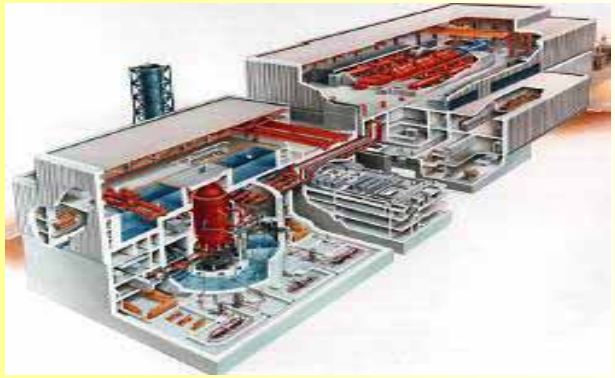
2008 AEC-NRC Bilateral Technical Meeting

Overview of Digital I&C for Taiwan Lungmen Project



Chang-Fu Chuang

Atomic Energy Council

May 12~13, 2008

Table of Contents

Introduction

- Lungmen Project consists of two GE-ABWR units. It started in March 1999, and was suspended in Oct. 2000 for 110 days due to government decisions. [ref p.12]
- Lungmen Project adopts modern fully-integrated digital design for control, communications, and human-system interfaces (HSIs). Digital systems have significant differences from analog systems in design and architecture.
- Challenges-limited technical guidance and regulatory precedent, and the technology is still evolving.

Long-term cooperation with USNRC through AE-IN-NR-C18 program. [ref p.13]

Overview of Lungmen Digital I/C Systems (1/2)

- Overall architecture consists of five levels: sensor/actuator level, local level, system level, plant-wide level and utility-wide level. [ref p.14]
- Design process started with system design, followed with human factors engineering, hardware design, and software design proceeding in parallel. Total system integration was tested in FAT and will be tested again in site testing. [ref p.15]
- Multiple designer/supplier/implementer-interface coordination and technical integration complicated. [ref p.16]

Overview of Lungmen Digital I/C Systems (2/2)

- Human Factors Engineering Program Review Model specified in NUREG-0711 is adopted for evaluation of the HSI design. The Verification & Validation (V&V) activities have been separated into V&V-1, V&V-2, and V&V-3. [ref P.17]
- The way operational information is displayed and the way operators perform control in the Main Control Room are much different from those in conventional control rooms. [ref P.18]
- Operators have to navigate from among 45 video display units (VDUs) and ~1,000 operation screens (in 3 hierarchy levels) to get operational information. [ref P.19]

Bases of Regulation

- Taiwan Requirements

  " Nuclear Reactor Facilities Regulation Act “ , "Detailed Regulations for Implementation of the Nuclear Reactor Facilities Regulation Act " and applicable domestic industrial codes and standards.

- Country-of-Origin Codes and Standards

  Compliance with country-of-origin codes and standards is pre-requisite. Particularly, Chapters 7 and 18 of USNRC Standard Review Plan (SRP) are major bases.

  Chapter 7 Instrumentation and Controls
  - 7.8 Diverse Instrumentation and Control Systems
  - 7.9 Data Communications Systems
  - Appendix 7.0-A Review Process for Digital I&C Systems

  Chapter 18 Human Factors Engineering [ref p.20]

Current Regulatory Activities (1/2)

- Review of FSAR Submittal (Ch.7 & Ch.18)

1. Received Taipower's FSAR submittal on August 15, 2007.
2. In response to acceptance review by AEC, Taipower submitted Amendment of FSAR Chapter 7 and 18 in early March, 2008.
3. Review process has been established. Review team consists of AEC staff and members from INER and domestic scholars and experts.
4. Use of USNRC Interim Staff Guidance as referenced review criteria where appropriate.

Current Regulatory Activities (2/2)

- Site Audit

1. Perform, on sampling basis, witnesses and audits of testing activities at site, including post-construction tests (PCT), pre-operation tests and start-up tests, etc.
2. PCT is ongoing now. Site Audits for PCT include RMU cabinets tests and I/O tests and datalink tests, etc.

Current Major Regulatory Issues/Concerns (1/1)

- Data Communications Network [ref p.21~25]
- Cyber Security [ref p.26~27]
- Software Safety Analysis Process and Results [p.28]
- Human Factors Engineering V&V [p.31~32]
- Integration Tests [p.33~34]
- Fiber Optical Performance [p.35]
- Diversity and Defense-in-Depth Analysis [p.36]
- Software V&V and CM
- Full-Scope Simulator Implementation Activities
- EMI, RFI, Grounding Issues

Conclusions and Recommendations

- “Asking the Tough Questions -- Making the Tough Calls.”

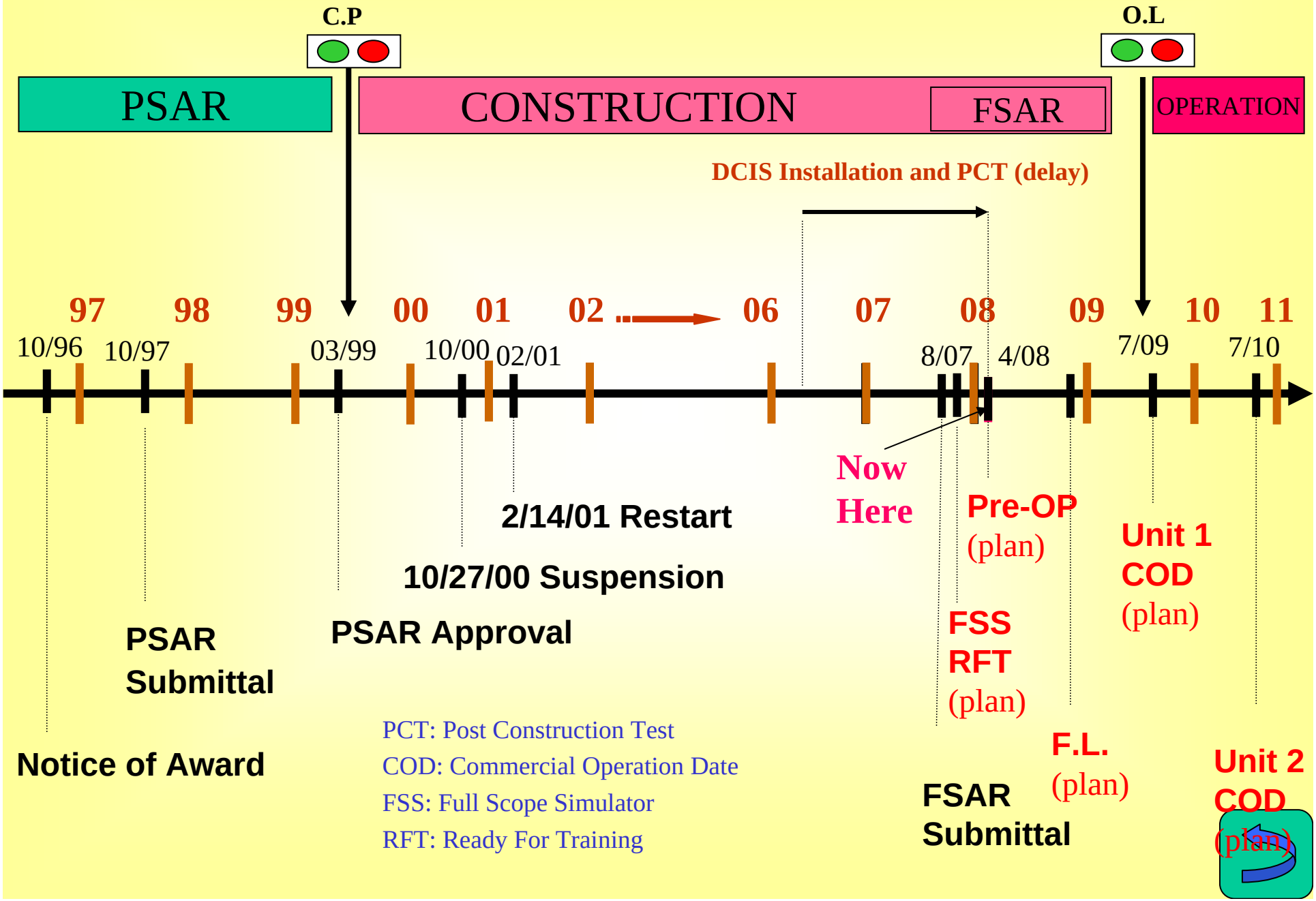
  Digital I&C licensing is a challenging task since there is limited precedent and the technology is still evolving. As the first project to follow U.S. codes and standards, and regulations on plant-wide digital I&C, the challenge is more obvious in the Lungmen project.

- Thanks to the long-term cooperation program, AEC has had USNRC support in due course, and thus been able to deal with the issues/problems encountered so far. We are pleased to share our experience with the USNRC.

- Submittal of the the FSAR signifies beginning of an important stage in the two-step licensing process for Lungmen. We expect to have more interactions and strengthened cooperation between both parties in this stage.

Thanks for your attention !

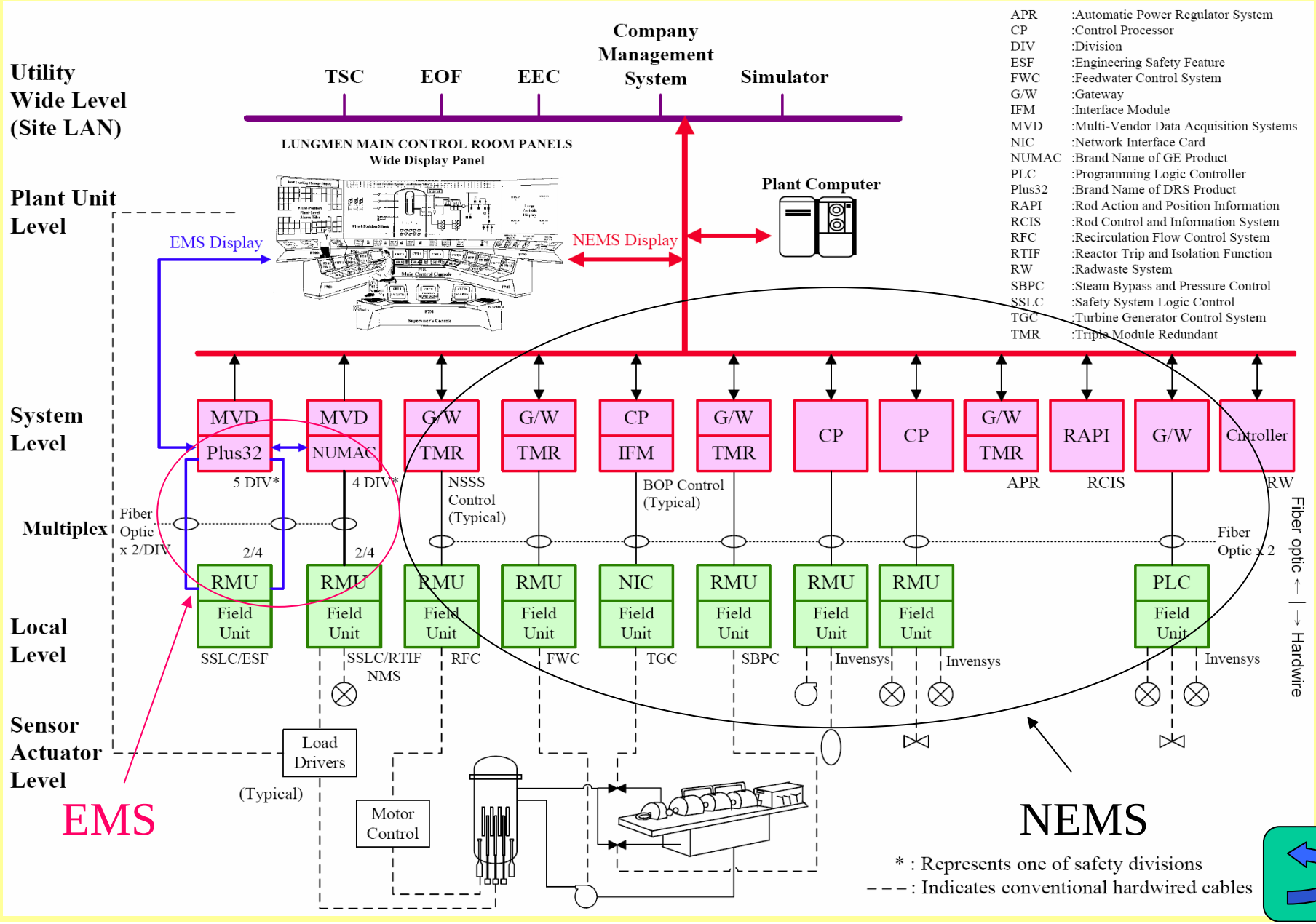
Key Milestones



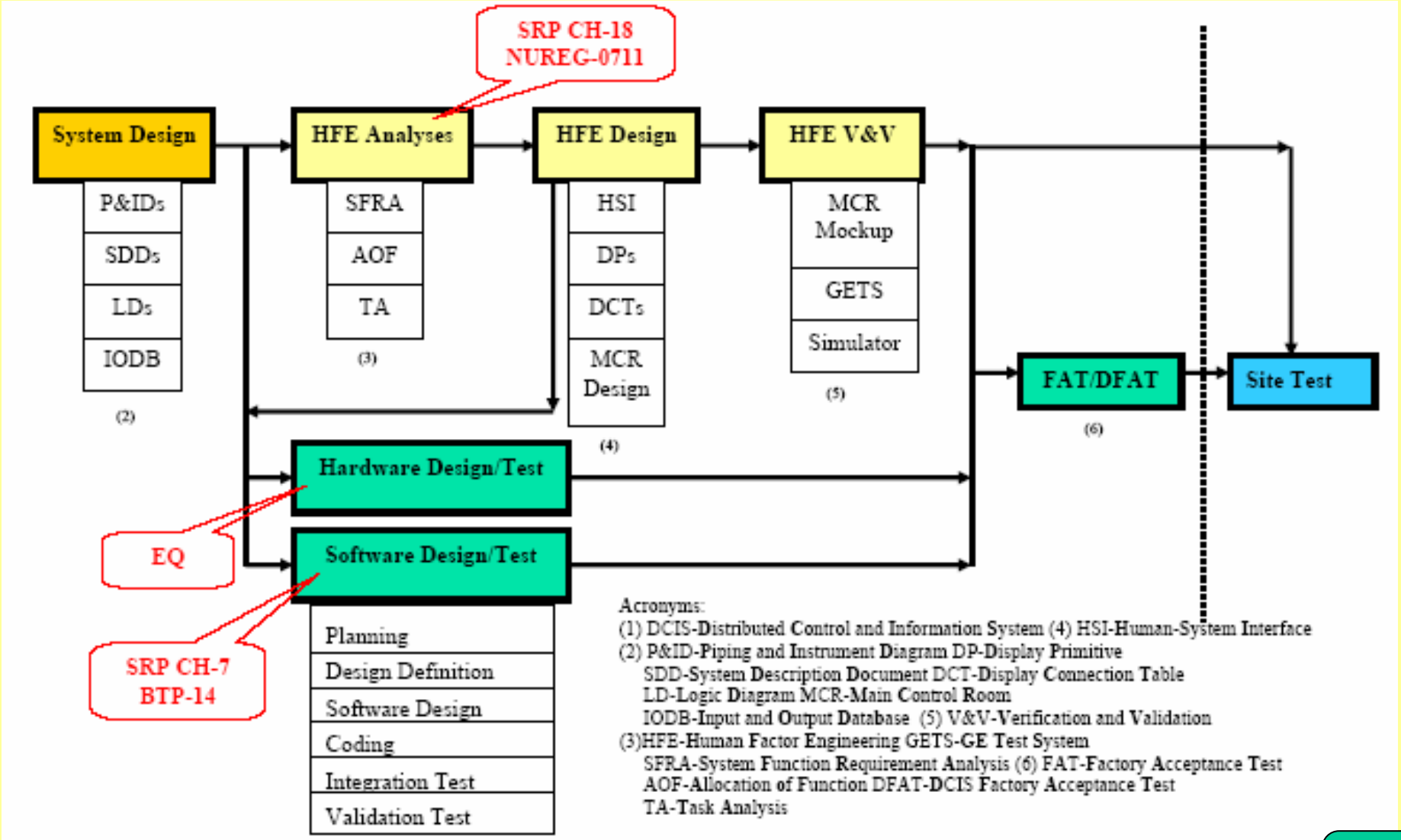
Three USNRC experts joined AEC delegation auditing GE in June, 2000.

- NRC Mr. Chiramal attended the technical meeting between AEC and TPC in 2004
- Two NRC experts will visit Lungmen in July, 2008.

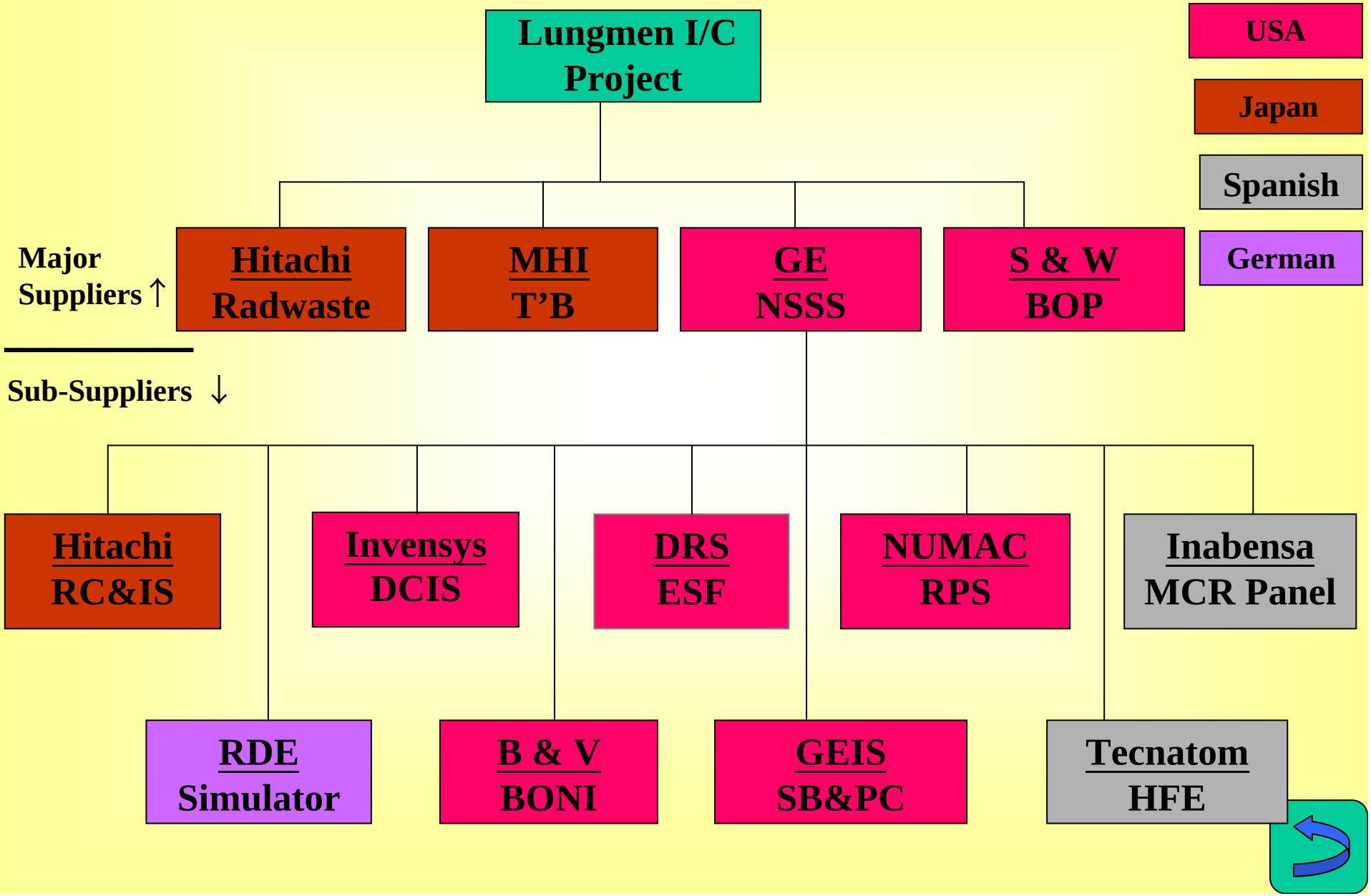
Overall architecture of Lungmen I&C systems



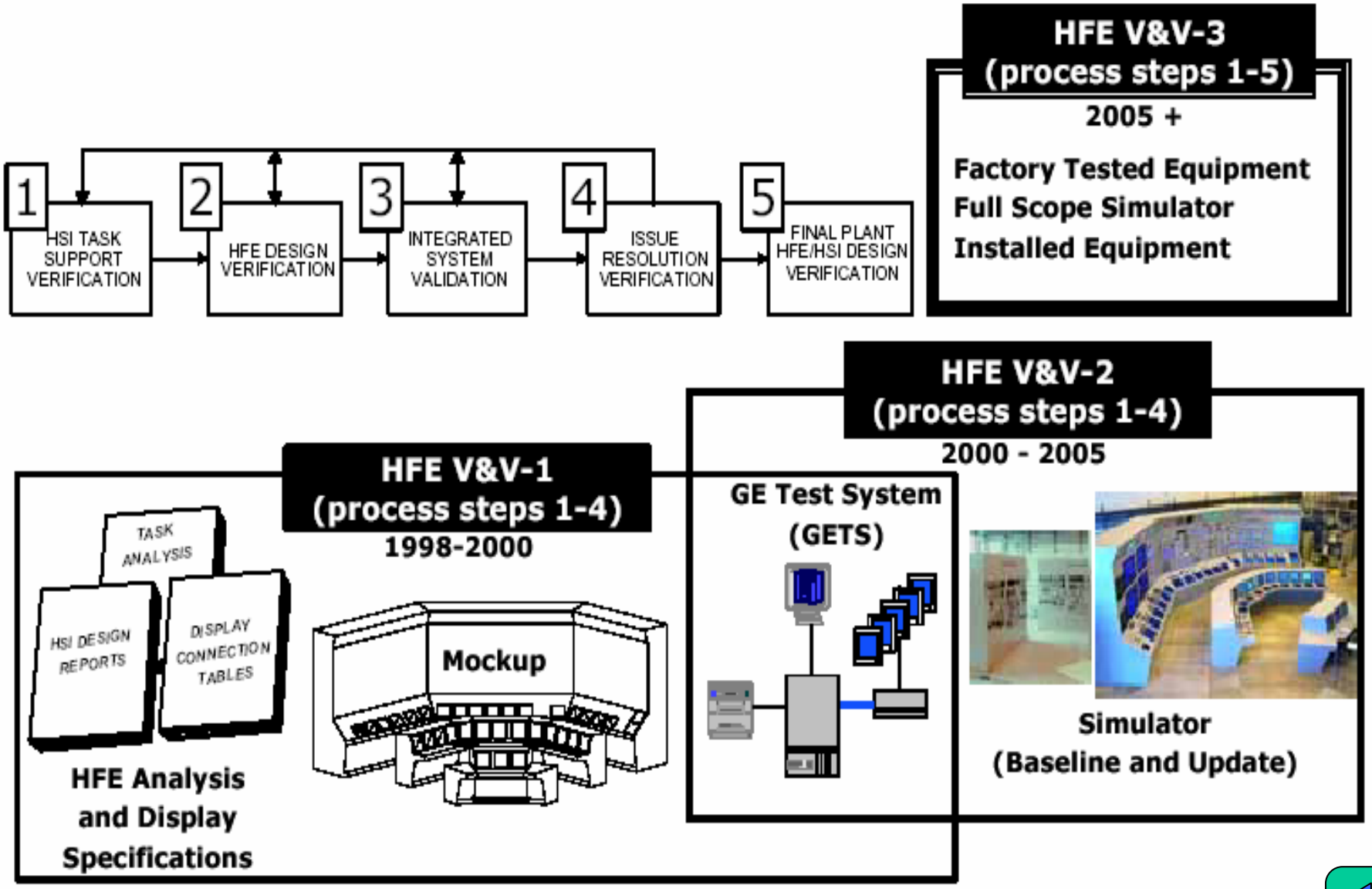
Design Implementation Flowchart



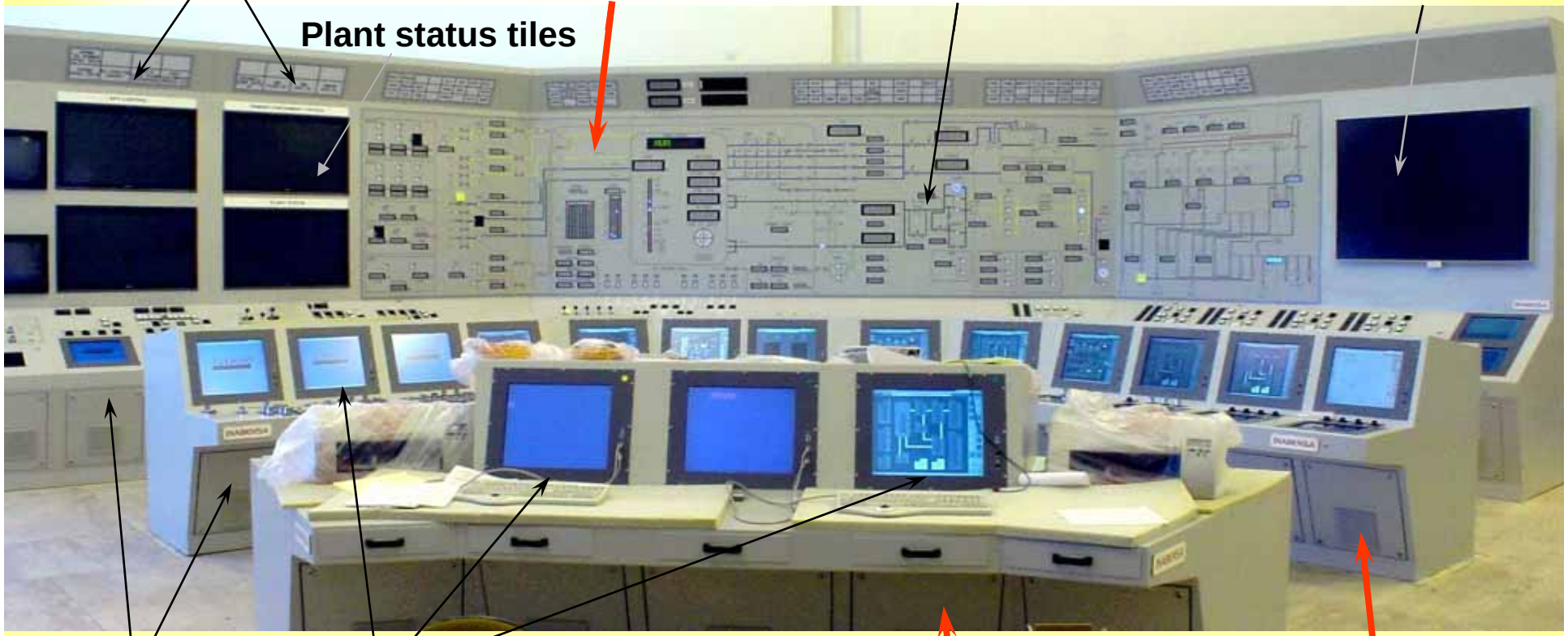
Major Digital I&C Systems and Various Vendors



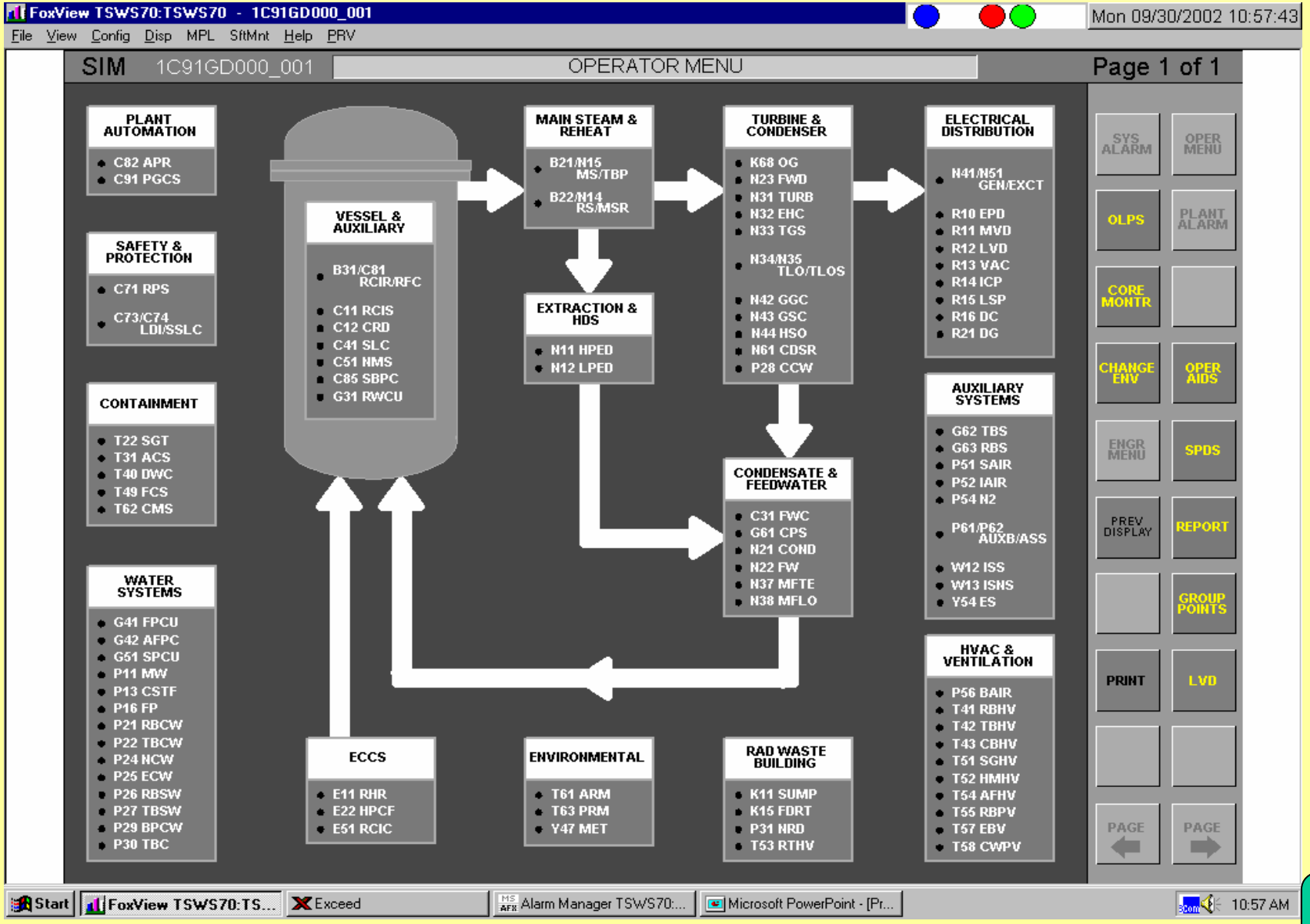
The Implementation of HFE V&V Plan



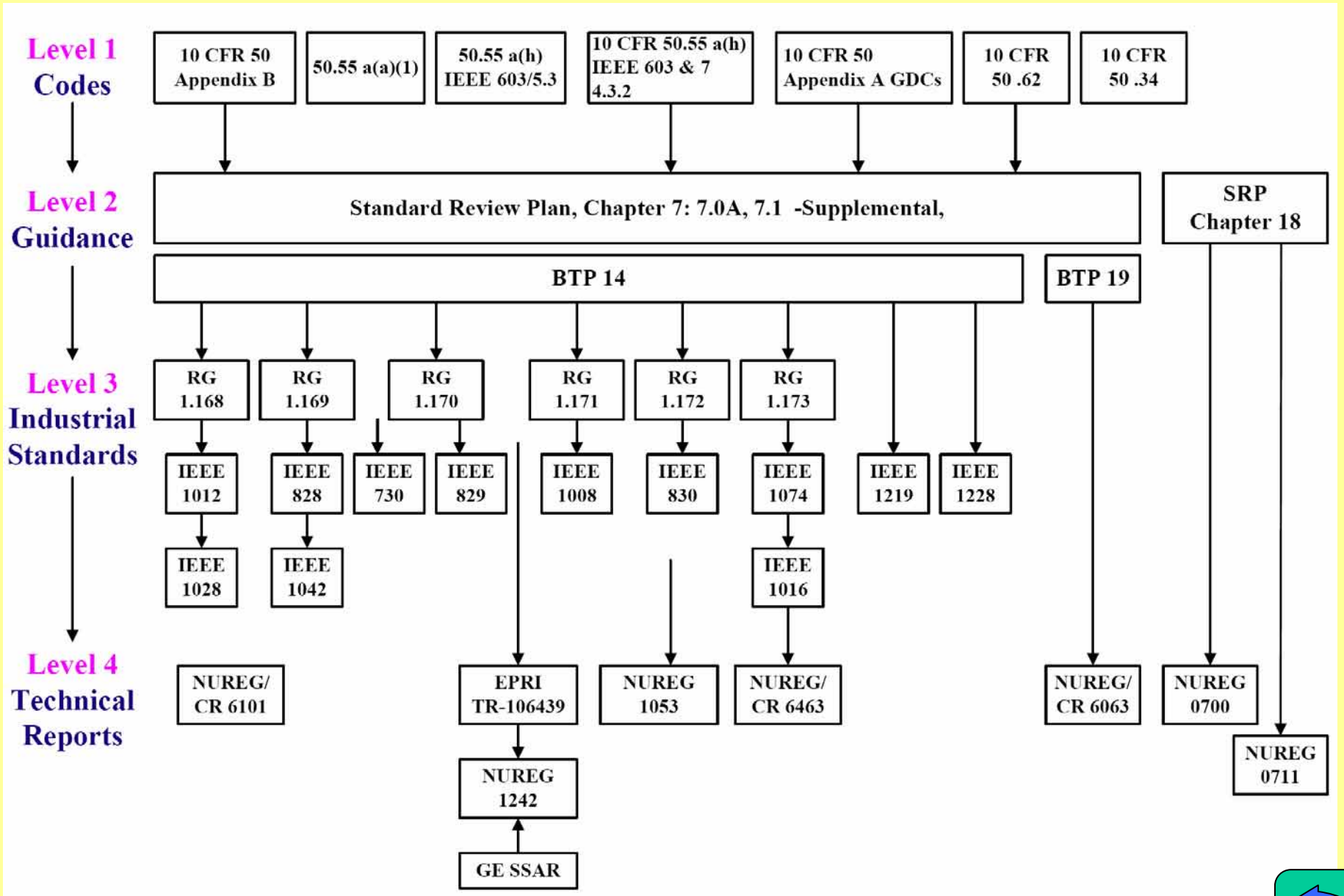
Main Control Room



Front Page of Operation Menu on VDU



Structure of Country-of-Origin Codes and Standards



Current Major Regulatory Issues/Concerns

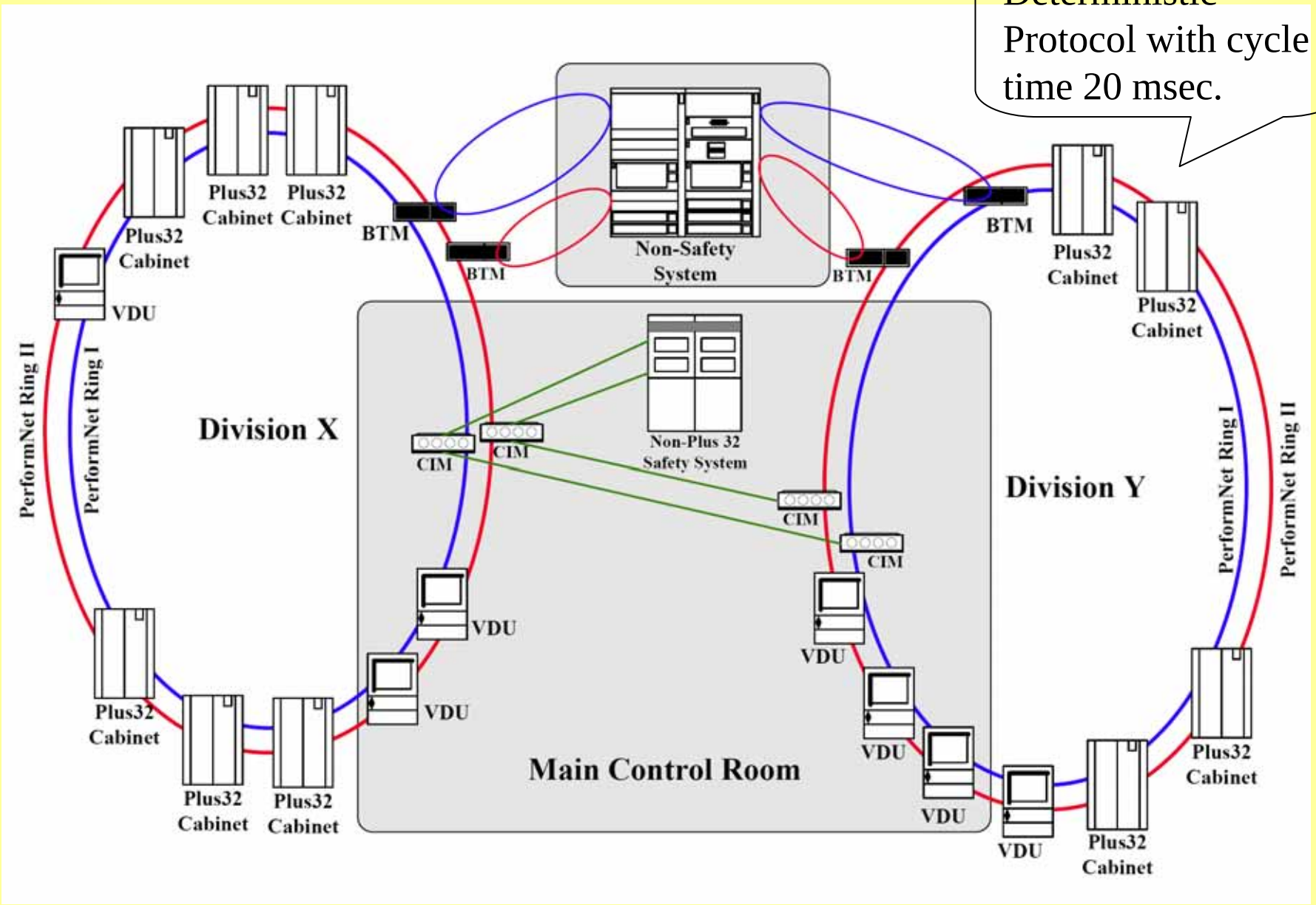
- Data Communications Network

  - Network and multiplex systems are classified as safety class (EMS) and non-safety class (NEMS).

  - EMS must be Class 1E-qualified system with deterministic communications protocol design. [P.22]

    1. EMS Platform Certification.
    2. Dedication issue of DRS VDU Touch Screen Controller.
    3. Concern that deterministic protocol design with 20 ms may affect the time resolution of Sequence of Events (SOE) in root cause analysis while plant in operation in the future.

EMS Network Architecture



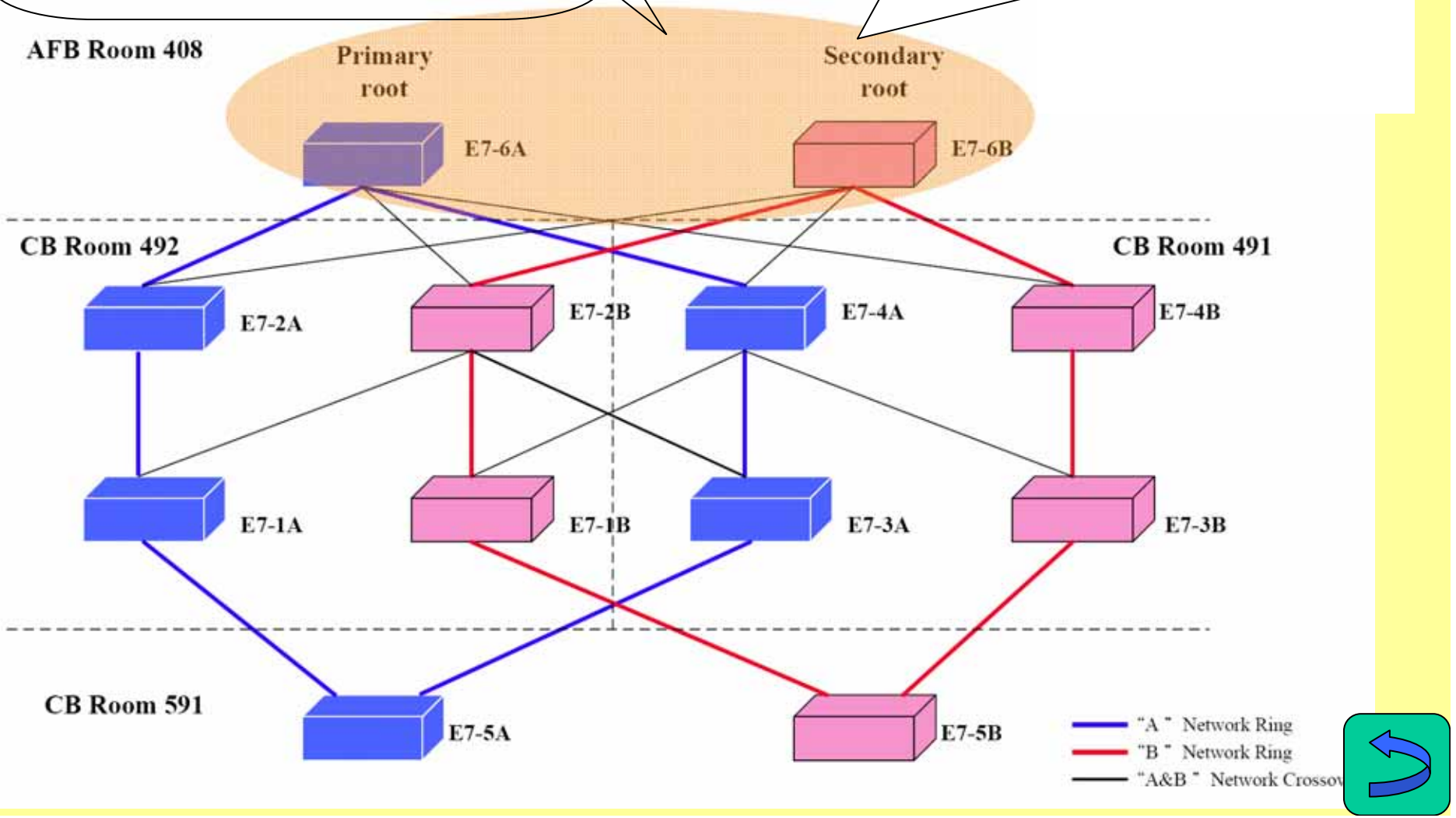
Current Major Regulatory Issues/Concerns

- Data Communications Network
  - NEMS Network real-time performance, including time response and data loading in normal operation, transient, emergency conditions, etc., is our concern.
    1. Failure of Both Ethernet Root Switches. [P.24]
       Originally in the event that pair root switches are lost simultaneously, the resulting network reconfiguration would be completed in ~20 seconds. After corrective action, E7-2B and E7-4A will become root switches within several ms once the pair root switches are lost simultaneously.
    2. Some data flow paths exceed the predefined response time 1.5s in FAT; further review on them is needed. [P.25]

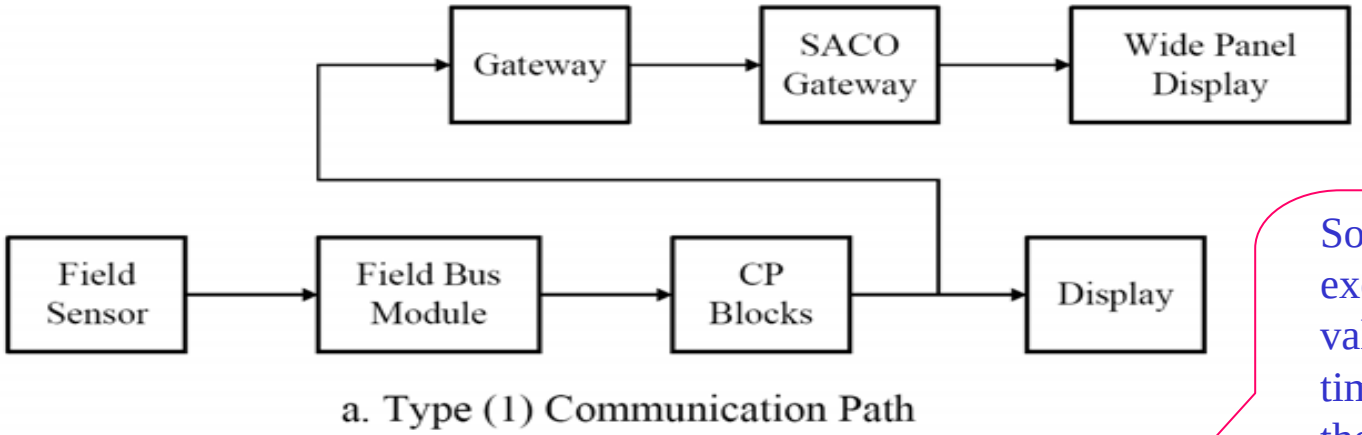
NEMS Ethernet Switch Redundant Ring Network

Originally in the event that pair root switches are lost simultaneously, the resulting network reconfiguration will take ~20 seconds.

After corrective action, E7-2B and E7-4A will become root switches within several ms once the 6A/6B pair root switches are lost simultaneously.

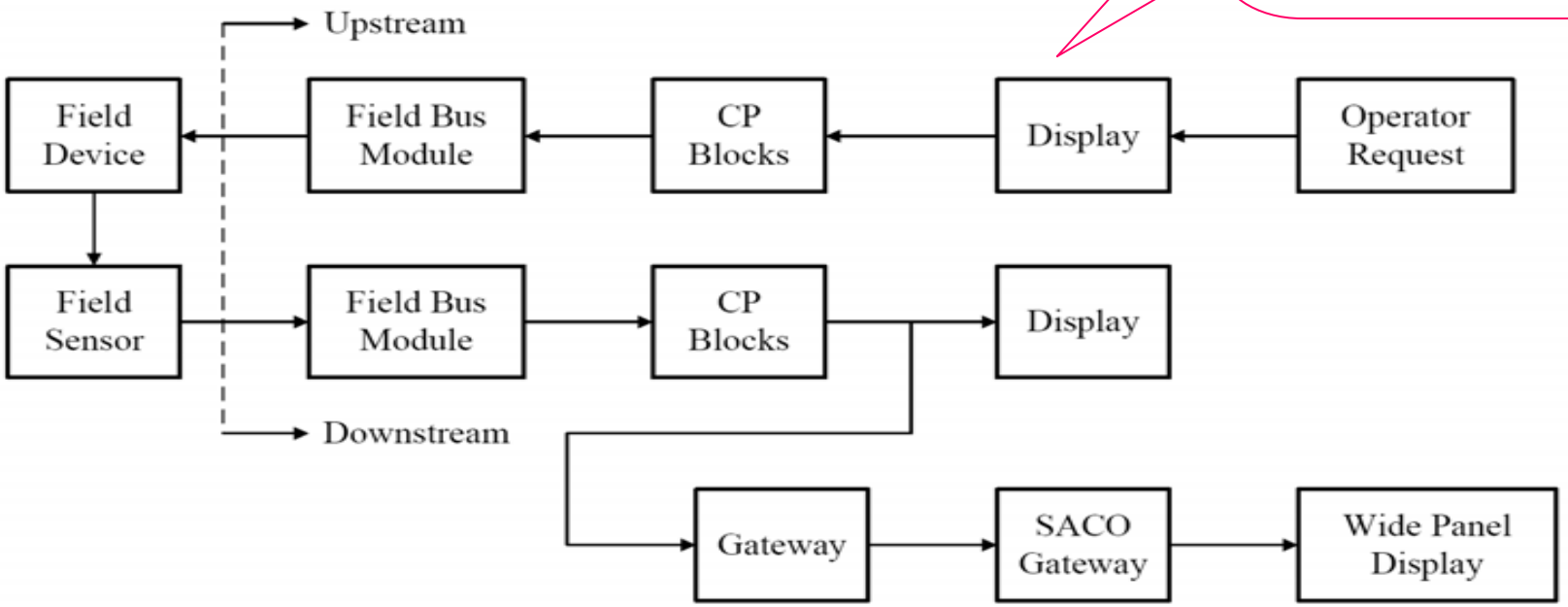


Typical Communications Paths



a. Type (1) Communication Path

Some data flow paths exceed the predefined value of 1.5 s response time. Further review on them is needed.



b. Type (2) Communication Path

Current Major Regulatory Issues/Concerns

- Cyber Security
  - There is no specific cyber security requirement in TPC Lungmen Spec. However, the security requirements is part of the overall system requirements. User access capabilities, especially via networks, are restricted for protection against potential cyber security threats. Remote access to the control network is prohibited.
  - A Security Policy shall be developed by power plant to delineate control over
    (1) access to the software functions,
    (2) use of safety system services,
    (3) data communications with other systems,
    (4) the list of personnel who may access / use the system.

Current Major Regulatory Issues/Concerns

- Cyber Security
  - USNRC has conducted studies on Cyber Security and Vulnerabilities, and continued working on this important topic. We expect new regulations and guidance to be issued for this topic in near future.
- We will study them thoroughly for retrofitting to the existing NPPs as appropriate.

Current Major Regulatory Issues/Concerns

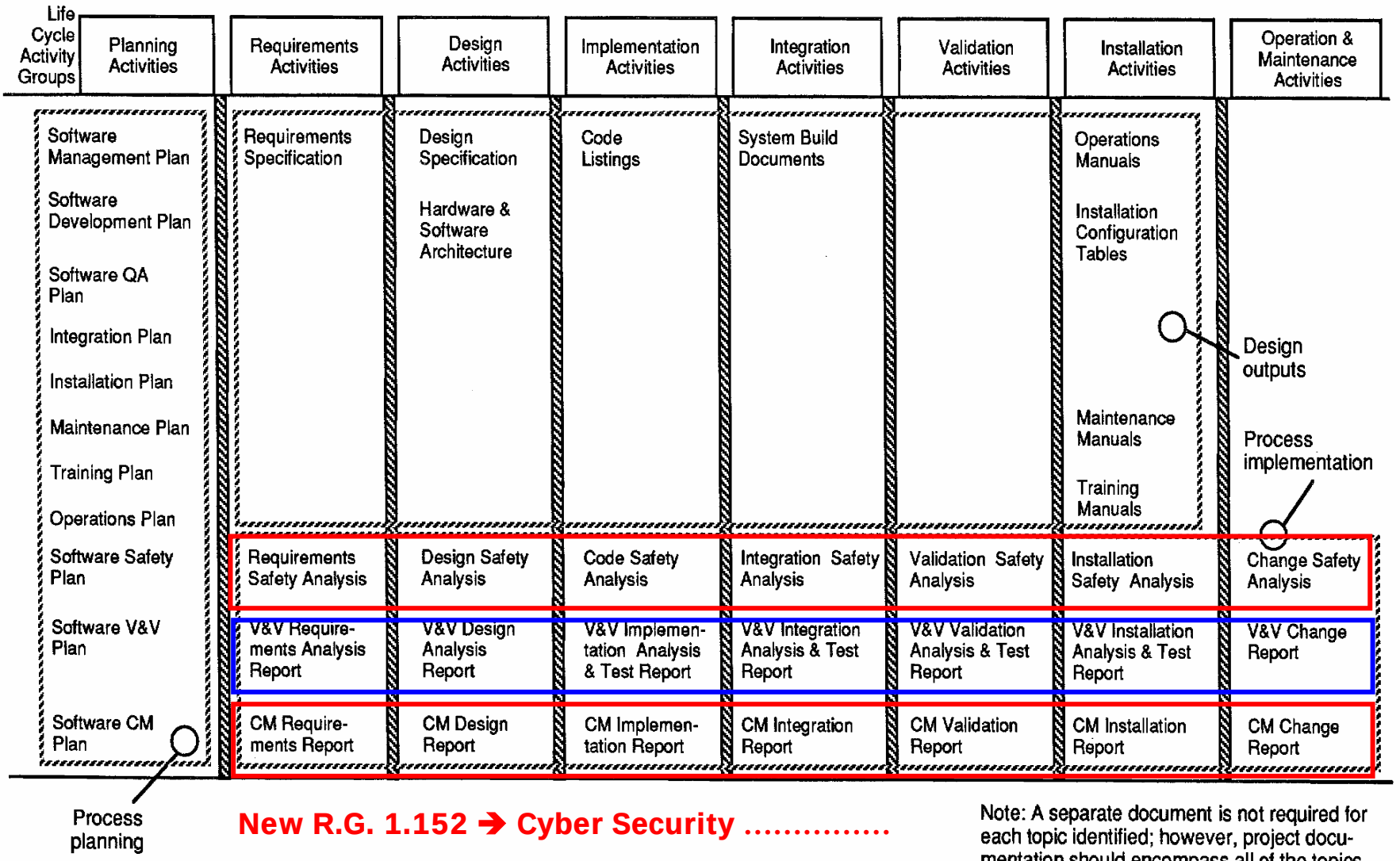
- Software Safety Analysis Process and Results
  - SSA is to identify potential system safety threats originated from the unintended software features that were created during software development process.
  - No specific guidance was endorsed by USNRC for performing SSA. So, it was difficult to reach consensus on how to perform SSA activities and how to prepare/review SSA reports among all parties concerned. It has taken extra time and effort to agree on the SSA process.

Current Major Regulatory Issues/Concerns

- Software Safety Analysis Process and Results (cont.)
  - Lots of discussions were held, with final resolutions reached as follows:
    1. To apply FMEA method used in Hazard Analysis & Defense in Depth for SSA for all safety systems.
    2. To apply FMEA method used in Abnormal Condition Event Analysis, based on IEEE-7-4.3.2-1993, for new software of safety systems, such as RTIF, and Class 1E Video Display Units (VDUs).
    3. TPC to hire a third party to perform “Parallel Validation of Software Safety Analysis” to validate the vendor’s SSA activities and results.

NUREG-0800 SRP

BTP 7-14: Guidance on Software Reviews for Digital Computer-Based I&C Syste



New R.G. 1.152 ➔ Cyber Security .....

Note: A separate document is not required for each topic identified; however, project documentation should encompass all of the topics.

30

Current Major Regulatory Issues/Concerns

- Human Factors Engineering (HFE) V&V

- V&V is to assure that the design of the HSI conforms to HFE principles. The V&V activities for the Lungmen project have been separated into three phases; V&V-1, V&V-2, and V&V-3, depending on the design progress and the tools available for use.

- The MCR design still needs to go through the HFE V&V-3 for final integrated system validation and as-built design verification. .

- A VDU operational configuration strategy is being developed for management and operation of the large number of VDUs in the MCR under different operating modes, to guide and limit the freedom of VDU usage. The strategy will be subject to V&V before it is finalized for use in the LMNPP.

Current Major Regulatory Issues/Concerns

- Human Factors Engineering (HFE) V&V

  - NUREG-0700 Rev. 1 (1996) and NUREG-0711 Rev. 0 (1994) were committed in the LMNPP's Preliminary Safety Analysis Report (PSAR, 1997). The current version of NUREG-0700 is Rev. 2 (2002), and of NUREG-0711 Rev. 2 (2004).

  - Guidelines on maintainability of digital I&C equipment provided in the new version of NUREG-0700 are adopted for the Lungmen Project. The additional program elements specified in the new version of NUREG-0711 is under investigation for adoption.

Current Major Regulatory Issues/Concerns

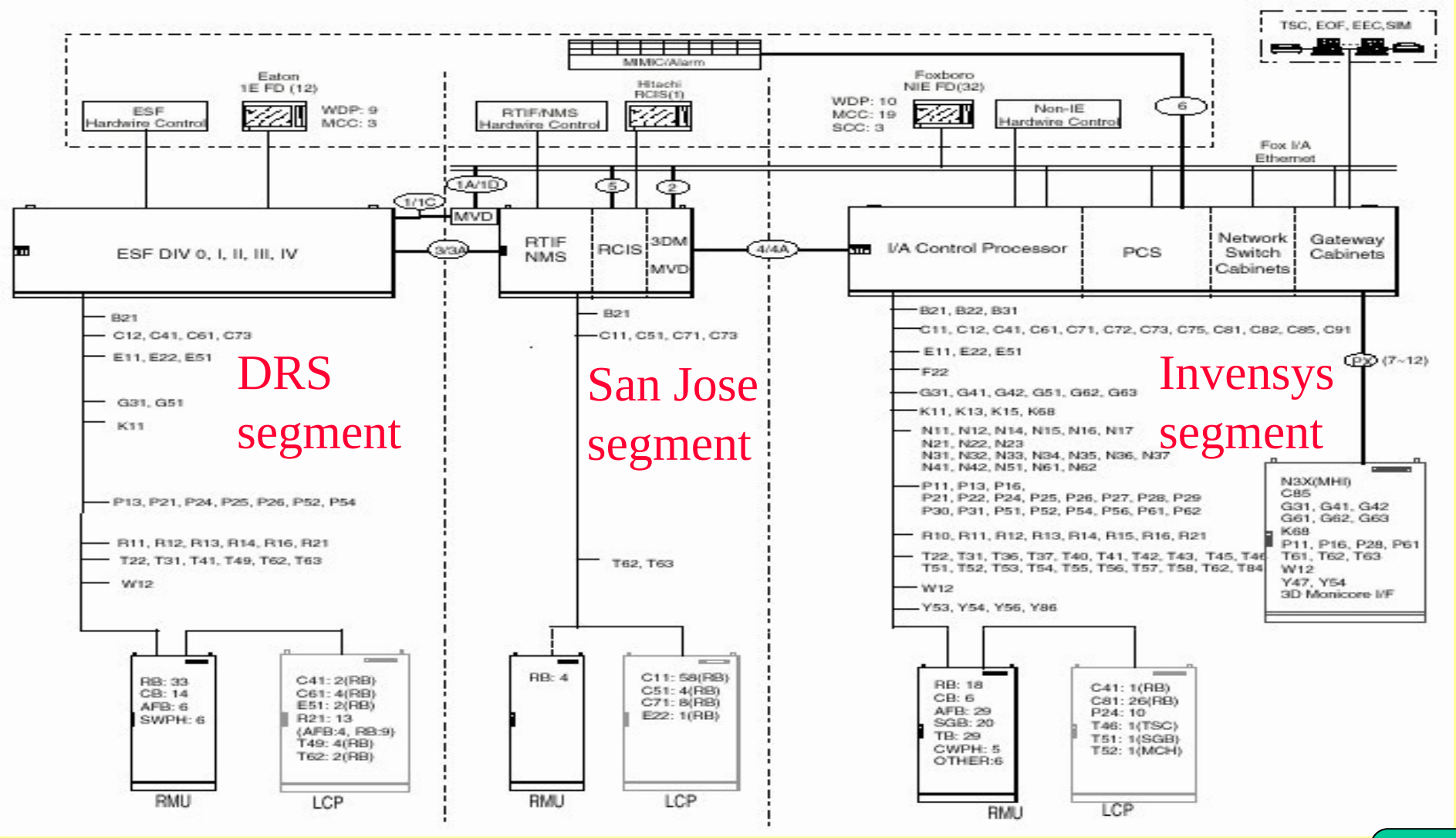
- Integration Tests (FAT & SAT)

- FAT has been performed at major suppliers based on a segmented testing approach. The FAT serves as the last validation before shipping to the site. Completeness of test coverage, and potential interface and integration problems are of concern. [P.30]

- As SAT is the first opportunity the DCIS is connected and tested together, the SAT will play a more important role than that for the conventional NPP, in confirming the total integration of the DCIS. It is a concern that the leading designer is not responsible for conducting the SAT. Another concern is that insufficient time is allocated for the site tests.

- Of concern also, is the process for test execution and for resolutions of discrepancies during SAT.

Segmented FAT Overview



Current Major Regulatory Issues/Concerns

- Fiber Optical Performance

  - Fiber construction and identification, attenuation.
  - Treatment of fiber optic joining points (FOJP), where the fibers come together, high-quality fusion splice with low splice loss, low reflection, high mechanical strength, and long-term stability are all important items for regulation.

Current Major Regulatory Issues/Concerns

- Diversity and Defense-in-Depth Analysis

- To demonstrate that the design has adequate coping capability in the event of a digital common cause failure
- Branch Technical Position HICB-19
  - For each anticipated operational occurrence in the design basis occurring in conjunction with each single postulated common-mode failure
  - To calculate the plant response using best-estimate (realistic assumptions) analyses
  - No radiation release exceeding 10% of the 10 CFR 100 guideline value
  - No violation of the integrity of the primary coolant pressure boundary

Current Major Regulatory Issues/Concerns

- Diversity and Defense-in-Depth Analysis (cont.)
  - To clarify whether or not Lungmen FSAR Ch15 needs to be modified in order to reflect the effects of software common mode failure :
    - GE concludes that BTP-19 does not require that the analysis in Chapter 15 of FSAR to be modified to reflect the effects of software common mode failure. Also, the issue of software common mode failure is considered beyond the design basis from EPRI and industry
    - The requirement that the digital RPS should be protected against CCFs is imposed by the USNRC no matter how the software common mode failure is classified, namely, beyond design basis or not. [ref]
    - Final resolutions need to be reached in the future