# RIC 2006
# Session Th5D – Digital I&C

## Licensing of Digital I&C Systems

## Point of View of the Regulatory Body in Finland

Jukka Laaksonen
Director General
STUK, Radiation and Nuclear Safety Authority

# Background (1/2)

**In Finland we have the following NPP's:**

Loviisa 1&2, current power 500 MW, start up 1977,1980

- VVER-440 type (PWR) reactors with strong inherent safety – most transients are very slow and mild, and there is little need for fast response of the reactor protection system (RPS)

Olkiluoto 1&2, current power 840 MW, start up 1979,1980

- Asea Atom BWR reactors

Olkiluoto 3, power 1600 MW, under construction since February 2005

- EPR type (PWR) reactor – transients fast as common for large PWR's

# Background (2/2)

Loviisa units are in the process of replacing their original RPS with new digital I&C systems, with manual hardwired back-up (slow transients!)

- STUK has approved the project plan and I&C system conceptual design
- system requirements and systems architecture are being reviewed

Olkiluoto units have replaced their original turbine control systems and some safety relevant systems with digital I&C systems

- plans for RPS replacement have not yet been submitted for regulatory review

Olkiluoto 3 will have RPS that is implemented with digital I&C systems and hardwired back-up for reactor trip signal

- STUK has approved I&C system conceptual design
- system requirements and systems architecture are being reviewed

# General viewpoints (1/4)

Reactor Protection Systems at NPP's have to meet two general requirements:

1. Reliable actuation of Reactor Trip (RT) or Engineered Safety Features (ESFAS) when needed

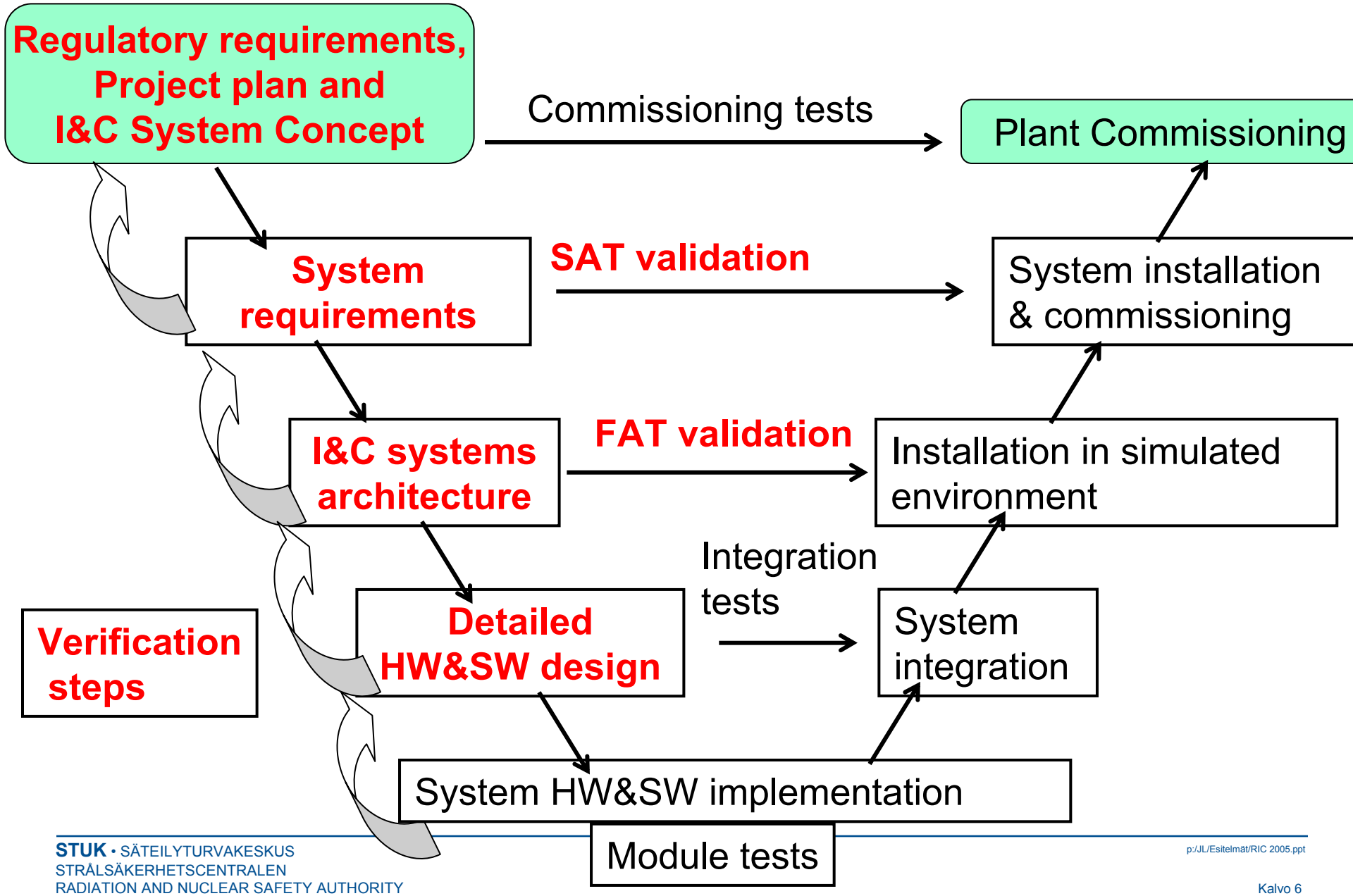
2. Avoiding spurious actuation that would cause a major plant transient, such as fast pressure drop in primary or secondary circuit or pumping cold water to primary or secondary circuit

# General viewpoints (2/4)

Digital I&C systems are generally more reliable and accurate than the analogue systems, but the concern is possibility of common cause failures that result from SW errors and could impact at the same time all redundant RPS divisions (channels)

- special concern is the possibility of spurious actuation which is more difficult to prevent

Absence of errors cannot be shown by testing, but low likelihood of errors can be demonstrated based on organized implementation. Commendable approach is the V-model given in the IEC and IEEE standards.


Regulatory requirements, Project plan and I&C System Concept
Commissioning tests
Plant Commissioning
System requirements
SAT validation
System installation & commissioning
I&C systems architecture
FAT validation
Installation in simulated environment
Integration tests
Verification steps
Detailed HW&SW design
System integration
System HW&SW implementation
Module tests

# General viewpoints (3/4)

**Reliable actuation** of RT and ESFAS is ensured at Finnish NPP's with

- four redundant and physically separated identical divisions, fail safe channels as feasible, and actuation principle 2/4
- independent and diverse defense lines
- logical systems architecture with multiple processors and system auto-diagnostics
- functional diversity in signals (i.e., actuation on different physical parameters or their combinations)
- reliable hardware: qualified platforms
- reliable software: systematic development of application SW and its qualification

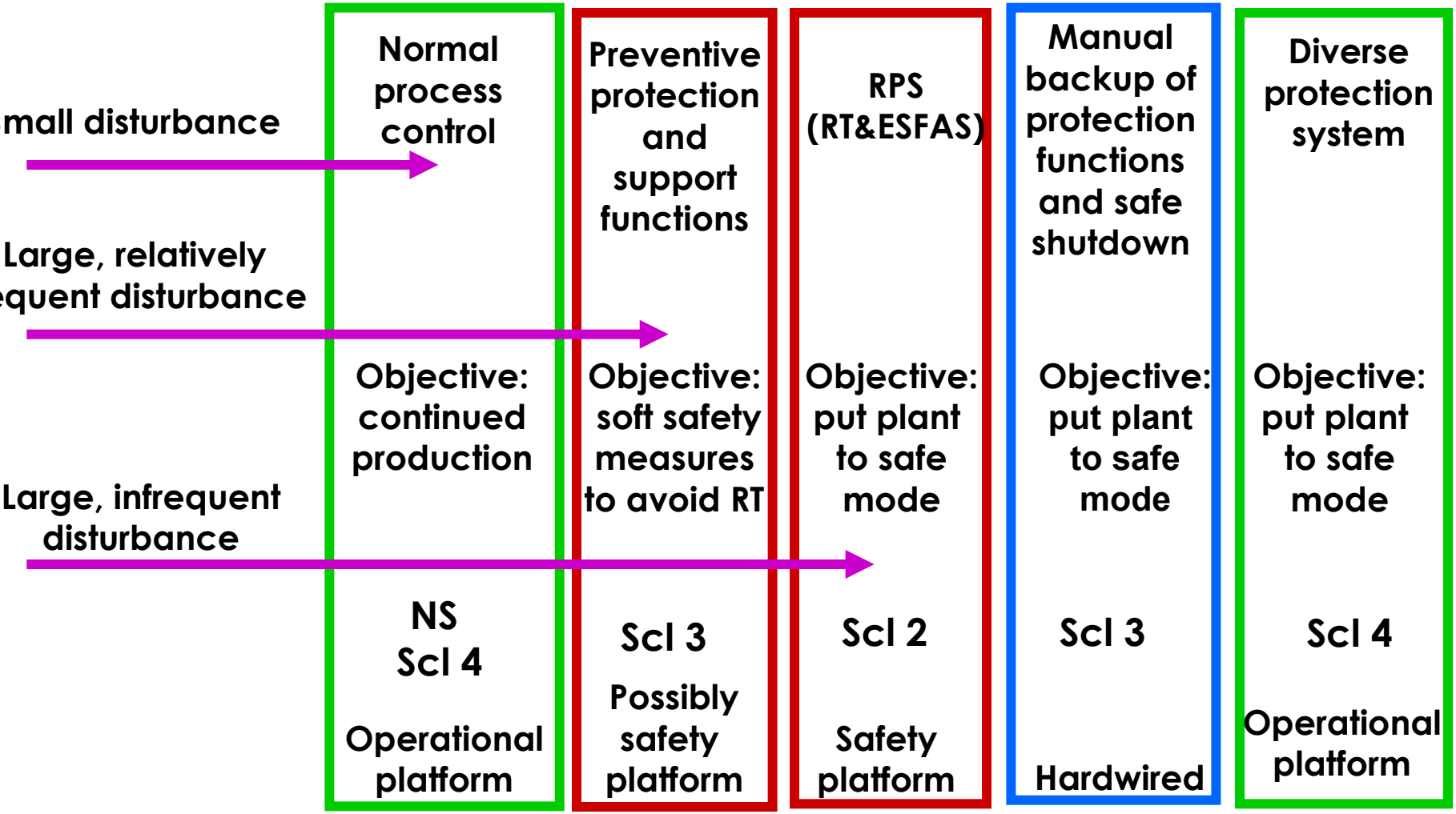
# General viewpoints (4/4)

**Avoiding spurious actuation** is ensured with

- logical systems architecture with multiple processors and system auto-diagnostics
- reliable hardware: qualified platforms
- reliable software: systematic development of application SW and its qualification

Diversity and Defense in Depth at the systems level do not help against spurious actuations

# Loviisa 1&2 – diverse defense lines of new I&C systen



# Loviisa 1&2 - remarks on diversity lines

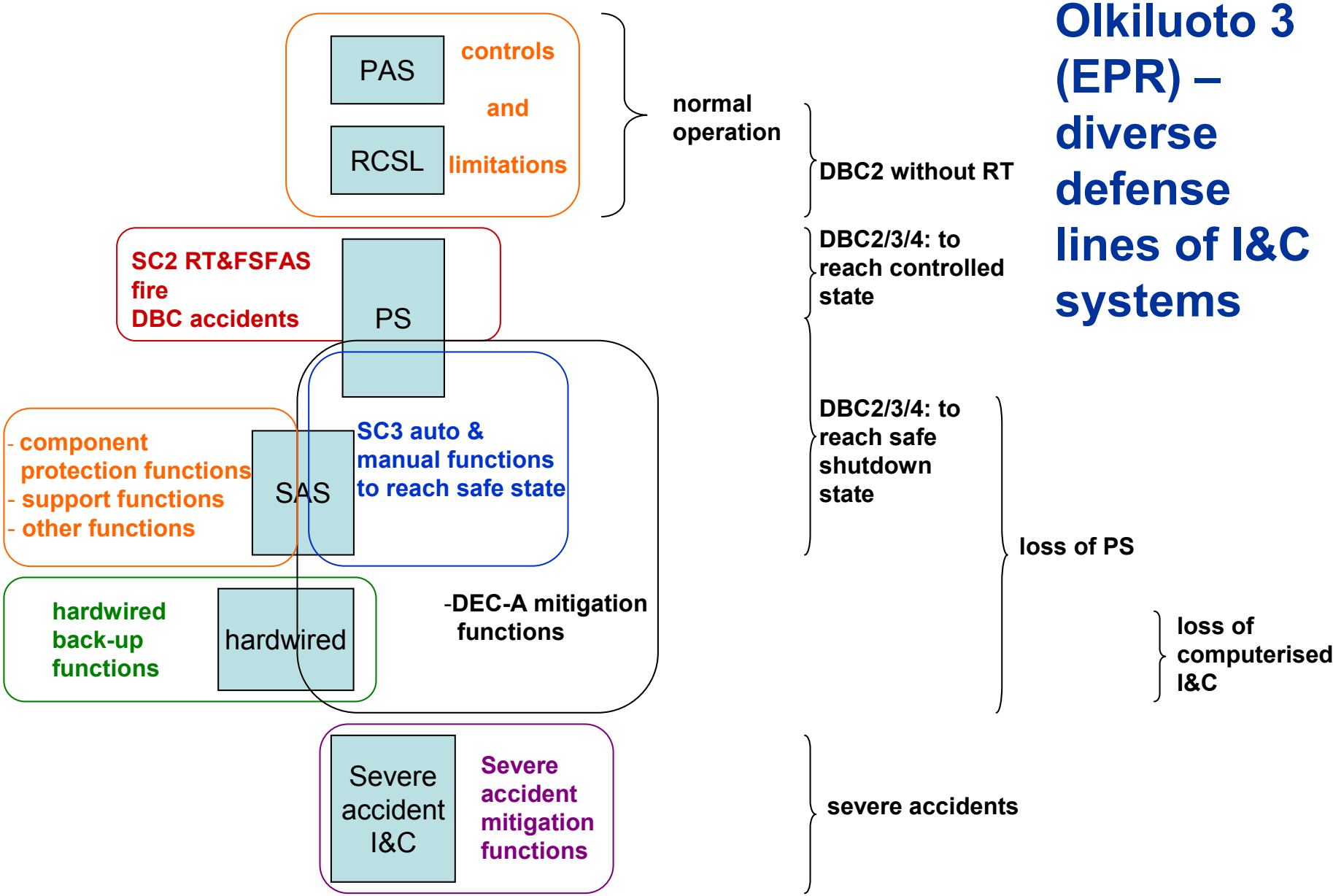
All protective functions can be actuated with manual hardwired system

- full back-up to RPS signals is provided

As another independent line of protection, diverse protection system provides automatic functions

- implemented with digital I&C that uses different platform than RPS
- diverse protection includes only a limited scope of RPS signals; this is considered adequate because of slow transients

# Olkiluoto 3 (EPR) – diverse defense lines of I&C systems



# Olkiluoto 3 - remarks on diversity lines (1/2)

Normal process control (PAS)

- uses Siemens TXP platform, non-nuclear safety classified

Limitation system (RCSL)

- uses FANP TXS platform, safety classified
- provides normal reactor power control with control ro
- actuates soft protection methods that reduce reactor power or shutdown the reactor in disturbance conditions (DBC2) with the aim to avoid actuation of RT or ESFAS

# Olkiluoto 3 - remarks on diversity lines (2/2)

Main line protection system (PS) covers all ”design basis events” (DBC2/3/4) and also several ”design extension events” (DEC-A)

- uses FANP TXS platform, safety classified

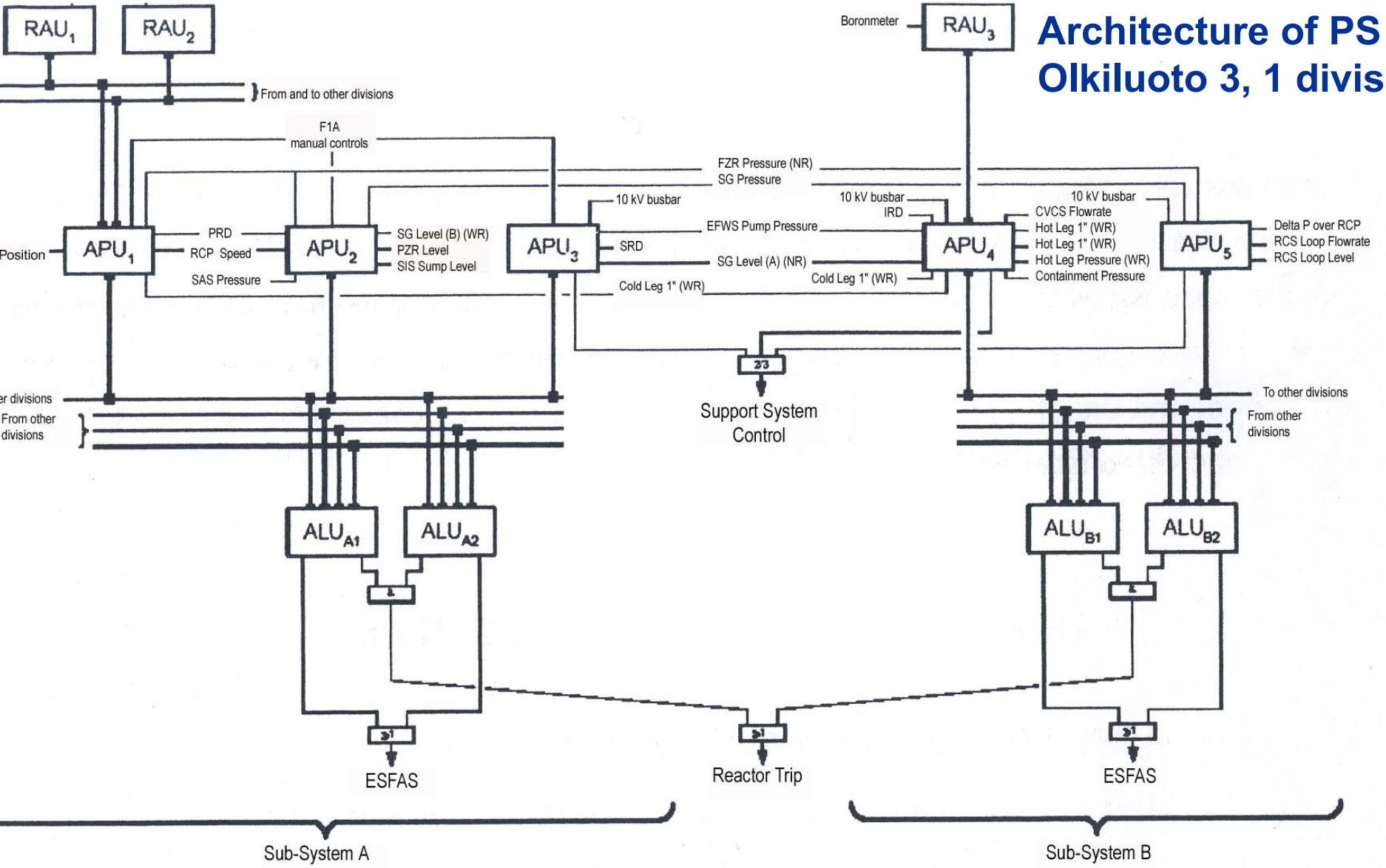
Digital back-up (SAS) for PS has more limited scope than PS

- SAS uses Siemens TXP platform, same as operation controls
- digital back-up is automatic for functions where fast response is needed (less than 30 minutes), otherwise manual

Hardwired back-up

- provides all automatic RT signals
- all other protective functions can be actuated manually with a hardwired system

# Architecture of PS o
# Olkiluoto 3, 1 divisio



# Explanations for "*Architecture of PS of Olkiluoto 3*"

Picture presents all signals and processors used for actuation of RT or ESFAS (one out of 4 divisions)

- PS section used for automatic reduction of steam pressure and emergency feedwater control is not shown here

Each big box represents one computer unit

Small boxes are hardwired logic units

RAU – Remote Acquisition Unit dedicated for neutron monitoring or boron monitoring signal treatment

APU – Acquisition and Processing Unit (signal validation, threshold detection, etc.)

ALU – Actuator Logic Unit (actuation management, voting between divisions, etc.)

# Views on involvement of regulatory experts in implementation of digital I&C systems

Smooth and cost efficient process for installing and licensing digital I&C systems requires active and **frequent interaction** between vendor, licensee, and regulatory body experts who represent various technical disciplines.

**More steps and hold points** for review and assessment are evidently needed **than in installing other type of systems, especially regarding software.**

# Regulatory requirements (1/3)

- **Regulatory requirements** need to be made well **known to all parties before a project** for installing new I&C systems is started
  - *organizational and quality requirements, including requirements on work processes*
  - *technical requirements*

- In addition, the licensee and all suppliers **need to know at which stage and to which depth the regulator wants to review various issues, and what the hold-points are**

# Regulatory requirements (2/3)

***Organizational and quality management requirements:***

- interactions between the licensee and suppliers,
- competences available to the participating organizations,
- work processes and tools to be used in design,
- verification and validation process,
- change control,
- ensuring software and data security, and
- use of independent assessors in various stages of the project

# Regulatory requirements (3/3)

***Technical requirements**:*

- principles for safety classification and its connection with requirements on quality management,
- dependability targets,
- separation of control, limitation, protection and back-up functions,
- physical isolation and segregation,
- fault detection, auto-testing, testability during operation,
- degree of redundancy and diversity,
- human interfaces, and
- qualification of equipment

# System requirements (1/5)

- *System requirements* for the I&C design are derived from the plant characteristics
  - Independent from the implementation of the I&C systems
  - I&C systems could be considered as black boxes at this stage; however, the specific features of digital I&C, e.g. the SW CCF potential, must be taken into account

# System requirements (2/5)

- *System requirements* need to be provided by experts who have a thorough knowledge on the plant's main and auxiliary systems and who understand the plant behavior in transient situations
  - The requirements must be supported with adequate deterministic safety analysis

# System requirements (3/5)

- *System requirements* must be unambiguous, accurate, and presented in a formal manner that is easily understandable to the I&C designers

- *System requirements* must be independently assessed by experts with same knowledge as those who wrote them.
  - Assessment is needed before moving to the actual I&C design stage

# System requirements (4/5)

- *System requirements* include
  - tasks for each I&C system and system boundaries towards the plant systems,
  - safety categorization (classification) of systems,
  - interaction and interconnections between systems,
  - input and output signals,
  - response of the I&C system to input failures (“fail safe” at input),
  - defense against potential incorrect outputs (“fail safe” at output),
  - variations, response times, and delays inherent to physical behavior of process parameters and equipment (e.g., for avoiding wrong response to short peaks),
  - possible use of common sensors and common actuators for control, limitation and protection tasks,
  - priorities between signals coming from different I&C systems, and
  - incorporating the I&C systems into the rest of the plant (power supply, operating environment, lay out, etc.)

# System requirements (5/5)

- Also requirements for the equipment qualifications need to be specified:
  - operability in specified environmental conditions for required times (temperature, pressure, humidity, radiation),
  - electromagnetic compatibility, and
  - operability or survival in seismic events
- **It is commendable that the regulators approve system requirements and equipment qualification requirements before starting the actual I&C design**

# I&C systems architecture / design (1/3)

- I&C experts must
  - convert the *system requirements* into a logical I&C systems architecture,
  - incorporate the diversity and Defense in Depth into the design, and
  - address all other *technical requirements*

- Basis for system choices should be explained in design documents

# I&C systems architecture / design (2/3)

- Close interplay between the plant systems experts, safety analysts, and I&C experts within all involved organizations is crucial
  - Failure Mode and Effects Analyses to be made jointly by experts having various skills: confirm that the “fail safe” principle has been correctly applied
  - Independent assessors to verify the correctness of the I&C architecture against the *system requirements*
  - Risk and reliability analysis: balance of the systems architecture and reliability targets for various I&C system parts

# I&C systems architecture / design (3/3)

- **Review and approval of the I&C systems architecture by the regulator is highly commendable before starting detailed hardware and software design** of the I&C systems.

- This would help to avoid potential conflicts caused by different interpretation of the requirements between the parties.

# Hardware and software design (1/3)

- Derivation of detailed hardware and software requirements from the *technical requirements* and *system requirements* should be described and documented by the I&C designers
  - adequate documentation permits independent assessors and licensee and regulatory experts to check correct interpretation of the requirements

# Hardware and software design (2/3)

- Platform and other equipment must be qualified against a requirement level commensurate with the safety significance of the system being designed
  - Evidence on qualification of existing hardware modules to be provided in QA documents, including proof of participation of a competent expert organization in qualification process

- Suitability analysis is required from the supplier to show that all relevant requirements for the proposed equipment are met

# Hardware and software design (3/3)

- For implementation of the coding and programming of the software, it is necessary that the supplier uses systematic methods and tools, and incorporates formal error checking into computer programs.

- **Licensee and regulatory experts should assess the evidence on hardware qualification and the programming process and the methods, but in our experience a detailed regulatory inspection of HW and SW modules would bring little added value**.
  - auditing the suppliers and and **qualification organizations** is done as part of the assessment

# Verification, validation and commissioning

- Verification is aimed to ensure that software modules are correctly produced and fault free
  - verification must be considered already when setting software requirements
  - verification steps must be documented to permit subsequent auditing
- Vendor must conduct adequate simulation in representative environment to validate dependable and correct system functions.
- Independent assessors need to be used for verification and validation tasks.
- **Regulatory experts should assess the verification and validation process and make audits as needed to achieve confidence.**