Teollisuusautomaation standardit
Osio 2

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

Toiminnallinen turvallisuus: periaatteet

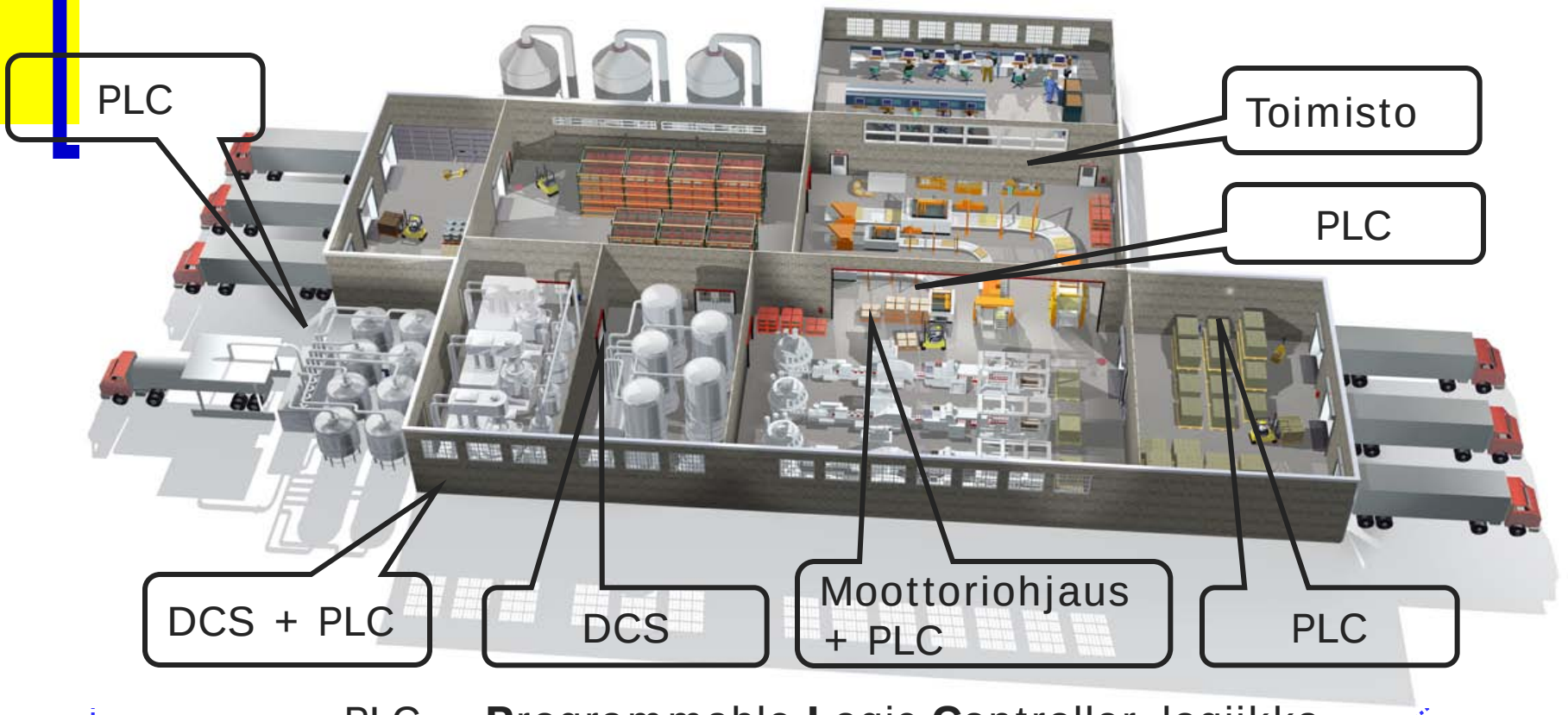
Matti Sundquist
Sundcon Oy

Teollisuusautomaatio

- Elektroniikan kehitys on nopeuttanut teollisuusautomaation käyttöönottoa.
- Nykyaikaiset tehtaat integroituvat:
  - vaakasuoraan: koneita, laitteita ja prosesseja yhdistetään toisiinsa
  - pystysuoraan: valmistuksen automaatiojärjestelmiä yhdistetään muihin automaatio- ja hallintojärjestelmiin ja koko tehdasta ohjataan yhtenä kokonaisuutena.

Ks. seuraavat kuvat.

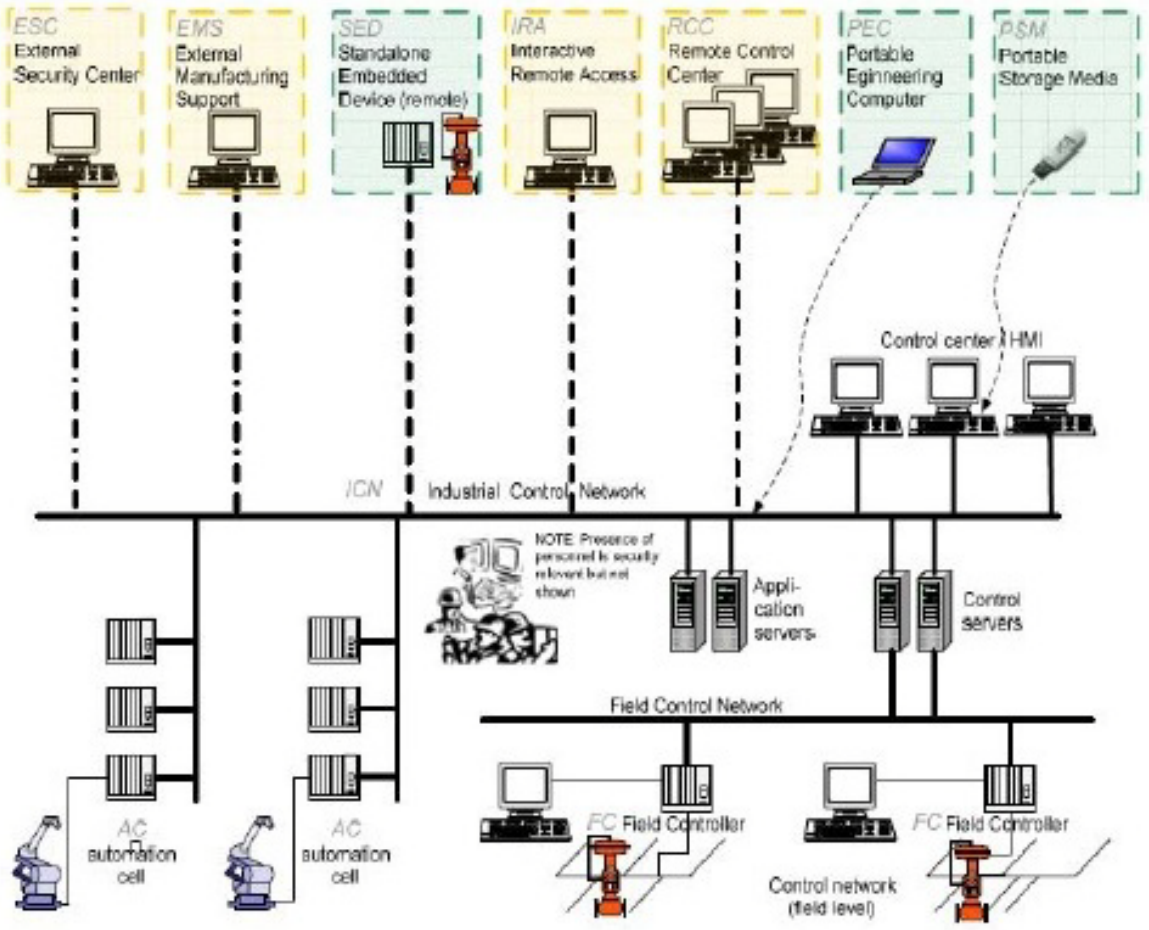
Automaatiojärjestelmien vaakasuora integraatio



PLC = **P**rogrammable **L**ogic **C**ontroller, logiikka

DCS = **D**istributed **C**ontrol **S**ystem, hajautettu ohjaus

Automaatiojärjestelmien pystysuora integraatio

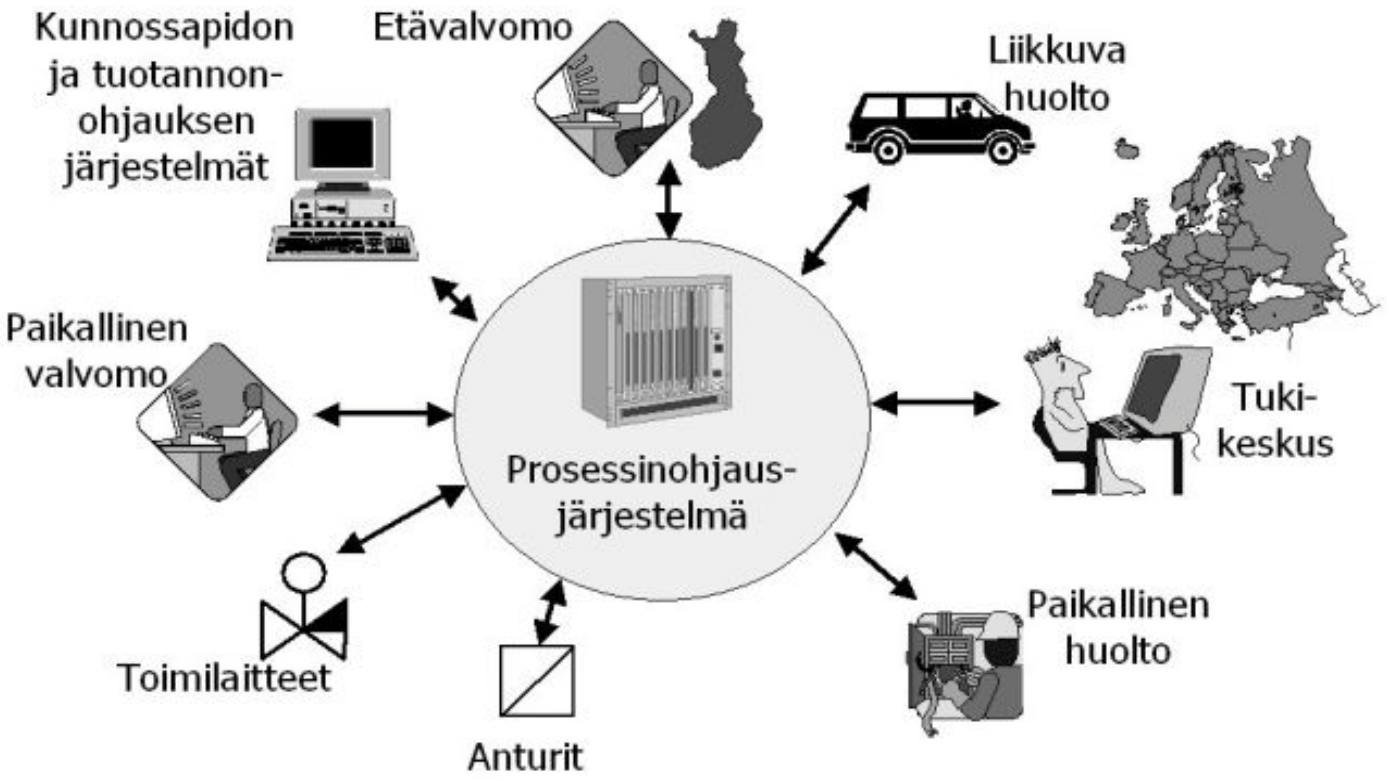


Teollisuus-ethernet

Kenttäväylät

Anturi-/laiteväylät

Automaation liityntöjä muihin tietoverkkoihin

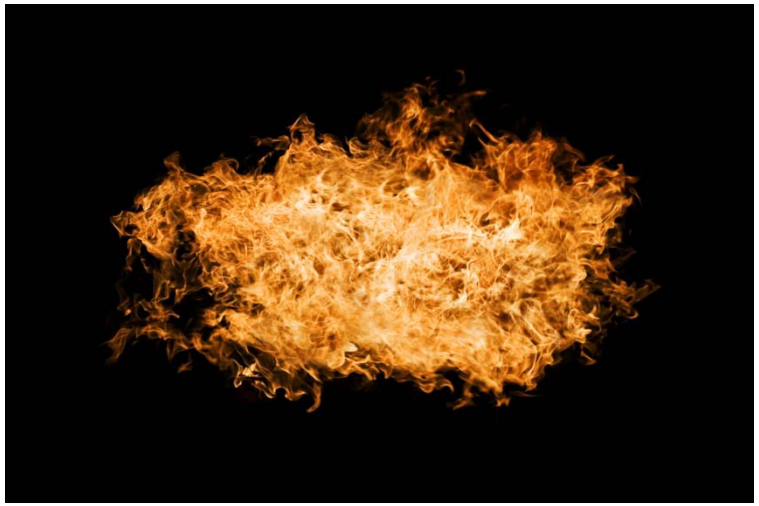


Lähde: Fortum

Ei-toivotut tapahtumat

Vahingot:

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



Lähde:
futureimagebank.com

Teollisuusautomaation riskit

- Teollisuusautomaatio aiheuttaa turvallisuusongelmia seuraavilla alueilla:
  - ohjelmistojen virheet
  - järjestelmien yhteensopivuuden ongelmat
  - tietoturvauhkat
  - tietoliikenteen virheet
  - langaton ohjaus ja etäohjaus
  - operaattorin tekemät virheet.

Teollisuusautomaation turvallisuus

- Turvallisuus on yhdistettävä saumattomasti muihin toimintoihin ja se on otettava huomioon jo suunnittelun aikana, koska valmiin järjestelmän korjaaminen voi olla hankalaa.
- Automaatiojärjestelmien suunnittelussa tarvitaan turvallisuuden hallintajärjestelmää.
- Turvallisuus on varmistettava suunnittelun ja toteutuksen elinkaaren kaikissa vaiheissa ja kaikkien osapuolten vastuut on tehtävä alusta alkaen selväksi.
- Perustuu standardisarjaan IEC 61508 (ks. osio 3).

Toiminnallinen turvallisuus

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

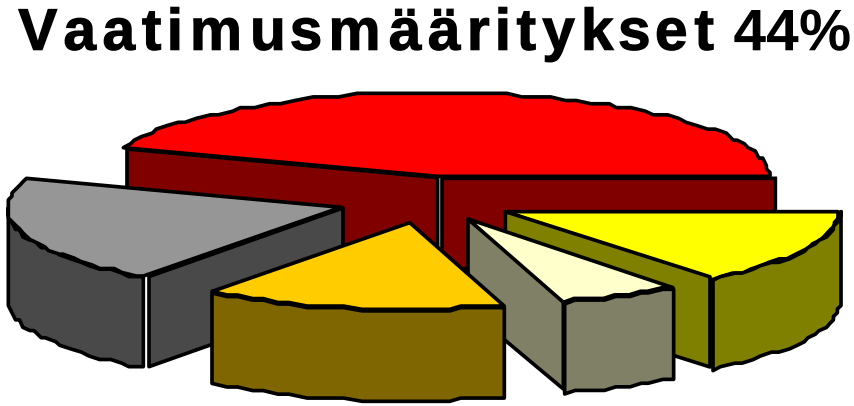
oikeasta toiminnasta.

Toiminnallisen turvallisuuden kaksi lähtökohtaa

1. Turvatoimintojen oikea toiminta, joka perustuu riskin arvioinnin tuloksiin ja vaatimusmäärittelyyn eli turvatoiminnoilla estetään ei-toivottuja tai vahingollisia toimintoja.
2. Edellä mainittujen (oikeiden) turvatoimintojen luotettavuus, joka perustuu riskin arvioinnin tuloksista johdettuihin suoritustasoihin.

Perustana on standardisarja IEC 61508 ja sen sovellusstandardit eri aloilla
(koneet, prosessit jne.)

Vahinkojen syitä (prosessiteollisuus)



Enemmän painoa vaatimusmäärityksiin ja muutosten hallintaan!

Lähde: HIMA

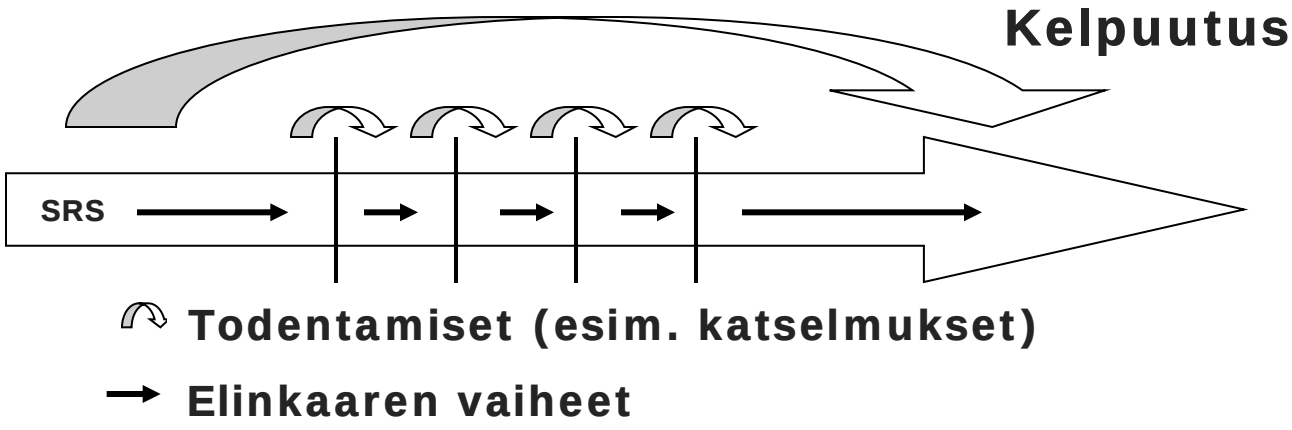
Toiminnallisen turvallisuuden hallinta

- Toiminnallisen turvallisuuden hallintaan tarvitaan järjestelmällistä lähestymistapaa:
  - turvallisuuden elinkaaritarkastelu
  - rakenteinen (puolustuksellinen) ohjelmointi ja moduulirakenne
  - toimilohkokirjastot ja testatut (sertifioidut) ohjelmistomoduulit, joissa on standardoidut rajapintojen määritykset

Katso osiot 3 ja 4.

Turvallisuuden elinkaarimalli

Edellisen vaiheen lähtötiedot ovat seuraavan vaiheen tulotietoja



SRS = Turvallisuusvaatimusten erittely
(**S**afety **R**equirements **S**pecification)

Lähde: M. Sundquist

Tietolähteitä

Toiminnallisen turvallisuuden tietolähteitä:

- SESKOn komitea SK 65 ”Teollisuusprosessien ohjaus” www.sesko.fi
- Suomen Automaatioseura ry (turvallisuusjaosto), www.automaatioseura.fi
- IEC
  Functional Safety Zone
  (standardisarja IEC 61508)

Tietoa standardeista

- Säädökset

  www.finlex.fi
- Suomen standardisoimisliitto SFS ry
  (mm. luettelo voimassaolevista SFS-standardeista)

  www.sfs.fi
- SESKO ry – sähkö- ja elektroniikka-alan standardit
  www.sesko.fi
- MetSta ry – metalliteollisuuden standardit

  www.metsa.fi

Tietoa standardeista

- IEC – kansainväliset sähkö- ja elektroniikka-alan standardit
  www.iec.ch
- CENELEC - eurooppalaiset sähkö- ja elektroniikka-alan standardit
  www.cenelec.eu
- ISO – kansainväliset standardit (muut kuin sähkö)
  www.iso.org
- CEN – eurooppalaiset standardit (muut kuin sähkö)
  www.cen.eu