Ydinvoimalaitosten automaatio ja sen viranomaisvalvonta

TKK, TCS Forum 12.1.2007

Juhani Hyvärinen
STUK / Ydinvoimalaitosten valvonta

STUK

Sisältö

- Ydinvoimalaitoksen toiminta; sen
  - vaarallisuus
  - turvallisuus
- Automaation tehtävät ja käytettävät tekniikat
  - säätö
  - suojaus
  - esimerkkeinä Teleperm XP ja XS
- Turvallisuusvaatimukset ja niiden täyttymisen arvioiminen
  - viranomaisvalvonta

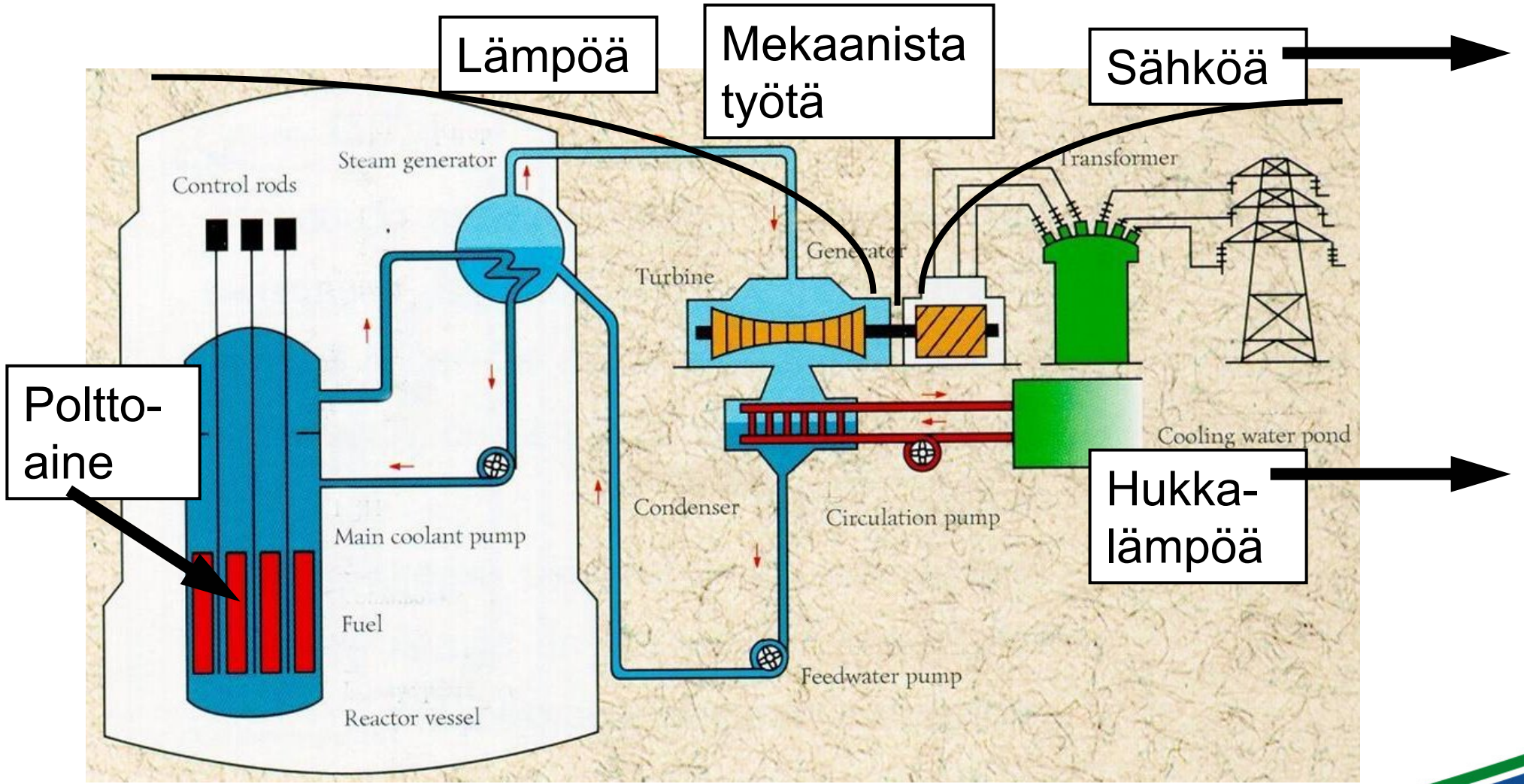
Ydinvoimalaitoksen toiminta

Ydinvoimalaitoksen tekniikkaa

- Ydinvoimala on sähköä tuottava lämpövoimala
  - uraaniytimien fissioreaktio ⇒ lämpö ⇒ sähkö + (hukka)lämpö
- Lähin vertailukohta hiili(lauhde)voimala; ydinvoimalassa
  - eri polttoaine
  - matala höyrynpaine ja lämpötila
  - huono hyötysuhde (sähköteho/p.a.:n lämpöteho)

	Höyryn paine (bar)	*Lämpötila (°C)*	*Hyötysuhde (%)*	*Polttoaineen kulutus vuodessa / 1000 MWe*
Ydin	*45-80*	*250-300*	*33-38*	*30 tn*
Hiili	*250*	*550*	*45*	*1 800 000 tn*

Voimalaitosprosessi



Ydinvoimalaitoksen vaaratekijät (1/2)

- Ominaisvaara on säteily
  - fissiotuotteet radioaktiivisia: paljon, tallessa polttoaineessa
  - aktivoitumistuotteet: ”vähän”, kulkevat (primääri)prosesseissa
  - suora säteily reaktorista - vain käynnin aikana
  - käytetty polttoaine säteilee pitkään

- Turvallisuussuunnittelu tähtää aktiivisuuden leviämisen estämiseen
  - normaalikäytössä
  - mahdollisissa häiriöissä ja onnettomuuksissa
  - reaktorisydämen tuhoutuessa (ns. vakava onnettomuus)
  - vaikka laitos joutuisi pahanteon kohteeksi - paitsi sotatoimet

Ydinvoimalaitoksen vaaratekijät (2/2)

- Tyypillisiä aktiivisuusmääriä käynnin aikana
  - reaktorisydämessä >100 miljoonaa TBq (tonneja aktiivisuutta); reaktorin lämpötehosta 7% on tätä
  - primäärijäähdytteessä n. 200 TBq (grammoja aktiivisuutta)
  - tuorehöyryssä 3 TBq/s (kiehutuslaitos), 0,000 000 014 TBq/s (painelaitos)
- Tyypillisiä annosnopeuksia
  - kevytvesireaktorin kyljessä 500 Sv/h (γ), 2000 Sv/h (n)
  - Lo: höyrystintilassa 0,1~0,8 Sv/h (γ), 0,1~1,7 Sv/h (n); turbiinilaitoksella ~0,000 000 2 Sv/h (pelkkää taustaa)
  - Ol: suojarakennus ~0,025 Sv/h (γ), turbiinilaitoksella <0,025 Sv/h
- vuosiannosraja 0,020 Sv; hengenvaarallinen 5-6 Sv

Turvallisuussuunnittelun perusidea

- Pidetään radioaktiiviset aineet tallessa ja pois ihmisten ilmoilta
- Keino: ”syvyyspuolustus”
  - rakenteellinen = leviämisesteet
    - tiivis polttoaine
    - ehjä primääripiiri
    - tiivis suojarakennus
  - toiminnallinen = häiriöiden/onnettomuuksien
    - ennaltaehkäisy
    - vaikutusten kestokyky
    - seurausten lieventäminen
- Kehitetty turvallisuussuunnittelun perusfilosofiaksi jo 50-luvulla


Toiminnallinen syvyyspuolustus
(Radiologisten ympäristö-) Seurausten **rajoittaminen**
Vakavien onnettomuuksien **hallinta**
Oletettujen onnettomuuksien **hallinta**
Häiriöiden ja vikojen **hallinta**
Häiriöiden, vikojen jne **ehkäisy**
Turvallisuusmarginaalit ja tekninen laatu
Säätö, rajoitus, suojaus, häiriöohj
Turvallisuusjärjestelmät, hätätilanneohjeet
Vakavan onn. hallintajärjestelmät ja -ohjeet
Valmiustoiminta, vastatoimet laitoksen ympäristössä

Ydinreaktorin turvallisuuspiirteitä

- Reaktorisydän rakennetaan pysymään käynnissä
  - pysäyttäminen vaatii aina toimenpiteitä
- Sammutettunakin reaktori tuottaa **jälki**lämpöä (~1%); johtuu fissiotuotteiden radioaktiivisuudesta
  - pitää jäähdyttää koko ajan, tai sulattaa itsensä

⇒ Tehon hallinta ja jäähdytys on aina turvattava: **keskeiset turvallisuustoiminnot**

  - tehon hallinta (sammutus)
  - reaktorin jäähdytys
  - aktiivisten aineiden pidättäminen (suojarakennus)

  - valvonta ja ohjaus
  - varavoima

Turvallisuustoimintojen suunnittelu

- Toteutetaan luontaisesti tai erityisillä järjestelmillä
  - luontaiset takaisinkytkennät, hitaus, turvallisuusmarginaalit
  - ”passiiviset” järjestelmät, toimivat luonnonvoimaisesti
    - painovoima, varastoitu kaasunpaine
    - vaatii usein valvontaa, käynnistyksen / ohjauksen
  - ”aktiiviset” järjestelmät toimivat ulkoisella käyttövoimalla (sähköllä)
    - vaativat aina valvontaa ja käynnistyskäskyjä
- Järjestelmissä tyypillistä
  - **vikakestoisuus**: 2..4-kertaiset samanlaiset osajärjestelmät
  - **erilaisuus**: sama tehtävä tehdään usealla eri tavalla ja/tai erilaisilla laitteilla
  - **erottelu**: osajärjestelmät eri tiloissa, suojassa ulkoisilta vaaroilta
- Turvallisuustoiminto (prosessi), siihen kuuluvat mittaukset ja ohjaukset sekä käyttövoima kaikki suunnitellaan samojen yleisperiaatteiden mukaan

Automaatiotekniikka ydinvoimaloissa

Automaatiotekniikka ydinvoimaloissa

- Pääprosessien säätö
  - normaalia voimalaitostekniikkaa, ajetaan peruskuormaa 100% teholla
  - suunnitteluvaatimuksena korkea luotettavuus (vähän häiriöitä = hyvä turvallisuus *ja* hyvä talous)
  - esimerkkijärjestelmä: Siemensin Teleperm XP -tuoteperhe

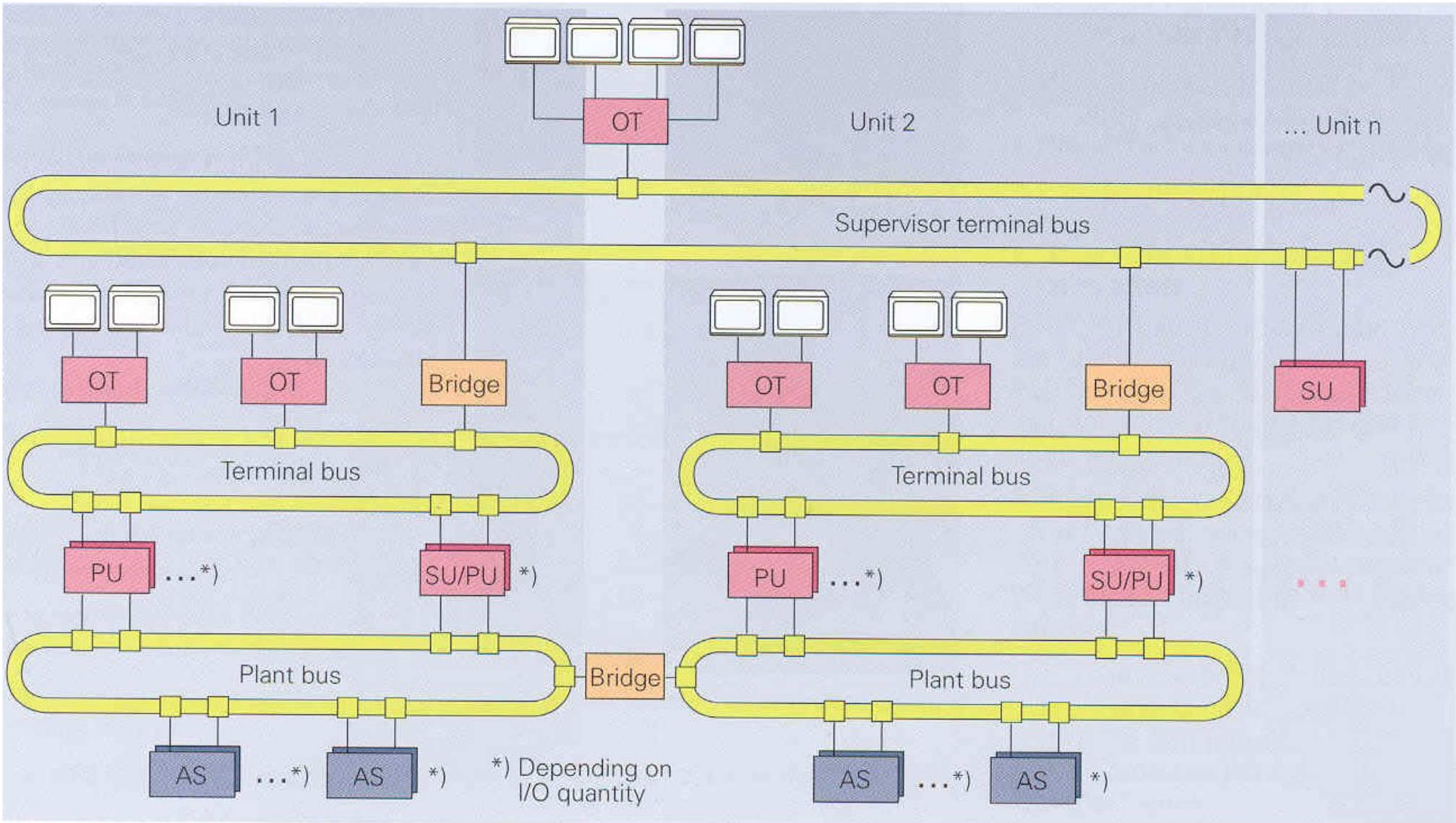
- Häiriö- ja vikatilanteet: rajoitus- ja suojaustoiminnot
  - suunnitteluvaatimuksena erittäin korkea luotettavuus ja laatu, vaikka ei ”oikeasti” ohjaa juuri koskaan
  - turvallinen vikautuminen (fail-safe) rakennettu sisään
  - esimerkkijärjestelmä: Arevan Teleperm XS -tuoteperhe

- Laitetekniikka
  - kenttälaitteet (mittausanturit, toimilaitteet) yksinkertaista ”tyhmää” tekniikka - usein sijaitsevat säteilevissä oloissa
  - säädöt ja logiikat viime vuosiin asti analogiatekniikkaa

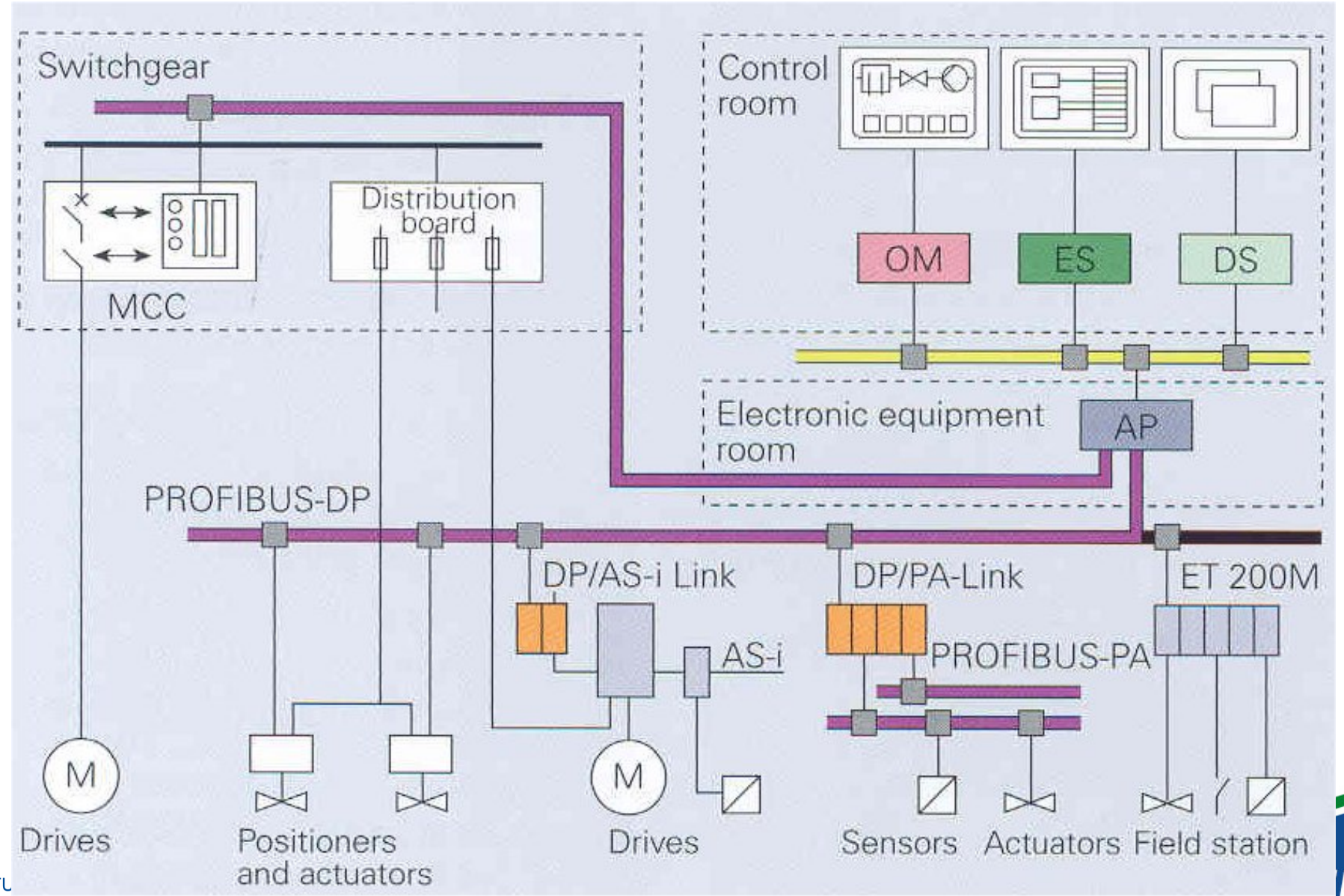
Teleperm XP piirteitä

- järjestelmärakenne rengasverkko (Ethernet)
- kenttälaitteet, prosessiasemat, näyttölaitteet sekä engineering- ja kunnossapito liittyvät kaikki suoraan samaan verkkoon
- tuoteperheessä myös turvallisuusorientoituneita moduleja, esimerkiksi fail-safe prosessoriyksikkö
  - sisältä synkronoitu ja kaksiredundanttinen, vertailija pysäyttää jos eri prosessorien outputit poikkeaa toisistaan
- suunnittelutyökalut osa pakettia; koodataan graafisella työkalulla käyttäen valmiita ohjelmamodulikirjastoja

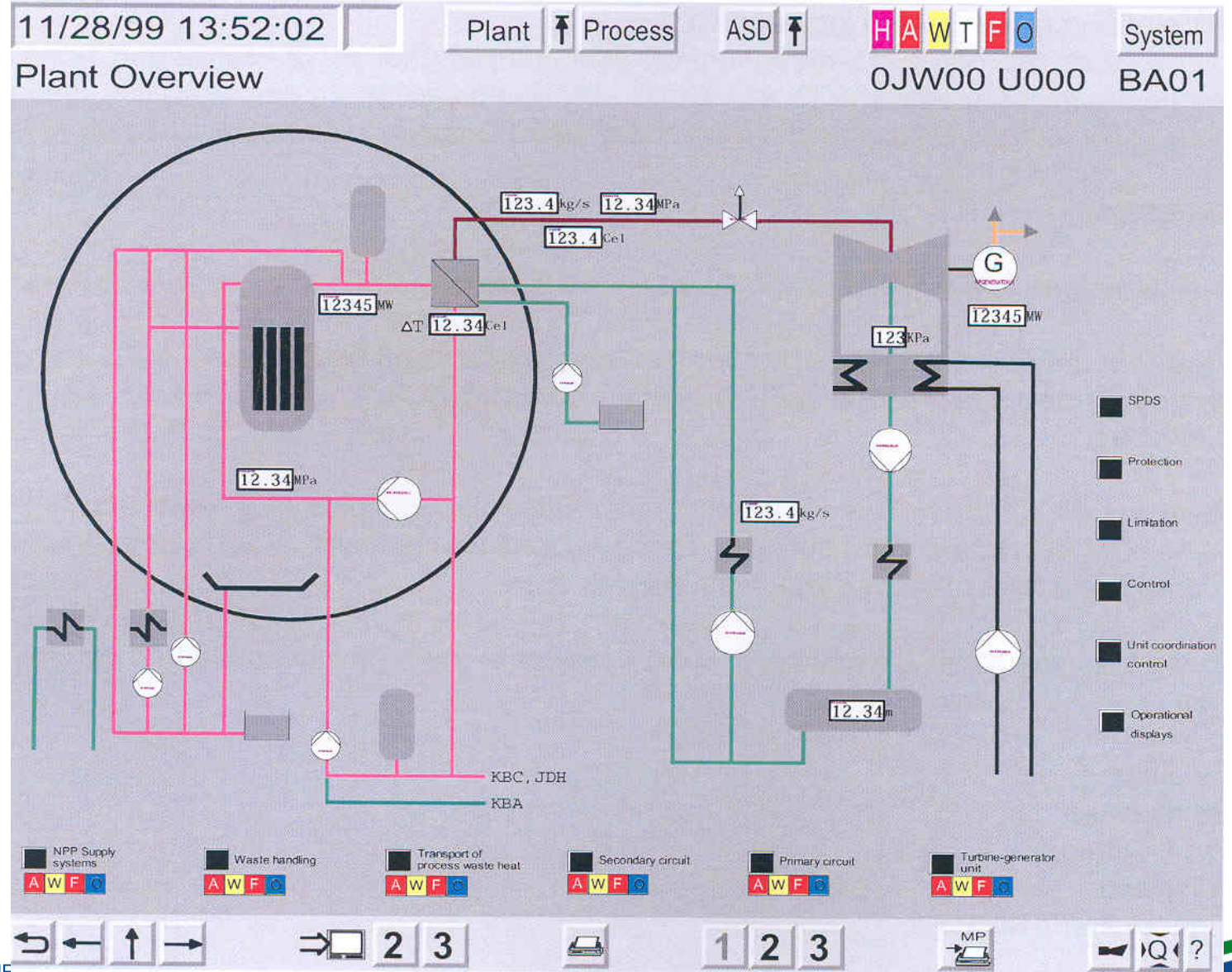
TXP tyypillinen yleisarkkitehtuuri [1]



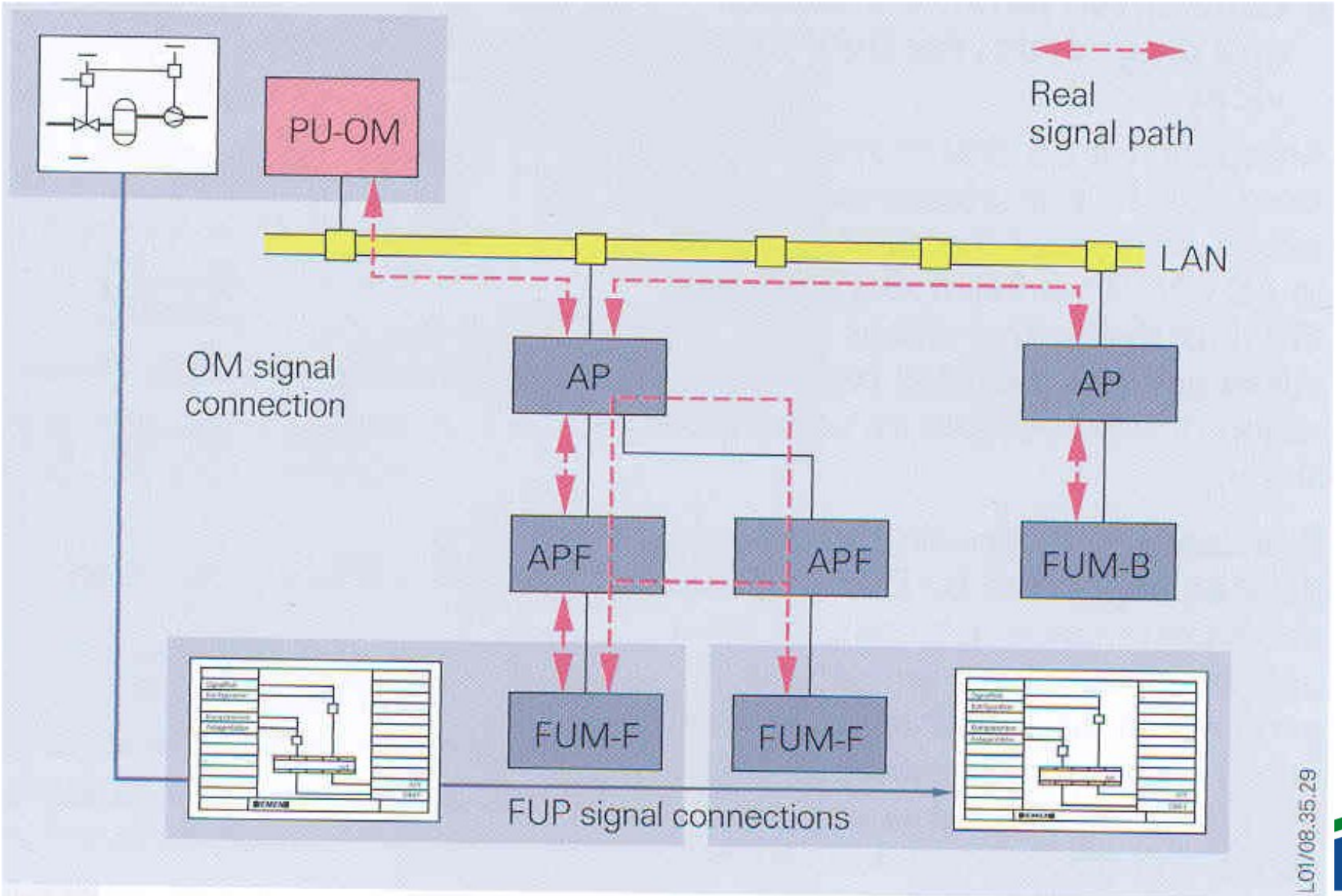
TXP ”automaatiopää” + kenttälaiteliityntä [1]



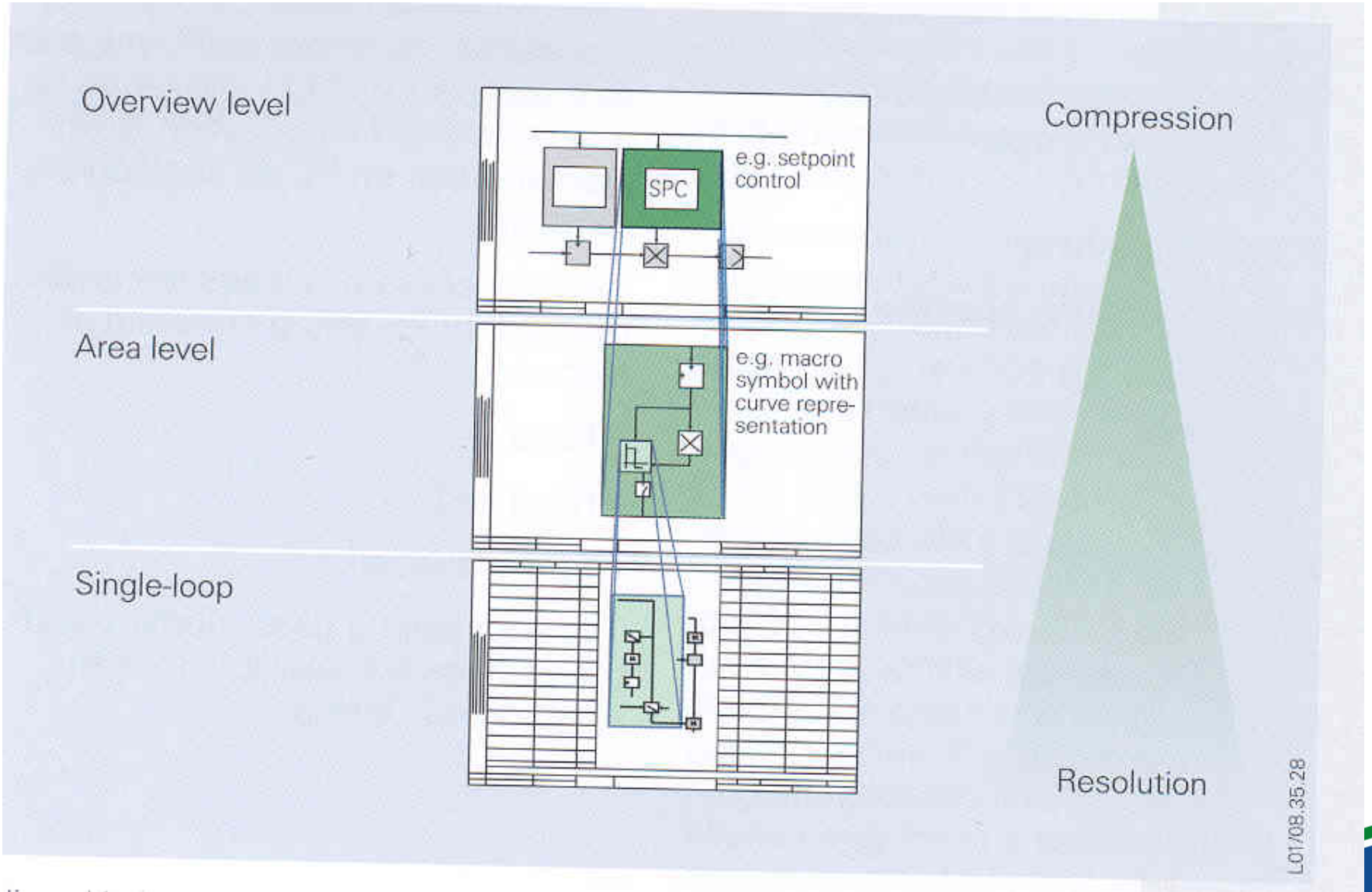
TXP valvomokäyttöliittymää [2]



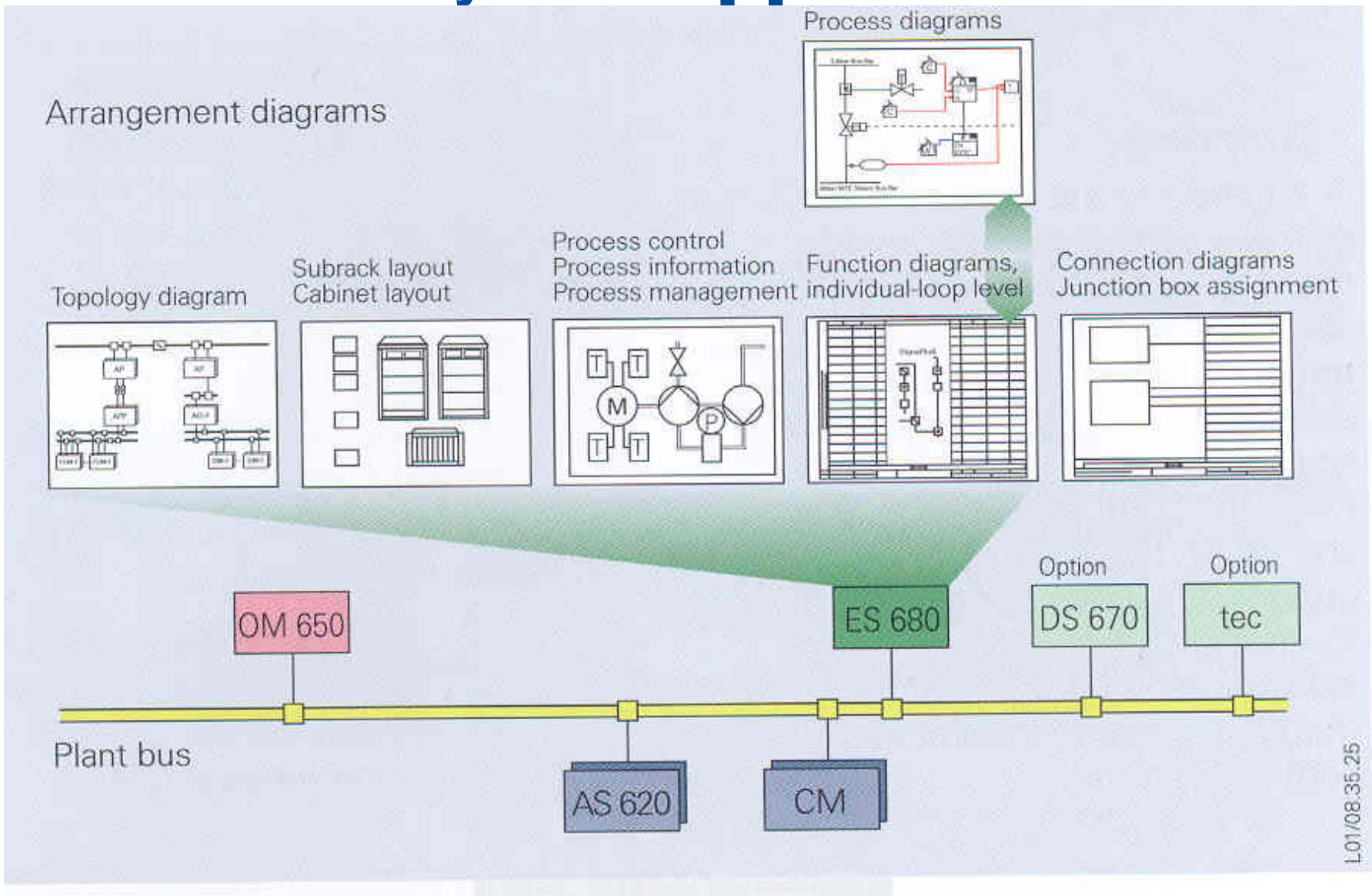
TXP signaalin kulku [1]



TXP ohjelmointihierarkia [1]



TXP suunnittelutyöasema [1]

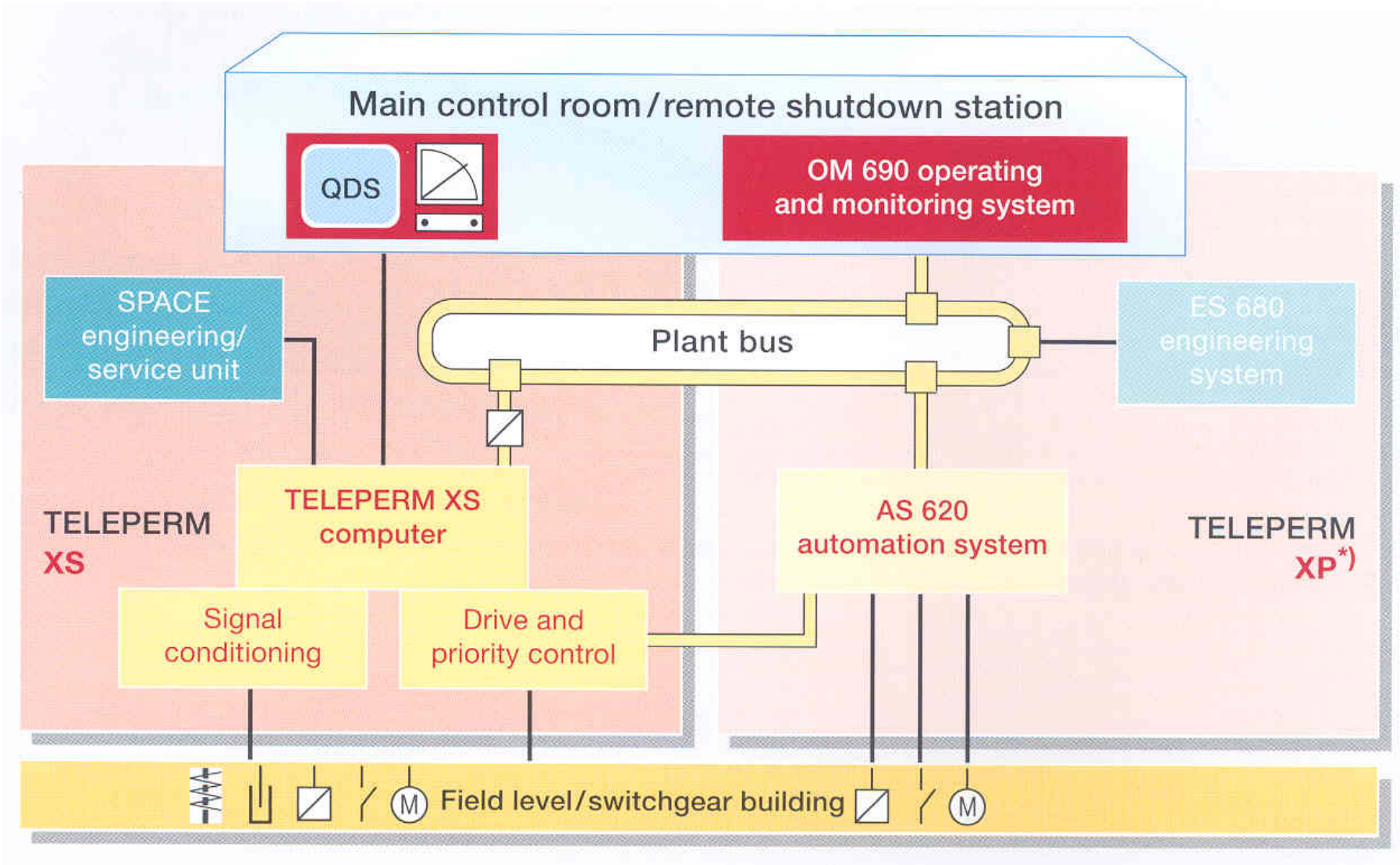


Teleperm XS piirteitä

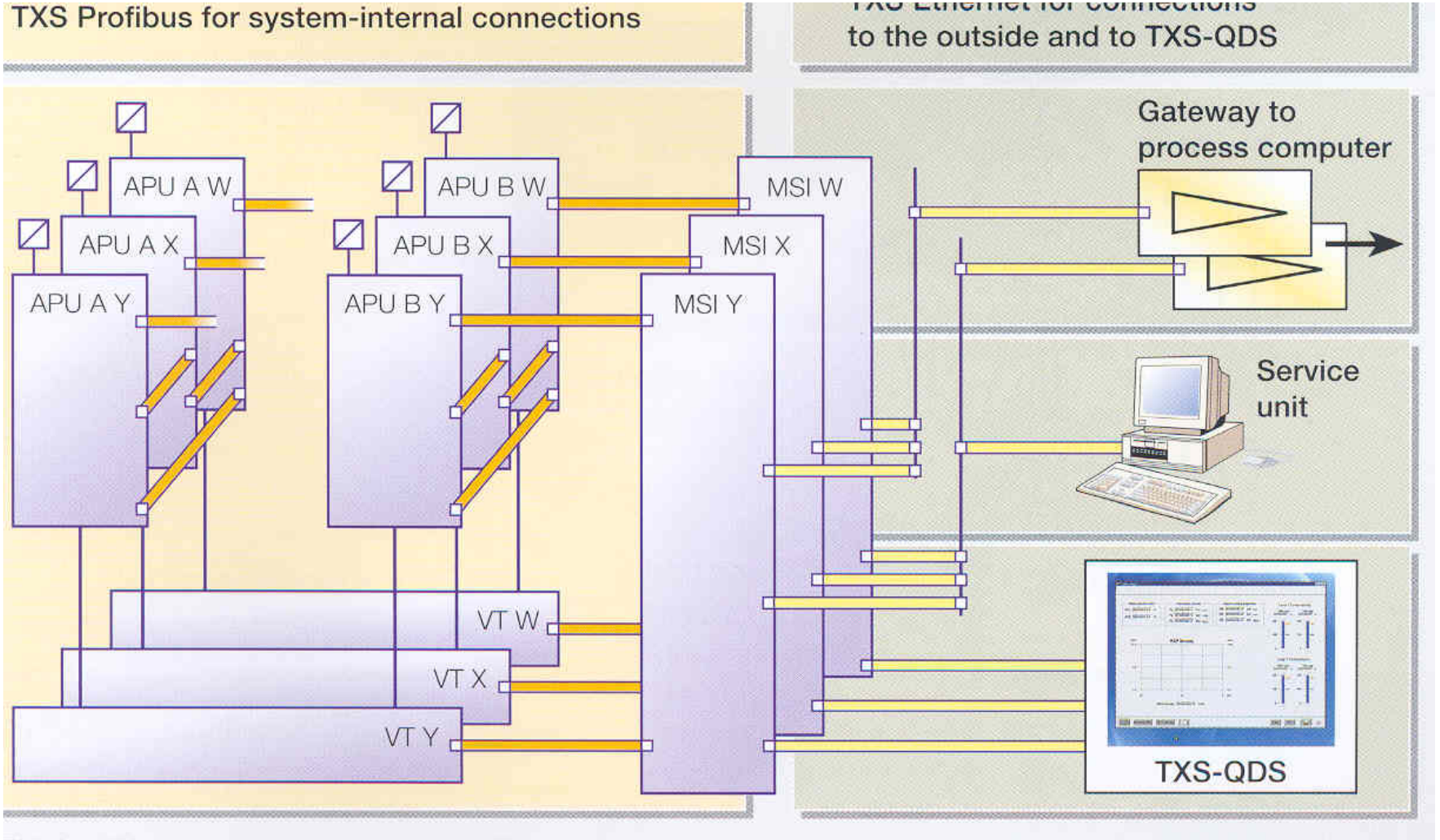
- signaaliliikenne point-to-point (Ethernet), asynkronista
- kenttälaitteet, tietoliikenne- ja sovellusprosessorit sekä toimilaiteohjaimet kootaan tarkoin harkittavaan redundanttisen arkkitehtuurin
- signaaliprosessoinnissa paljon vertailua redundanssien kesken
- turvallisuusominaisuuksia
  - paljon itsediagnostiikkaa, fail-safe käyttäytyminen
  - signaalien validiteetin valvonta, hallittu hylkääminen
- näyttölaitteet joko suoraan langoitettuja tai gatewayn kautta verkkoyhteydellä

- suunnittelutyökalut osa pakettia; koodataan graafisella työkalulla käyttäen valmiiksi kelpoistettuja ohjelmamodulikirjastoja
- suunnitteluprosessi määritelty tarkkaan

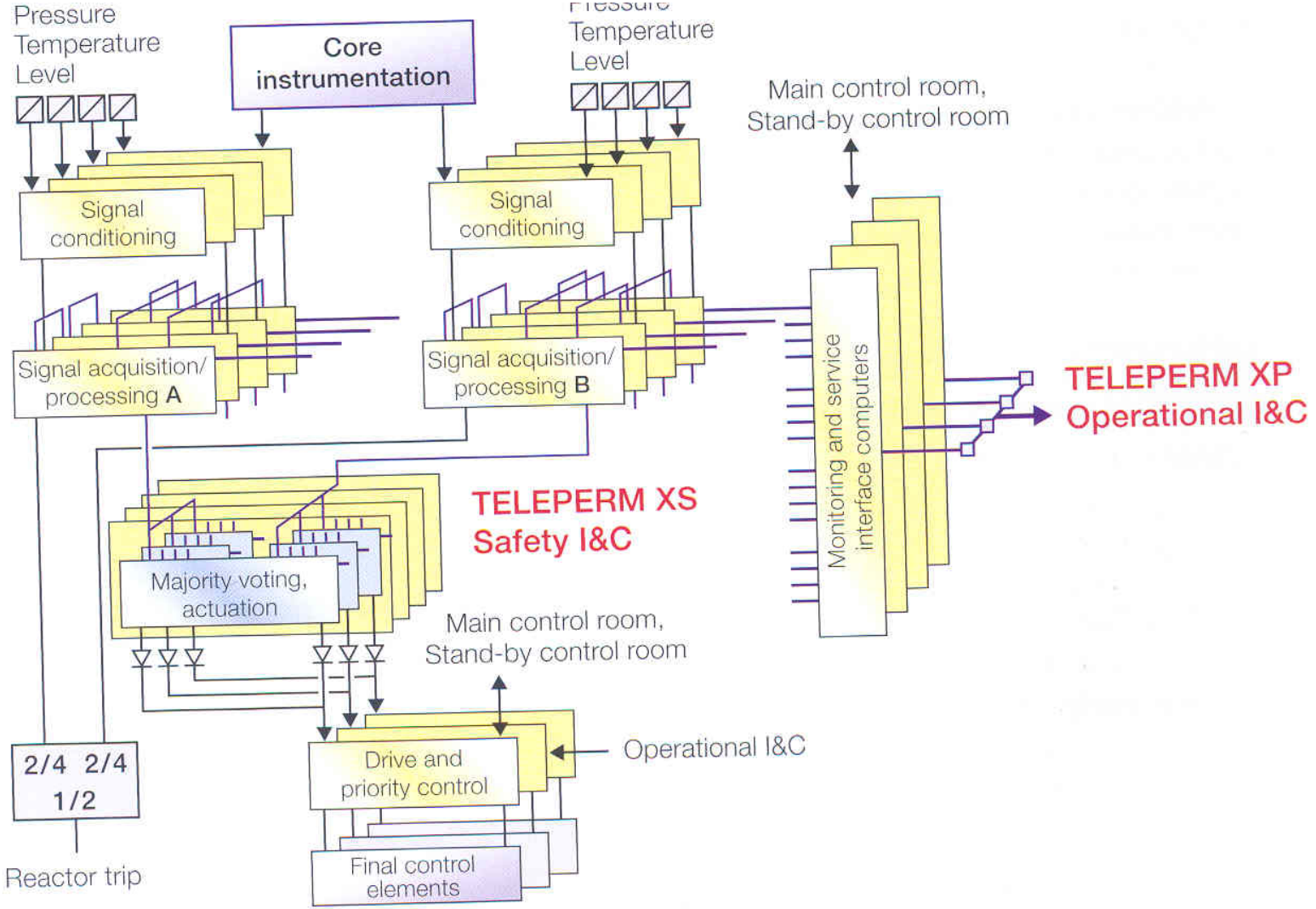
TXS ja TXP samassa laitoksessa [3]



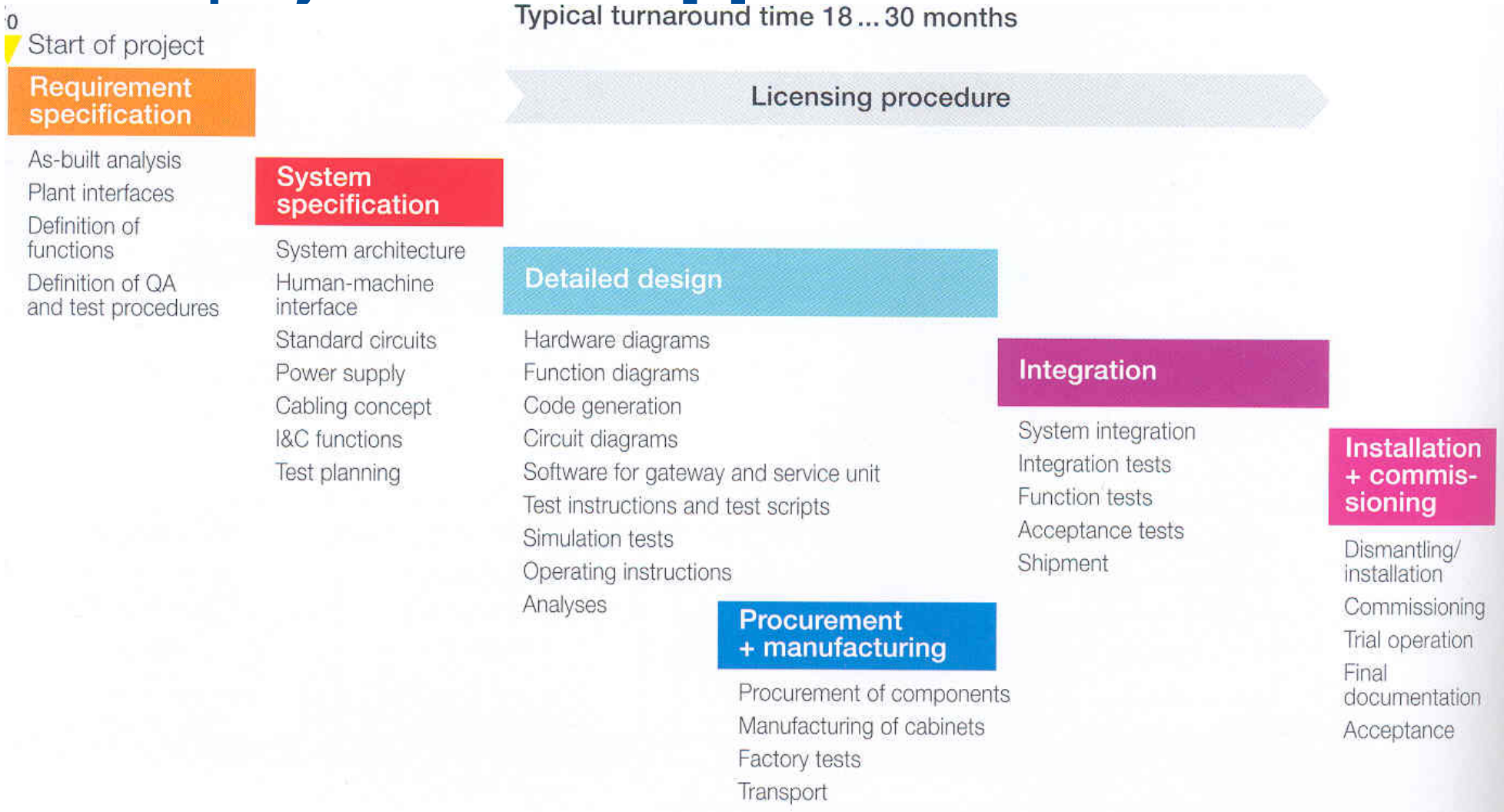
TXS perusarkkitehtuuri ja liitynnät valvomoon [3]



TXS tyypillinen suojausjärjestelmän arkkitehtuuri [3]

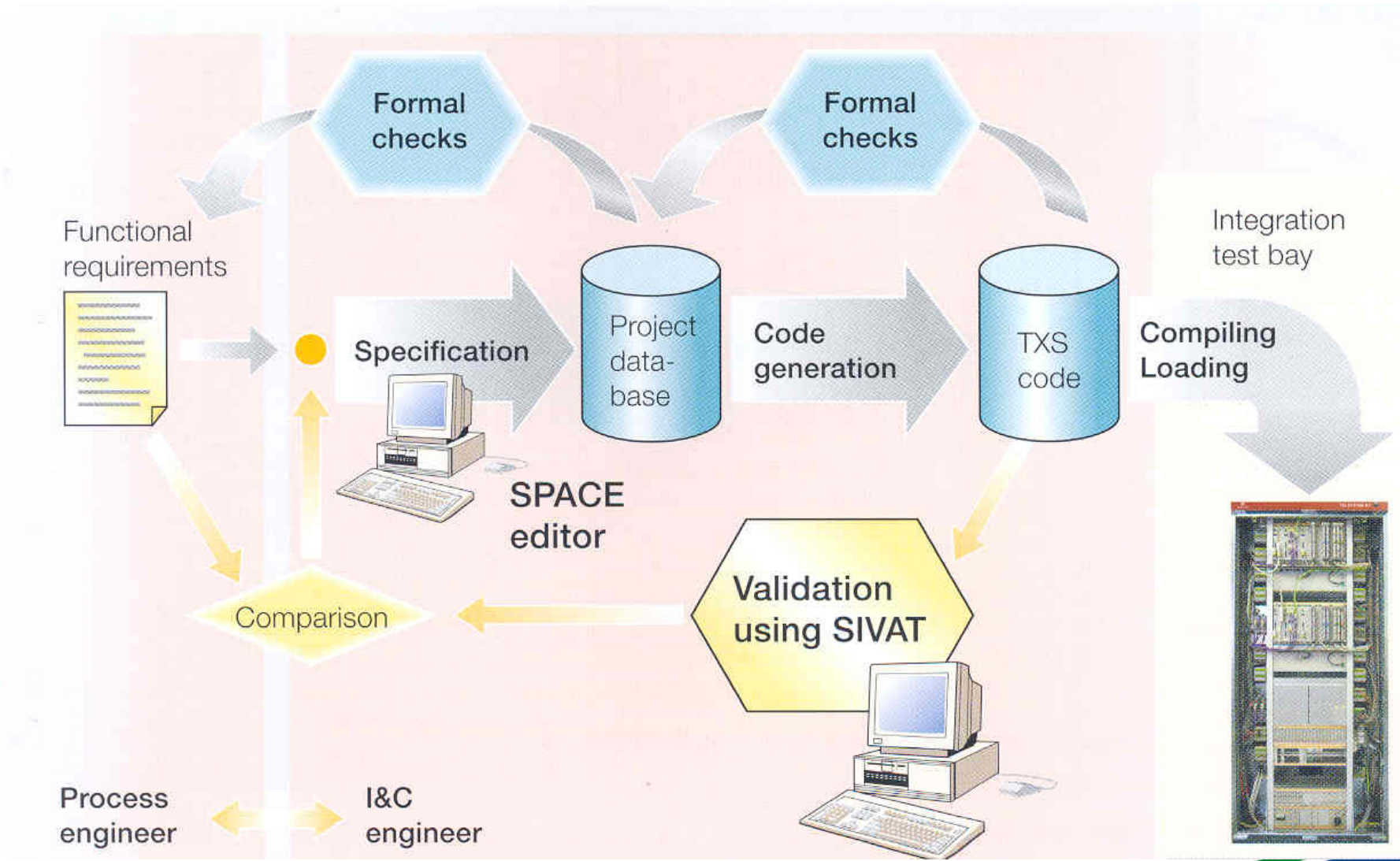


TXS projektin vaiheet [3]

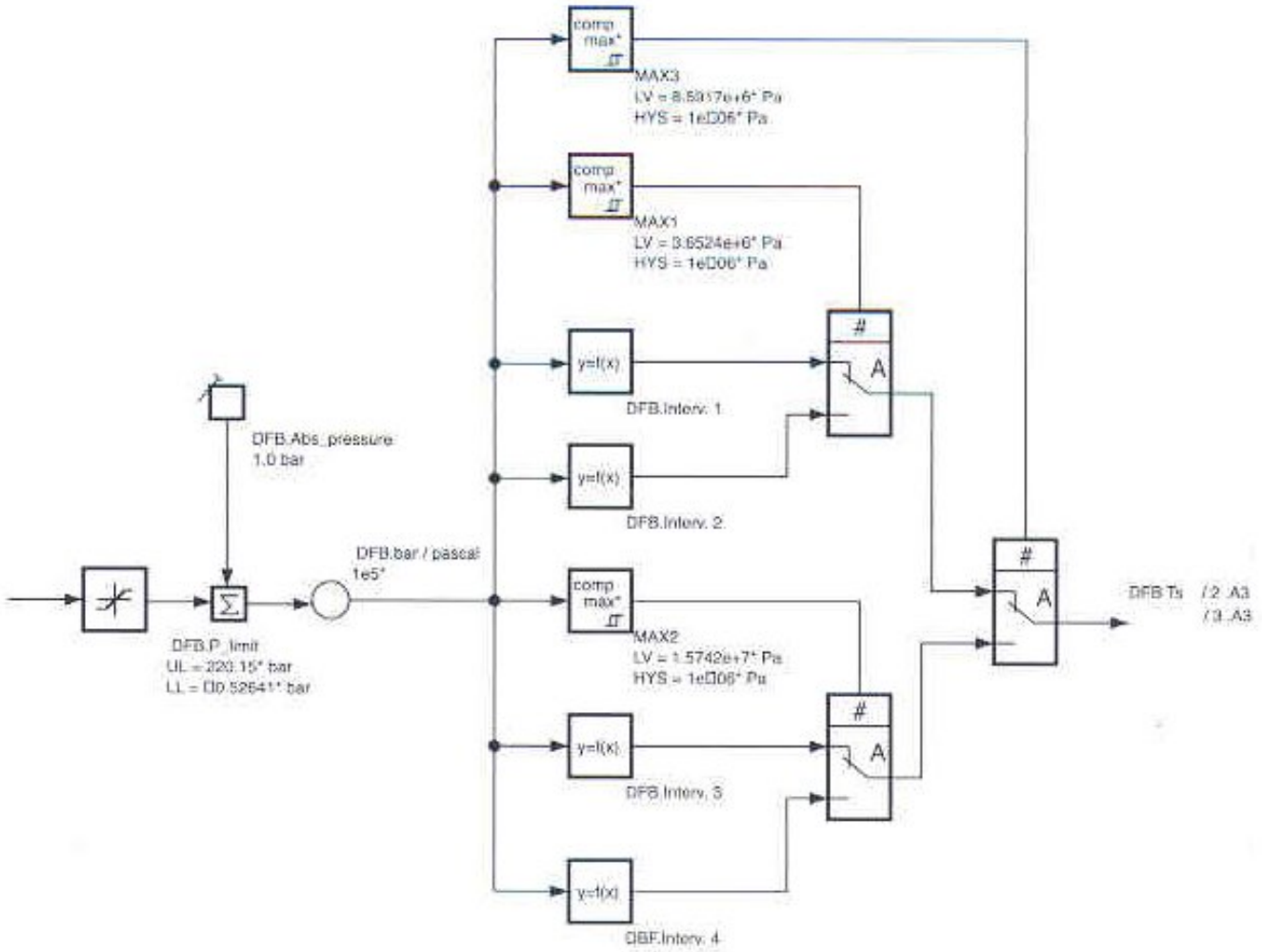


ard project management process for safety I&C.

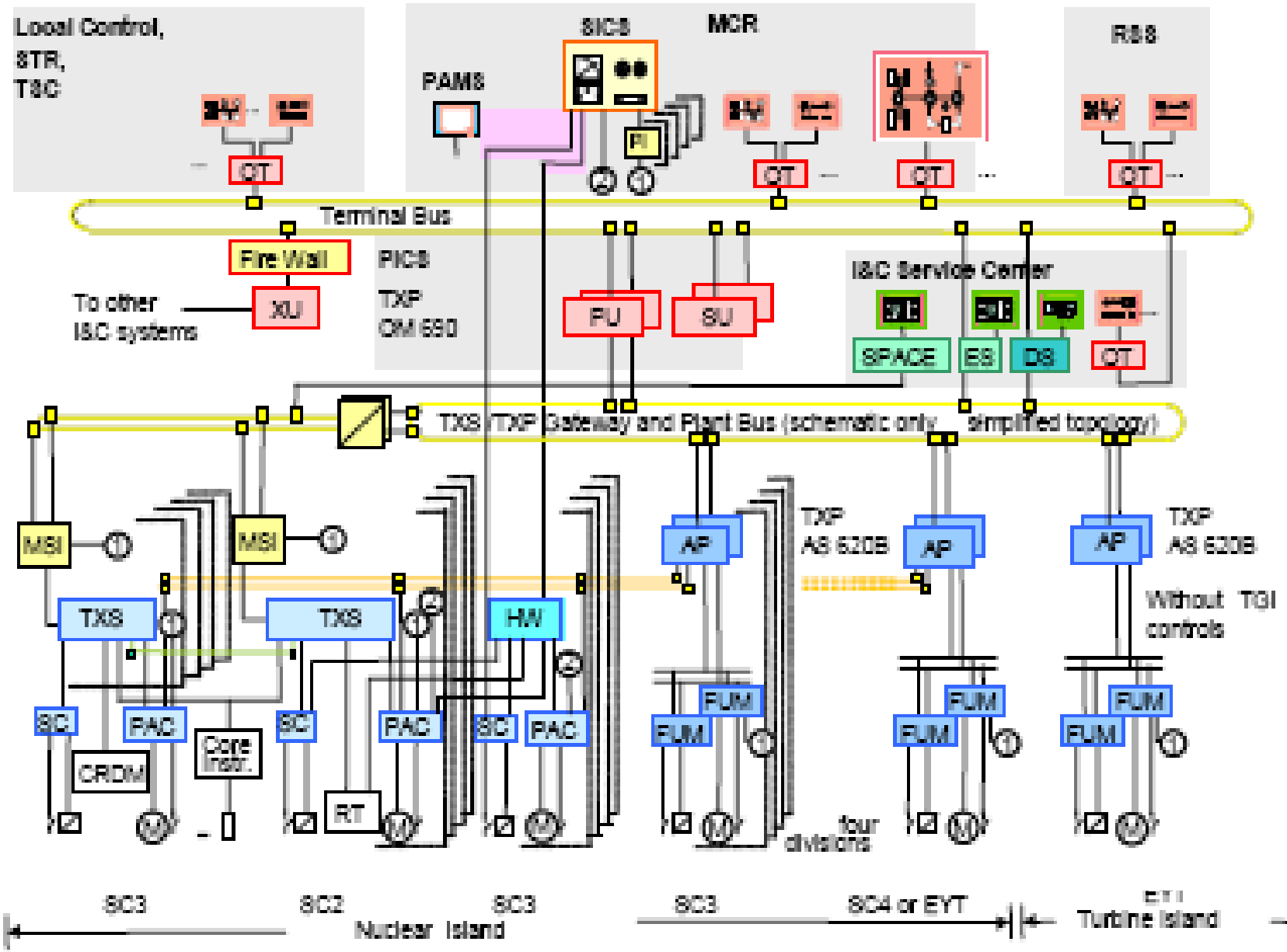
TXS sovelluskehitys pääpiirteissään [3]



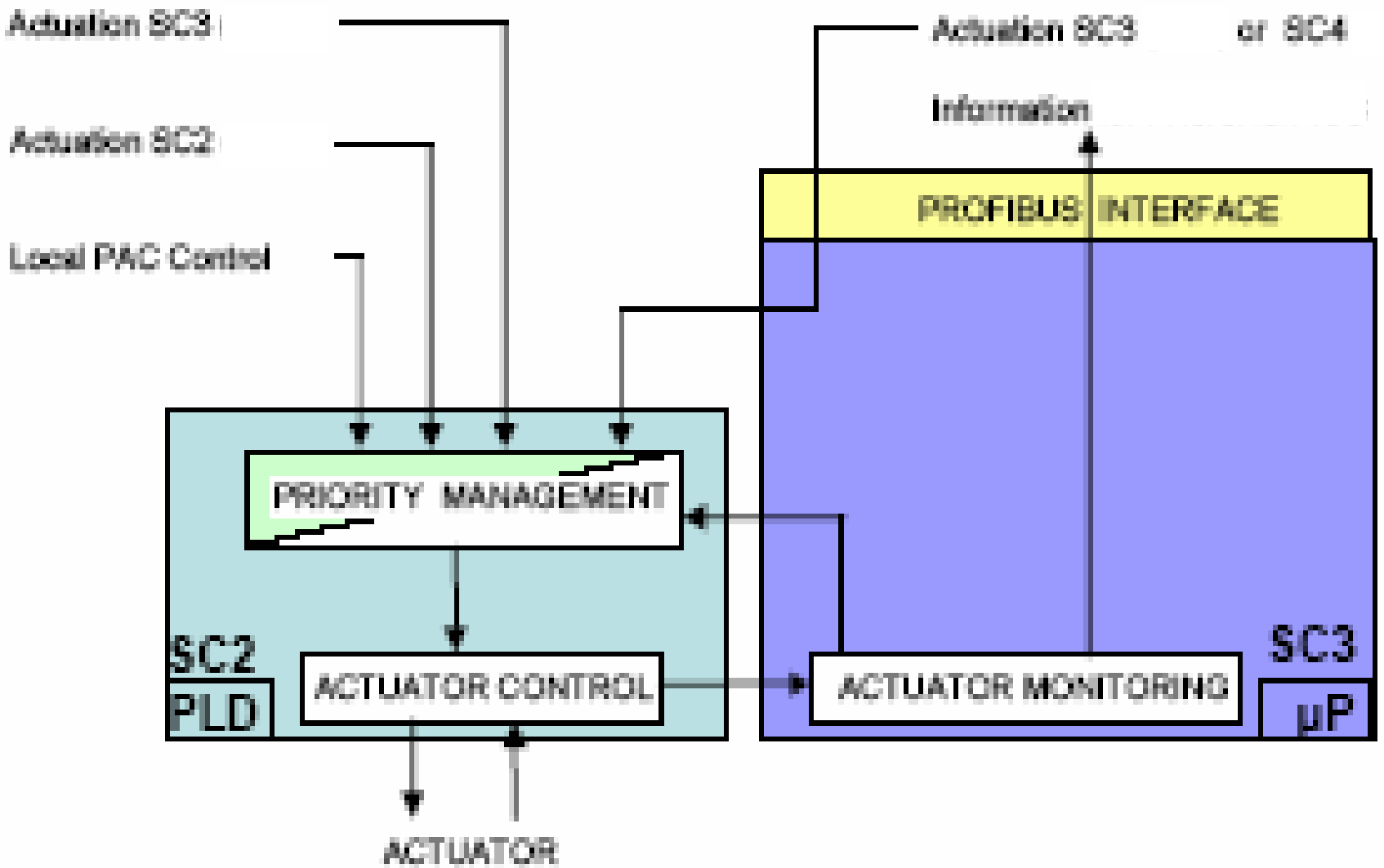
Esimerkki TXS softasta [3]



Esimerkki koko laitoksen systeemiarkkitehtuurista



Prioriteettivalitsin ja laiteohjain



Teleperm XS perustietoa

- Sovellusprosessorina AMD K6, 266 MHz, 2 MB ROM ja 8 MB EPROM
- tietoliikenne 12 MBit/s Profíbus tai 10 MBit/s Ethernet
- laaja valikoima analogia- ja binääri-IO-kortteja

- prioriteettiohjaimen logiikkaosuus FPGA

- prosessorien käyttöjärjestelmänä MICROS
- modulit koodattu C:llä
- kehitystyökalut Linuxin päällä
- kehitteillä erilllinen Qualified Display System (QDS) - näyttölaite turvallisuuskriittisiin sovelluksiin

Automaation valvonta

Turvallisuusvaatimusten täyttyminen

- Ydinenergian käyttö on luvanvaraista; valtioneuvosto, KTM, STUK
- Jakamaton vastuu turvallisuudesta on luvanhakijalla / luvanhaltijalla
- Luvanhaltijan toimintaa valvotaan voimalaitosprojektin kaikissa vaiheissa
  - periaatepäätös
  - rakentamislupa
  - käyttölupa (rajalliseksi ajaksi)
  - käytön aikana (laitosturvallisuus, materiaalivalvonta)
  - käytöstä poisto
  - jätehuolto
- Valvonta on jatkuvaa toimintaa
- Kansainvälinen valvonta: kv. ydinturvallisuussopimus

Valvonnan perusteet

- Ydinenergialaki oikeuttaa / velvoittaa
- Tekniset vaatimukset
  - Valtioneuvoston päätökset (=> kohta Valtioneuvoston asetukset)
  - STUKin julkaisemat YVL-ohjeet
  - kansainväliset ja suomalaiset standardit
    - IAEA:n
    - IEC, IEEE, KTA, DIN, ISO, ...
    - SFS, ...
  - suomalainen säännöstö löytyy STUKin kotisivuilta www.stuk.fi

Automaatioteknisiä erityisvaatimuksia

- Automaatio, erityisesti ohjelmoitava, tarvitsee huomiota:
  - yhteisvikojen välttäminen <=> diversifiointi järjestelmäsuunnittelussa
  - kelpoistus testaamalla osin mahdotonta, paikataan suunnittelu tarkkaan vaiheistamalla ja dokumentoimalla (suunnittelun elinkaarimalli, V&V)
  - hyvät mallit menettelyille löytyvät standardeista

- Yhteensopivuus laitosympäristön kanssa
  - kelpoistaminen ympäristöolosuhteisiin (myös onnettomuustilanteen aikaiset olosuhteet)
  - sähköiset häiriöt, EMC-yhteensopivuus
  - tietoturvallisuus, tiedonsiirto
  - version hallinta, käyttöliittymä, ...

Järjestelmien rakenteen arvioinnista

- Ydinvoimalaitoksen automaatiojärjestelmien rakenteelle tehdään arvio, jossa tarkastellaan
  - syvyyspuolustuksen toteutuminen
  - moninkertaisuus <> vikasietoisuus
  - erilaisuusperiaatteen toteutuminen eri tasoilla (signaali, logiikka, toiminto) (<> yhteisvikasietoisuus)
- Lyhyesti, DinD&D, tai D3, Defence-in-Depth & Diversity
- Käytännössä automaatio jaetaan käyttö-, rajoitus- ja suojausjärjestelmiksi => ”syvyys”
- Tarkastelussa tiivis yhteys turvallisuussuunnitteluun, prosessisuunnitteluun, onnettomuusanalyyseihin ja luotettavuusanalyysiin
- Järjestelmät luokitellaan turvallisuusmerkityksen mukaan

Redundanssi ja diversiteetti

- Neljäredundanttinen suojausautomaatio on ydinvoimaloissa yleinen: ”optimaalinen” tasapaino viansieto <> monimutkaisuus
  - laukaisee toiminnon yleensä 2/4 äänestyksellä, yksi vika ei aiheuta turhaa laukaisua
  - kestää satunnaisvian, laukaisee joko 1/3 tai 2/3
  - huollettavissa lennosta kanava (redundanssi) kerrallaan
    - huollon aikanakin kestää (estävän) yksittäisvian
  - lisäredundansseissa (>4) yhteisviat alkavat dominoida järjestelmäluotettavuutta täysin
- Diversiteettiä eli erilaisuutta käytetään yhteisvikoja vastaan
  - signaalidiversiteetti: yhteen tapahtumaan liittyvä suojaustarve havaitaan **usean fysikaalisen suureen** perusteella
  - laite- ja laitealustadiversiteetti: käytetään samanlaisiin tehtäviin **eri tavoin toimivia laitteita**, jopa eri fysikaalisia periaatteita
  - toiminnallinen diversiteetti: suoritetaan samaa tehtävää **usean** eri **prosessijärjestelmän** avulla
  - hintana laitoksen (turvallisuusperusteiden) lisääntyvä monimutkaisuus

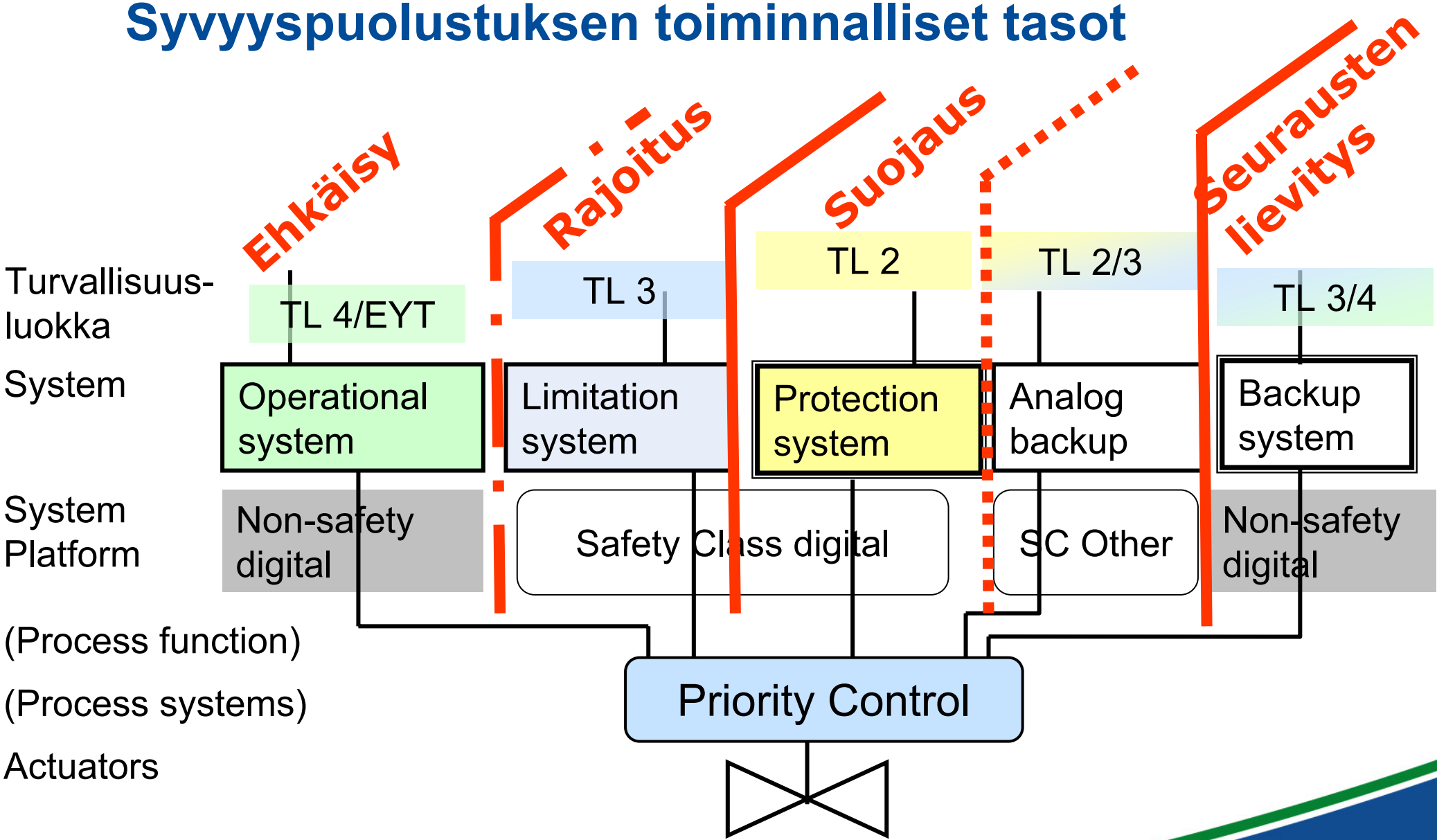
Turvallisuusluokitus

X

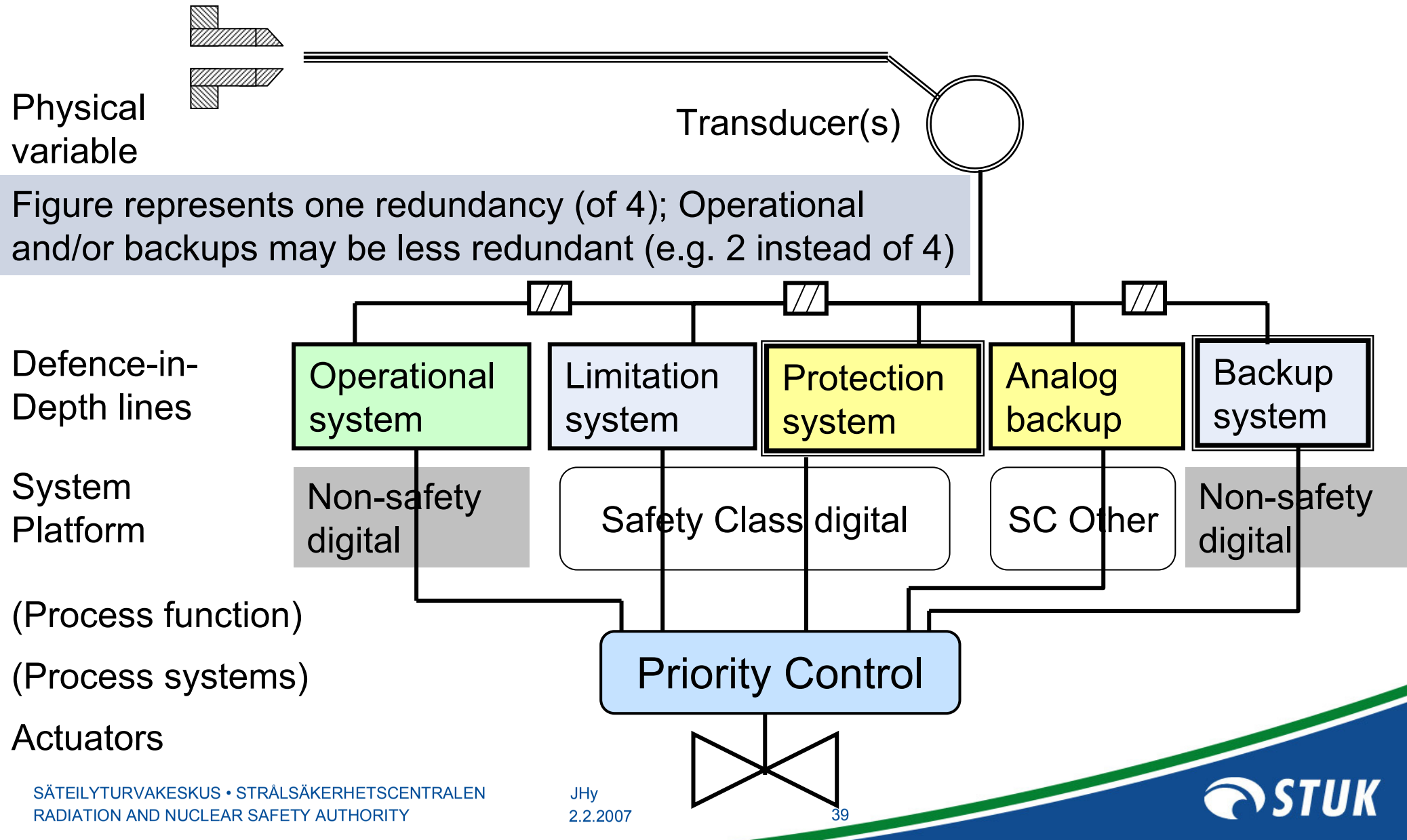
X

Laitostoiminto		Fyysinen etenemiseste	
TJRL = Toiminto ja sitä toteuttava(t) Järjestelmä(t), Rakenteet ja Laitteet		Ei saa missään tapauksessa rikkoutua	1*
		Aiheuttaa rikkoutuessaan merkittävän turvallisuushaasteen ja vaatii välitöntä turvallisuustoimintojen käynnistymistä	1
2	Turvallisuustoiminto, joka vaaditaan oletettavien alkutapahtumien hallintaan turvallisuusanalyysissä etenemisesteille asetettujen hyväksymiskriteerien puitteissa	Ei TL 1, mutta liittyy jollain tapaa	2
		Eteneemiseste, jonka eheyden varmistavat turvallisuustoiminnot alkutapahtuman jälkeen	
3	TJRL, joiden vikaantuminen vaatii turvallisuutoimintoja tai jotka ovat muuten merkittäviä alkutapahtumien estämiselle/hallinnalle/valvonnalle	Etenemisesteisiin tai radioaktiiviseen materiaaliin liittyvät rakenteet ja laitteet, mutta eivät TL 1/2	3
4	Jonkin verran merkitystä, muttei TL 1/2/3		4
EYT	Ei varsinaista merkitystä laitoksen turvallisuusarviolle		EYT

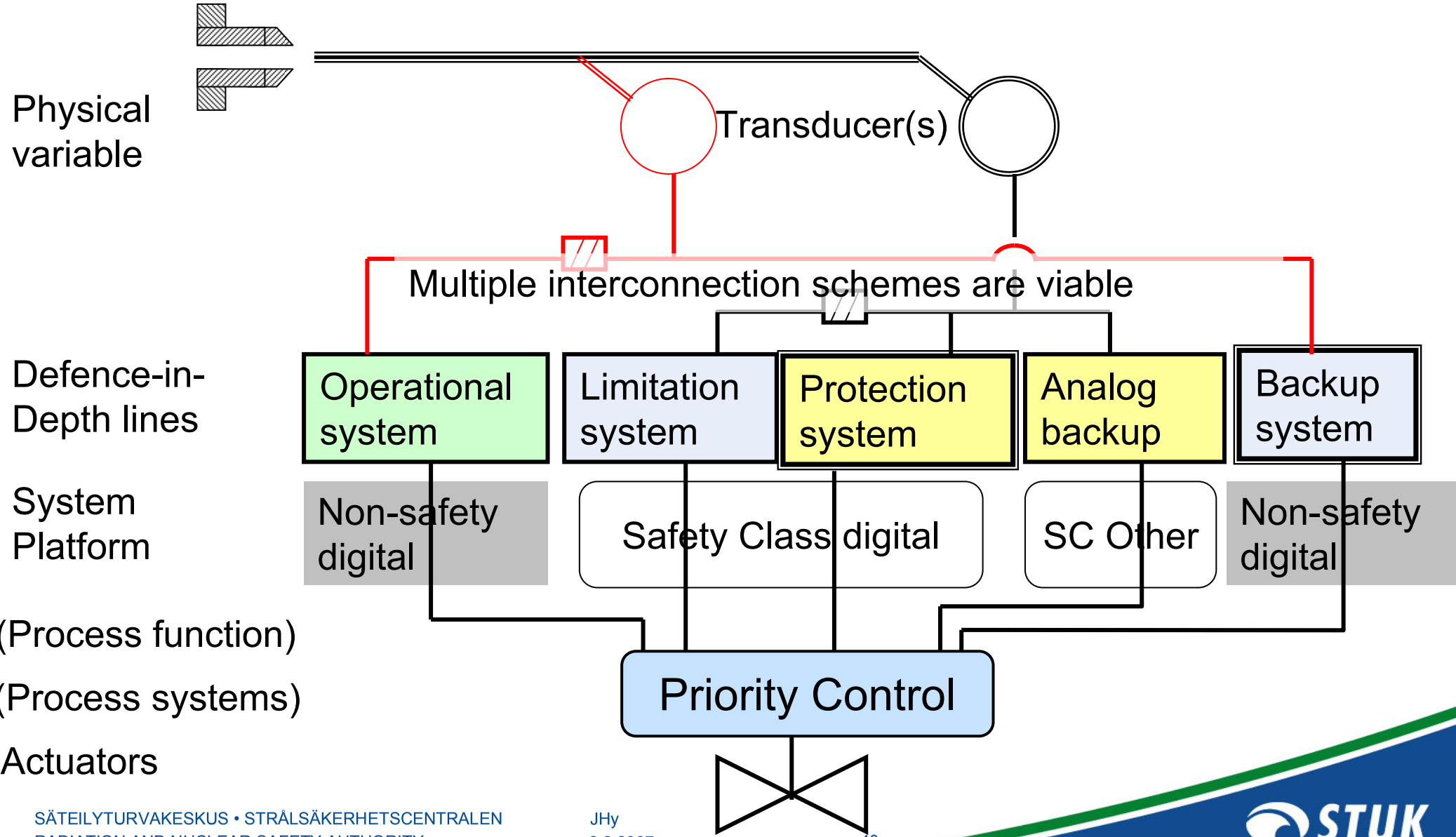
Syvyyspuolustuksen toiminnalliset tasot



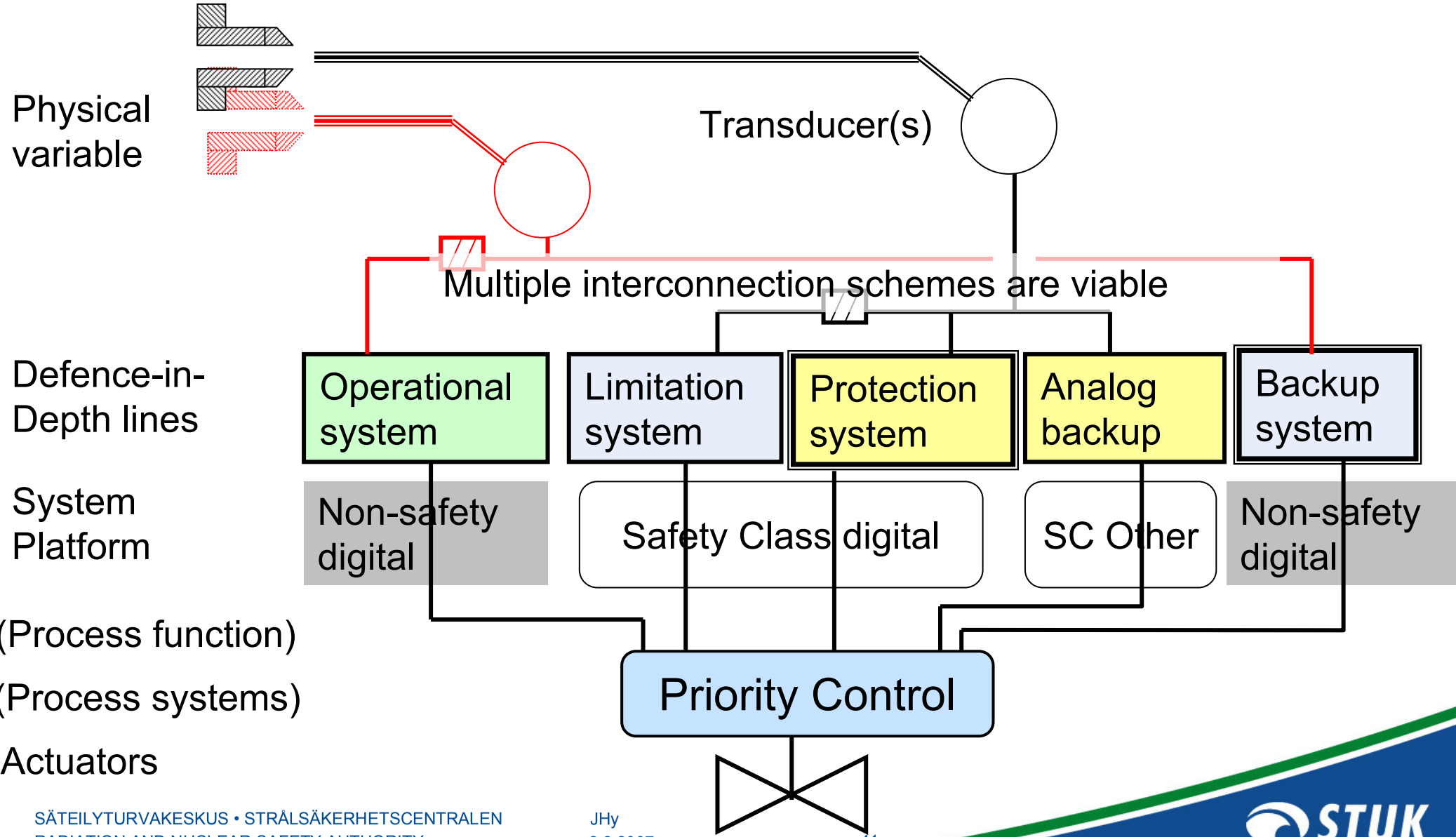
Signal diversity 1/4: none



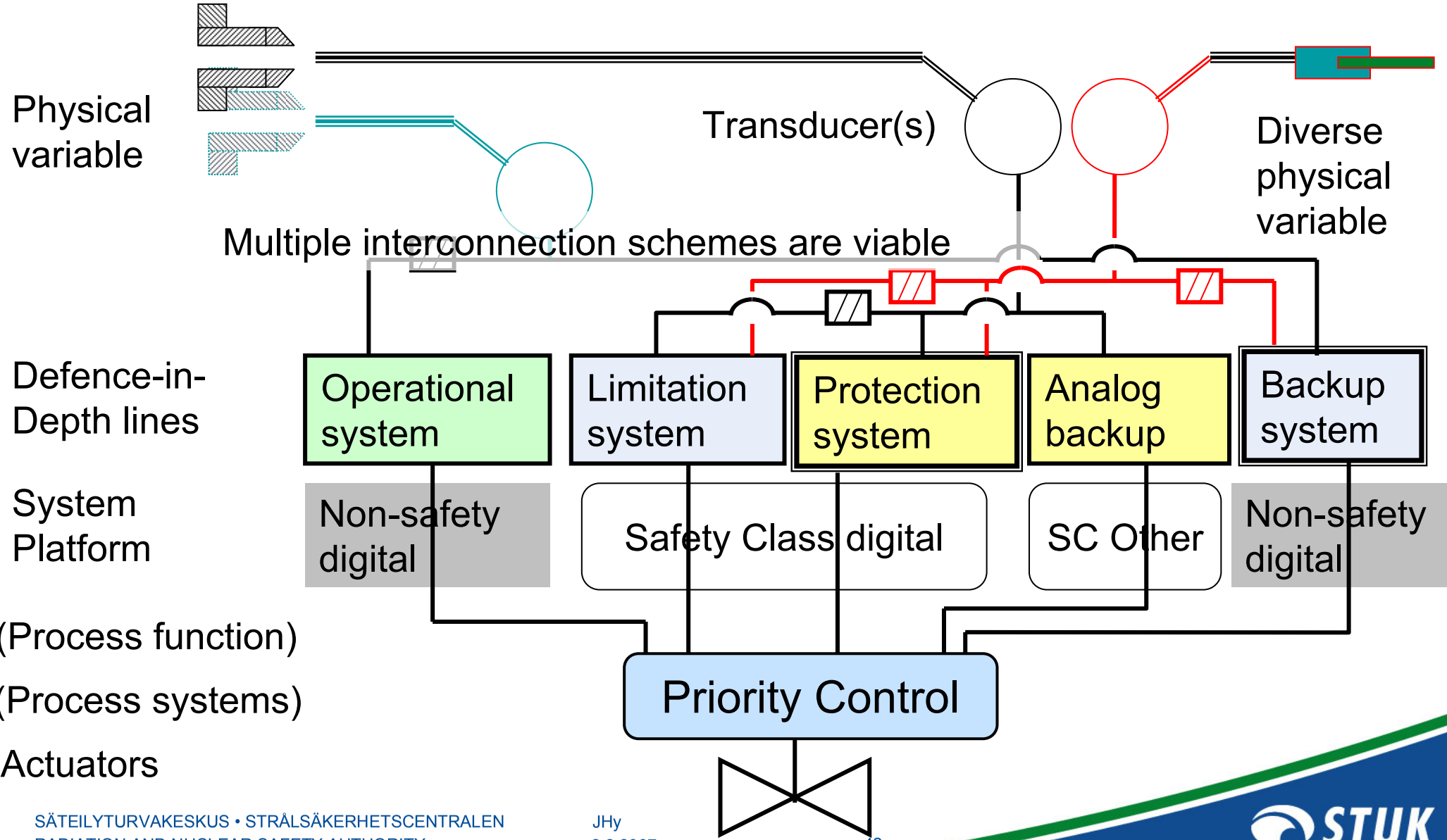
Signal diversity 2/4: transducers



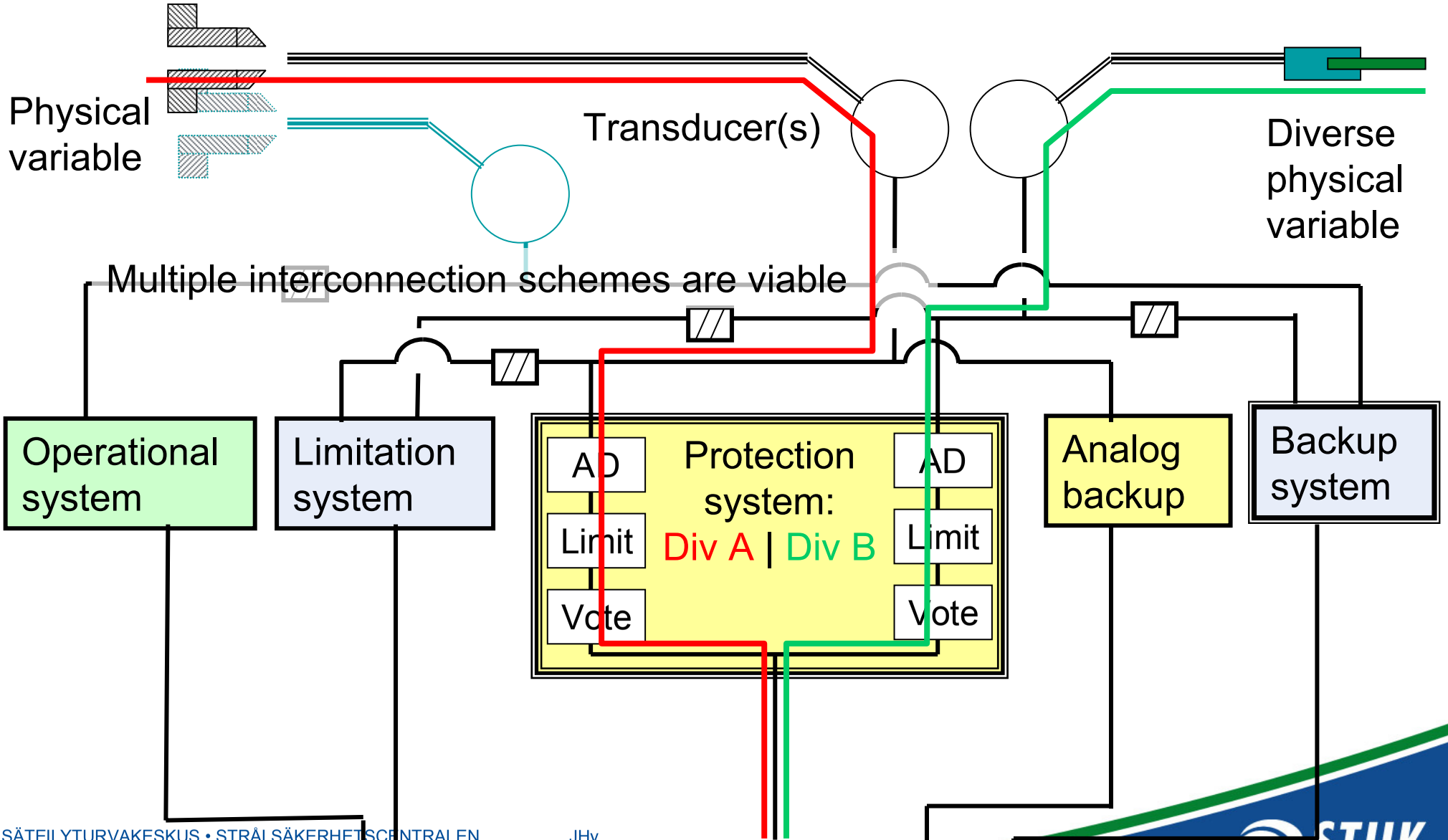
Signal diversity 3/4, measurement pts



Signal diversity 4/4, diverse variables



Intrinsic Diversity in PS

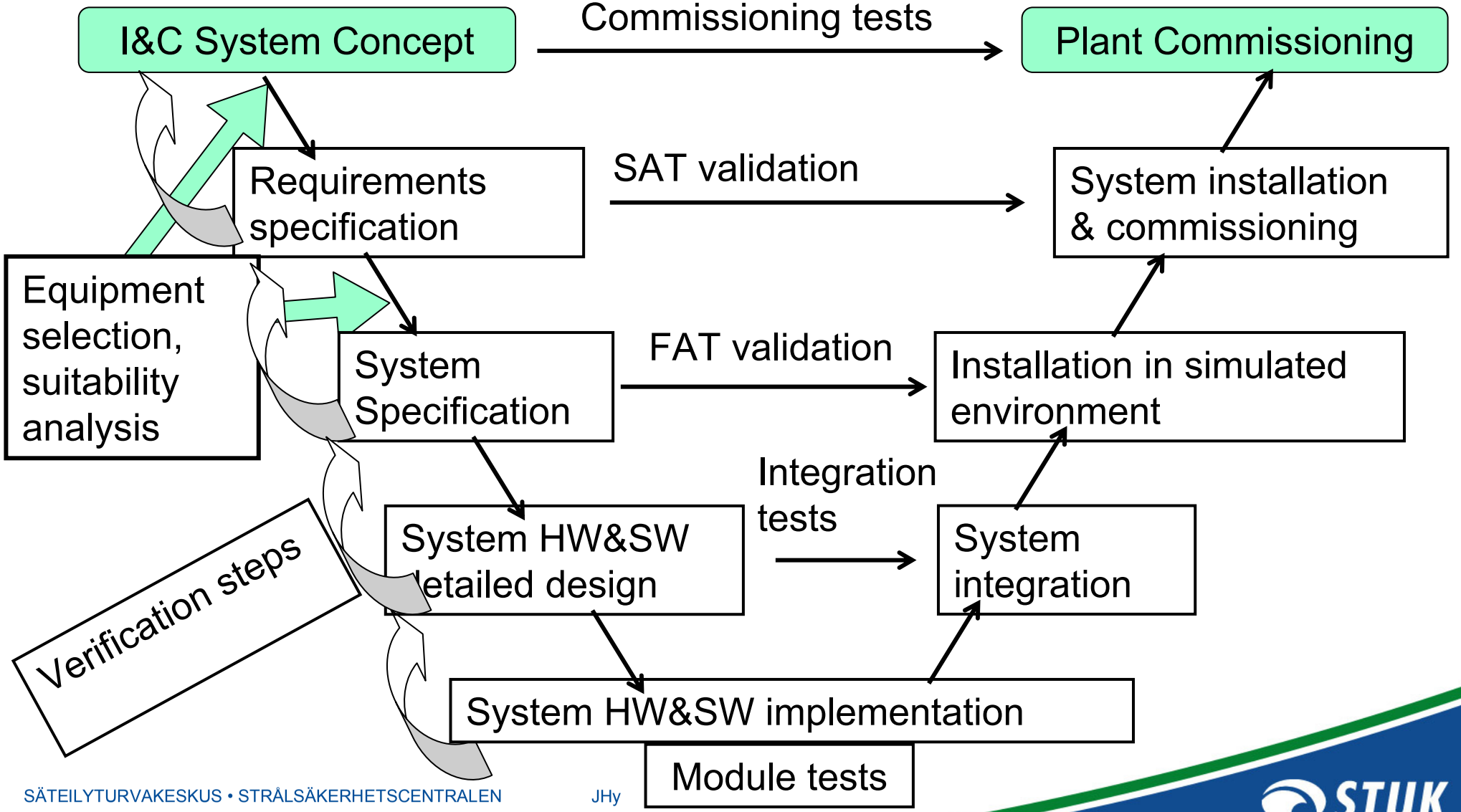


Mitä on kelpoistaminen?

- Osoitetaan, että automaatiojärjestelmä tai laite
  - täyttää toiminnalliset ja suorituskykyvaatimuksensa = on korkeaa laatua
  - kaikissa sen käyttötilanteissa niissä ympäristöolosuhteissa, joihin se on suunniteltu - myös onnettomuusolosuhteissa, jos kokee niitä

- Työn määrä ja laatu riippuvat järjestelmän tai laitteen toiminnon turvallisuusmerkityksestä / laatuluokasta
  - voi sisältää kokeita, analyysejä, käyttökokemuksia, laadunhallintaa (työprosessidokumentteja)
  - Verification and Validation, V&V: osoitetaan että on noudatettu hyvin määriteltyä vaiheistettua suunnittelumallia

V-Model of I&C System Design Life Cycle [IEC & IEEE]



Meneillään olevia isoja projekteja

- Olkiluoto 3 yksikön rakentaminen
  - 1600 MWe painevesireaktori
  - TXP + TXS + ”langoitettu” varmistus, sekä automaattinen että manuaalinen
  - videovalvomo, muutama mosaiikkitaulu
- Loviisa 1 ja 2 automaatiouudistus
  - kenttälaitteita lukuun ottamatta kaikki automaatio vaihtuu
  - TXP + TXS + manuaalinen langoitettu varmistus
  - hybridivalvomo; mosaiikkitauluja jää jonkin verran
- Olkiluoto 1 ja 2 automaatiouudistus
  - käyttöautomaatiota uusittu 2003-2006
  - suojausjärjestelmän uudistus alkanee lähivuosina
  - hybridivalvomo

Yhteenveto

- Ydinvoimalaitos on iso lämpövoimala
  - normaali voimalaitosprosessin säätö
  - lisäksi monikerroksinen ja moninkertainen suojausautomaatio
- Turvallisuustoiminnoilla estetään radioaktiivisten aineiden vapautuminen laitokselle tai ympäristöön
- Ohjelmoitava tekniikka on vahvasti tulossa myös ydinvoimaloihin
  - haasteita valvontakäytännöille
- Tyypillisesti automaatiotoiminnot kootaan isoiksi järjestelmiksi, jotka toteutetaan sopivilla modulaarisilla alustoilla
  - turvallisuusjärjestelmissä erityisvaatimuksia rakenteen, laadun, luotettavuuden suhteen
- Viranomaisvalvontaa on paljon

Viitteet

[1] Teleperm XP System Overview - The Process Control System for Economical Power Plant Control. Brochure by Siemens AG, Power Generation (not dated)

[2] Teleperm XP OM 690 Overview - The Process Operation and Monitoring System for Nuclear Power Plants. Brochure by Siemens Power Generation (not dated)

[3] Teleperm XS System Overview; Instrumentation and Control. Brochure by Areva NP GmbH (2006)

Liitteet

Automaatioon liittyvät YVL ohjeet

- Yleiset vaatimukset:
- YVL 1.0 - turvallisuusperiaatteet 12.1.1996
- Järjestelmäsuunnittelu
- YVL 2.0 - järjestelmien suunnittelu, 1.7.2002
- YVL 2.1 - järjestelmien, rakenteiden ja laitteiden turvallisuusluokitus, 26.6.2000
- YVL 2.7 - vikakriteerien soveltaminen, 20.5.1996
- Automaatiotekniikka
- **YVL 5.5** Ydinlaitoksen automaatiojärjestelmät ja –laitteet, 13.9.2002
- (YVL 5.2 Ydinlaitosten sähköjärjestelmät ja laitteet)

Muita ohjeita ja standardeja

- IAEA Safety Standards Series, NS-G-1.3, ”Instrumentation and control systems important to safety in nuclear power plants”, Safety Guide, March 2002.
- IAEA Safety Standards Series No. NS-G-1.1, ”Software for Computer Based Systems Important to Safety in Nuclear Power Plants”, Safety Guide, September 2000.
- IEC 61513 ”Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems”, First edition 2001-03.
- IEC 60880 ”Software for computers in the safety systems of nuclear power stations”, First edition 1986.
- IEC 60880-2 ”Software for computers important to safety for nuclear power plants – Part 2: Software aspects of defence against common cause failure, use of software tools and of pre-developed software”, First edition 2000-12.

Muita ohjeita ja standardeja

- IEC 60987 ”Programmed digital computers important to safety for nuclear power stations”, First edition 1989-11.
- IEC 62138 ”Nuclear Power Plants – Instrumentation and Control – Computer-based systems important for safety – Software aspects for I&C systems of class 2 and 3”, 2003.
- IEC 60780 ”Nuclear Power Plants – Electrical equipment of the safety systems – Qualification”, Second edition 1998-10.
- IEC 61226 ”Nuclear Power Plants – Instrumentation and Control Systems important for Safety – Classification, 2nd Edition 2005-02

- EN 19265, Common position of European nuclear regulators for the licensing of safety critical software for nuclear reactors, May 2000