Teollisuusautomaation standardit

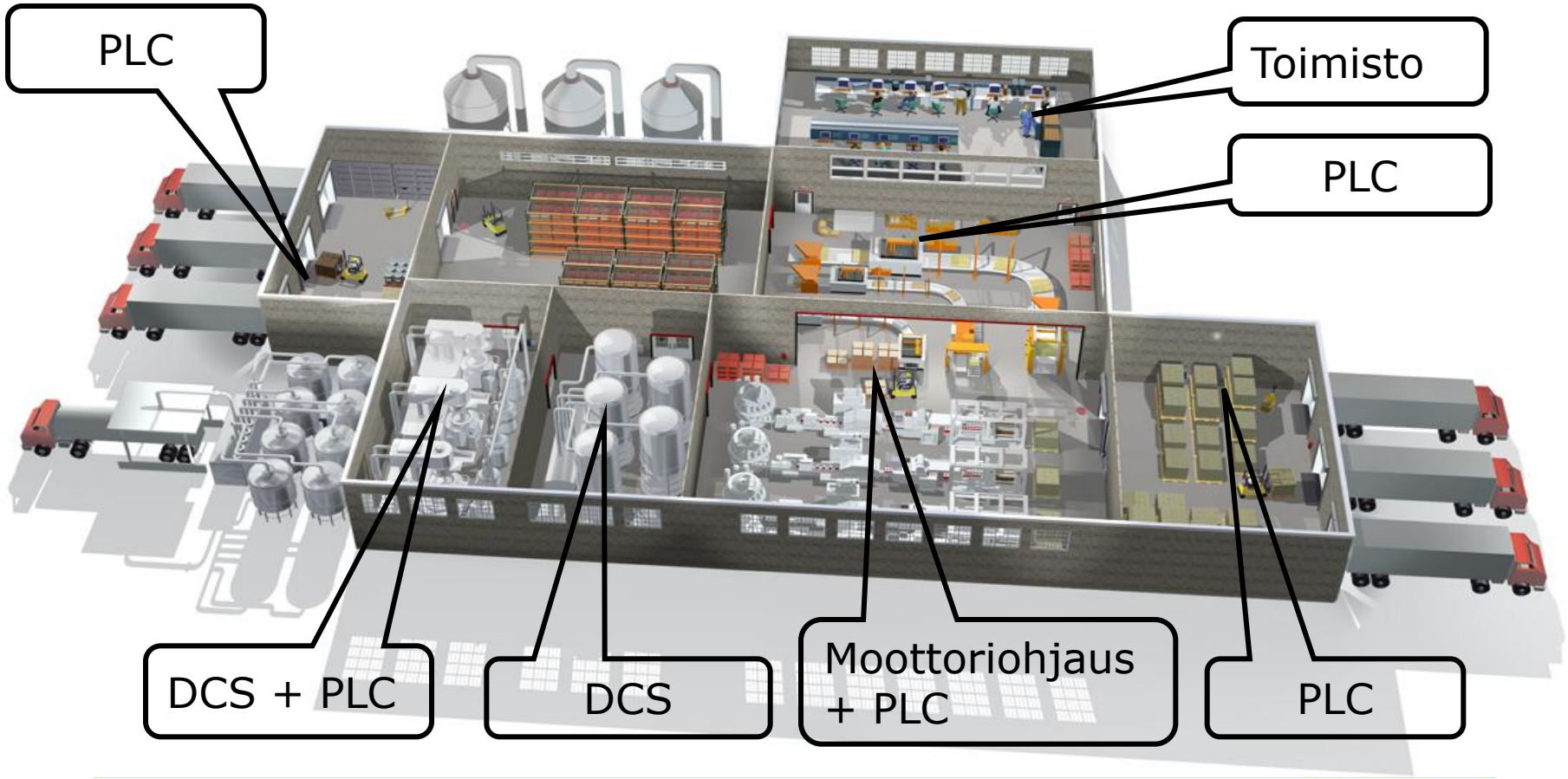
Toiminnallinen turvallisuus: periaatteet
Standardisarja IEC 61508

Matti Sundquist
Sundcon OY

matti.sundquist@sundcon.fi

SESKO

Automaatiojärjestelmien vaakasuora integraatio



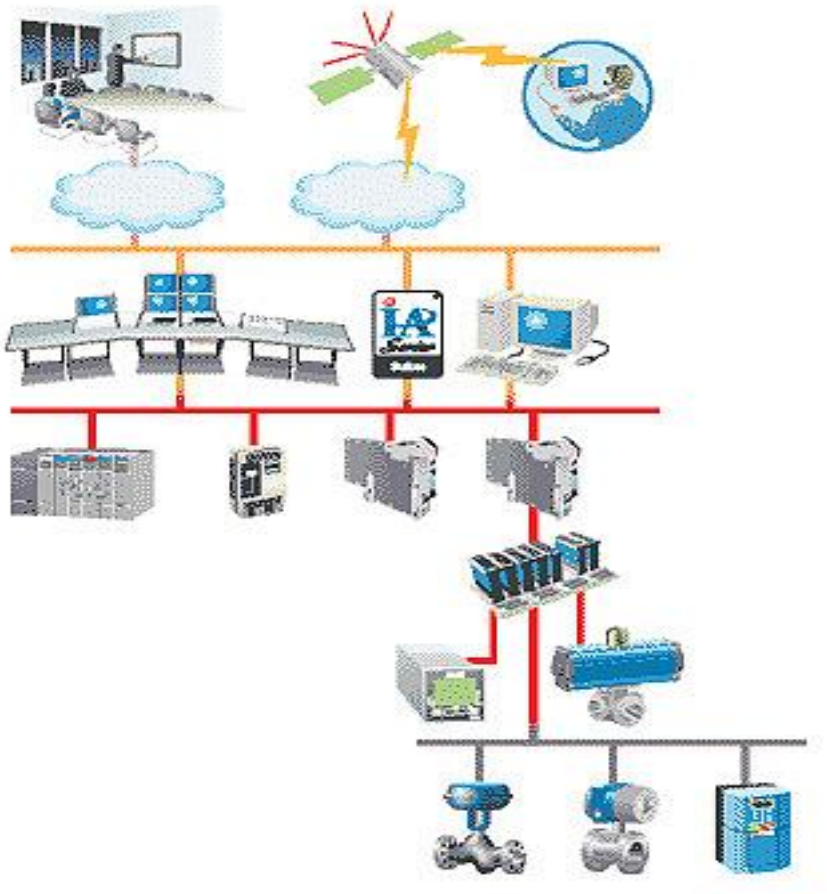
SESKO

Automaatiojärjestelmien pystysuora integraatio

Teollisuus-ethernet

Kenttäväylät

Anturi/laiteväylät



SESKO

Ei-toivotut tapahtumat

Vahingot:

- Ihmisille tai eläimille
- omaisuudelle
- ympäristölle
- liiketoiminnalle
  - tuotteille (laatu)
  - tuotannolle (käyttökatkokset).

SESKO

Teollisuusautomaation turvallisuus

- Turvallisuus on yhdistettävä saumattomasti muihin toimintoihin ja se on otettava huomioon jo suunnittelun aikana, koska valmiin järjestelmän korjaaminen voi olla hankalaa.
- Turvallisuus on varmistettava suunnittelun ja toteutuksen elinkaaren kaikissa vaiheissa ja kaikkien osapuolten vastuut on tehtävä alusta alkaen selväksi.
- Perustuu standardisarjaan IEC 61508.

Toiminnallinen turvallisuus

- Toiminnallinen turvallisuus on se kokonaisturvallisuuden osa, joka liittyy ohjelmoitavaan järjestelmään ja riippuu
  1. sähköisen/elektronisen/ohjelmoitavan elektronisten turvallisuuteen liittyvien järjestelmien
  2. muun teknologian (esim. hydrauliikka /pneumatiikka) turvallisuuteen liittyvien järjestelmien
  3. ulkoisten riskin vähennysmenetelmien (esim. mekaaninen varoventtiili)

  oikeasta toiminnasta.

Toiminnallisen turvallisuuden hallinta

- Laadunhallintajärjestelmien (ISO 9000) on oltava kunnossa (turvallisuus, ympäristöturvallisuus, tietoturva, käytettävyys jne.)
- Toiminnallisen turvallisuuden hallintaan tarvitaan järjestelmällistä lähestymistapaa:
  - turvallisuuden elinkaaritarkastelu (IEC 61508-1)
  - rakenteinen (puolustuksellinen) ohjelmointi ja moduulirakenne
  - toimilohkokirjastot ja testatut (sertifioidut) ohjelmistomoduulit, joissa on standardisoidut rajapintojen määritykset.

Tietoturvatietoisuus

- Yleinen virheellinen käsitys: tietoturva on vain tekniikkaa
- Parasta on tietoturvatietoisuus yhdistettynä sopivaan tekniikkaan
- Johdon sitoutuminen on välttämätön edellytys tietoturvalle
- Luotava tietoturvakulttuuri

SESKO

Standardin IEC 61508 yleiset periaatteet

Tekn.lis. Matti Sundquist, Sundcon Oy

matti.sundquist@sundcon.fi

Koneiden ohjausjärjestelmien suunnittelustandardit

IEC/CENELEC:

- IEC 61508 1…7 (”kattostandardi” toiminnallisesta turvallisuudesta) uusittavana
- IEC 61511 1..3 (sovellusstandardi prosessiteollisuudelle) uusittavana
- IEC 62061 (sovellusstandardi koneille)
- IEC 60204-1 (koneiden sähkölaitteistot)

- ISO/CEN:
  - ISO 13849-1 (ohjausjärjestelmästandardi vanha CEN 954-1:1996,joka on voimassa 29.11.2009 saakka)
  - ISO 13849-2 (edellisen kelpuutus) uusittavana.

Tietolähteitä

- IEC:n toiminnallisen turvallisuuden verkkosivut http://www.iec.ch/functionalsafety
- Standardin IEC 61508 osa 0: Toiminnallinen turvallisuus ja IEC 61508
- William E. Goble: Control Systems, Safety Evaluation & Reliability, 2nd Edition, ISA
- Ed Marszal and Eric Scharpf: Safety Integrity Level selection, ISA
- IEC standardit: www.iec.ch, www.sesko.fi
- Sesko SK 65: www.sesko.fi
- Sundcon Oy: www.sundcon.fi

IEC 61508-4 Uusia termejä

Uudet termit käytössä, esimerkiksi:

- Systemaattinen kyvykkyys (systematic capability, SC 1…4)

  "Systematic capability which applies to an element with respect to its confidence that the systematic safety integrity meets the requirements of the specified safety integrity level"

  Jos on toistaan riippumattomat elementit SC1 + SC1 = SC2
- Vaarallinen vikaantuminen (dangerous failure)
- Turvallinen vikaantuminen (safe failure)
- Elementin turvatoiminto (element safety function)

Perusongelmat ja menettelytavat

- Turvallisuuteen liittyvien toimintojen toteuttaminen sähköisten ja elektronisten ohjausjärjestelmien avulla: toiminnallinen turvallisuus (functional safety)
- Turvajärjestelmien luokitus vaadittavan riskin vähentämisen tason mukaisesti
- Ratkaisuna on riskin arvioinnin perusteella asetettavat vaadittavat SIL- tai PL-tasot ja järjestelmän suunnittelun jälkeen arviointi niiden saavuttamisesta.

Turvallisuuden eheys SIL (Safety Integrity Level)

- Todennäköisyys sille, että turvallisuuteen liittyvä järjestelmä toteuttaa hyväksyttävästi vaadittavat turvatoiminnat kaikissa määritellyissä olosuhteissa ja määriteltynä ajanjaksona (”Turvatoiminnon luotettavuus”).
- SIL 1...4 tasot on määritelty kvantitatiivisesti eli kuinka usein korkeintaan turvatoiminnon saa menettää kun sitä tarvitaan (= vaade).

Turvatoiminnot ja vaadetaajudet

Kone tai laite:

- lievät tapaturmat vs. vakavat ja kuolemaanjohtaneet tapaturmat
- käyttö- ja turvatoimintoja ei aina voi erotella (jatkuvien vaateiden toimintamuoto).

Prosessit:

- seurausanalyysit (esim. lukuisia altistuneita, kemikaalipäästön leviäminen)
- käyttö- ja turvajärjestelmät toistaan erotetut (harvojen vaateiden toimintamuoto).

Tiheiden tai jatkuvien vaateiden toimintatapa

- Tiheiden tai jatkuvien vaateiden toimintatapa on kyseessä kun vaade turvatoiminnolle tulee useammin kuin kerran vuodessa tai jatkuvasti
- Turvatoiminnon epäonnistumisen todennäköisyyttä mitataan käsitteellä PFH (Probability of Dangerous Failure/hour) , joka numeerisesti vastaa vikatajuutta λ_d (Failure Rate) seuraavasti:

  $PFH_d \Leftrightarrow \lambda_d$ [1/h]. Esim. PFH = $5x10^{-5}$/h = 0,00005/h $\Leftrightarrow \lambda_d$ = 0,00005/h = noin 0,5/ vuosi = 1 /2vuotta (1 vuosi on 8760 h, noin 10000 h)

  HUOM. PFH_d merkitään nykyisin PFH.

Turvallisuuden eheyden tasot

Tiheiden vaateiden tai jatkuvan toiminnan toimintatapa.

Vaarallisen vikaantumisen todennäköisyys tuntia kohden PFH_d:

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}	

Tiheiden tai jatkuvien vaateiden toimintatapa

- Toisin kuin alajärjestelmien luotettavuutta mitataan PFH:lla, komponenttien vikaantumista mitataan vikaantumistajuudella λ (Failure Rate).
- Komponenttien luotettavuus esitetään tavallisesti keskimäärisenä aikana vaaralliseen vikaantumiseen (Mean Time To Dangerous Failure, MTTFd)

  HUOM. $\lambda = 1/MTTF$ (jos vikatiheys on vakio)

  Esim. $\lambda_d = 0.5/\text{vuosi} = 1/MTTF_d = \text{vuosi}/2 = 0{,}5$ vuotta

Harvojen vaateiden toimintatapa

- Harvojen vaateiden toimintatapa on kysessä kun vaade turvatoiminnolle tulee harvemmin kuin kerran vuodessa
- Turvatoiminnon onnistumisen todennäköisyyttä mitataan käsitteellä PFD (Probability of Failure on Demand)
- Prosessiteollisuudessa käytetään 95 %:sti PFD:tä.

Turvallisuuden eheyden tasot

Turvallisuuden eheydentasot: vaadittavat vikaantumisen enimmäisarvot turvatoiminnolle harvojen vaateiden tapauksessa PFD.

Keskimääräinen vaarallisen vikaantumisen todennäköisyys PFD_{avg} turvatoimintoa vaadittaessa:

SIL 4: $\geq 10^{-5} \ldots < 10^{-4}$

SIL 3: $\geq 10^{-4} \ldots < 10^{-3}$

SIL 2: $\geq 10^{-3} \ldots < 10^{-2}$

SIL 1: $\geq 10^{-2} \ldots < 10^{-1}$

Riskin vähennyskerroin RRF

Riskin vähennyskerroin (Risk Reduction Factor, RRF) mittaa turvatoiminnon aikaan saaman turvatoiminnon vikaantumisen (menettämisen) todennäköisyyden pienentämiskertoimen eli se vastaa SIL-tasoja:

RRF = 1/PFD

- SIL 4 => RRF = 1000…10000
- SIL 3 => RRF = 100…1000
- SIL 2 => RRF = 10…100
- SIL 1 => RRF = 1..10

SIL-tasojen erot

- Vaatimustaso kasvaa olennaisesti mentäessä ylemmälle SIL-tasolle, esim. SIL 2 => SIL 3 työmäärä voi 10-kertaistua
- Tämä johtuu pääasiassa tarkemmmasta suunnittelusta, dokumentoinnista ja ennen muuta ohjelmistokehityksestä (testaukset)

Turvallisuuteen liittyvien ohjaustoimintojen suunnittelu

Tekn.lis. Matti Sundquist, Sundcon Oy

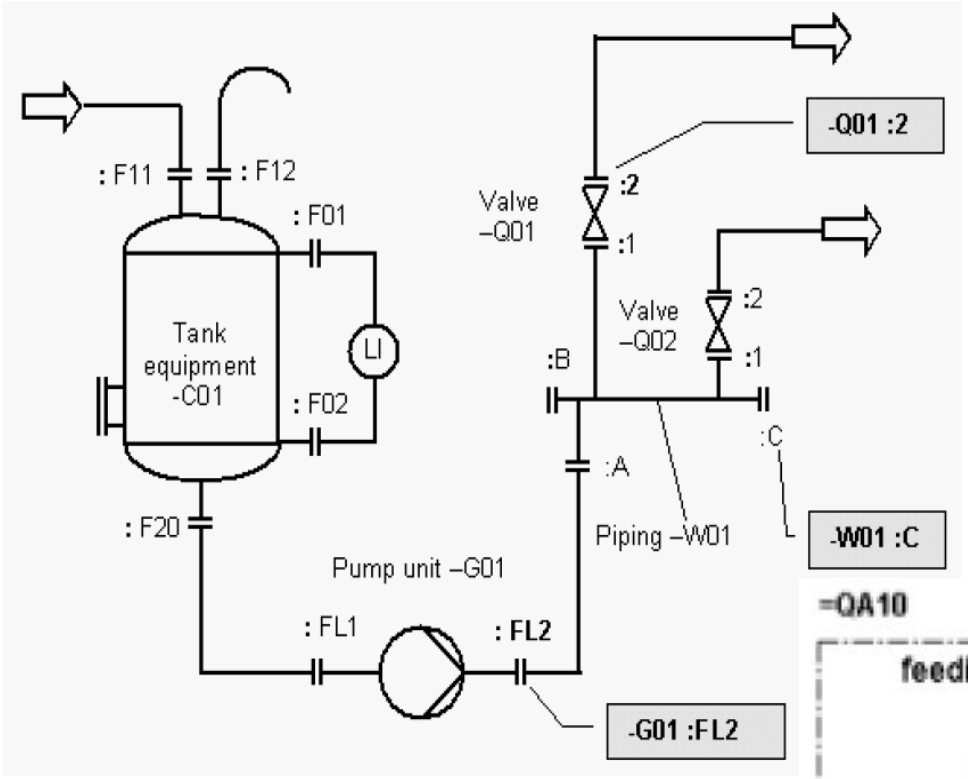
www.sundcon.fi

matti.sundquist@sundcon.fi

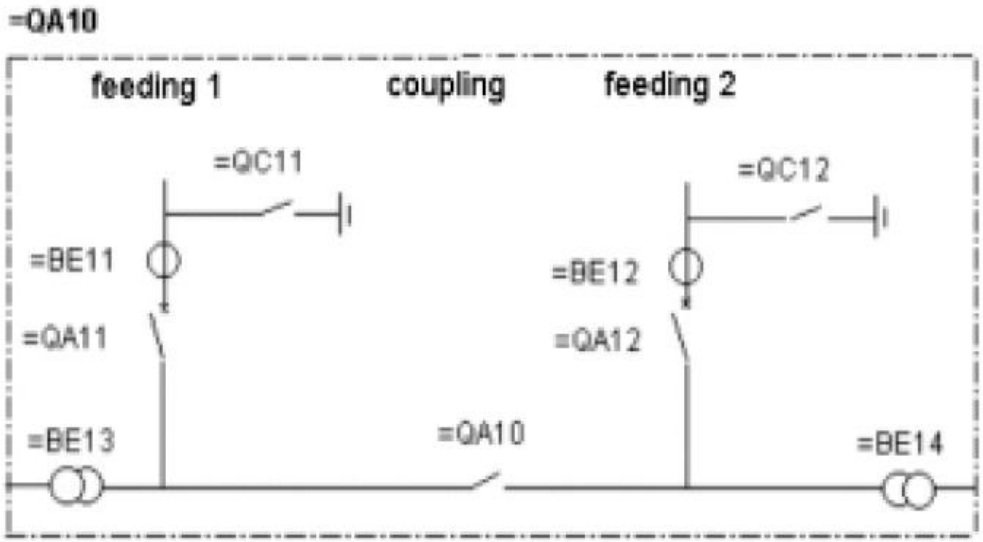
Suunnitteluvaiheet

- Peruskonsepti
- Vaara- ja riskianalyysi
- Kokonaisturvallisuuden ja laadun hallinta
- Prosessi- ja sovellussuunnittelu
- Turvallisuuden perussuunnittelu
- Turvatoimintojen määrittely
- Järjestelmän valinta
- Toteutussuunnittelu
- Rakentaminen/FAT-testaus
- Käyttöönotto/SAT-testaus
- Riippumaton ulkopuolinen arviointi
- Käyttötuki, seuranta ja huolto
- Jatkokehittäminen
- Muutokset ja modernisointi
- Käytöstä poisto

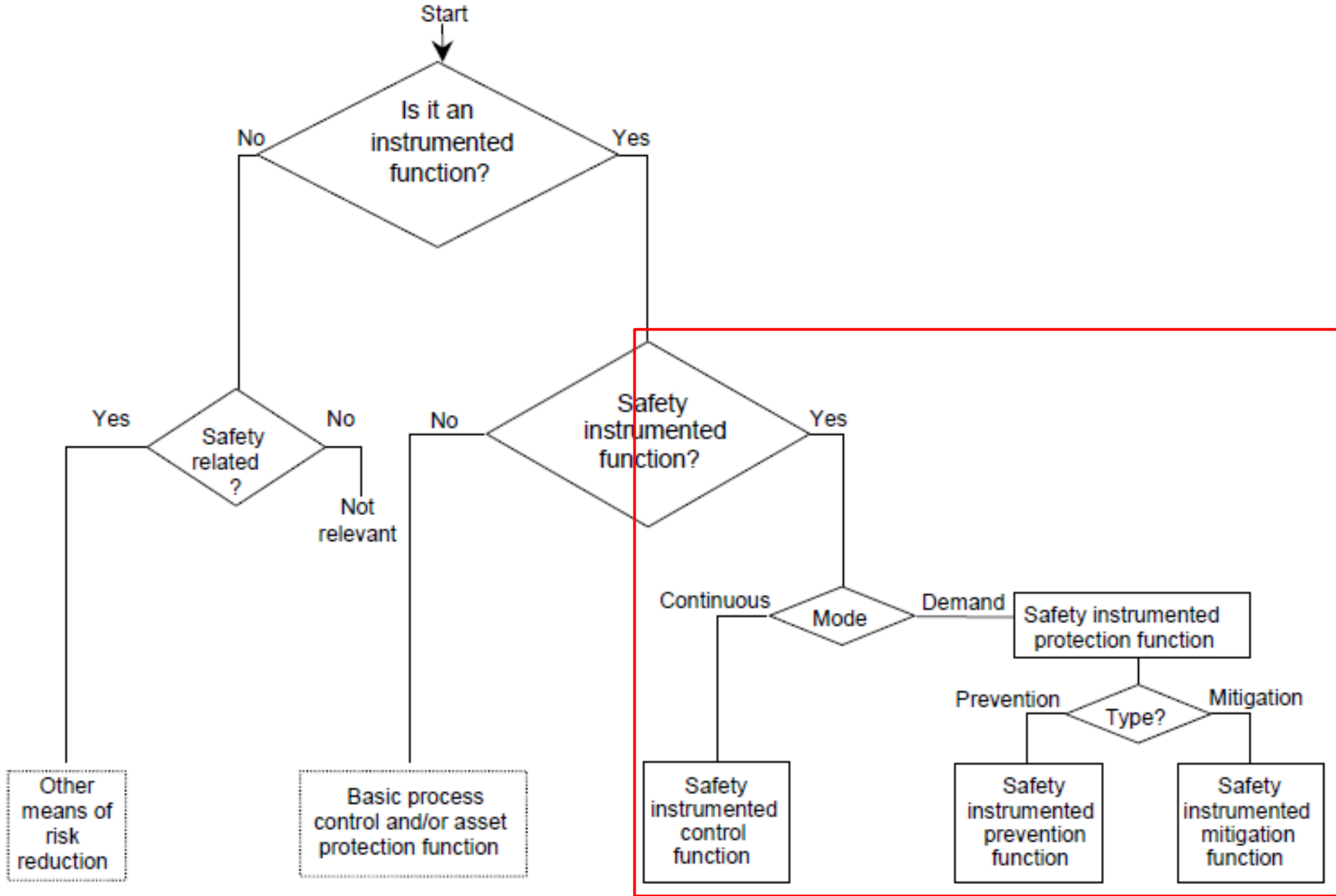
Käyttöautomaation suunnittelu



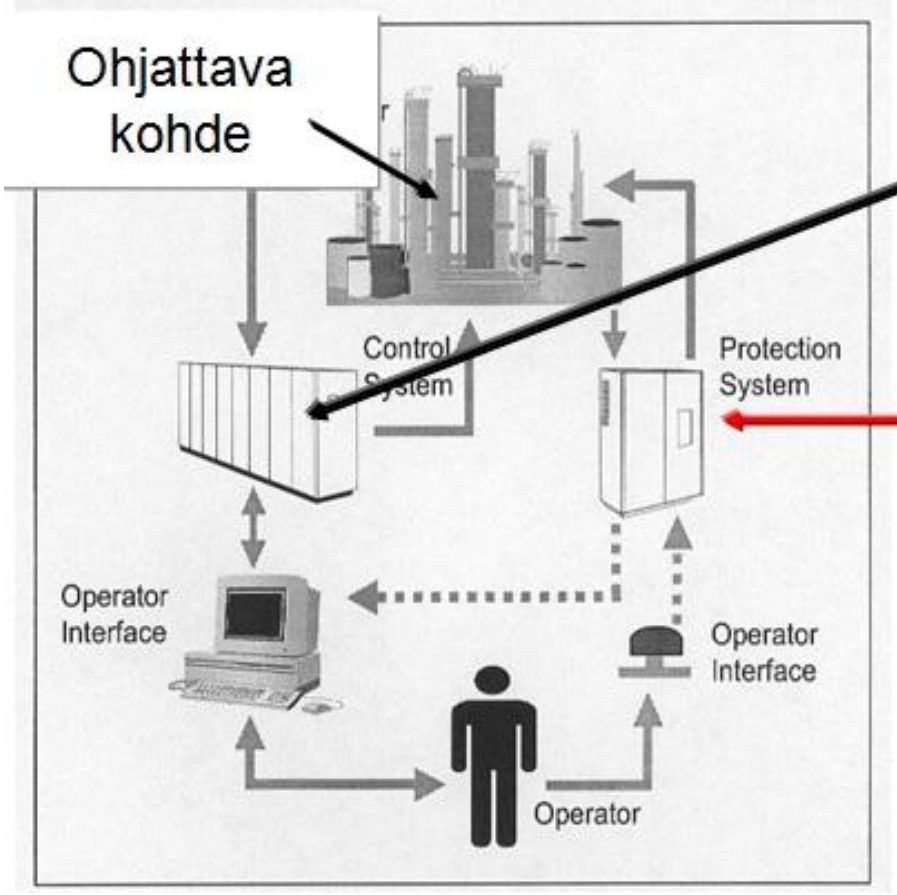
Kohteet muodostavat määritellyn kokonaisuuden aineen, energian tai informaation käsittelemiseksi. Kohteilla on oltava yksilöllinen tunnuksensa, jotta niihin liittyvä informaatio on hallittavissa.



Toimintojen erittely



Tyypillinen prosessin turvajärjestelmä



Perusjärjestelmä

(Basic Process Control System, BPCS

Turvajärjestelmä

(Safety Instrumented system, SIS)

Terminologiaa

Standardien EC 61508 ja 61511 termien eroja

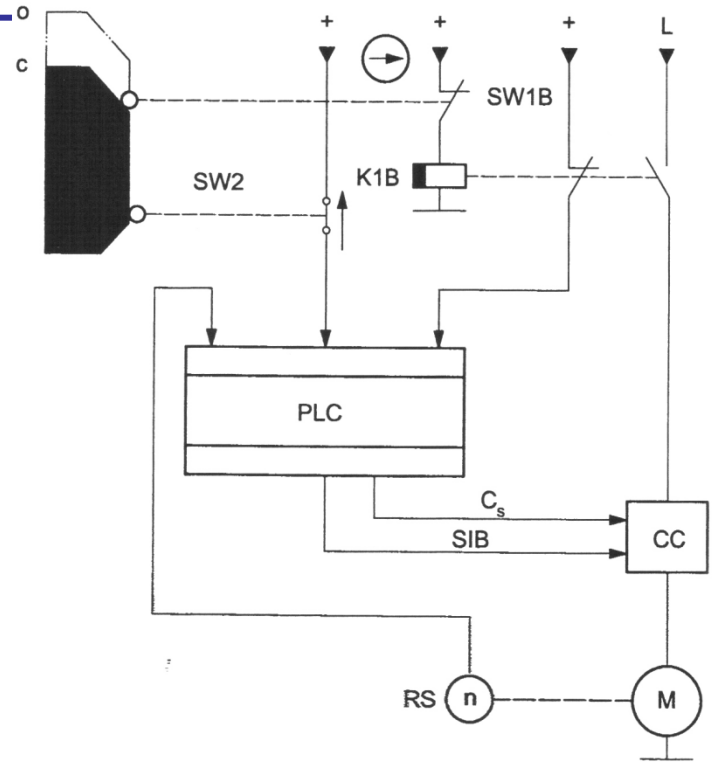
A.2 Terminology

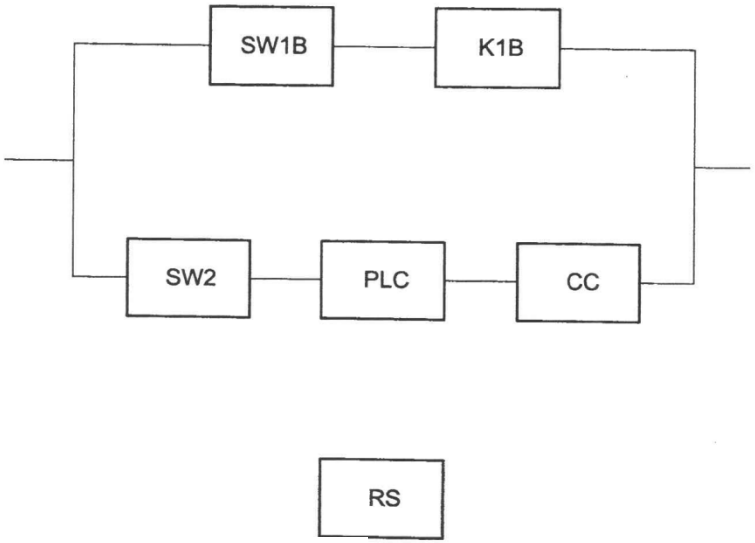
IEC 61508-4	IEC 61511-1	Comment
E/E/PE safety related system	SIS	IEC 61508 refers to E/E/PE safety related systems while IEC 61511 refers to safety instrumented systems
PES	SIS	IEC 61508 "PES" includes sensors and final control elements, while IEC 61511 uses the term SIS.
Process control system	Basic process control system	Basic process control system is a global term for the process sector
EUC	Process	IEC 61508 refers to EUC (equipment under control) while IEC 61511 refers to process
Safety function	Safety instrumented function (SIF)	IEC 61508 safety function implemented by E/E/PES, other technology safety related system, or external risk reduction facilities. IEC 61511 SIF is implemented solely by SIS

Vaatimusmäärittely

- Vaatimukset laitteiden turvallisuuden eheydelle
  - arkkitehtuuriset rajoitukset
  - satunnaisten vaarallisten vikaantumisten taajuus.
- Vaatimukset järjestelmän turvallisuuden eheydelle
  - vikaantumisten välttäminen
  - järjestelmän vikojen hallinta.
- Vaatimukset järjestelmän toiminnalle vikaantumisen tunnistuksessa.
- Vaatimukset turvallisuuteen liittyvän järjestelmän ohjelmiston suunnitteluun ja kehittämiseen.

Lohkokaavioesitys





Merkintöjen selitys:

SW1B	toimintaankytkentälaite
K1B	kontaktori
SW2	kytkin
PLC	ohjelmoitava logiikka
CC	virranmuunnin
RS	pyörimisanturi

Laitekaavio ja sen luotettavuuslohkokaavio

Turvallisuuteen liittyvän ohjausjärjestelmän osia

Laitteiden ja ohjelmiston kokoonpano (arkkitehtuuri):

- anturit (esim. rajakytkimet)
- ohjelmoitava elektroniikka (logiikka)
- toimilaitteet (esim. venttiilit, moottorit)
- sulautettu ohjelmisto (esim. ASIC)
- sovellusohjelmisto (esim. lohkokaaviot, parametrointi)
- jne.

Turvajärjestelmän suunnittelu

Turvajärjestelmä voidaan toteuttaa kahdella vaihtoehtoisesti:

a) valitaan järjestelmä etukäteen suunnitelluista järjestelmistä (tai niiden osista), jos ne täyttävät turvallisuusvaatimusten määrittelyn (Safety Requirements Specification, SRS) vaatimukset

   HUOM. Tuotesertifikaatit tai laskelmat eivät sellaisenaan takaa turvallisuutta.

a) suunnitellaan turvallisuuteen liittyvä järjestelmä kokonaan itse.

   HUOM. Lopputuloksen turvallisuustason ratkaisee turvallisuuden hallinta (Safety Management).

Arkkitehtuuri
Satunnaisvikaantumiset
Diagnostiikan kattavuus
Yhteisvikaantumiset

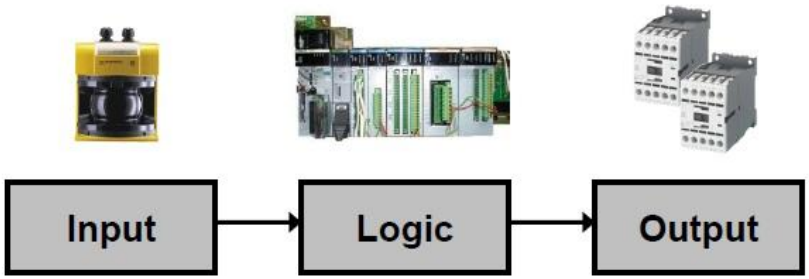
Tekn.lis. Matti Sundquist, Sundcon Oy

www.sundcon.fi

matti.sundquist@sundcon.fi

Alajärjestelmät

Jokaisen alajärjestelmän parametrien avulla lasketaan alajärjestelmän PFD rakenteen muodostavien kanavien ja testauskanavien sekä siihen kuuluvien lohkojen ja/tai elementtien parametrien avulla.



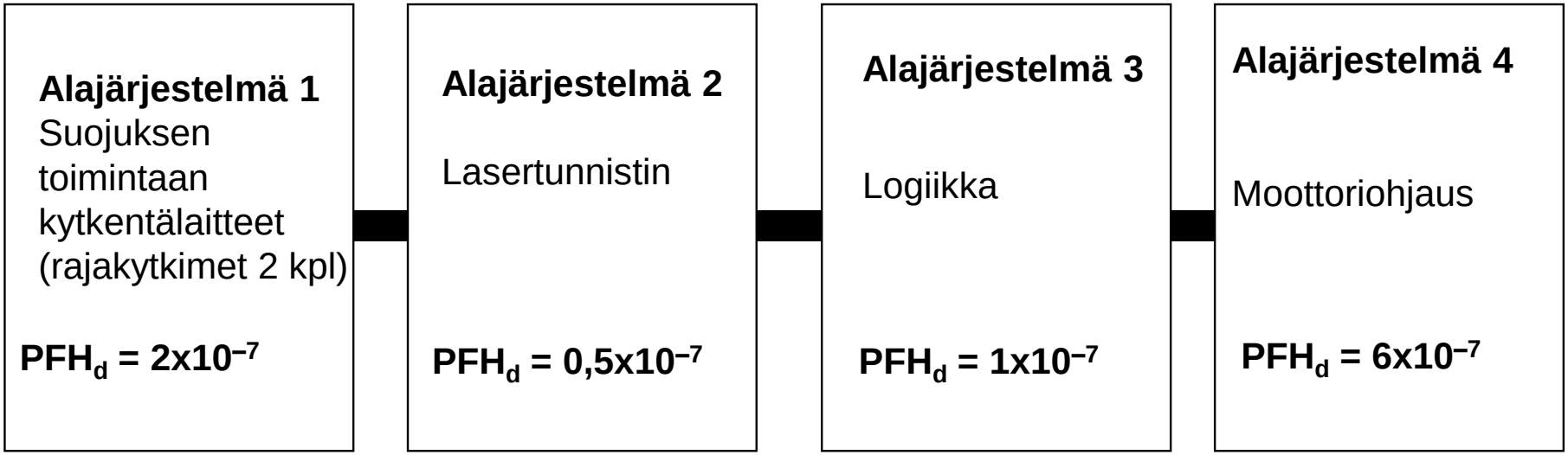
Lähde: Siemens

Usein valitaan kolme alajärjestelmää (tulot, logiikka, lähdöt)

Yksikanavaisen järjestelmän vaarallinen vikaantumien

Tiheiden vaateiden toimintatapa

Esimerkiksi vaadittava SIL-taso on 2 eli $PFH_d = 10^{-7}…10^{-6}$



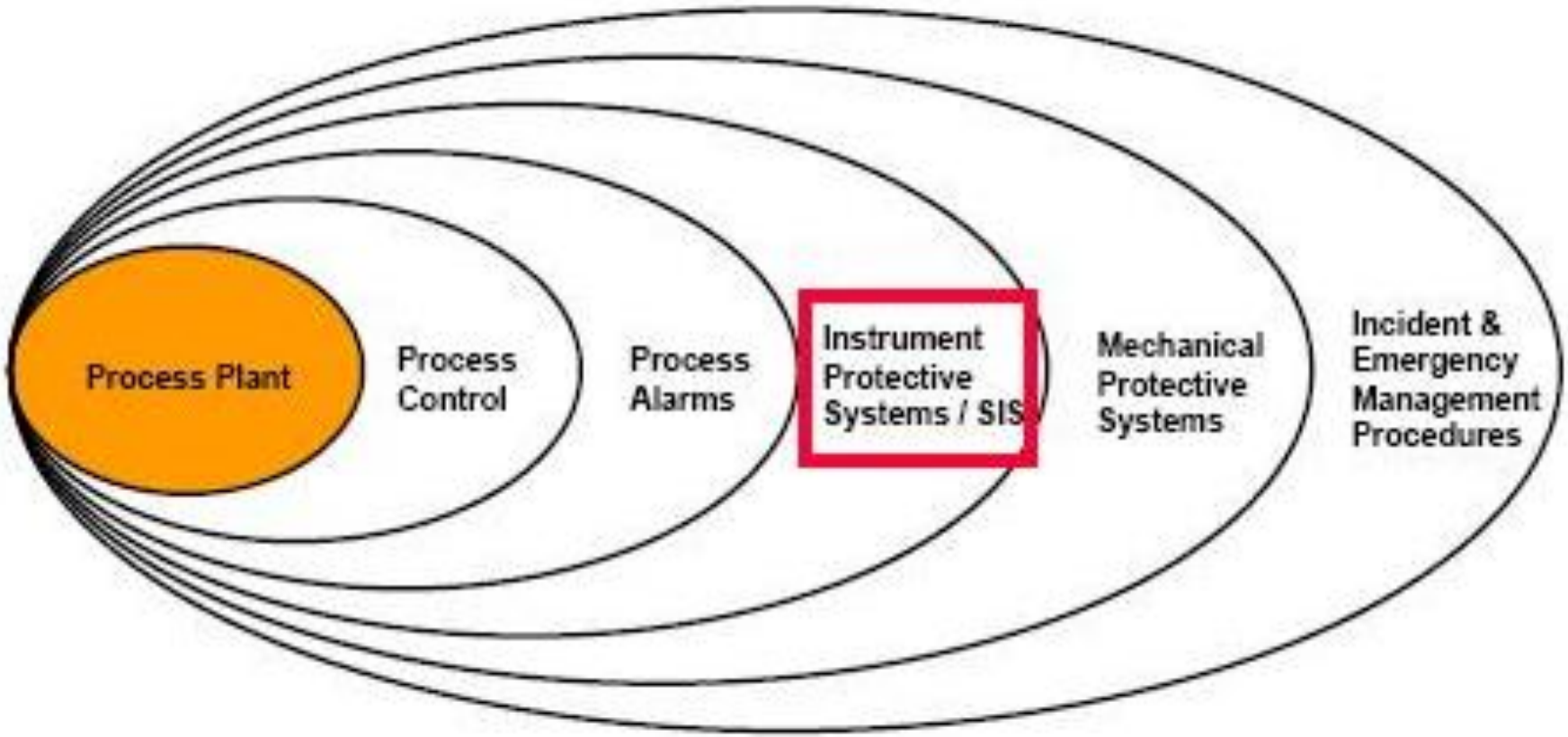
Järjestelmän vaarallisen vikaantumisen todennäköisyys:

$PFH_{dtot} = PFH_{d1} + ... + PFH_{dn} + P_{TE}$ TE = Tiedonsiirron vikaantuminen

$PFH_{dtot} = (2 \times 10^{-7}) + (0{,}5 \times 10^{-7}) + (1 \times 10^{-7}) + (6 \times 10^{-7}) = 9{,}5 \times 10^{-7}$

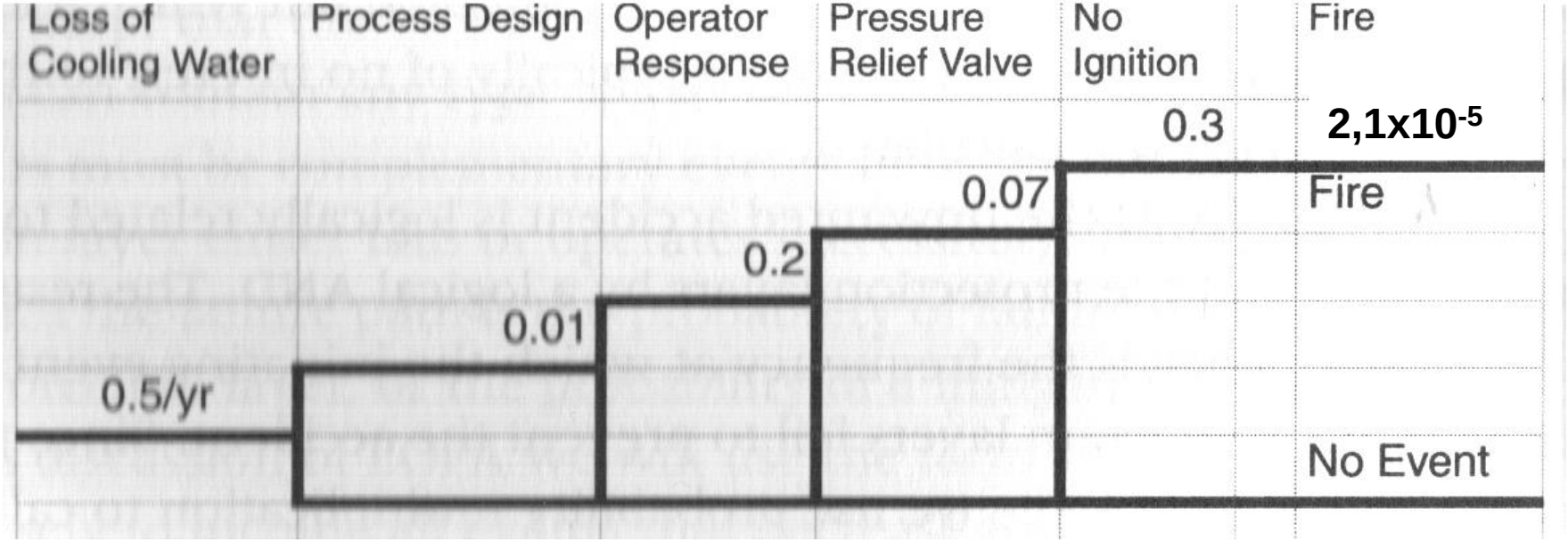
$PFH_{dtot} < 10^{-6}$ => SIL 2

LOPA-malli


Process Plant
Process Control
Process Alarms
Instrument Protective Systems / SIS
Mechanical Protective Systems
Incident & Emergency Management Procedures

LOPA diagrammi

Harvojen vaateiden toimintatapa



Tulipalon taajuus: λ_{loppu} = **0,5 x 0,01 x 0,2 x 0,07 x 0,3 = 2,1x10^{-5} 1/h = 1,84 vuotta**

1 vuosi = 8760 tuntia

Redundanttinen arkkitehtuuri

Monikanavaiset järjestelmät MooN

M out of N (MooN)

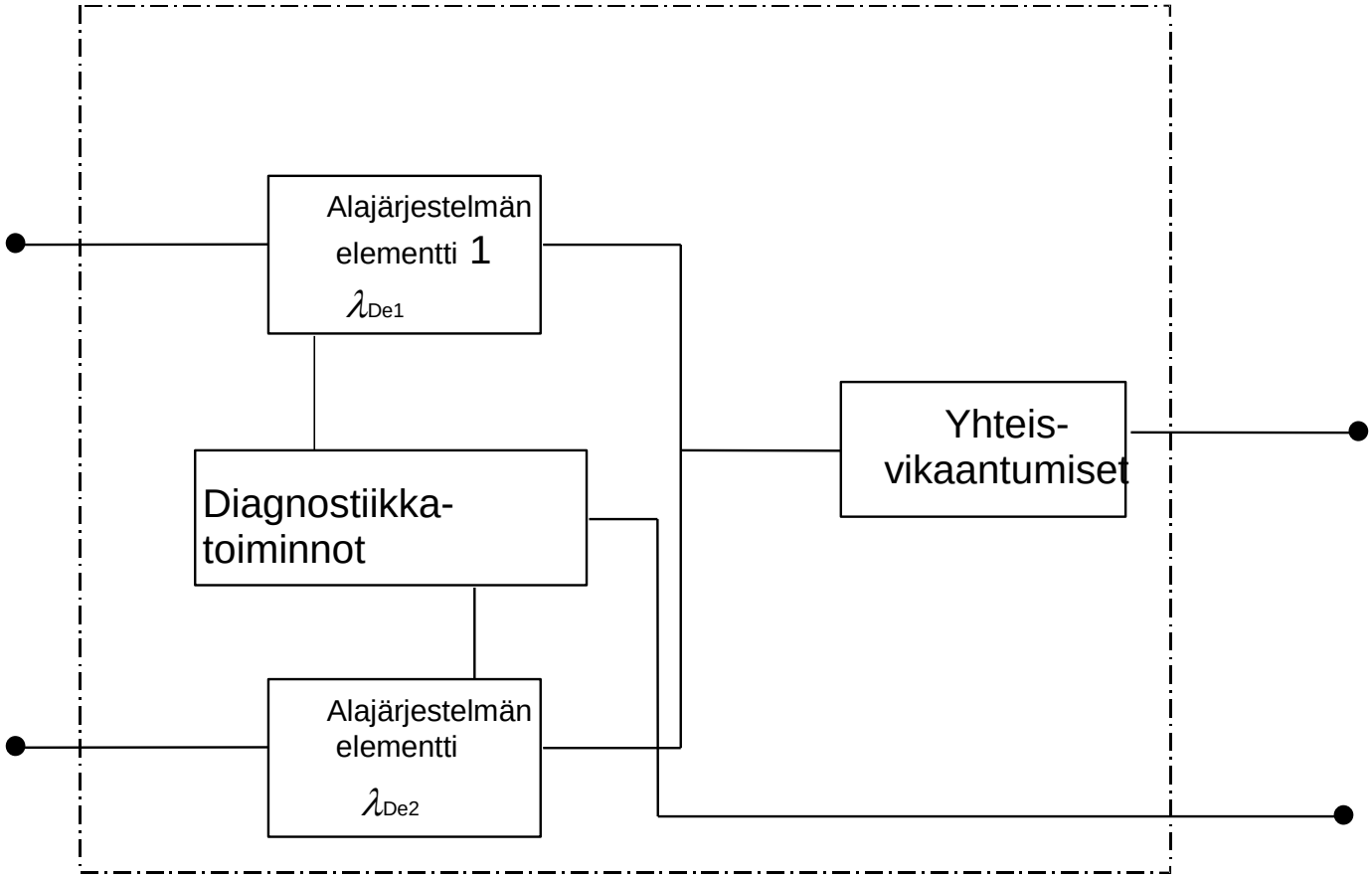
N = käytettävien kanavien lukumäärä,

M = Turvatoimintoon vähintään tarvittavien kanavien lukumäärä

- 1oo1
- 1oo2
- 1oo2D
- 1oo3
- 2oo2
- 2oo2D
- 2oo3
- 2oo4

Esimerkki 1oo2-rakenteesta

Järjestelmän perusarkkitehtuuri D: vikasietoisuus (HT) yksi ja diagnostiikkatoiminnot mukana



Järjestelmän elementit

λ_{De1} : alajärjestelmän elementin 1 vaarallisten vikaantumisten taajuus

$\mathbf{DC_1}$: alajärjestelmän elementin 1 diagnostiikan kattavuus

λ_{De2} : alajärjestelmän elementin 2 vaarallisten vikaantumisten taajuus

$\mathbf{DC_2}$: alajärjestelmän elementin 2 diagnostiikan kattavuus

$$\lambda_{DssD} = (1 - \beta)2 \{[\lambda_{De1} * \lambda_{De2} * (DC_1 + DC_2)] * T_2/2 +$$
$$[\lambda_{De1} * \lambda_{De2} * (2 - DC_1 - DC_2)] * T_1/2 \} + \beta * (\lambda_{De1} + \lambda_{De2})/2$$

$$PFH_{DssD} = \lambda_{DssD} * 1h$$

Diagnostiikka

Diagnostiikan kattavuus DC (Diagnostc Coverage)

$$DC = \sum \lambda_{\mathrm{DD}} \; / \; \lambda_{\mathrm{Dtotal}}$$

Turvallisten vikojen osuus SFF (Safe Failure Fraction)

$$\left(\sum \lambda_{\mathrm{S}} + \sum \lambda_{\mathrm{DD}}\right) / \left(\sum \lambda_{\mathrm{S}} + \sum \lambda_{\mathrm{D}}\right)$$

Erilaiset viat:
S = Turvallinen (Safe), D = vaarallinen (Dangerous), DD = havaittu vaarallinen (dangerous Detected), total = kaikki)

Standardissa IEC 61508-6 on pisteytysmenetelmä yhteisvikojen arvioimiseksi (beta-tekijä).

Esimerkki diagnostiikasta

- Yksinkanavainen arkkitehtuuri: yksi vikaantuminen johtaa turvallisuuteen liittyvän ohjaustoiminnon vikaantumiseen, mutta järjestelmässä on vikadiagnostiikkaa DC:

  $PFD_D = PFD_{De1} (1 - DC_{D1}) + \ldots + PFD_{Den} (1 - DC_{Dn)}$,
  missä

  D = vaarallinen (Dangerous), e = elementti, DC1..n = elementtien 1…n diagnostiikan kattavuus

Arkkitehtuurin rajoitukset

Suurin turvallisuuden eheyden taso (SIL Claim Limit), joka voidaan osoittaa kyseistä järjestelmää käyttävälle turvallisuuteen liittyvälle ohjaustoiminnolle

Turvallisen vikaantumisen osuus (SFF)	**Laitteiston vikasietoisuus (ks. huomautus 1)**		
	0	**1**	**2**
< 60 %	**Ei sallittu**	**SIL1**	**SIL2**
60 % - < 90 %	**SIL1**	**SIL2**	**SIL3**
90 % - < 99 %	**SIL2**	**SIL3**	**SIL3**
≥ 99 %	**SIL3**	**SIL3**	**SIL3**
Huom 1. Laitteiston vikasietoisuus *N* tarkoittaa, että *N*+1 vikaa voi johtaa turvatoiminnon menettämiseen.			

Esimerkki arkkitehtuurin rajoituksesta

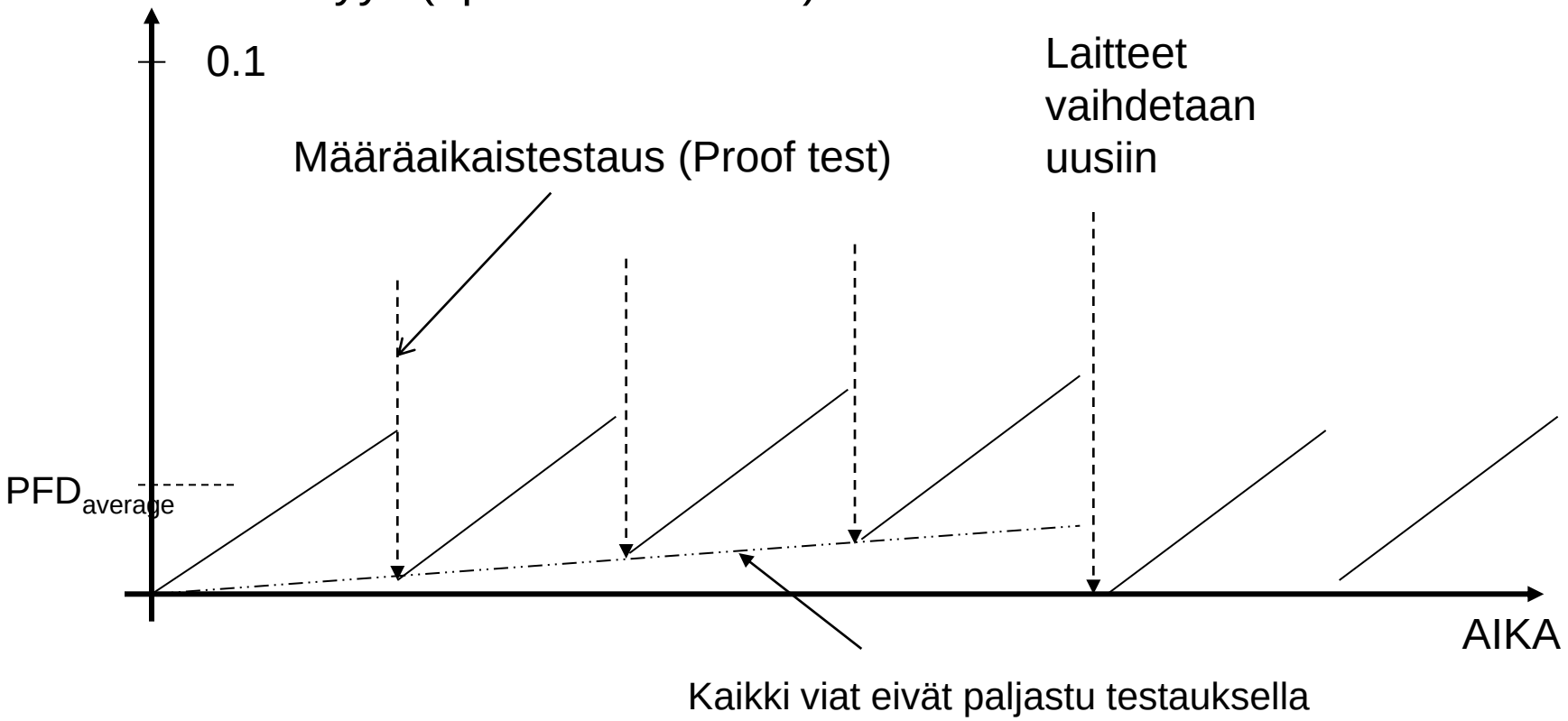
FT (Fault Tolerance) eli vikasietoisuus = 1

$$SFF = (\lambda_{S1} + \lambda_{DD1} + \lambda_{S2} + \lambda_{DD2}) / (\lambda_{S1} + \lambda_{D1} + \lambda_{S2} + \lambda_{D2})$$

Arkitehtuurin rajoitusten taulukon mukaisesti:

jos SFF < 60 % , SIL = 1
jos 60 % < SFF < 90 % , SIL = 2
jos 90 % < SFF, SIL = 3

Määräaikaistestaukset



Yhteisvikaantuminen

- Yhteisvikaantuminen (Common Cause Failure, CCF) tarkoittaa kahta tai useampaa vikaantumista, jotka johtuvat samasta syystä (esim. EMC-häiriö, jännitepiikki).
- Yhteisvikaantumiset on ongelma redundanttisissa järjestelmissä (esim. kahdennukset).
- Yhteisvikaantumiset voivat liittyä:
  - arkkitehtuuriin (useampi kanava)
  - eri teknologioiden yhdistelmään (erilaiset kanavat)
  - sovellukseen (
  - ympäristötekijöihin (EMC)
- Standardissa IEC 61508-6 on pisteytysmenetelmä yhteisvikojen arvioimiseksi (beta-tekijä).

Laitteiston systemaattinen turvallisuuden eheys

Tekn.lis. Matti Sundquist, Sundcon Oy

www.sundcon.fi

matti.sundquist@sundcon.fi

Systemaattinen turvallisuuden eheys

- Kolme vaihtoehtoista reittiä:
  - Reitti 1S: systemaattisten virheiden välttäminen ja niiden hallinnan vaatimukset
  - Reitti 2S: näyttö siitä, että sekä laitteisto että ohjelmisto on käytössä hyväksi koettu (Proven In Use, PIU)
  - Reitti 3: Tämä koskee etukäteen kehitettyjä (valmiita) ohjelmistoja (ohjelmistoelementtejä).

Systemaattisten virheiden hallinta #1

- Menetelmät fyysisen ympäristön hallintaan (esimerkiksi lämpötila, kosteus, vesi, tärinä, pöly, korroosiota aiheuttavat aineet, sähkömagneettinen yhteensopivuusja sen vaikutukset).
- Menetelmät jännitteen katkeamisen, jännitteen vaihteluiden, ylijännitteen ja alijännitteen vaikutusten varalta.
- Ohjelman suorituksen valvontaa virheellisten ohjelmajaksojen paljastamiseksi.
- Menetelmät tietoliikenteen aiheuttamien virheiden vaikutusten hallintaan.
- Ylimitoitus sopivalla kertoimella (esim. 1,5), jos pienempi kuormitus tai ylimitoitus parantaa luotettavuutta.

Systemaattisten virheiden hallinta #2

Menetelmiä:

- Käytetään lepovirtaperiaatetta.
- Pakkokäyttöinen toimintatapa.
- Pakkotoimiset laitteet:
  - mekaanisesti toisiinsa kytketyt koskettimet
  - suora avaustoiminto.
- Vikaantumismuotojen suuntaaminen (fail safe periaate) .
- Divergenttinen laitteisto.
- Vikaantumisten paljastaminen automaattsilla testauksilla.
- Redundanttisen laitteiston testaukset .