikutukset
  - sähkönsyöttö.
- Testausmenetelmiä
  - testaus syöttämällä järjestelmään vikoja
  - staattiset, dynaamiset ja vikaantumisanalyysit
  - simulaatiot
  - musta laatikko (black box)-testit
  - pahimman tilanteen testit (worst case test).

Muutosten hallinta

- Ohjausjärjestelmän muutostarpeita aiheuttavat mm.:
  - turvallisuusvaatimusten muutokset
  - käyttöolosuhteiden muutokset
  - vahingot ja tapaturmat
  - käsiteltävän materiaalin muutokset
  - koneen tai sen käyttötapojen muutokset.

Menettelytapa muutoksissa

- Pyydetyn muutoksen syyt ja vaikutukset ohjausjärjestelmän toiminnalliseen turvallisuuteen on analysoitava ja dokumentoitava.
- Kaikki ohjausjärjestelmään vaikuttavat muutokset on dokumentoitava.
- Muutettujen dokumenttien perusteella on tehtävä täydellinen dokumentoitu toimintasuunnitelma.
- Muutostyöstä on tehtävä selkeä päätös ennen muutostyön aloittamista.

Keskeisiä standardeja

- ISO 14121:2007
  (ent. ISO 14121:1999 ja EN 1050)
  ”*Koneturvallisuus - Riskin arvioinnin periaatteet*”
- SFS-EN ISO 12100:2010
  (ent. ISO 12100-1 ja –2:1992 ja
  ent. EN 292-1 ja 2:1991)
  ”*Koneturvallisuuden perusstandardit*”
- IEC 60204-1:2007
  ”*Koneturvallisuus - Koneiden sähkölaitteistot. Osa 1: Yleiset vaatimukset*.”

  Kaikki nämä standardit on julkaistu suomi-englanti versioina.