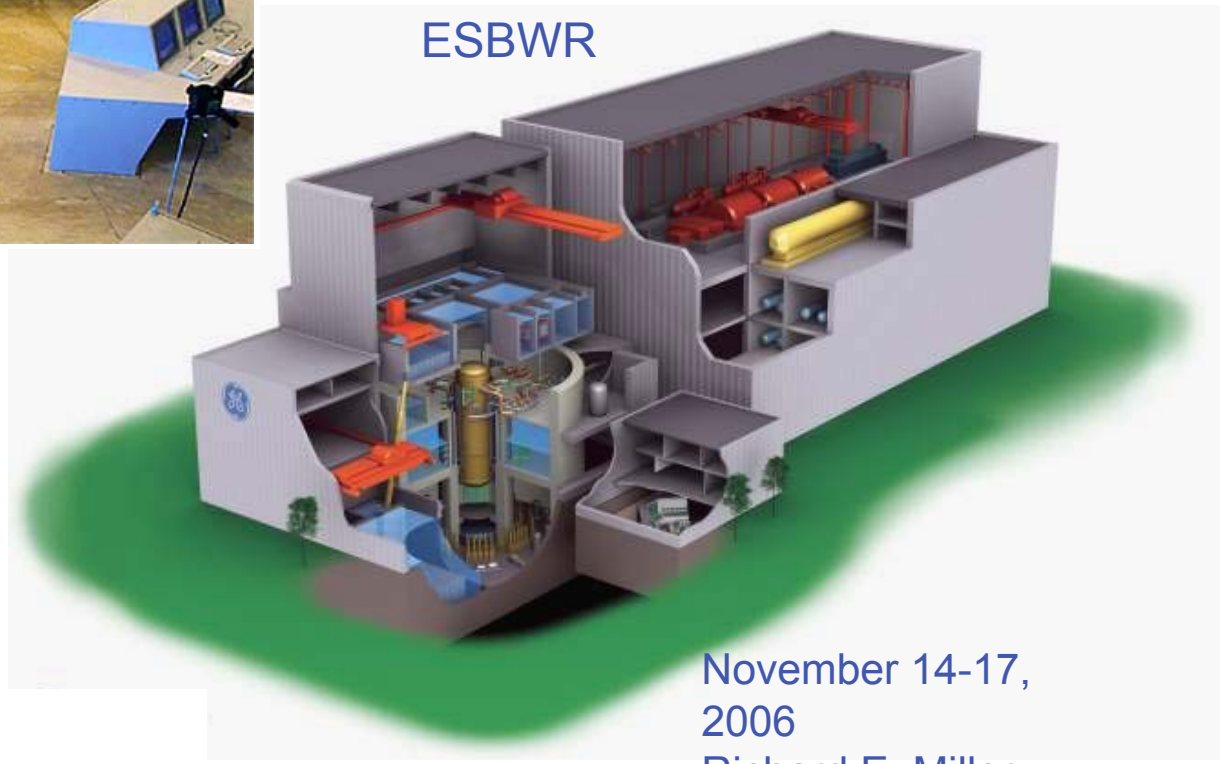
ESBWR Instrumentation & Controls - NRC Audit

November 14 - 17, 2006

Digital Control Room

ESBWR



imagination at work

November 14-17, 2006

Richard E. Miller

ESBWR Instrumentation & Controls - NRC Audit Agenda

Tuesday, November 14th

0800 – GE Setup

0830 – Entrance Meeting – Introductions

0900 – Agenda Overview

- Sessions – with no proprietary information (Main Presentation Slides)
- Sessions with proprietary information (Supplemental Presentations and Handouts as marked “Proprietary”)

Presentations and Discussions

0915 – DCIS Equipment Location Overview and Control Room Panel

Layout

ESBWR Instrumentation & Controls - NRC Audit Agenda (Continued)

Tuesday, November 14th - Continued

0945 – DCIS Architecture Top Down Overview

- E-DCIS (Safety-Related DCIS) - (Some *Proprietary Information*)
  - NUMAC (RPS & NMS Functional Block Diagrams)
  - SPINLINE3 (ECCS/ESF Functional Block Diagram)
  - IEEE-603 (10CFR50.55a(h) Compliance Documentation – LTRs
- NE-DCIS (Nonsafety-Related DCIS) and Displays
- Data Communication and Isolation
- Post Accident Monitoring
- Interlock Systems
- RTNSS
- Cyber Security & R.G. 1.152 Compliance

ESBWR Instrumentation & Controls - NRC Audit Agenda (Continued)

Tuesday, November 14th Continued

1200 – Lunch

1245 – DCIS Architecture Top Down Overview – Continued

1630 – Daily Summary, Readjust Agenda, and Discuss Next Day's Agenda

ESBWR Instrumentation & Controls - NRC Audit Agenda (Continued)

Wednesday, November 15th

0730 – GE - Setup

0800 – Technical Specifications – I&C

1030 – Independent Verification Requirements and eMatrix (eIV)

1100 – ERM/ECN Document Requirements and eMatrix (ERM/ECN and eDRF)

1130 – Software Overview

1200 – Lunch

1230 – Diverse Protection System

1300 – COL Participation in I&C Design Process Life Cycle Activities

1345 – ITAAC Update

1500 – Commercial Grade Dedication Process

1530 – Equipment Qualification Process for Multiple Vendors

1600 - Daily Summary, Readjust Agenda, and Discuss Next Day's Agenda

ESBWR Instrumentation & Controls - NRC Audit Agenda (Continued)

Thursday, November 16th

0730 – GE - Setup

0800 – System Review / Audit Preliminary Simplified Logic Diagrams (*Proprietary Documents*)

1200 – Lunch

1300 – Simulated Assisted Engineering (SAE) Modeling Demo – RWCU (*Proprietary Session*)

1400 - RAIs in Process – I&C

1600 - Daily Summary and Discuss Next Day's Agenda

ESBWR Instrumentation & Controls - NRC Audit Agenda (Continued)

Friday, November 17th

0800 – GE - Setup

0845 – New Introductions

0900 to 1000 – Open Item Discussion

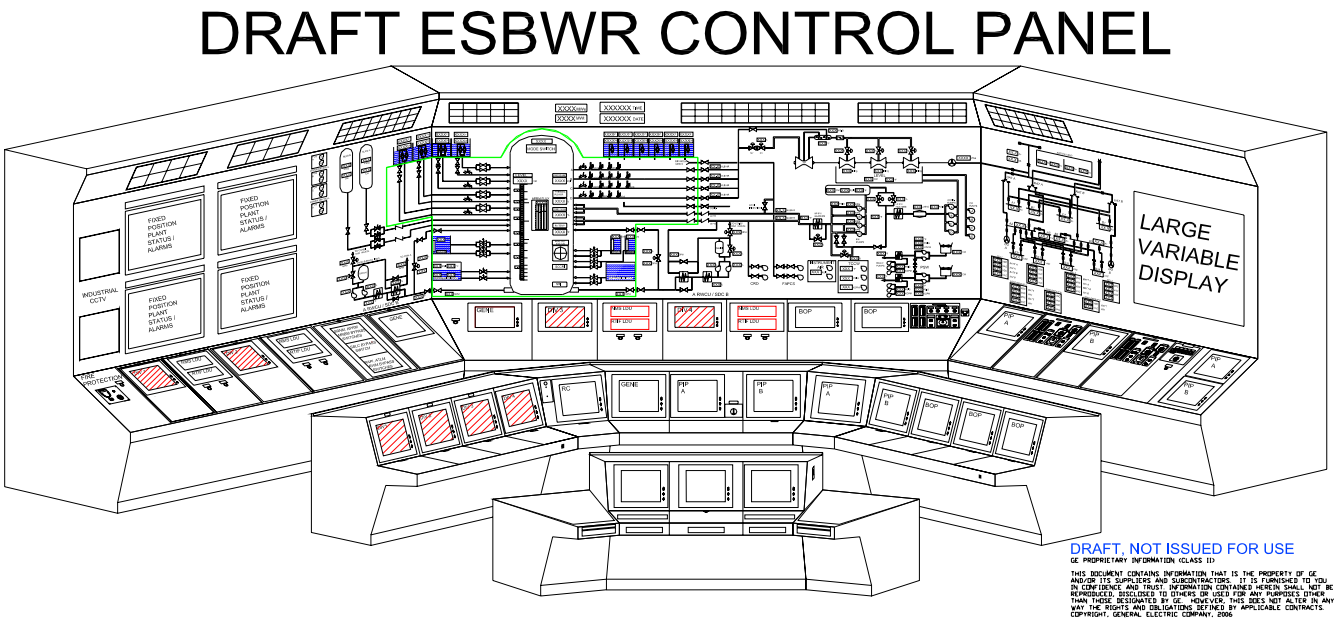
1000 to 1100 – Public Meeting – Audit Results

1100 - Exit

DCIS Equipment Location Overview and Control Room Panel Layout

Rich Miller and Ira Poppel

ESBWR Control Room Panels



ESBWR Instrumentation & Controls - NRC Audit

ESBWR Control Room

>Draft design must await HFE analysis and approval

>Design is not final but rather a “vision” to help design the DCIS that must support it

>Lungmen/K6/7 design is basis

>Draft design has good initial HFE basis

ESBWR Instrumentation & Controls - NRC Audit

ESBWR Wide Display Panel

>Provides main plant mimic

>Provides electrical system mimic

>Provides backup safety-related displays

>Provides backup plant investment protection displays

>Provides fixed alarm/annunciators

>Provides fixed plant status/alarm displays

>Provides for Fire Protection system operation

>Provides large variable display (LVD)

- Any nonsafety VDU format can be repeated on the LVD

ESBWR Wide Display Panel (continued)

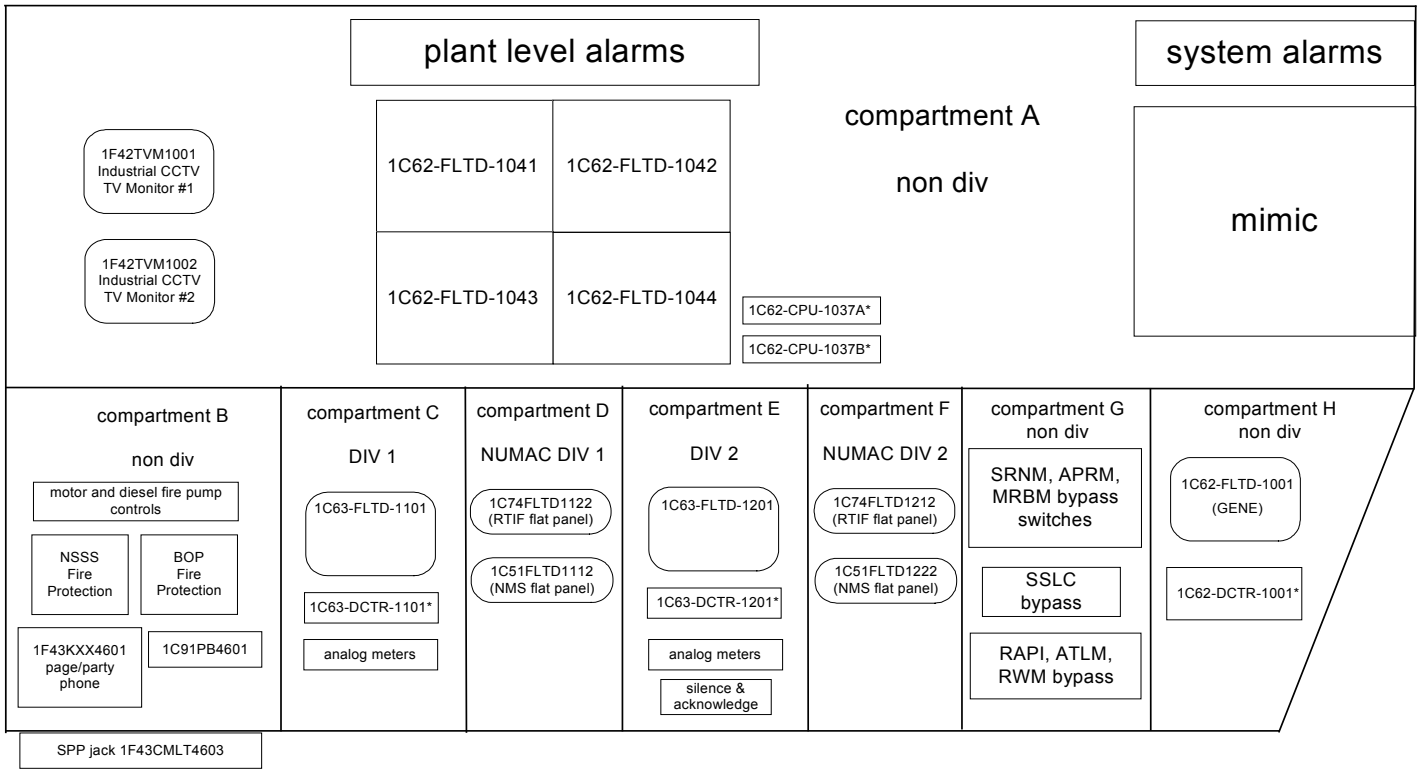
>Provides location for infrequent operations

- APRM/LPRM calibration
- RTIF/NMS surveillance
- ECCS surveillance
- Manual main generator synchronization
- Manual diesel generator synchronization and testing
- HVAC setup and adjustment
- Fire protection system monitoring

ESBWR Instrumentation & Controls - NRC Audit

ESBWR Benchboards

WIDE DISPLAY PANEL
1H11PL1703 COMPARTMENTS

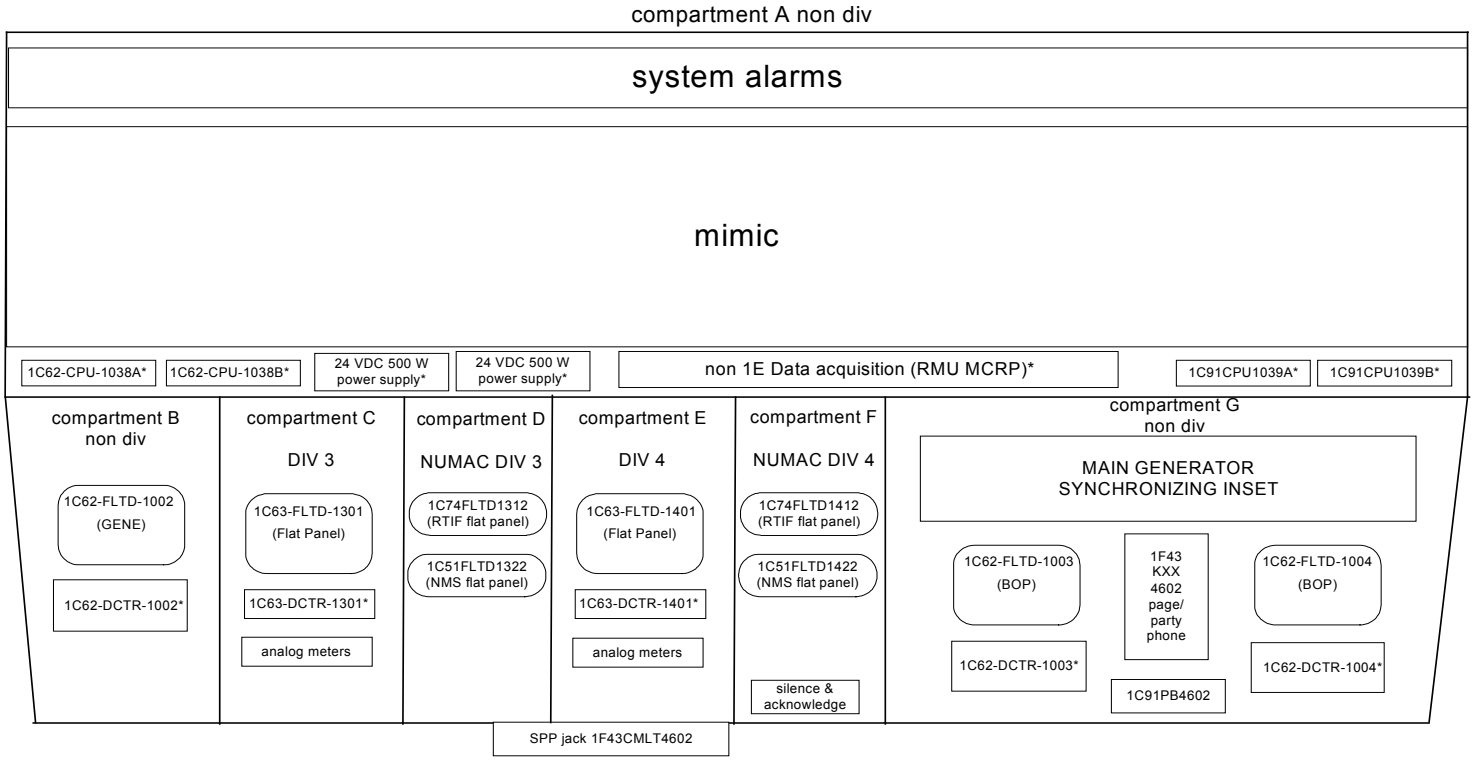


* inside cabinet

ESBWR Instrumentation & Controls - NRC Audit

ESBWR Benchboards (continued)

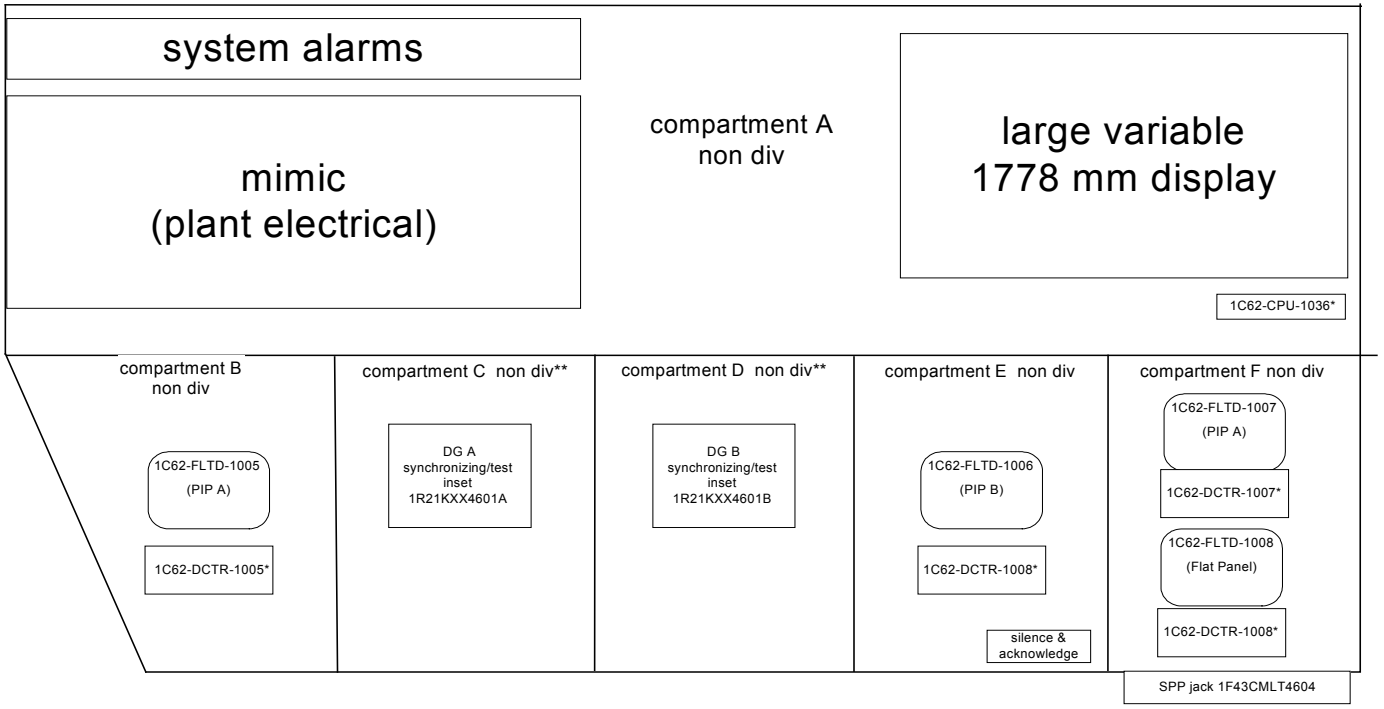
WIDE DISPLAY PANEL
1H11PL1704 COMPARTMENTS



* inside cabinet

ESBWR Benchboards (continued)

WIDE DISPLAY PANEL
1H11PL1705 COMPARTMENTS



* inside cabinet

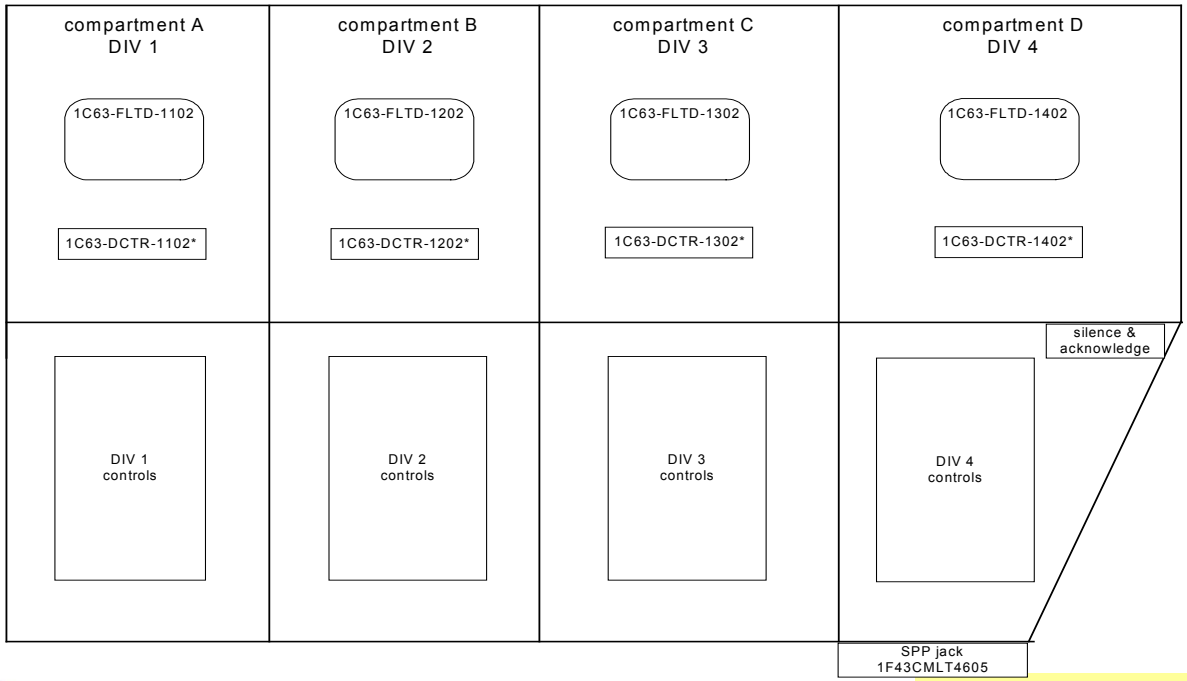
** fire barrier compartments

ESBWR Main Control Console

- Main safety system monitoring and control
- Main nonsafety system monitoring and control
- GENE, PIP A, PIP B and BOP displays
- Plant automation monitoring and control
- Manual and automatic control rod control
- Designed for one operator but can accommodate two operators

ESBWR Benchboards (continued)

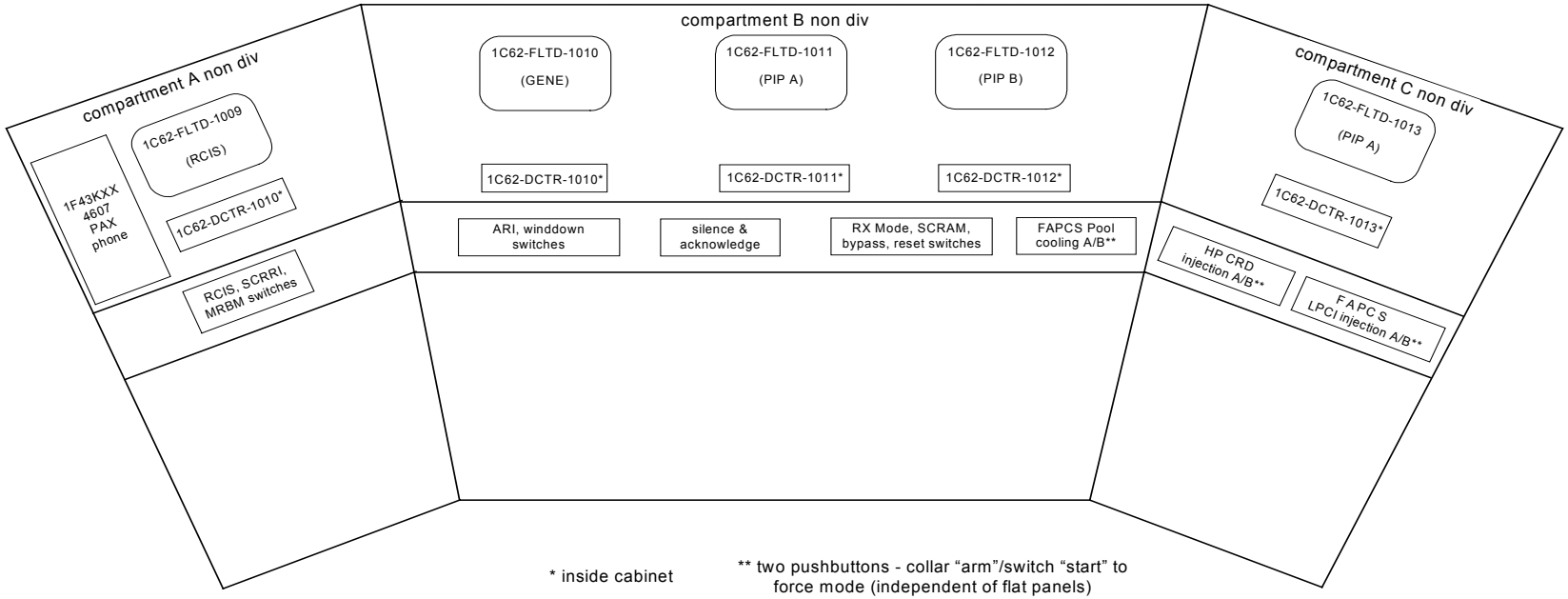
MAIN CONTROL CONSOLE
1H11PL1700 COMPARTMENTS



* inside cabinet

ESBWR Benchboards (continued)

MAIN CONTROL CONSOLE
1H11PL1701 COMPARTMENTS

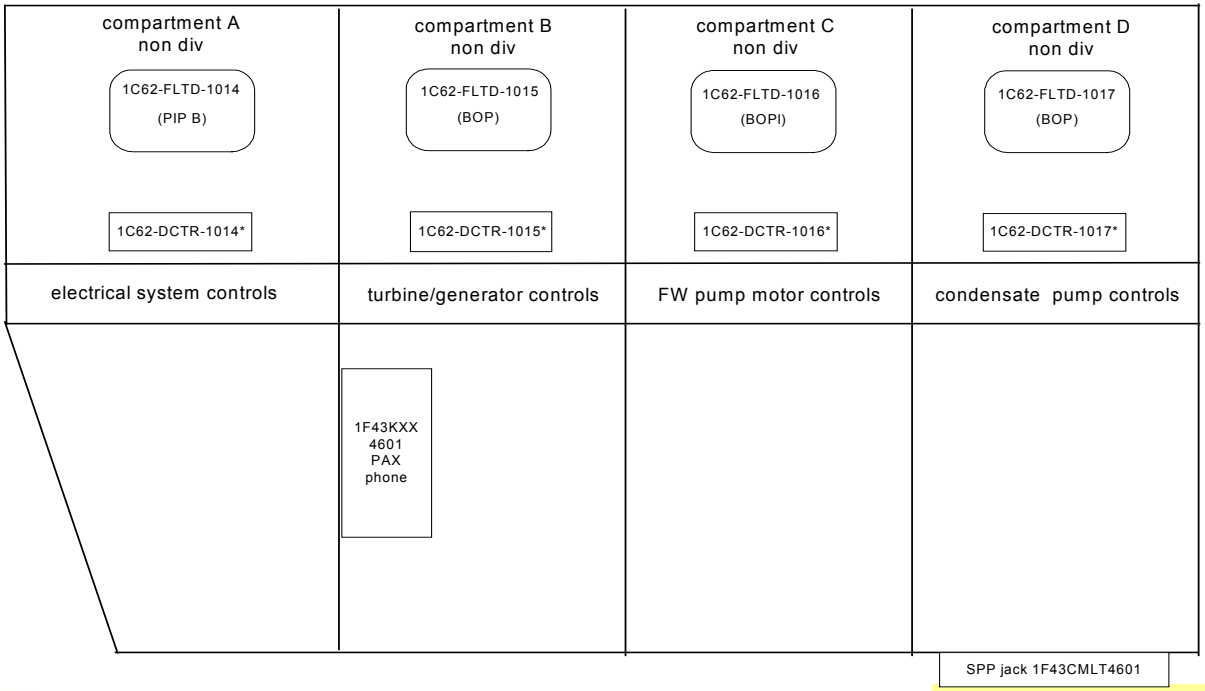


* inside cabinet

** two pushbuttons - collar "arm"/switch "start" to force mode (independent of flat panels)

ESBWR Benchboards (continued)

MAIN CONTROL CONSOLE
1H11PL1702 COMPARTMENTS



* inside cabinet

ESBWR DCIS Locations

- Many DCIS cabinets have been located to specific rooms in the various buildings
  - Rooms and cabinets must have compatible environmental ratings

ESBWR Safety/Nonsafety DCIS Rooms

ESBWR DCIS CABINET LIST

(PIP A and BOP NE-DCIS) CB room 3301

1C62-PL-0301 DPS (TMR) (GENE)
1C62-PL-0302 SBPC (TMR) (BOP)
1C62-PL-0303 FWC (TMR) (BOP)
1C62-PL-0304 turb/gen control (TMR) (BOP)
1C62-PL-0305 PAS (TMR) (BOP)
1C62-PL-0306 turb auxiliary (BOP)(MK6e)
1C62-PL-0307 generator auxiliary (BOP)(MK6e)
1C62-PL-0308 elect system/main/UAT (BOP)(MK6e)

1C62-PL-0321A FAPCS A (PIPA)(MK6e)
1C62-PL-0322A RWCU/SDC A, CRD A (PIPA)(MK6e)
1C62-PL-0323A elect syst A, diesel gen A (PIPA)(MK6e)
1C62-PL-0324A EB/TB HVAC A, inst air A (PIPA)(MK6e)
1C62-PL-0325A RB, CB, FB HVAC A (PIPA)(MK6e)
1C62-PL-0326A RCW, chillers, drywell cooling A (PIPA)(MK6e)
1C62-PL-0327A PSW, PSW clg twrs, PSW PH HVAC A (PIPA)(MK6e)
1C62-PL-0328A PIP A local RMU (PIPA)(MK6e)

1C62-PL-0331A ATLM A, RWM A, SIU A (GENE)
1C62-PL-0332A MRBM A, PAS MVD A, DPS MVD A, AFIP (GENE)
1C62-PL-0333A SPDS A (PCS)
1C62-PL-0334A alarm/annunciator A (PCS)
1C62-PL-0335A core thermal power/flow A (PCS)
1C62-PL-0336A fiber optic interface panel
1C62-PL-0337A ATLM/MRBM/RWM/SIU/3D monicore/RAPI gateway

1C62-PL-0341A RTIF/NMS div 1-3 gateways (GENE)
1C62-PL-0342A ECCS/ERF div 1-3 gateways (GENE)
1C62-PL-0343A BIMAC gateway A (PIPA)
1C62-PL-0344 mimic gateway (PCS)
1C62-PL-0345 fire protection panel gateway (PCS)
1C62-PL-0347 offgas, cond polish, cond stor/xfer, gateway panel (BOP)

1C62-PL-0351 on line procedure monitor cabinet (PCS)
1C62-PL-0352 alarm response procedure cabinet (PCS)
1C62-PL-0353 system 1 (vib mon) server cabinet (PCS)
1C62-PL-0354A UDH/PDH workstation bridge cabinet A (PCS)

1C62-PL-0361A network switch cabinet A (PIPA)
1C62-PL-0362A network switch cabinet A (GENE/PCS)
1C62-PL-0363A network switch cabinet A (BOP)

1C62-PL-0371A historian (PCS)
1C62-PL-0371C historian (PCS)
1C62-PL-0371E historian (PCS)
1C62-PL-0372 fast TRA historian (PCS)

1C62-PL-0384 scram test panel (GENE)

1C62-PL-0391A electrical protective relaying cabinet A
1C62-PL-0391C electrical protective relaying cabinet C
1C62-PL-0392 clock cabinet
1C62-PL-0393 firewall panel (PCS)
1C62-PL-0394 fire protection panel

(PIP B and BOP NE-DCIS) CB room 3302

1C62-PL-0309 elect system/RAT system (BOP)(MK6e)
1C62-PL-0310 main condenser (BOP)(MK6e)
1C62-PL-0311 normal heat sink (BOP)(MK6e)
1C62-PL-0312 cond/fw/drains (BOP)(MK6e)
1C62-PL-0313 closed cooling water (BOP)(MK6e)
1C62-PL-0314 serv air/cont inert/floor drain (BOP)(MK6e)
1C62-PL-0315 misc HVAC (BOP)(MK6e)

1C62-PL-0321B FAPCS B (PIPB)(MK6e)
1C62-PL-0322B RWCU/SDC B, CRD B (PIPB)(MK6e)
1C62-PL-0323B elect syst B, diesel gen B (PIPB)(MK6e)
1C62-PL-0324B EB/TB HVAC B, inst air B (PIPB)(MK6e)
1C62-PL-0325B RB, CB, FB HVAC B (PIPB)(MK6e)
1C62-PL-0326B RCW, chillers, drywell cooling B (PIPB)(MK6e)
1C62-PL-0327B PSW, PSW clg twrs, PSW PH HVAC B (PIPB)(MK6e)
1C62-PL-0328B PIP B local RMU (PIPB)(MK6e)

1C62-PL-0331B ATLM B, RWM B, SIU B (GENE)
1C62-PL-0332B MRBM B, PAS MVD B, DPS MVD B (GENE)
1C62-PL-0333B SPDS B (PCS)
1C62-PL-0334B alarm/annunciator B (PCS)
1C62-PL-0335B core thermal power/flow B (PCS)
1C62-PL-0336B fiber optic interface panel
1C62-PL-0337B ATLM/MRBM/RWM/SIU/3D monicore/RAPI gateway

1C62-PL-0341B RTIF/NMS div 2-4 gateways (GENE)
1C62-PL-0342B ECCS/ERF div 2-4 gateways (GENE)
1C62-PL-0343B BIMAC gateway B (PIPB)
1C62-PL-0346 met, area rad, env mon, seismic mon gateway (PCS)
1C62-PL-0348 radwaste gateway panel (BOP)
1C62-PL-0349 makeup water, aux boiler gateway panel (BOP)

1C62-PL-0354B UDH/PDH workstation bridge cabinet B (PCS)

1C62-PL-0361B network switch cabinet B (PIPB)
1C62-PL-0362B network switch cabinet B (GENE/PCS)
1C62-PL-0363B network switch cabinet B (BOP)

1C62-PL-0371B historian (PCS)
1C62-PL-0371D historian (PCS)
1C62-PL-0371F historian (PCS)
1C62-PL-0373 SOE historian (PCS)

1C62-PL-0381A RCIS RAPI A (GENE)
1C62-PL-0381B RCIS RAPI B (GENE)
1C62-PL-0382 scram timing analysis panel
1C62-PL-0383 emergency rod insertion panel

1C62-PL-0391B electrical protective relaying cabinet B
1C62-PL-0395 area radiation monitoring panel
1C62-PL-0396 meteorological panel
1C62-PL-0397 seismic monitoring panel

CB room 3110
(div 1 E-DCIS)

1C63-PL-1301 NMS
1C63-PL-1302 RTIF
1C63-PL-1303 PRM
1C63-PL-1305 SSLC
1C63-PL-1306 test/gateway
1C63-PL-1307 ECCS RMU

CB room 3120
(div 2 E-DCIS)

1C63-PL-2301 NMS
1C63-PL-2302 RTIF
1C63-PL-2303 PRM
1C63-PL-2305 SSLC
1C63-PL-2306 test/gateway
1C63-PL-2307 ECCS RMU

CB room 3130
(div 3 E-DCIS)

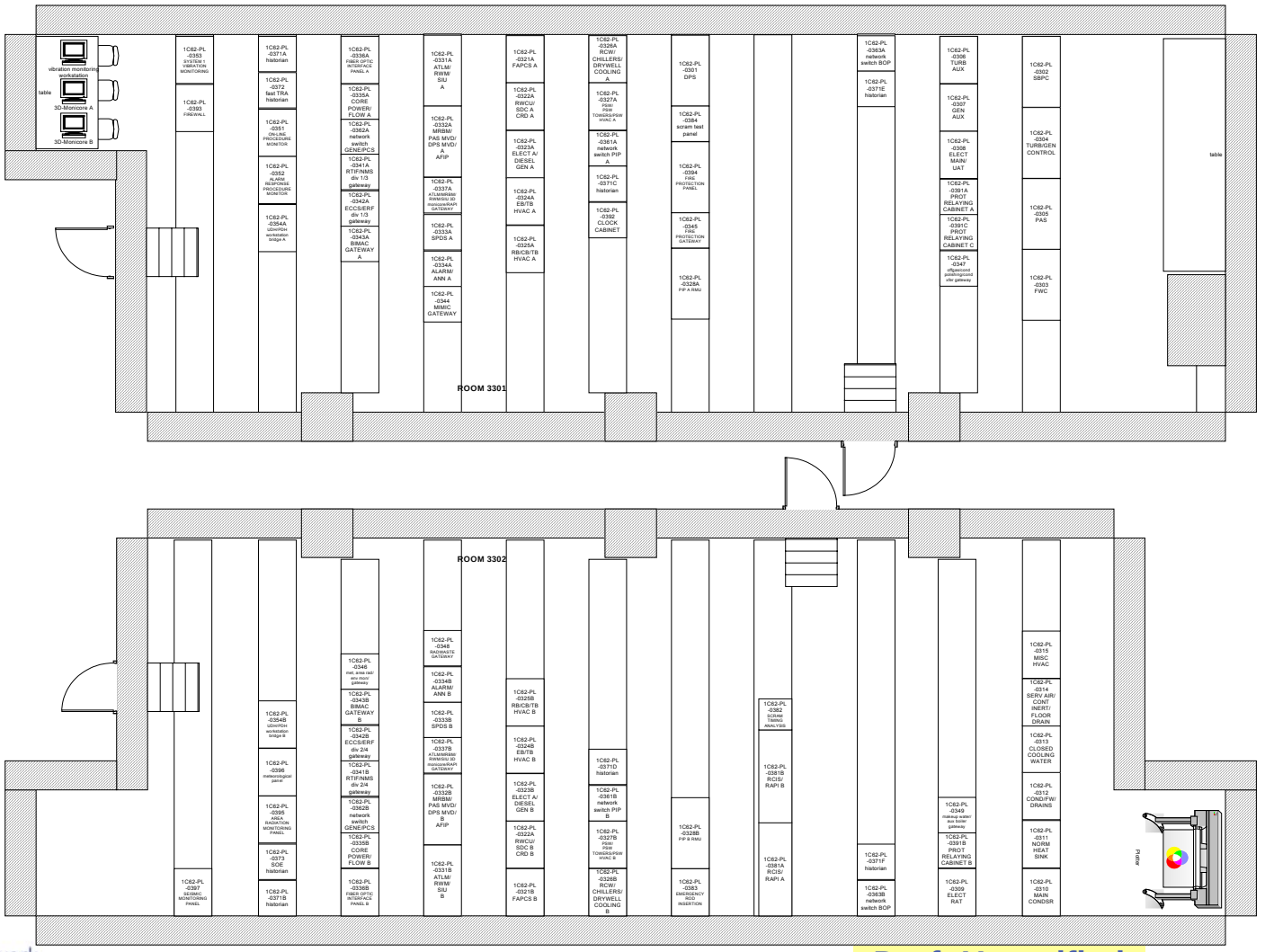
1C63-PL-3301 NMS
1C63-PL-3302 RTIF
1C63-PL-3303 PRM
1C63-PL-3305 SSLC
1C63-PL-3306 test/gateway
1C63-PL-3307 ECCS RMU

CB room 3140
(div 4 E-DCIS)

1C63-PL-4301 NMS
1C63-PL-4302 RTIF
1C63-PL-4303 PRM
1C63-PL-4305 SSLC
1C63-PL-4306 test/gateway
1C63-PL-4307 ECCS RMU

ESBWR Instrumentation & Controls - NRC Audit

ESBWR Nonsafety DCIS Rooms

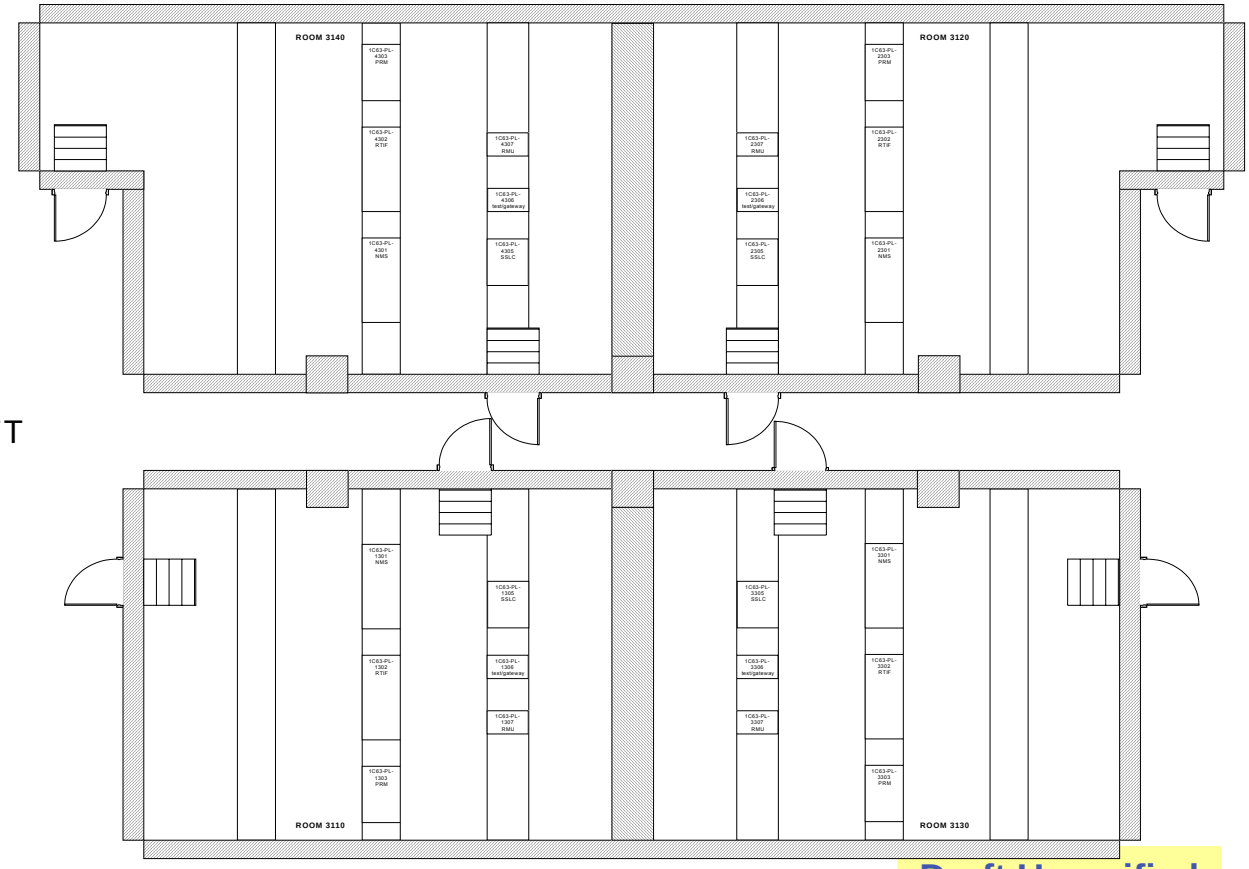


DRAFT

ESBWR Instrumentation & Controls - NRC Audit

ESBWR Safety DCIS Rooms

CONTROL BUILDING ROOM 3110/3120/3130/3140



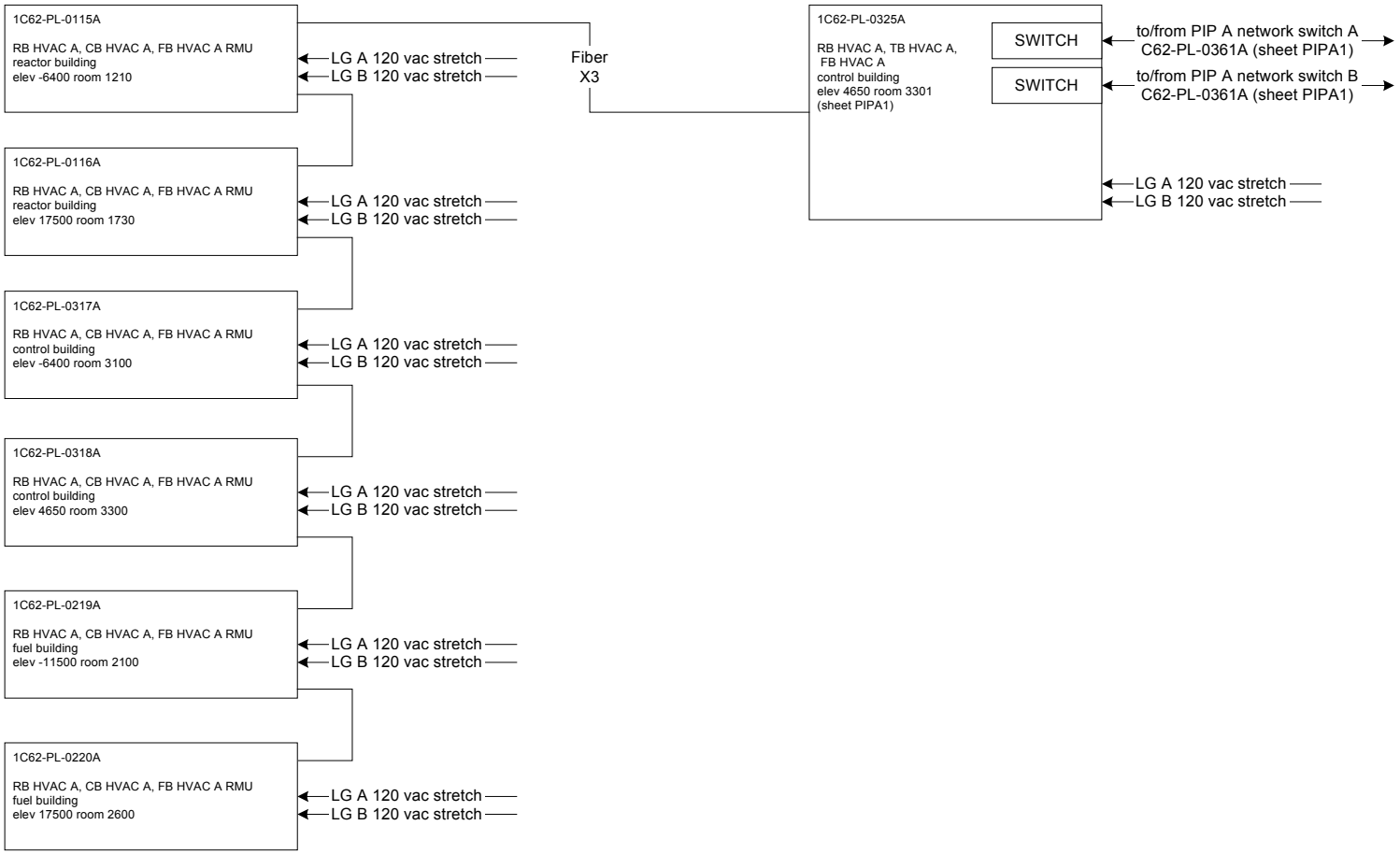
DRAFT

imagination at work

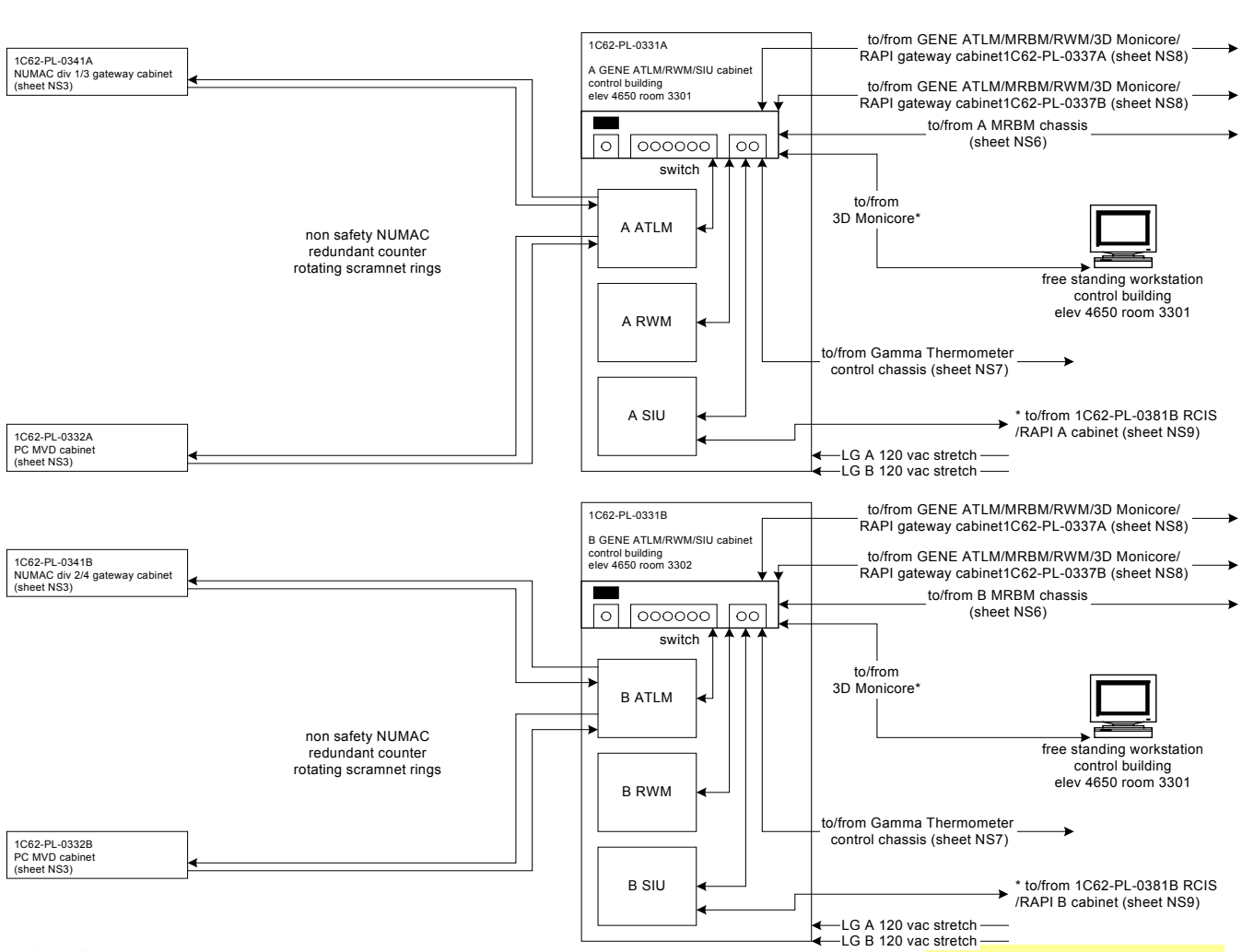
Draft Unverified

ESBWR PIP A Room Location Example

ESBWR DCIS - PIP A NETWORK - RB HVAC A, CB HVAC A, FB HVAC A

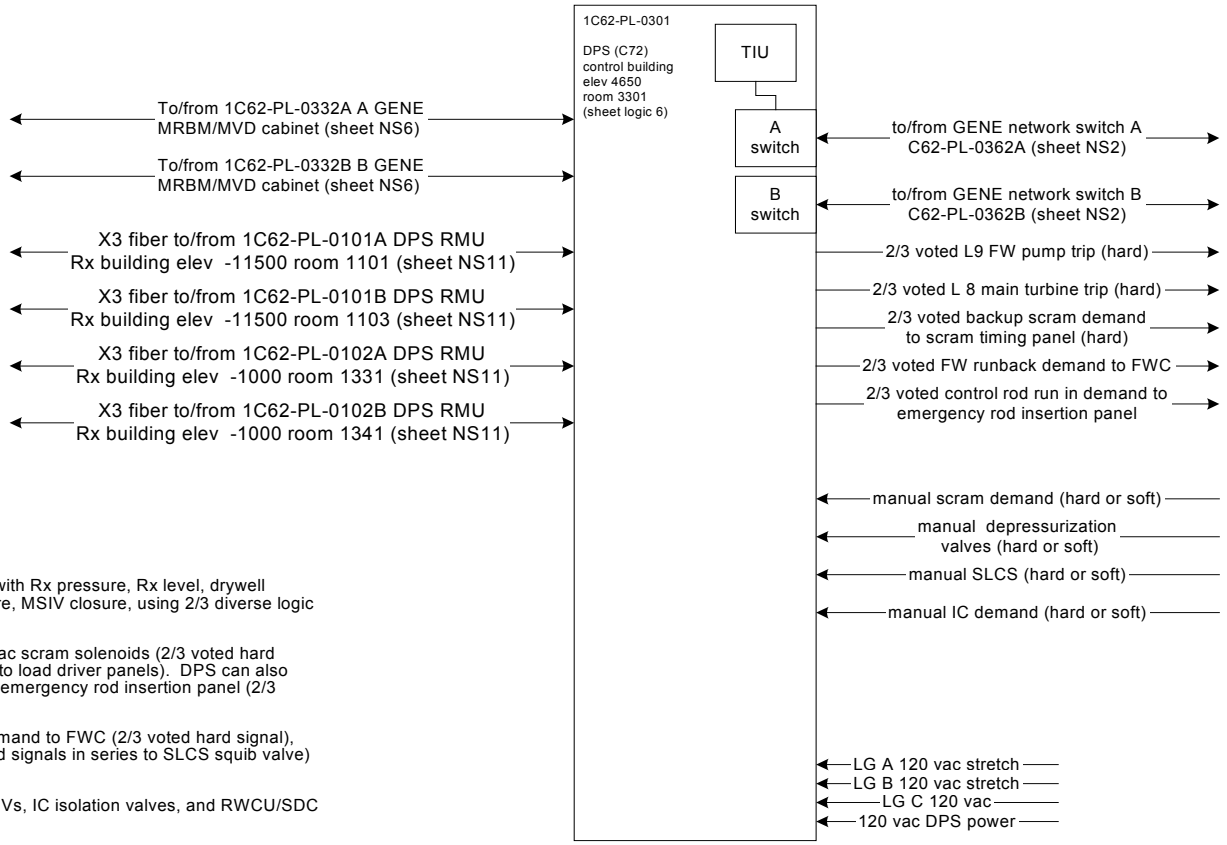


ESBWR GENE Room Location Example



ESBWR GENE Room Location Example

ESBWR DCIS - DIVERSE PROTECTION SYSTEM (C72)



C72/DPS TMR uses “fail as is” logic

DPS provides backup scram function with Rx pressure, Rx level, drywell pressure, suppression pool temperature, MSIV closure, using 2/3 diverse logic and 2/4 non safety sensors.

DPS scram opens return side of 120 vac scram solenoids (2/3 voted hard signal to scram timing panel, fiber link to load driver panels). DPS can also issue control rod run in demand to the emergency rod insertion panel (2/3 voted hard signal).

ATWS provides feedwater runback demand to FWC (2/3 voted hard signal), SLCS (two 2/3 voted fiber isolated hard signals in series to SLCS squib valve) for failure to scram.

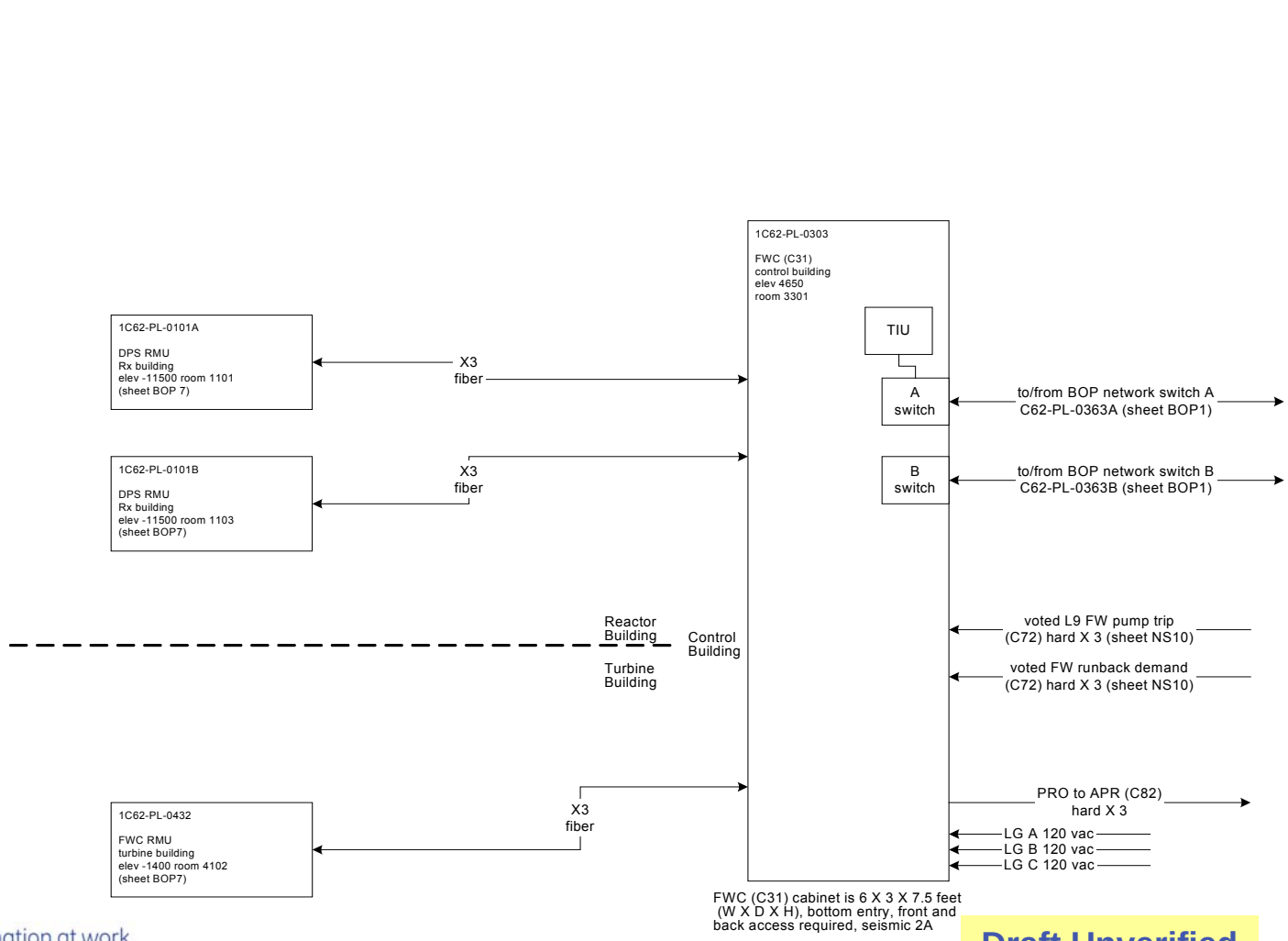
DPS provides diverse actuation to MSIVs, IC isolation valves, and RWCU/SDC isolation valves.

DPS provides diverse actuation to depressurization valves, DPV valves and GDCS valves (two 2/3 voted fiber isolated hard signals in series).

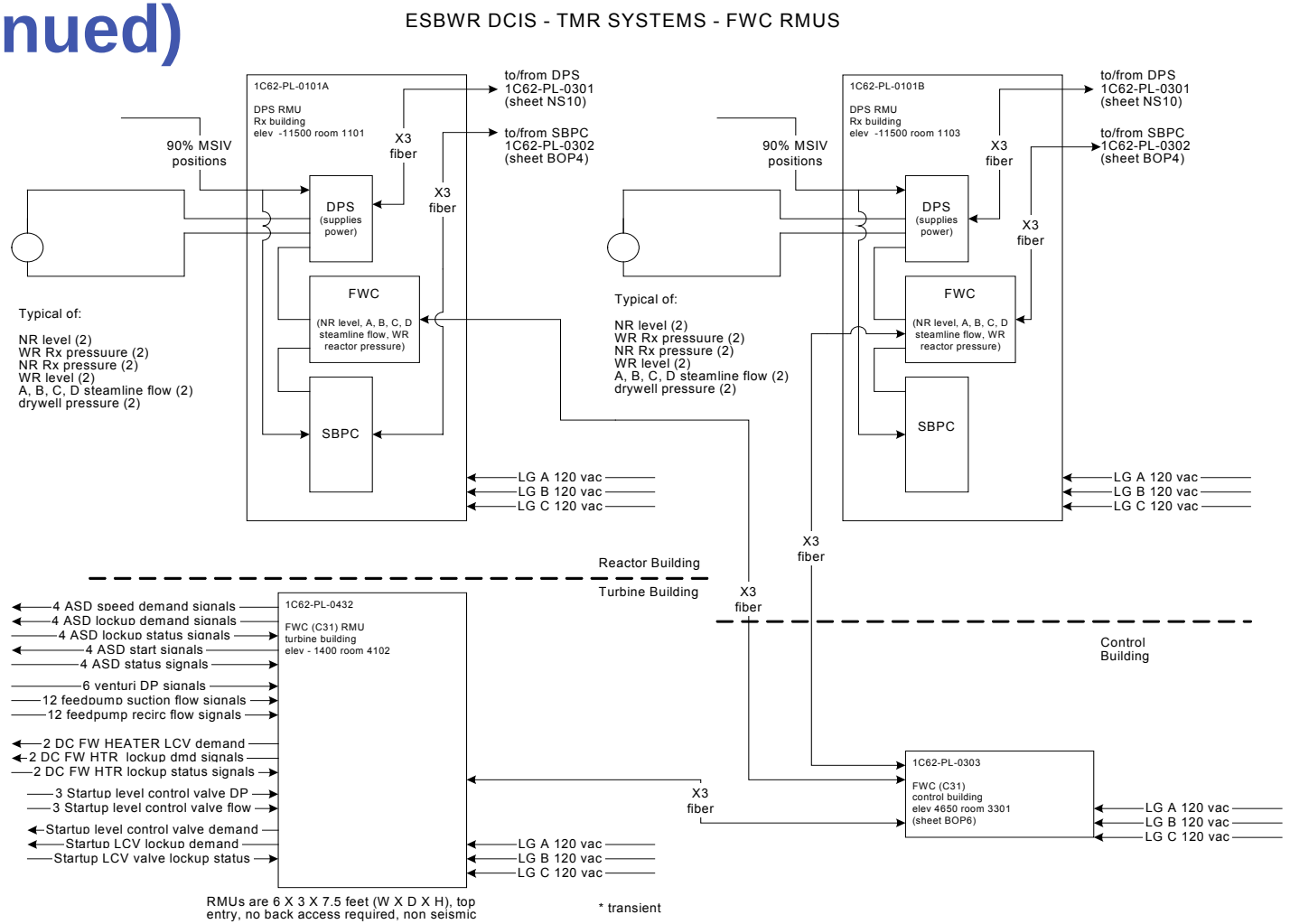
DPS provides level 8 turbine trip to N32 and level 9 feedwater breaker trip (2/3 voted hard signal

DPS cabinet is 6 X 3 X 7.5 feet (W X D X H), bottom entry, front and back access required, seismic 2A

ESBWR BOP Room Location Example



ESBWR BOP Room Location Example (continued)



ESBWR Organization of DCIS

ESBWR Instrumentation & Controls - NRC Audit

ESBWR DCIS Configuration Design

- >Software and hardware design and QA requirements discussed elsewhere
- >Regulatory requirements are known
- >Reliability requirements are known
- >Many installations provide non nuclear DCIS design guidance
- >MMIS and HFE “unknown”

ESBWR DCIS Design - Regulatory

- >Safety DCIS
  - Power, independence, isolation, N-1 (N-2)
- >Diversity
  - ECCS/RPS/DPS/nonsafety DCIS hardware/software platforms
- >1.97 R4 (later)
- >Interlocks (later)

ESBWR Instrumentation & Controls - NRC Audit

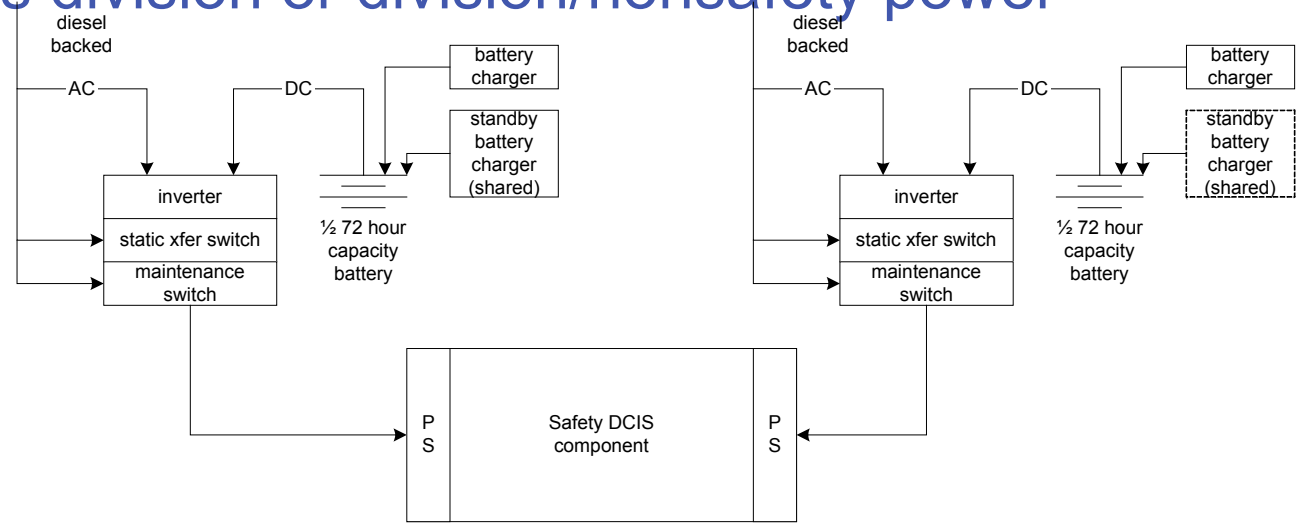
Safety DCIS Power

>All safety-related DCIS is redundantly powered

- Power component, power supply, power feed problems diagnosed

>All functions available within a division with single power failure

>No cross division or division/nonsafety power

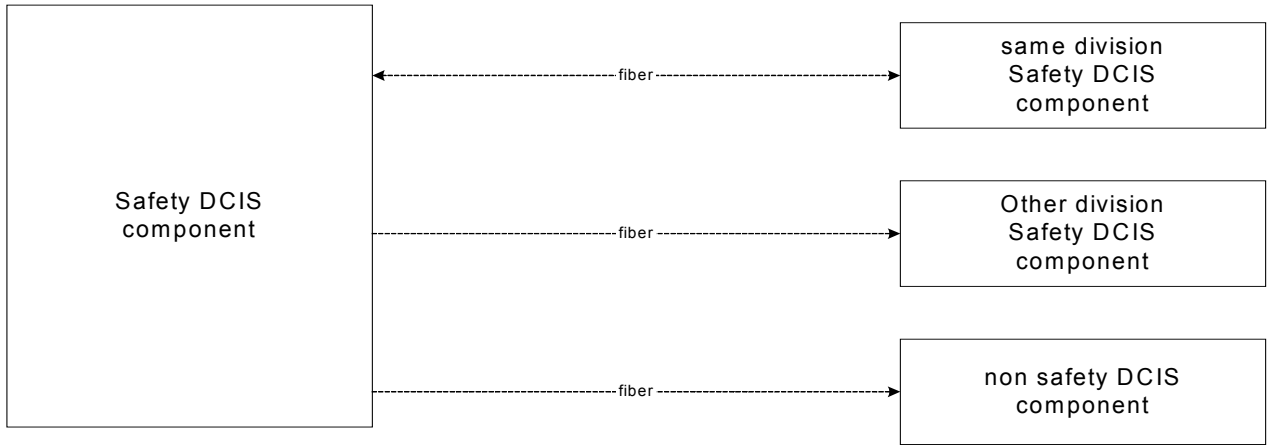


Safety DCIS Isolation

>All safety to nonsafety communication is fiber
- No copper communication

>All safety to safety communication is fiber
- No copper communication

>Most communication within a division is fiber
- Long distance, EMI, ground loop concerns eliminated



ESBWR Instrumentation & Controls - NRC Audit

Safety DCIS – N-1 (N-2)

>As with all current safety system DCIS design the ESBWR DCIS is designed to accept a single failure and not inadvertently actuate nor prevent actuation of a safety system.

>Unlike most existing BWR safety systems the ESBWR DCIS is additionally designed to have a division out of service in bypass, accept a single failure and not inadvertently actuate nor prevent actuation of a safety system

ESBWR Instrumentation & Controls - NRC Audit

ESBWR Diversity

>ESBWR reactor protection system uses a different hardware/software platform and sensors than nonsafety DCIS, ECCS, BIMAC, and DPS.

>ESBWR ECCS uses a different hardware/software platform and sensors than either reactor protection, nonsafety DCIS, BIMAC, and DPS.

>ESBWR ATWS/SLCS uses a different hardware platform than the reactor protection system and BIMAC

>DPS uses a different hardware/software platform than ECCS, reactor protection system or BIMAC

>BIMAC (severe accident) uses a different hardware/software platform than RPS, ECCS, DPS or nonsafety DCIS

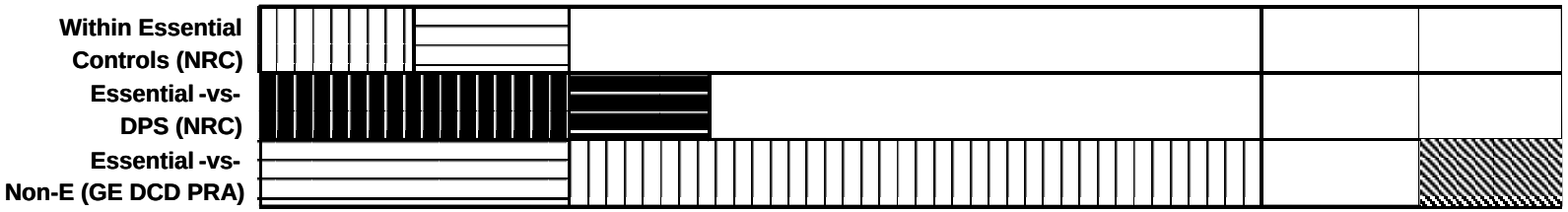
>Either safety or nonsafety DCIS can scram the plant and bring it to cold shutdown

ESBWR Instrumentation & Controls - NRC Audit

DCIS Platform Families

Safety	Safety-Related		Nonsafety-Related				
Category	E - DCIS		NE - DCIS				
System Families	RPS NMS	ECCS ESF	DPS	NUCLEAR CONTROL SYSTEMS	Balance of any NE-DCIS Systems	PCF	Severe Accident
Architecture	NUMAC	Redundant	Triple Redundant	Triple Redundant	Triple/Dual Redundant	Workstations	PLCs
Systems/ Subsystems	RPS LD&IS (MSIV) NMS ATWS/SLCS	ICS SRV/DPV GDCS SLCS LD&IS (Non-MSIV)	ECCS Backup	FWC, PAS (Automation) SB&PC, T/G Control	PIP A, PIP B Balance Of Plant (Power Generation)	HMI, Alarms, SPDF, Historian, 3D Monicore	Deluge System (GDCS Subsystem)

Diversity Strategy



Nonsafety DCIS Design Bases

>Unlike the safety DCIS, the nonsafety DCIS configuration has few formal design bases

>GE has established the following design bases

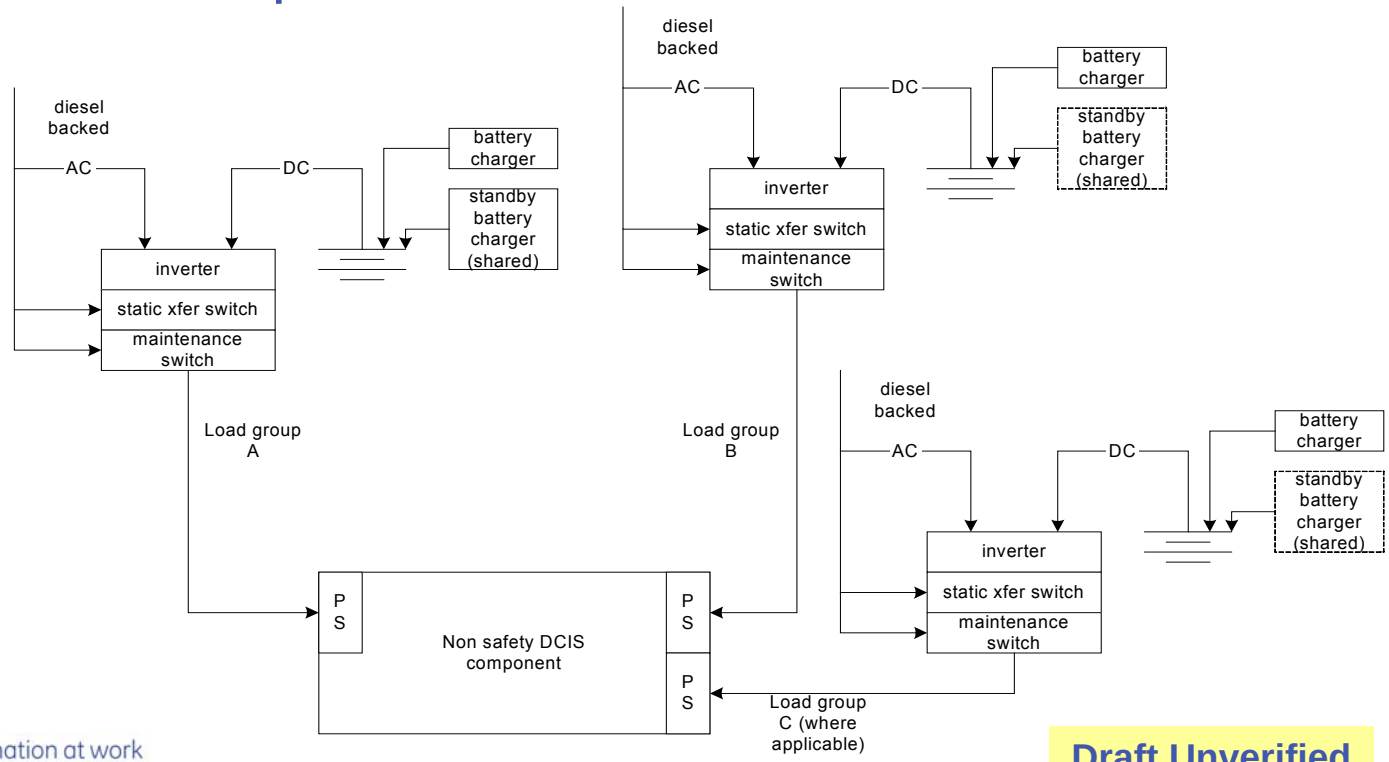
- Diversity where required from RPS/ECCS
- Single failure proof for power generation
  - Redundant power
  - Redundant communications
- Triply redundant where required
- Segmentation
  - PIP A, PIP B, BOP, GENE, PCS

ESBWR Instrumentation & Controls - NRC Audit

Nonsafety DCIS Power

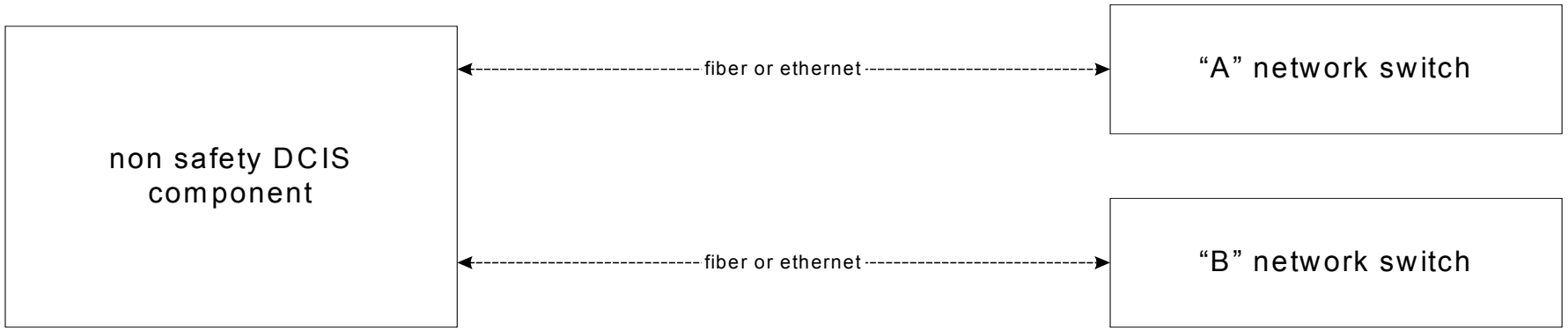
>Nonsafety DCIS is supported by three uninterruptible power systems

>Nonsafety DCIS cabinets have two (or three for TMR) power feeds and can operate on either without loss of function



Nonsafety DCIS Communications

- >Nonsafety DCIS communications (network and important data links) are redundant
- >Most safety-related inter and safety/nonsafety communications are redundant
- >No single communications failure will affect safety or nonsafety power generation functions



Most Important Safety and Nonsafety DCIS Design Bases

E-DCIS and NE-DCIS components and configuration must be designed to support presently undefined requirements

MMIS, HFE, 1.97 R4, future logic

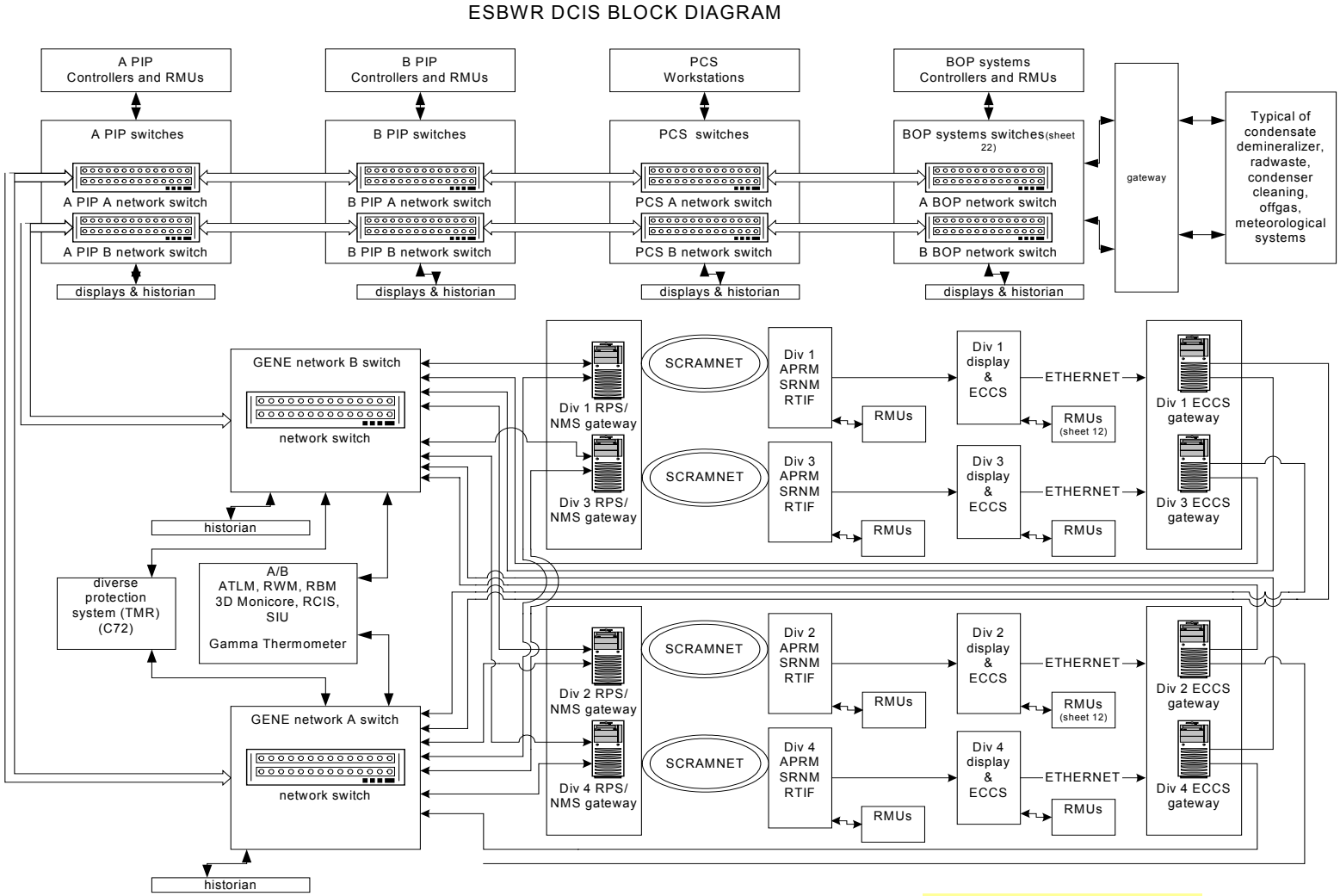
ESBWR Organization of DCIS

ESBWR organized around:

- > Safety DCIS
- > Nonsafety DCIS
  - – Network switches
    - GENE network (contains gateways and DPS)
    - PIP A network (contains RTNSS)
    - PIP B network (contains RTNSS)
    - PCS network (contains alarms, recording)
    - BOP network (power generation)

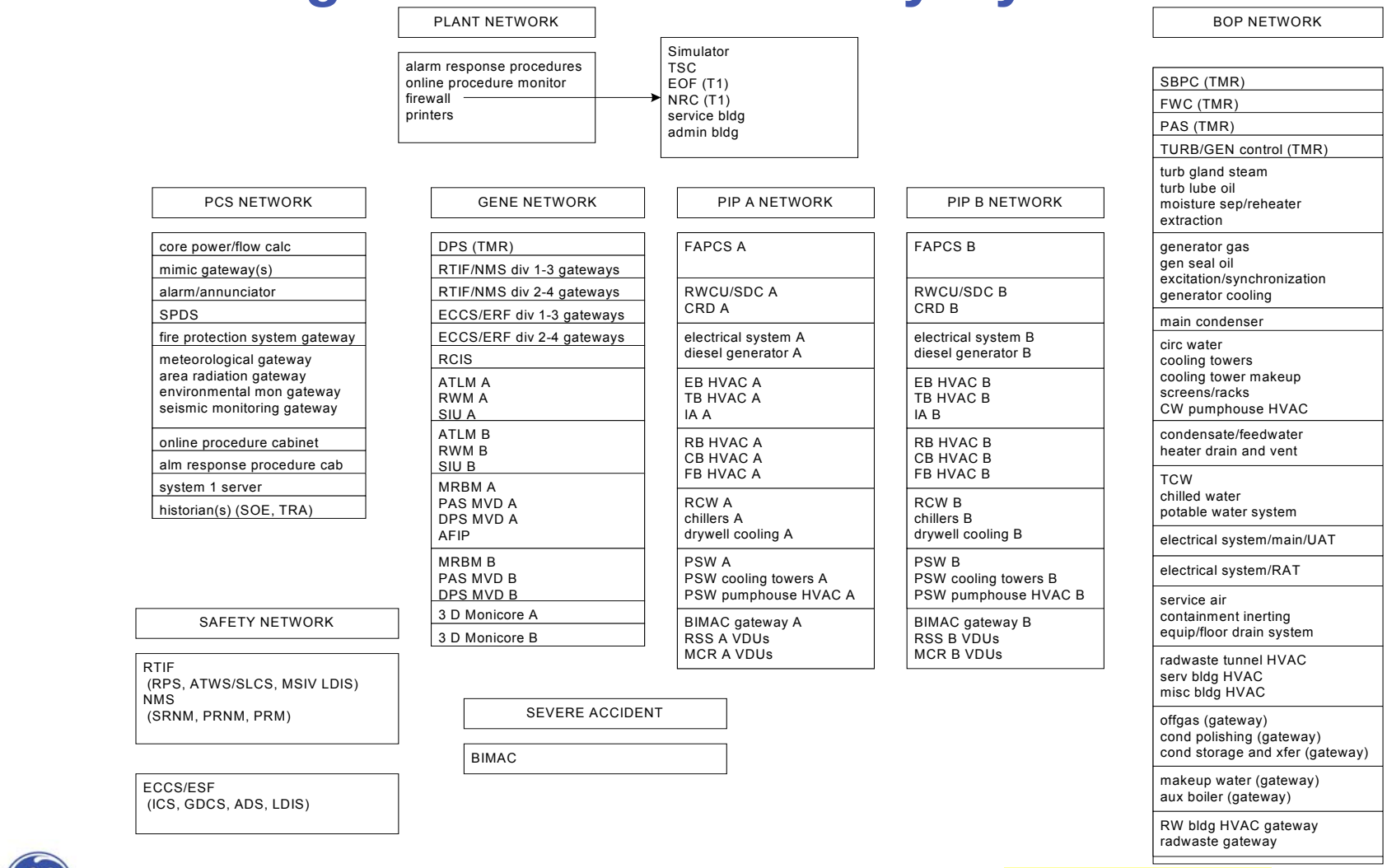
ESBWR Instrumentation & Controls - NRC Audit

ESBWR Organization of DCIS



ESBWR Instrumentation & Controls - NRC Audit

ESBWR Organization of DCIS by System



NE-DCIS (Nonsafety-related DCIS) and Displays

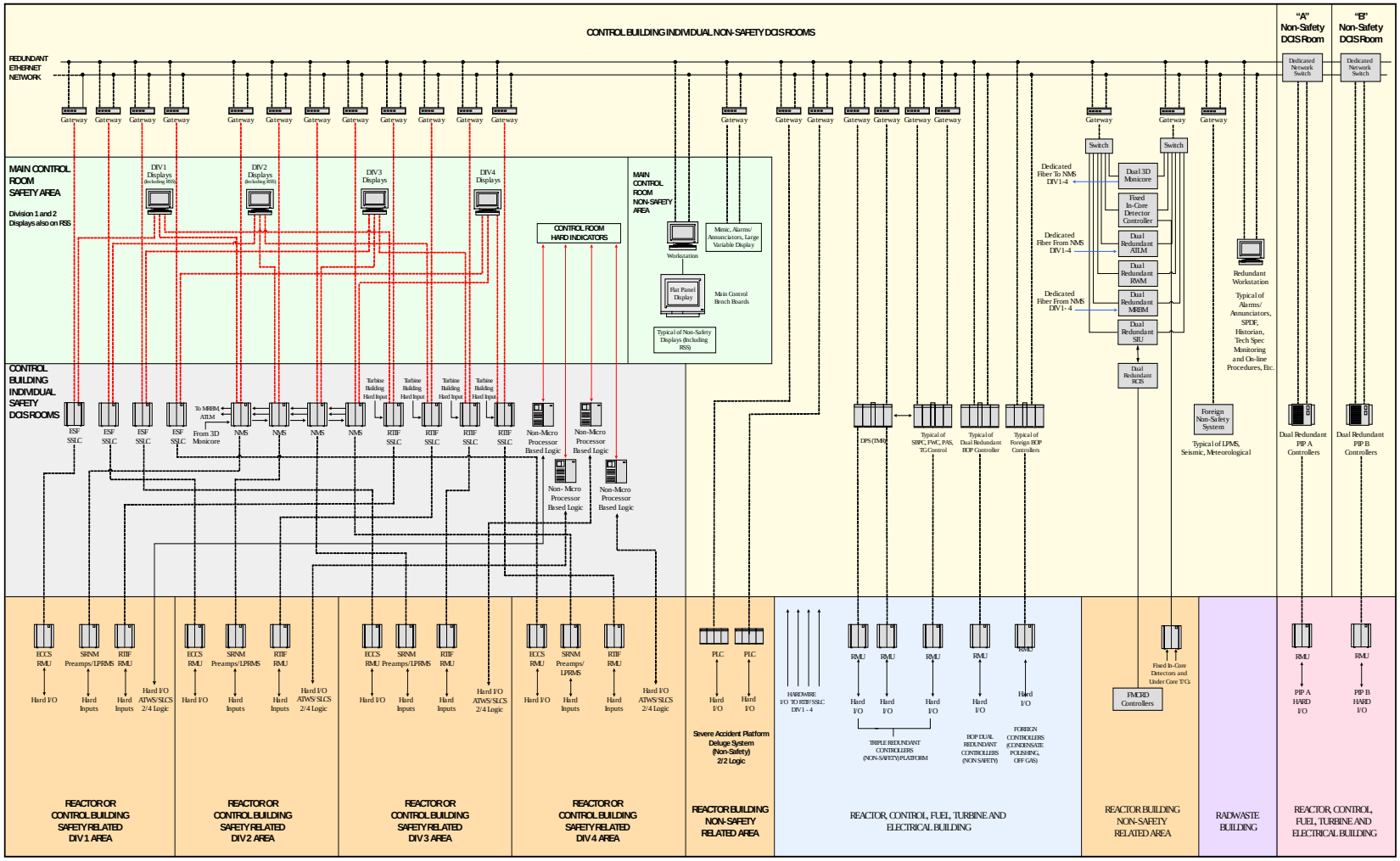
ESBWR Network Diagram

"Traditional" network diagram does not adequately convey the actual ESBWR DCIS

ESBWR Instrumentation & Controls - NRC Audit

GE imagination at work

ESBWR NETWORK DIAGRAM (PROPOSED)



ESBWR Nonsafety Networks

Before the adequacy of the DCIS design configuration can be determined, it is important to understand how all of the parts of the ESBWR networks operate.

ESBWR Instrumentation & Controls - NRC Audit

ESBWR Network Loading

Many and varied time delays through system

Concern is that data will be lost

- > Most importantly, operator control inputs will be delayed/ignored
- > Monitoring of plant processes will be corrupted because of time delays
- > Data will not be recorded for effective post event analysis
- > Alarms will not be received

ESBWR Network Loading (continued)

>Concern is that a transient condition (i.e. a “data storm”) can somehow overload the network and cause loss of recorded (historian, SOE/TRA) or alarm data, slow displays or unresponsiveness to operator commands

>“Overloading the network” must be understood as almost meaningless since the switches break “the network” into 100’s of network segments which must be addressed individually

>The question becomes:

- “What does a transient do to the individual network segments?”

or

- “Can any kind of data traffic overload any network segment”

ESBWR Network Loading (continued)

Network loading is minimized by:

- Instead of one large application network, network switches are used to divide it into segments
  - Network switches reduce collision probability by removing/limiting traffic
  - Nodes that generally talk only to each other are confined to one segment and their traffic will not add to the traffic on another segment
  - However a switch will “pass through” messages intended for another segment
- Higher ethernet speeds dramatically reduce collision probability
  - For example a 1 gbit network has a message (packet) on the bus only one tenth as long as a 100 mbit network
- Assigning nodes to switches such that most of their traffic was with each other
  - minimizes uplink traffic
  - minimizes traffic in other switches

ESBWR Network Loading (continued)

Using “reporting by exception”

- Once communication between two nodes is initially established (for example display workstation to controller), further communication occurs only after a parameter changes “significantly”
- This technique keeps down network traffic in steady state and transient conditions
  - For example one or two reactor pressure signals are “recorded” with very small exceptions to provide high resolution, the many remaining reactor pressure signals are recorded with 7 kPag (10 psig) resolution

ESBWR Network Loading (continued)

1E Data Storm questions

"does a plant transient":

- Change the data acquisition rate for DS&S or NUMAC
- Change the 1E transmission time around the loop
- Change the data rate from NUMAC to DS&S
- Change the internal DS&S card or NUMAC processing rate
- Change the rate DS&S/NUMAC data are sent to the gateways
- Change the 1E display update rate

ESBWR Network Loading (continued)

Non 1E Data Storm questions

"Does a plant transient":

- Change the controller data acquisition rate
- Change the "worst case" display update calculations
- Change the internal SOE/TRA processing or the transmissions to the historians
- Change the gateway transmission rates
- Change the normal traffic data link transmission rates
  - Condensate polishing, meteorological, etc
- Change the gateway transmissions to the SOE/TRA high speed data collector workstation
- Change the alarm traffic to the various alarm workstations

ESBWR Network Loading (continued)

The answers to all but the last two questions is ----no-----

Since the gateways will report SOE/TRA data by exception to the historian, the traffic (packet) rate will increase

Plant alarms to the alarm/annunciator workstations will also increase

> This is a network design consideration

1E data acquisition/control deterministic “automatically”

Non 1E data acquisition/control deterministic by application

ESBWR Instrumentation & Controls - NRC Audit

DCIS "Overload Testing"

The most important consideration in avoiding collisions/overload is NOT testing but rather the initial assumptions and calculations used in setting up network configuration

By definition if test "scenario" is equal to or less than assumptions and calculations, the network will not be overloaded

Despite the above statements, FAT testing will "flood " the various network segments and observe display and control responsiveness

ESBWR Instrumentation & Controls - NRC Audit

"Transport" - Ethernet

- Ethernet is a standard network interconnection scheme
- "Nodes" or "stations" on Ethernet typically connect with a "NIC" (network interface card) card/interface
- There are no "master" nodes to control access
  - All nodes compete equally for the network bandwidth
- All Ethernet nodes have unique addresses
- Ethernet has evolved over the years from 1 mbit/sec to 1 gigabit/second
  - ESBWR uses at least 100 mbit/sec (switch ports) with 1 gigabit/second (switch) uplinks
- All nodes on the Ethernet network communicate in "packets" or "frames" which have a predefined format
- A packet can vary in length as needed to a maximum of ~ 1500 bytes (~ 12000 bits)
  - All packets identify the sending node and the receiving node

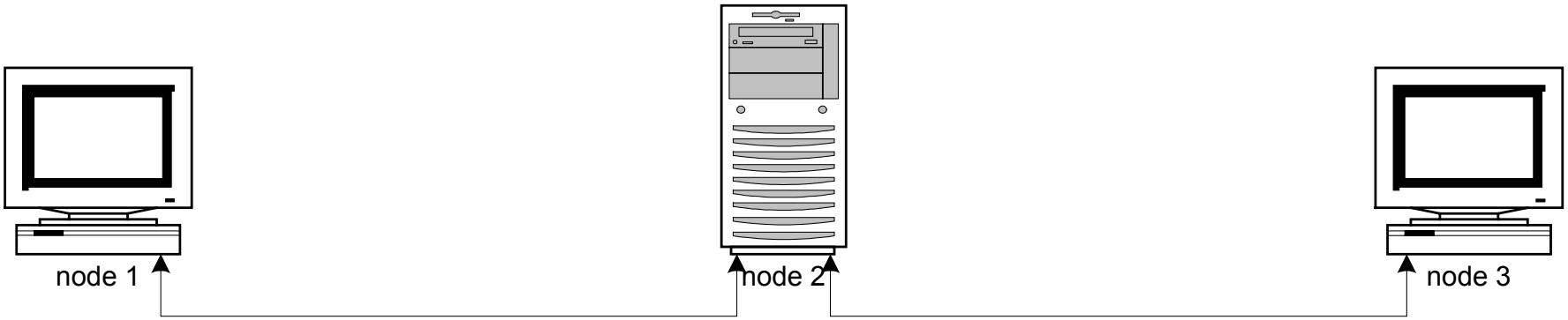
ESBWR Instrumentation & Controls - NRC Audit

"Transport" – Ethernet (continued)

- Ethernet "slot time" defined as 512 bits at 100 mbit/sec and 4096 bits for gigabit/sec networks
  - Translates to ~ 5/4 microseconds respectively
- Slot times used to ensure that all nodes on the network (those furthest apart) have time to detect a collision has occurred and inform originating node
- Slot times define round trip time/size (length) of the network
  - Slot time / speed of signal media (the network propagation speed - 20 – 30% speed of light)
  - Delays due to repeaters/switches, cable, interface cards etc
  - Typically about 200 meters (one way) without repeaters
- All messages must be at least one slot time in length (most are longer)
  - 512/8 = 64 bytes for 100 mbit/sec
  - 4096/8 = 512 bytes for 1 gigabit/sec

ESBWR Instrumentation & Controls - NRC Audit

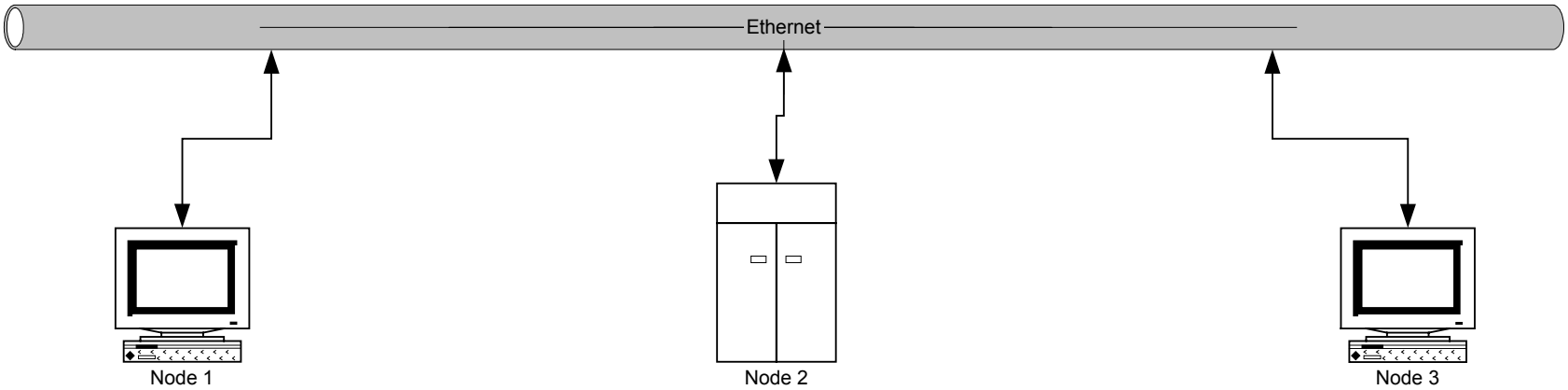
Minimal Network



Highly undesirable since nodes must individually handle all network traffic

ESBWR Instrumentation & Controls - NRC Audit

Ethernet Network



This is a “traditional” network

With no other traffic on the Ethernet, any two nodes can communicate at the network’s speed (i.e. 100 mbits/second)

If two nodes try to transmit simultaneously a “collision” occurs

Collisions are more likely at high internode communication rates and less likely as the network speed increases

Ethernet Network

Ethernet has several ways to minimize collisions and data loss

A sending node will not try to transmit if it senses data are already on the network

If two nodes nevertheless start a simultaneous transmission, a “jam” transmission sequence is started to allow all nodes on the network to become aware of the collision and then both sending nodes back off a random number of slot times and try again

- Process is “backoff”

If collisions reoccur then the random time is increased

  - After 16 tries the message is abandoned

ESBWR Network Concerns

ESBWR has 100's of nodes

> All workstations, historians, display workstations, controllers, RMUs, and gateways are nodes

Concern about "data storms" from large transients causing data loss, long operator response time, inability to control

ESBWR does not use the "traditional" network

Despite the above note that the maximum message size of 1500 bytes at 100 mbit/second requires ~ 120 microseconds to transmit

> Potential for ~1600 messages per second on 20% loaded network

Ethernet Switch

A network switch is a “switchboard” for all of the nodes connected to it’s ports

The switch “learns” the address of each node when that node is connected to a port

- > Maintains “address book” of each node/port
- > By definition also knows which addresses are not connected to it

When one node on a switch communicates to another on the same switch, the switch establishes a “dedicated “ (point to point) virtual connection

- > Allows full duplex mode of receive/transmit operation

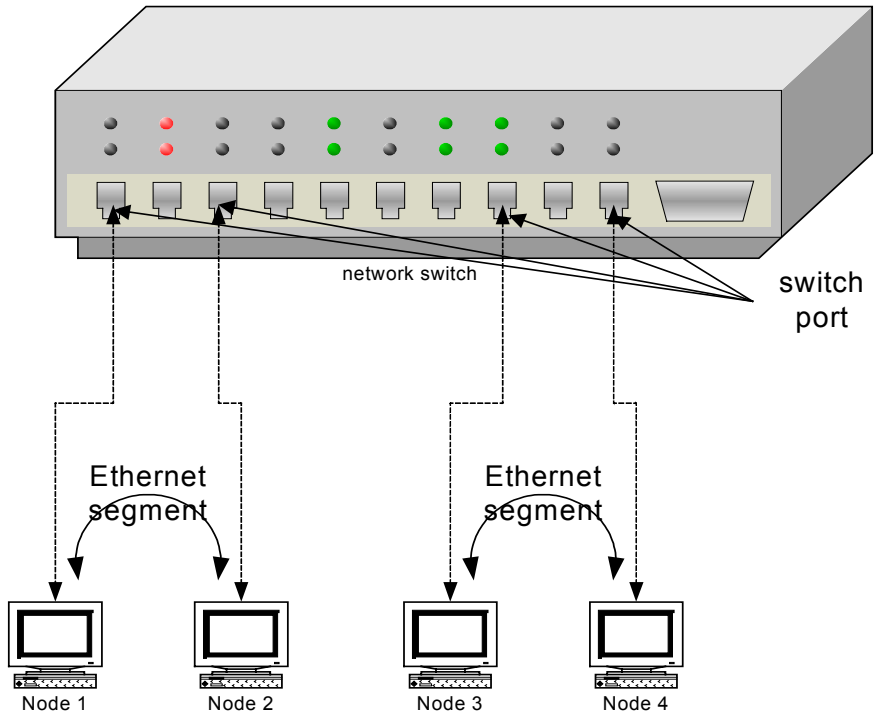
A switch can be rated by it’s individual port capacity and total backplane capacity (both in frames/second)

Ethernet Switch

For example, when node 1 sends a message to node 2, the switch establishes a direct connection with no possibility of collisions

Similarly and simultaneously the switch can establish a direct connection between nodes 3 and 4 with no collision possibility

If nodes 1 and 2 simultaneously try to send a message to node 3, the switch will let one go through and delay the other (maximum time 120 microseconds at 100 mbit/sec) before it is also sent



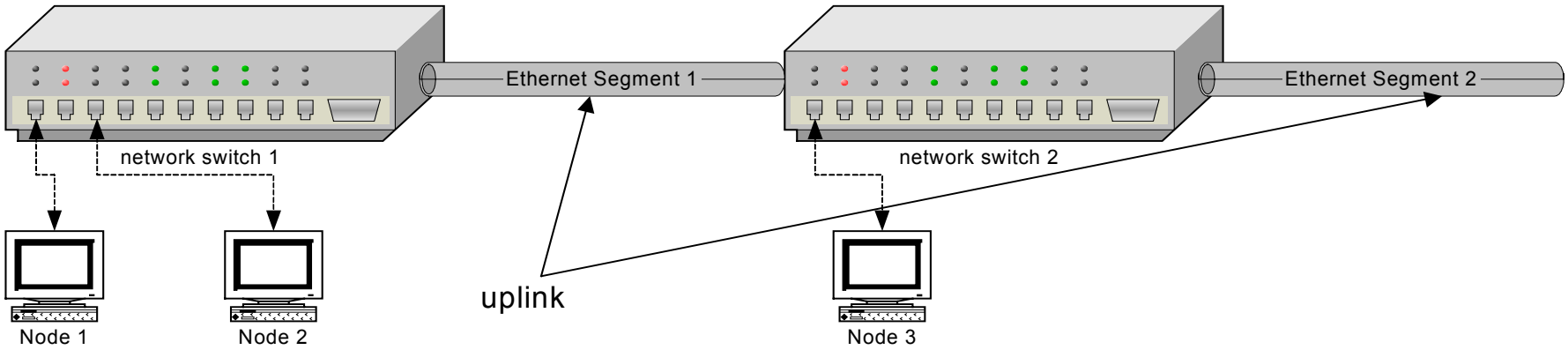
Ethernet Switch

Depending on how the various nodes (with known traffic rates) are assigned to the switch ports and depending on the switch capability, the question of "network saturation" becomes meaningless

Collisions/data loss are avoided as long as the traffic on each port is below its capacity and the switch is below its total backplane capacity

ESBWR Instrumentation & Controls - NRC Audit

Ethernet Switch



If node 1 communicates with node 2, switch 1 “knows” that node 2 is also connected to one of its ports and does not put the message on the “uplink”

If node 1 communicates with node 3, switch 1 knows that node 3 is not on one of its ports and puts the message on the uplink, the switch that does have node 3 connected will no longer forward the message and will instead direct it to node 3

Ethernet Switch

Depending on how the various nodes (with known traffic rates) are assigned to the switch ports and depending on which nodes most often communicate with each other and depending on the switch capability, the question of “network saturation” becomes meaningless

No traffic is on the uplink ethernet switch segments unless the nodes are on two different switches

ESBWR Ethernet Switch

The proposed ESBWR switches have 6 "blades" (cards) – each of which has 48 (full duplex) ports

- ***Total of 288 ports***

The ESBWR switches have 6 uplink ports

Each switch has dual power supplies and predicted 200,000 hour + MTBF

Each ESBWR unit has 5 switches (X2 for redundancy)

If ESBWR is a dual unit, "common" switches can be added

ESBWR Instrumentation & Controls - NRC Audit

Per ESBWR Switch Capacity

EACH port on an ESBWR switch has a capacity of 3.6 million frames/packets per second

EACH port on an ESBWR switch has a capacity of >15,000 frames/packets per second at maximum switch backplane capacity

EACH ESBWR switch “backplane” has a total capacity of 25 million frames/packets per second

Network Switch Overload Analysis

(numbers will change based on final design)

Per uplink segment

- 1 gigabit ethernet is a bit time of 1 nanosecond (.001 microseconds)
- Maximum propagation delay (defined) = 464 nanoseconds)
- Slot time = maximum acquisition time/minimum message size
  - = 4 microseconds
- Maximum packet length = 12144 bits (1518 bytes) = 12.144 microseconds
- Time needed to send a “collision free” message is 4 - 12 microseconds depending on packet size
- A collision occurs (ON THAT SEGMENT) if one node tries to send a message during the 4 - 12 microseconds another message is on the network segment
- If a collision is detected node will “back off” and resend when channel is free (typically 1 – 10 times slot time 4 – 400 microseconds)
- ~82345 maximum size message packets can be sent per second with no collisions

Application Network

288 nodes sending 50 packets per second on an uplink segment = 14400 packets per second

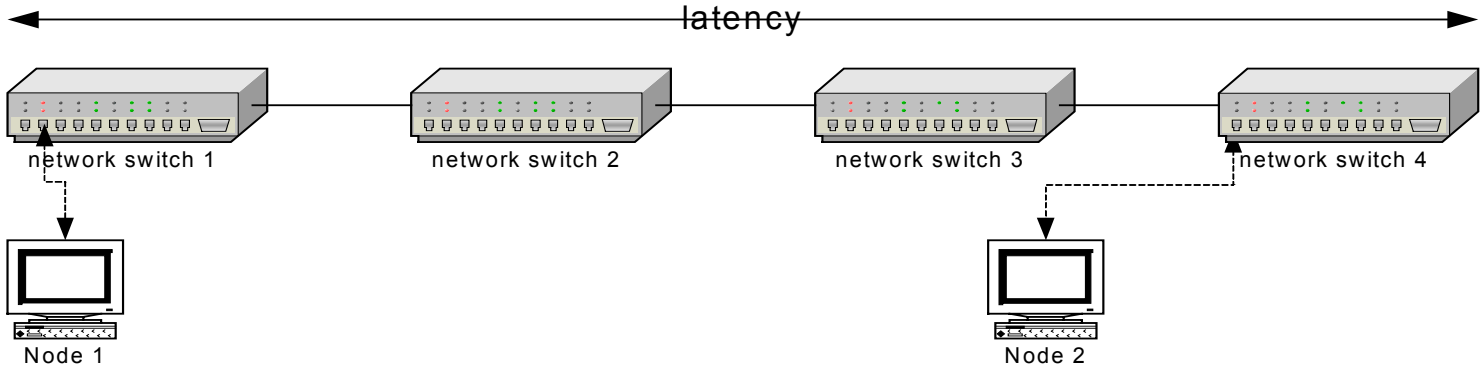
> = 17% of segment capacity

Although non deterministic it is well understood that the chance of a data collision is almost zero (~ one in a million) if the network is loaded to less than ~ 20% of its maximum capability

> and data collision does not mean loss of data or significantly affect response time

ESBWR Instrumentation & Controls - NRC Audit

ESBWR Switch Configuration



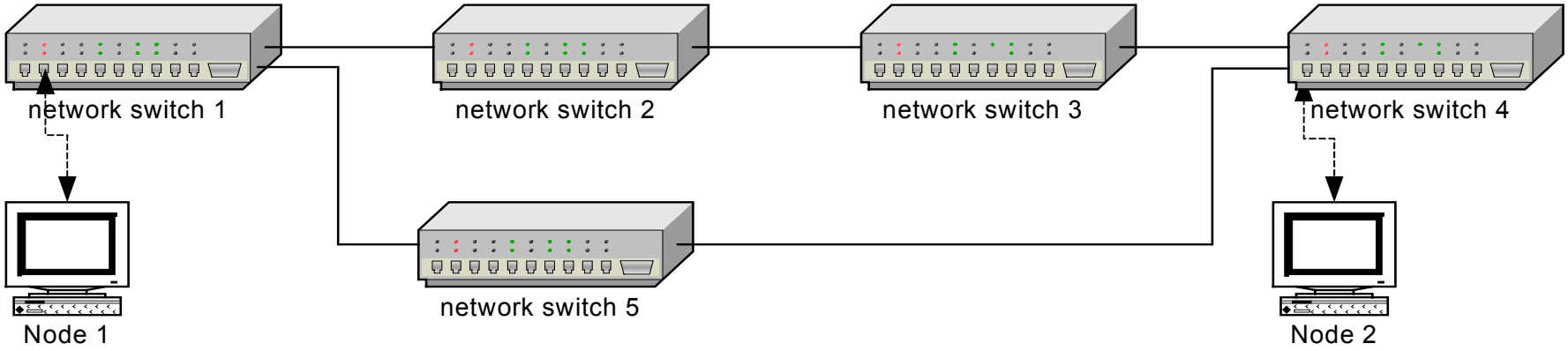
ESBWR switches are “store and forward” devices

- Receives and stores entire packet (instead of address only) before it can be forwarded
- Implies ~ 125 microsecond per switch for maximum 1500 byte message

A “series” five switch network would require 1250 microseconds round trip

- This is message “latency”

ESBWR Switch Configuration



Latency can be improved by minimizing the message “hops” by putting the switches into a radial network

- However radial network has no redundant paths

A “mesh” or ring network has redundant paths but requires many switch interconnections

ESBWR Switch Arrangement

Minimal redundant network requires each device to have at least two connections to two different devices

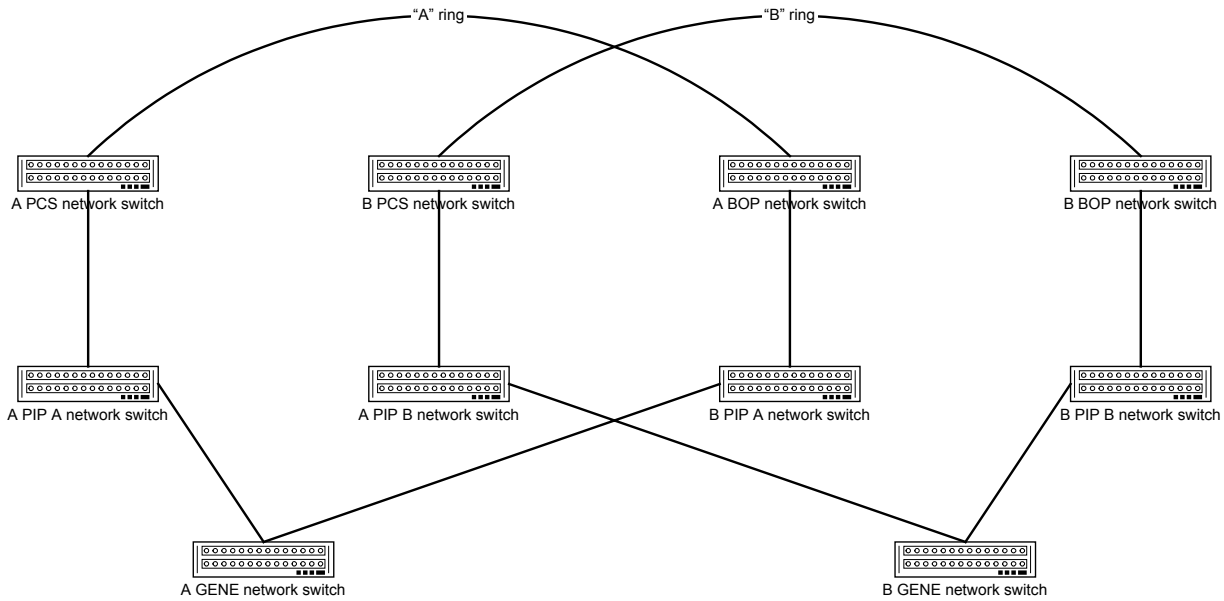
Ring topology is acceptable for redundancy but not latency

ESBWR switch arrangement removes single point of failure and is fast enough (lower latency) to meet real time application requirements

> "large rings" broken into smaller rings

ESBWR Instrumentation & Controls - NRC Audit

ESBWR Switch Configuration

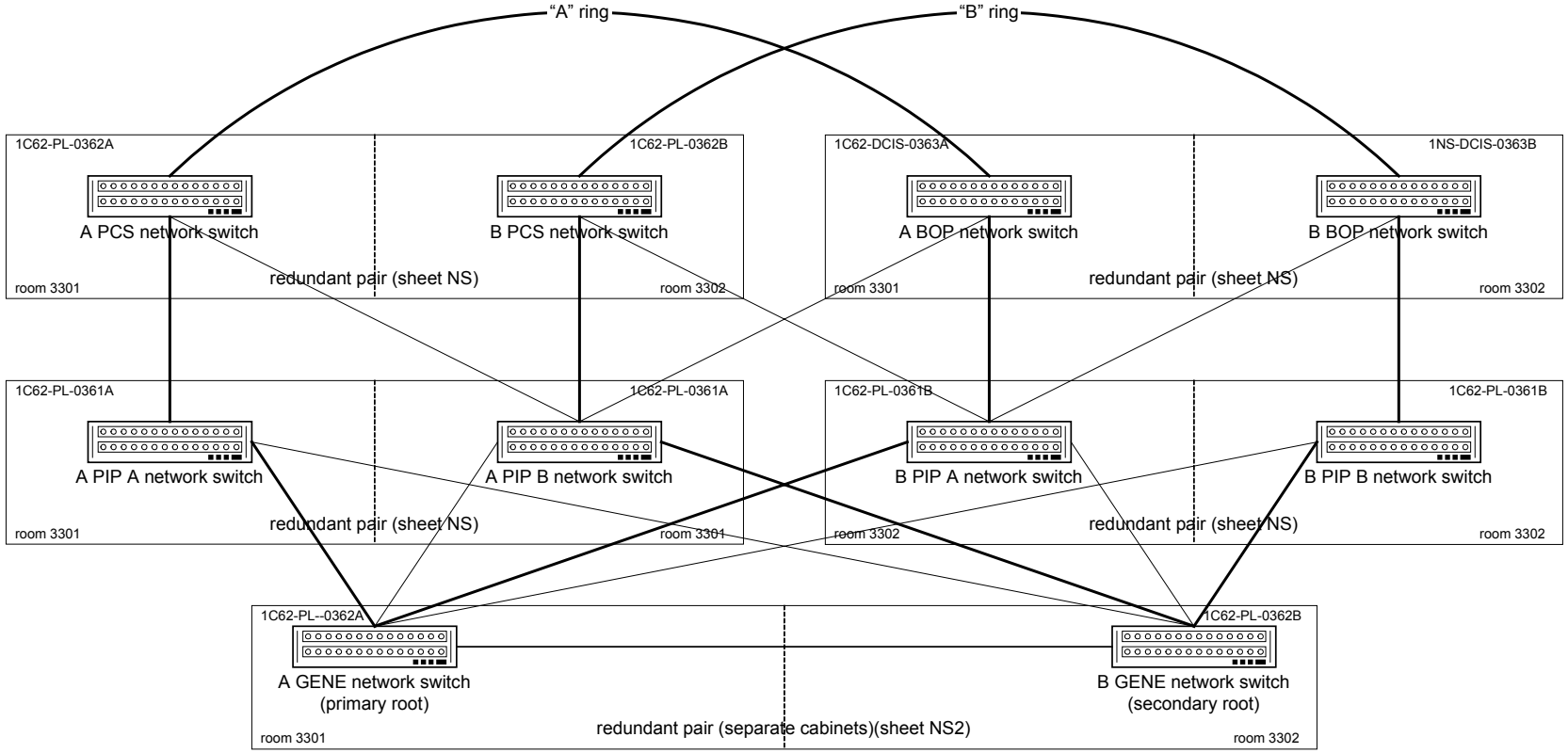


This is a simplified diagram of the ESBWR network switch arrangement

Each node is connected to an "A" and a "B" switch for complete redundancy

ESBWR Instrumentation & Controls - NRC Audit

Actual ESBWR Switch Configuration



Each network switch cabinet is 3 X 3 X 7.5 ft (W X D X H), seismic 2A, bottom entry, front and back access.

Each network switch cabinet supplied with LGA and LGB R13 120 vac power feed and an R15 120 vac power feed.

The non safety network switch backbone consists of two redundant rings (A ring and B ring) of switches connected in a spanning tree network. Every CP, datalink, data acquisition, display and workstation is connected to both rings.
Each switch uplink is 1 GB and each switch node is 100 MB.
Each switch is redundantly powered.

ESBWR Switch Configuration

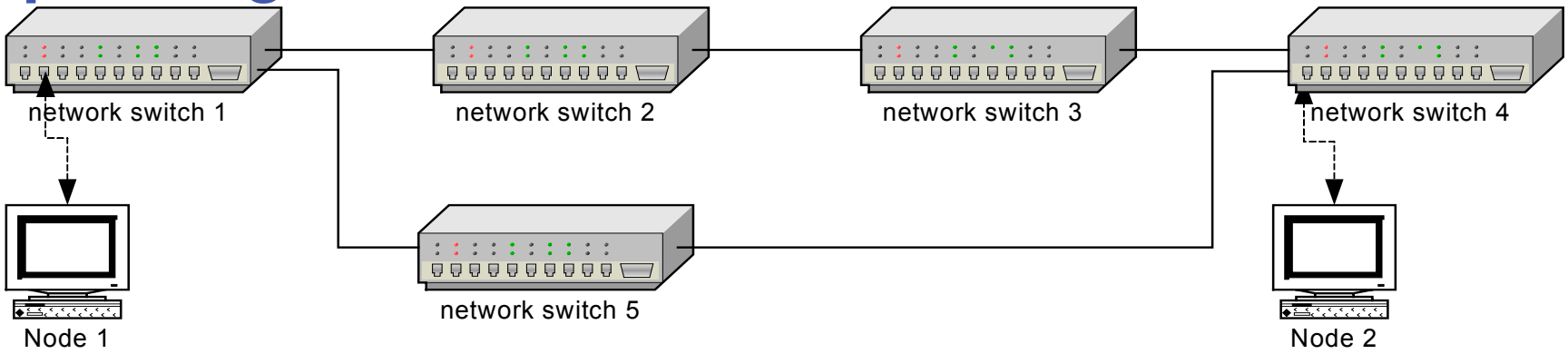
Previous page is a less simplified diagram indicating the actual interconnections (uplinks) between the network switches

Optimized to minimize latency

Data are not simply confined to one loop

ESBWR Instrumentation & Controls - NRC Audit

Spanning Tree Protocol



Redundant data paths (loops) create real “data storms”

> For example node 2 can receive message from node 1 from switch 1>2>3>4 or from switch 1>5>4 ----- collision

> Switch 4 has “learned” that node 1 is from switch 3 and from switch 1

Spanning tree protocol blocks redundant uplink switch ports

> If there is only one active path from the root switch to any node then there will be no loops in the topology

Switch (re)configuration is automatic and continuing to accommodate both failures and new nodes

> Result is the lowest (time) cost path and lowest latency

ESBWR Switch Configuration

The final ESBWR switch configuration has a maximum four switch “hop”

- Therefore a maximum latency of 1000 microseconds round trip

A single switch failure allows the redundant loop to take over with no system effect

Redundant paths allow more switch failures with increase in latency

It is important to understand that the (internal) switch configuration and data paths will change as the network is built up during installation and nodes (workstations, controllers, display workstations) are added.

ESBWR DCIS Description

ESBWR DCIS Description

>Describe the 1E DCIS

>Describe the non 1E DCIS

>Describe the nonsafety controllers

>Describe “gateways”

>Describe how ESBWR network DCIS operates

>Discuss operator response in terms of “real world” examples

>Discuss actual problems

ESBWR Safety DCIS

RPS, LDIS, NMS, ECCS are deterministic

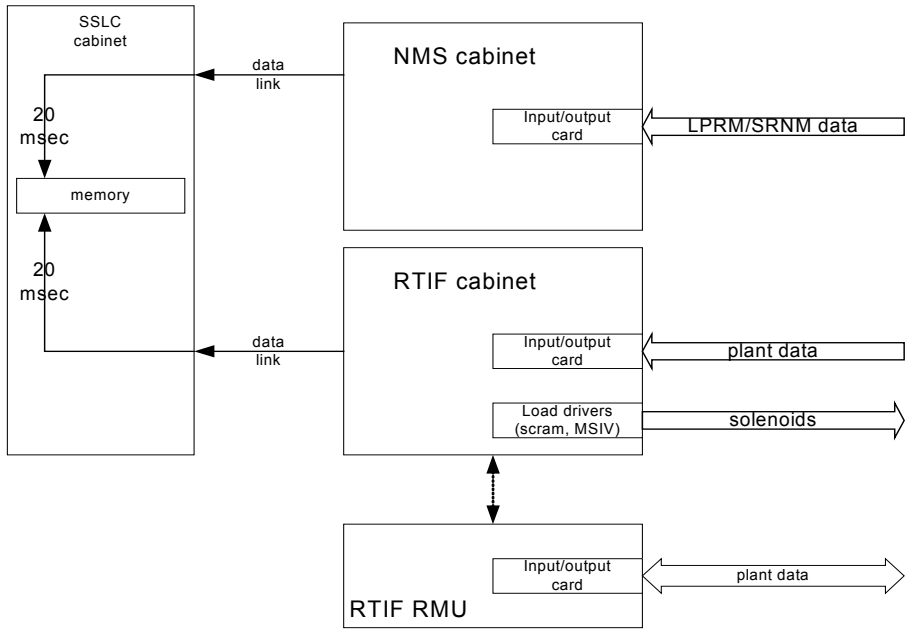
- All field data acquired at a fixed rate
- All field outputs produced at a fixed rate
- No collision possibility
- No data loss possibility
- No “data storm” or “overload”
- Data acquisition rate is constant and independent of plant conditions
- SCRAMNET and NERVIA are NOT ethernet

Rates are determined in initial design to be fast enough to perform required functions

- There is no failure mechanism for the design rate to change

ESBWR Safety DCIS - Displays

- Data links used to send NUMAC RTIF/NMS data to DS&S displays
- Data acquired by NUMAC at fixed rate
- Data sent by NUMAC at fixed rate
  - > No collision possibility
  - > No data loss possibility
  - > Completely deterministic
- Data acquisition and transmission rate is constant and independent of plant conditions
- NUMAC and DRS are asynchronous



ESBWR Safety DCIS – Displays (continued)

- All data on divisional ring available at deterministic rates for display
- For monitoring, displays updates every second asynchronously to data acquisition
- For control, operator commands available to ring every display update
- Operator commands reflected in field output at deterministic rates

ESBWR Safety DCIS - Control

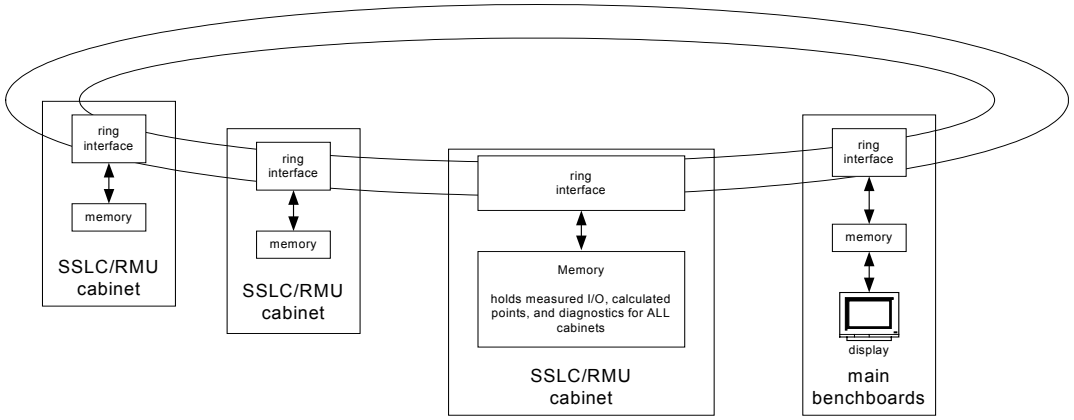
Timing requirements are design basis inputs to E-DCIS to determine data acquisition / parameter trip / 2 out of four / output rates

> ECCS
  - Although no ECCS requires high speed, most 1E control calculations run in 10's of msec
  - ECCS required time response (after built in logic time delays)
    - ~ 50 msec (solenoid/squib) (SRVs take ~ 400 msec to open)

> RPS (RTIF)/NMS
  - hardwired (to dedicated RMUs) inputs/outputs to meet scram timing requirements
  - <10 msec NUMAC calculation time
  - Required time response
    - 10s of msec for scram time requirements/SOE

ESBWR Instrumentation & Controls - NRC Audit

Safety DCIS Transport Time



> SCRAMNET and Nervia make all data available to all “nodes” (not ethernet nodes) on the rings

> About 5 microseconds SCRAMNET, 5 – 100 msec Nervia (application dependent)

> Transmission/reception is redundant

ESBWR Instrumentation & Controls - NRC Audit

Nonsafety Controllers

All “important” control (trips) is hardwired and deterministic
- Main turbine, water level, PAS, pressure control

All safety functions are deterministic
- Dedicated cabinets, redundant radial fiber, dual fiber rotating rings

All non 1E automatic control is deterministic by application
- “network”

Plant is designed on safety side to not require operator intervention for 72 hours

Plant should be designed (as good HFE practice) by responsible design organizations to not require operator intervention for minutes

ESBWR Instrumentation & Controls - NRC Audit

Nonsafety Control / Response Time

Plant should be designed on nonsafety side (as good HFE practice) by responsible design organizations to not require operator intervention for minutes (as opposed to seconds)

- This is because operator will, in general, not be looking at the correct display needed to respond to an alarm
- Annunciator > Alarm display > alarm response procedure > select system display > select control display

Safety of plant, general population and expensive power generation equipment must always be automatic

Response Time

Despite lack of need for “high speed” operator control, DCIS is more than fast enough for operator intervention.

Operator response time concerns are limited to manual actions

- > Usually done one at a time at operator’s pace
- > Most operator response to alarms is to verify that the correct automatic protection has correctly initiated
- > Most operator control and monitoring is to perform procedures at operator’s own pace

ESBWR Instrumentation & Controls - NRC Audit

Examples

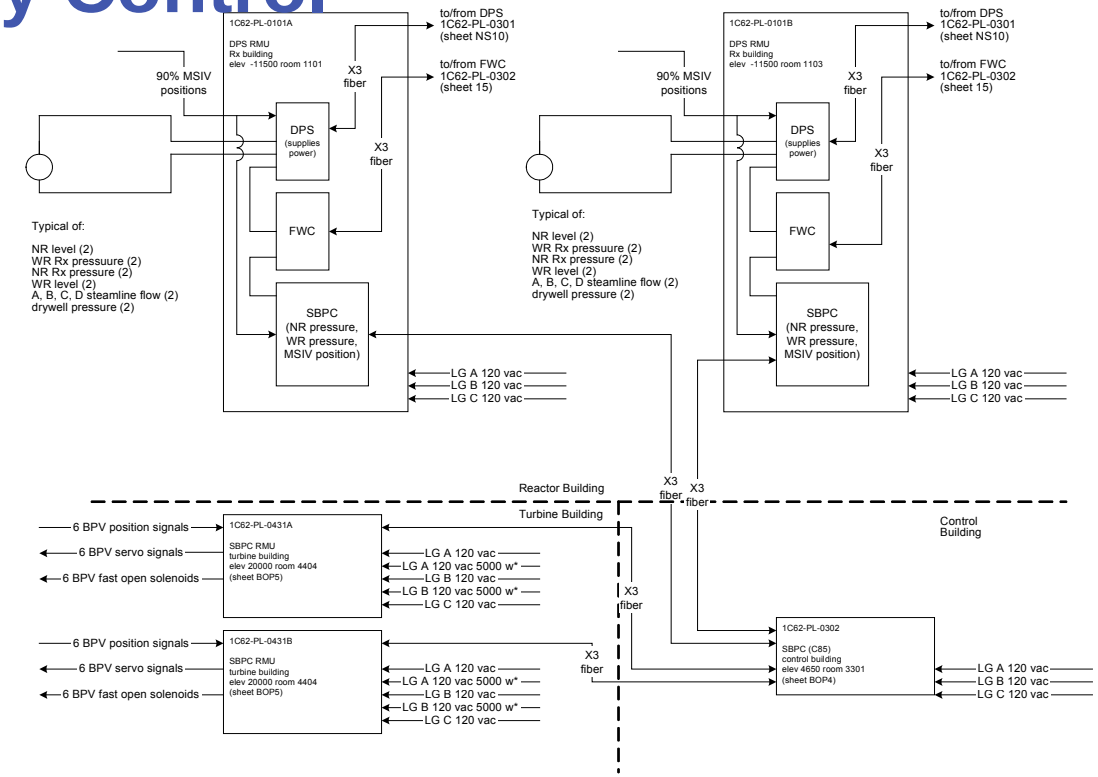
High turbine vibration at levels that are damaging are not "alarmed" to the operator for a manual turbine trip – instead turbine is tripped automatically

Very low reactor water level indicating a LOCA is not alarmed to the operator so he will turn on injection systems – instead the reactor is scrammed, depressurized and flooded automatically

Although manual intervention is always allowed, operator control is not normally necessary for power generation or safety

ESBWR Instrumentation & Controls - NRC Audit

Nonsafety Control



>Nonsafety controllers have/control their own data acquisition

>All automatic control is deterministic

>Closed loop control is not done over the network switch uplinks or normal gateways

>Only setpoints and manual demands are on switch/display links

Nonsafety Control

- Nonsafety controllers poll their own data acquisition
- RMUs are polled one at a time for their data
  - No collision possibility
  - No data loss possibility
  - Deterministic in that all data for that controller is collected within a defined time interval
- Above requirements are automatically met by following application rules about number and type of signals allowed per controller and required processing rates
- Most BWR nonsafety control loops run at approximately 100 msec
- Polling rate is constant and independent of plant conditions

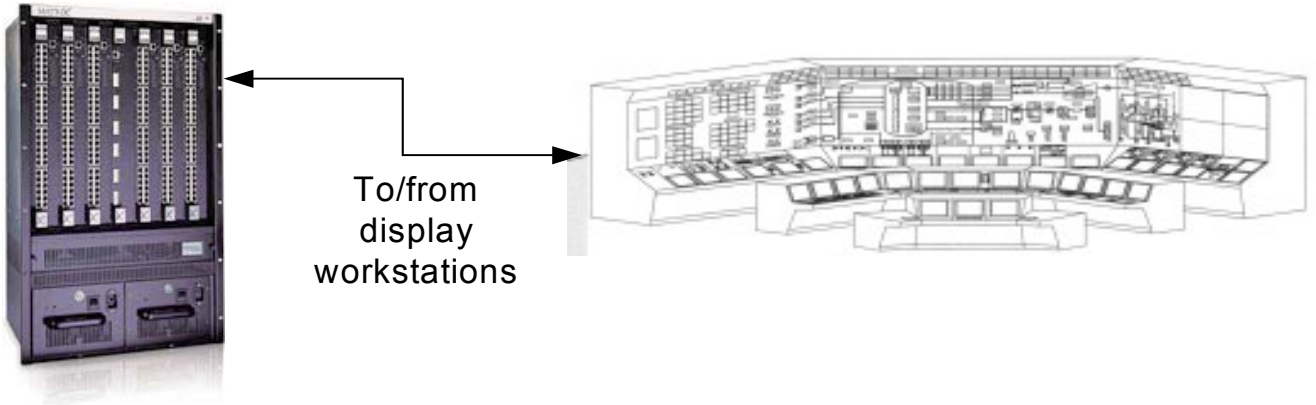
ESBWR Instrumentation & Controls - NRC Audit

Controller Loading

- Controllers are deliberately segmented by task
- Controllers are “loaded” by number of calculations, closed loop control, and I/O per unit time
- Calculation and closed loop control blocks well defined and deterministic (for example most PID algorithms must run at 100 msec)
- Controllers deliberately not loaded to max (often segmentation limits usage to less than 50%)
- If controller work approaches controller capability then calculations and/or I/O are shifted to another (or new) controller
- Potential for DCIS overload easily checked by reviewing calculations

ESBWR Instrumentation & Controls - NRC Audit

ESBWR Nonsafety Displays



- Each benchboard display or freestanding monitor has its own dedicated workstation
- Each display workstation has a dedicated (redundant) switch port
- Typically display workstation access data made available by controllers or other workstations to request data needed to support current display format (which may be needed only once or continuously)
  - After link is established data are supplied by exception
- ~20 workstation/displays per unit

ESBWR – Switch to Display

These data links are one of the few that are not “predefined” in that it is the operator that determines the traffic by his display selection

At any one time a display workstation will only have one format up

Displays update once per second

A typical format will have 100 points

Conservatively assuming all points come from different sources and ignoring reporting by exception indicates workstation to switch traffic is 100 packets/second on a 15,000 packet/second capable link

Assuming all controller data must go through the network switches and each controller is providing 5 packets/second to EACH display and all controllers were using the uplink

- 37 X 5 = 185 packets per second from controller to switch on 15,000 packets/second capable link
- ~ 160 CPs / 2 X 5 X 37 = 14,800 packets/second = ~ 18% of uplink capacity

Display Overload Analysis

- Assume 30 displays with 100 “values” per format all changing state in one second post transient. Further assume 8 bytes per sample
- Total is 24000 samples/second on network with collision free capacity of 3 million samples/second
- Clearly displays will never be network limiting
- Largest network load is SOE/TRA/historian

Non 1E Displays

Typical display timing for nonsafety DCIS displays

- > ~100 msec data acquisition
- > ~50-100 msec typical processing
- > ~100 msec typical controller to display workstation
- > 1 second display update

Total is ~300 msec if delivered to display workstation just before update

~1.30 sec if delivered to display workstation just after update

Display Uncertainty

The greatest portion of display uncertainty occurs because of the HFE decision to update displays no greater than once per second

ESBWR Instrumentation & Controls - NRC Audit

"Real World" Operation

Whatever the real or calculated data delay from the field to the display (which will almost always be better than the "worst case"), the operator will always be able to adequately control and monitor the plant

- >Feedpump suction pressure trip
- >Main turbine high vibration alarm
- >Loss of all feedwater flow
- >Roll turbine

Real Scenarios #1

- Feedpump suction pressure trip
  - Closed loop control
  - No operator intervention
  - Second to 10's of seconds timing for pump protection
- Operator receives trip alarm
  - Verifies (seconds)/SCRRI
  - Verifies standby feedpump auto start

Real Scenarios #2

Main turbine alarm high vibration

- Operator pages to vibration display and alarm display with response procedure
- Operator has minutes to hours otherwise if vibration was high enough turbine would trip automatically without operator
- Most likely operator response is to reduce turbine load/Rx power (minutes/hours)

Real Scenarios #3

Loss of all feedflow

- Automatic SCRAM on level 3
- Automatic IC initiation on level 2
- Level stabilizes above level 1
- Operator confirms CRD pump high pressure injection
- Operator confirms slowly increasing level

Real Scenarios #4

Roll Turbine

- > Operator calls up appropriate turbine display
- > VDU response to command immediate
- > Operator must hold “turbine roll” command for as long as it takes signal to get to turbine controller
  - – < 1 second
- > Turbine control system brings turbine to 400 RPM (1st speed breakpoint)
- > Operator monitors turbine signals

ESBWR Gateways

Gateways are used to translate from one hardware/software platform to another

Often used between safety and nonsafety DCIS components – always using fiber

Some components do not require gateways (safety and nonsafety directly connected through fiber) because same vendor is on either side (NMS to ATLM)

Some components use dedicated, high speed links and gateways to send control data from safety to nonsafety (NMS to MVD to DPS)

Normal gateways are used to put safety-related data onto the nonsafety networks for use in monitoring, alarming and recording

ESBWR Instrumentation & Controls - NRC Audit

ESBWR Gateways

Single failure of any gateway or datalink will not cause a scram or loss of power generation

Gateways are designed to handle their required # of signals at their required speed

Gateways are also used between different nonsafety DCIS components

- > Condensate polishing
- > Meteorological
- > Seismic monitoring
- > Area radiation monitoring etc

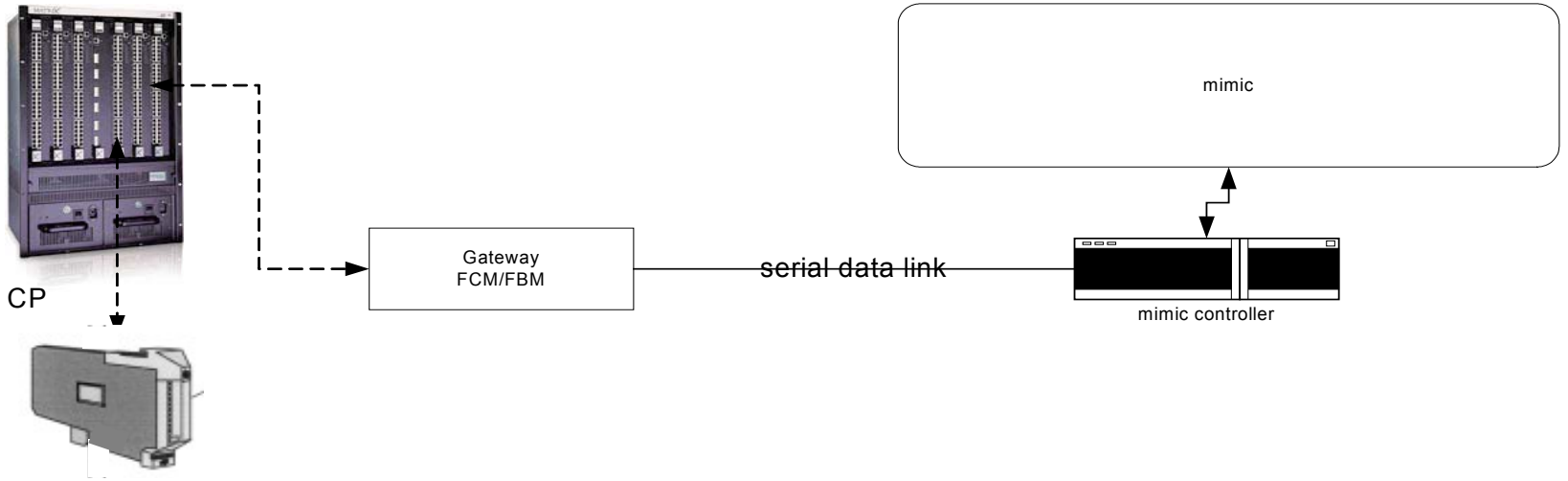
Actual Problems (from Lungmen)

Despite the actual capabilities of the Lungmen DCIS, simulator and module testing uncovered real application problems

Problems were NOT traceable to the DCIS network configuration

ESBWR Instrumentation & Controls - NRC Audit

Actual Problems



The mimic on the simulator was observed to be very slow in responding to plant transients

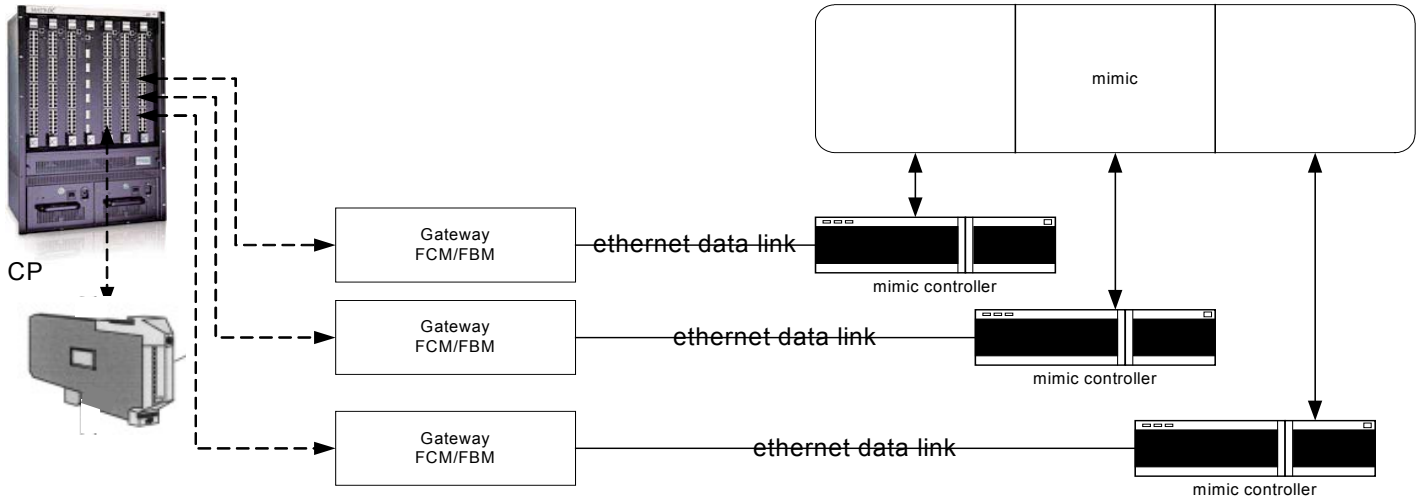
Many mimic elements had to be redrawn in a short time

The problem was NOT caused by the inability of the required data to be delivered to the mimic gateway in a timely manner

The mimic is a large “display” but driven through a gateway instead of a direct connection to a display workstation

ESBWR Instrumentation & Controls - NRC Audit

Actual Problems (continued)



Problem was traced to slow serial data link and single mimic controller

Lungmen will instead have three mimic controllers (so that each has to “draw” only one third of the mimic)

And three much faster point-to-point ethernet links driven by three gateways

Actual Problems (continued)

An additional concern was raised about the speed of the SPDS calculations both on the SPDS displays and for several of the mimic parameters

This concern was addressed by changing both hardware and software

- 10 CPs (more processing power) are now allocated for the SPDS and core thermal power calculation
- SPDS critical parameters will execute at 100 msec
  - Software changed to perform calculations in “parallel” instead of “series”
- All other SPDS calculations 500 msec to one second

The problem was not traced to data being sent too slowly to the SPDS processors

Post Accident Monitoring

ESBWR Instrumentation & Controls - NRC Audit

1.97 R4/Post Accident Monitoring

- This is an application problem and not a DCIS concern
- DCIS configuration
  - > Can acquire safety signals
  - > Can acquire redundant signals
  - > Can power signals with safety-related power
  - > Can acquire nonsafety signals
  - > Can acquire redundant nonsafety signals
  - > Can power nonsafety signals with diesel backed power
  - > Can present signals in a tabular predefined report
  - > Can put signals through the firewall to the TSC/EOF/nuclear data link
  - > Can present safety signals on safety displays
  - > Can present safety and nonsafety signals on nonsafety displays
  - > Can present signals on fixed plant status/alarm displays
  - > Can present signals in predefined HFE approved formats
  - > Can record all safety and nonsafety signals
  - > Can alarm on signal loss or out of range

Once a signal is acquired by the DCIS for ANY reason it can be used for any other reason

ESBWR Instrumentation & Controls - NRC Audit

1.97 R4/Post Accident Monitoring - Concerns

- A required 1.97 R4 signal could not be on the logics (and therefore plant I/O list and is therefore unavailable)
- A 1.97 R4 signal could be acquired as nonsafety only when it is needed safety
- A 1.97 R4 signal could be required redundantly and only be available as a single signal

In all cases spares will be available to acquire the “missing” signals and DCIS configuration remains unchanged

DCIS can wait for 1.97 Rev 4 HFE analysis

Interlock Systems

Interlocks

This is an application problem and not a DCIS concern

Interlocks are “logic”

For example FAPCS LPCI injection valve should not be opened at high reactor pressure

- “Standard” MOV valve logic will have open and/or close permissives
- Permissive can include (for example) measurement of four safety-related WR and four nonsafety-related WR reactor pressure signals and compare them to a common setpoint
- DCIS configuration
- Can acquire safety and nonsafety signals
- Can provide both safety and nonsafety-related logic
- Can be made fail safe (on loss of signals) or fail “as is” as necessary
- Can present permissive status on valve operating display
- Can alarm on signal or permissive status

Interlocks - Concerns

>A required interlock signal could not be on the logics (and therefore plant I/O list and is therefore unavailable)

>A logic could be incorrect

In all cases spares will be available to acquire the "missing" signals and logic can be verified and corrected, DCIS configuration remains unchanged

Interlocks can wait for system logics

DCIS Architecture Top Down Overview

Rich Miller and Ira Poppel

SPINLINE3 E-DCIS Architecture

Rich Miller, Jean-Michel Palaric, Dominique Moulin

Vere Joseph and Ira Poppel

ESBWR Instrumentation & Controls - NRC Audit

DS&S

Technology (Proprietary) Time: 1 hour

>SPINLINE3

>VDU

SPINLINE3/ESF (Non-Proprietary) Time: 1 hour

>Architecture

>IEEE 603 Compliance

NUMAC E-DCIS Architecture

Rich Miller, Bishara Kakunda, Ty Rogers, Chan Patel and Ira Poppel

IEEE-603 (10 CFR 50.55a(h)) Compliance Documentation - LTRs

Rich Miller and Steve Kimura

ESBWR Instrumentation & Controls - NRC Audit

LTR Presentations

>NUMAC LTR

>SPINLINE3 LTR

Plant Specific LTR Schedule

>NUMAC LTR – 10/30/2007

>SPINLINE3 LTR – 10/30/2007

ESBWR Instrumentation & Controls - NRC Audit

Conformance to IEEE Std. 603 - Demonstration

- Assigned new fulltime engineer to coordinate response to IEEE Std. 603 questions
- Writing LTR NEDO-33294, “ESBWR Safety Criteria for Instrumentation & Control Systems,” to address conformance to Standard
- Revising DCD/Tier 2, Chapter 7, Rev. 3, to tie IEEE Std. 603 criteria to specific equipment within Sections and Subsections
- Planning multiple FMEAs to demonstrate conformance to single-failure and independence criteria
- Planning summary LTR to present results of the multiple FMEAs for ESBWR Safety-Related I&C Systems

ESBWR Instrumentation & Controls - NRC Audit

Conformance to IEEE Std. 603 – Software Safety

- Safety-related software will be developed in accordance with the ESBWR I&C Software Safety Plan (EICSSP)
- Software hazard analyses (SHA) will be performed and documented per the EICSSP
- SHA will demonstrate that safety-related software will reliably perform required safety functions in the presence of design basis events and credible single failures
- SHA will demonstrate that safety-related software failures to not create additional hazards
- Planning summary LTR to present results of the SHAs for ESBWR Safety-Related I&C Systems

RTNSS

Rick Wachowiak

ESBWR Instrumentation & Controls - NRC Audit

Regulatory Treatment of Nonsafety System

- Functions Needed to Address ATWS (10 CFR 50.62)
- Functions Needed to Address SBO (10 CFR 50.63)
- Functions Needed for Post 72 Hour Safety
- Functions Needed for Seismic Events
- Functions Needed to Prevent Significant Adverse Systems Interactions
- Functions Needed to Meet the Probabilistic Safety Goals

ESBWR Instrumentation & Controls - NRC Audit

RTNSS Functions - Proposed

ARI

Feedwater Runback

Firewater Refill of Pools (IC/PCC, SFP) Using Diesel Pump

Firewater Refill of Pools Using External Connection

Post Accident Monitoring

> Functions requiring 1E power

LPCI Mode of Fuel and Auxiliary Pools Cooling (FAPCS)

SPC Mode of FAPCS

Some Manual Actuation Functions of Diverse Protection System (DPS)

ESBWR Instrumentation & Controls - NRC Audit

ATWS Mitigation – 10 CFR 50.62

Functions Required:

(c)(3) Each boiling water reactor must have an alternate rod injection (ARI) system that is diverse (from the reactor trip system) from sensor output to the final actuation device ….

(c)(4) Each boiling water reactor must have a standby liquid control system (SLCS) with the capability of injecting into the reactor pressure vessel a borated water solution ….

ARI is Non-Safety in ESBWR

SLCS is Safety-Related in ESBWR

Success Using SLCS Requires Successful Feedwater Runback

Feedwater Trip Should Also Be OK – needs to be confirmed

ARI is RTNSS

Feedwater Controller is RTNSS

Station Blackout – 10 CFR 50.63

ESBWR Has a 72 Hour Coping Period

Nothing More Should Be Required

SECY-94-084

- Diesels or Offsite AC Power Connection can be RTNSS based on PRA or long term safety

Diesels Must Be Able To Start After 72 Hours

ESBWR Instrumentation & Controls - NRC Audit

Seismic

Seismic Response is By Safety Related Components

Only Issue is Post 72 Hour Safety Following Seismic Event

Long Term Safety

All Initiating Events Must Be Considered

Required Functions

- Core Cooling
- Decay Heat Removal
- Post Accident Monitoring
- Control Room Habitability

ESBWR Instrumentation & Controls - NRC Audit

Long Term Safety - Phases

0 – 72 Hours	Safety Related, No Operators
3 – 7 Days	Resources Must Be On Site
7+ Days	Off Site Commodity Replacement

More Time Until Needed Results In Less Stringent Requirements

Repair Is OK If Backup Is Available (3+ Days)

“Walking Away” Not An Option

ESBWR Instrumentation & Controls - NRC Audit

RTNSS Based on PRA Results

Systems Needed to Meet Safety Goals

- CDF ≤ 10^{-4}
- LRF ≤ 10^{-6} (and containment performance goal)
- These are risk significant systems
- Higher level of treatment
- Manual actuation of ECCS via DPS is in this category

Systems Needed to Address Uncertainty

- These are not risk significant systems
- Maintenance Rule treatment
- Some functions of FAPCS are in this category

Cyber Security and RG 1.152 Compliance Documentation

Rich Miller, Dave Hamilton and Manny Moe

ESBWR Instrumentation & Controls - NRC Audit

Requirements/Guidelines

- RG 1.152, Rev. 2, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants* (January 2006)
- Federal Register, Part II NRC, *10 CFR Parts 50, 72, and 73 Power Reactor Security Requirements; Proposed Rule* (October 26, 2006)
- NEI 04-04, Rev. 1, *Cyber security Program for Power Reactors* (Nov. 18, 2005)
- Guideline on Licensing Digital Upgrades EPRI TR-102348 Revision 1 NEI 01-01 (*A Revision of EPRI TR-102348 to Reflect changes to the 10 CFR 50.59 Rule*) - (March 2002)
- NUREG/CR-6847 --- *Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants (September 2003)*

ESBWR Instrumentation & Controls - NRC Audit

Path Forward

> *Topical Report NEDE-33295, ESBWR Cyber Security Program Plan is being developed for submittal to NRC (December 30, 2007).*

Technical Specifications - I&C

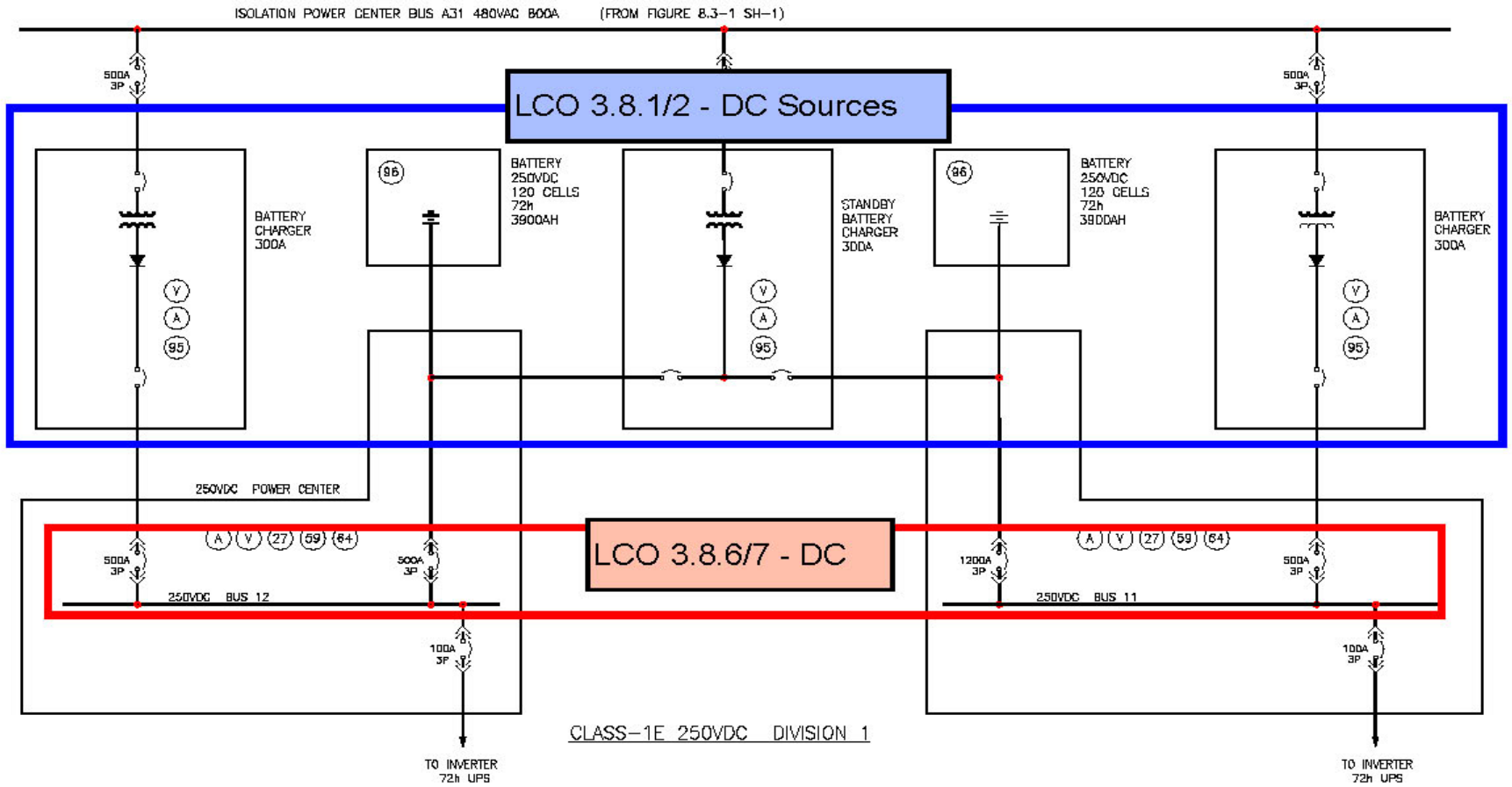
Dan Williamson

ESBWR Instrumentation & Controls - NRC Audit

> Section 3.3 LCOs – Include “N-2” Provisions
> Action Statements
> Surveillances
> Setpoints and “Setpoint Control Program”
> Bases

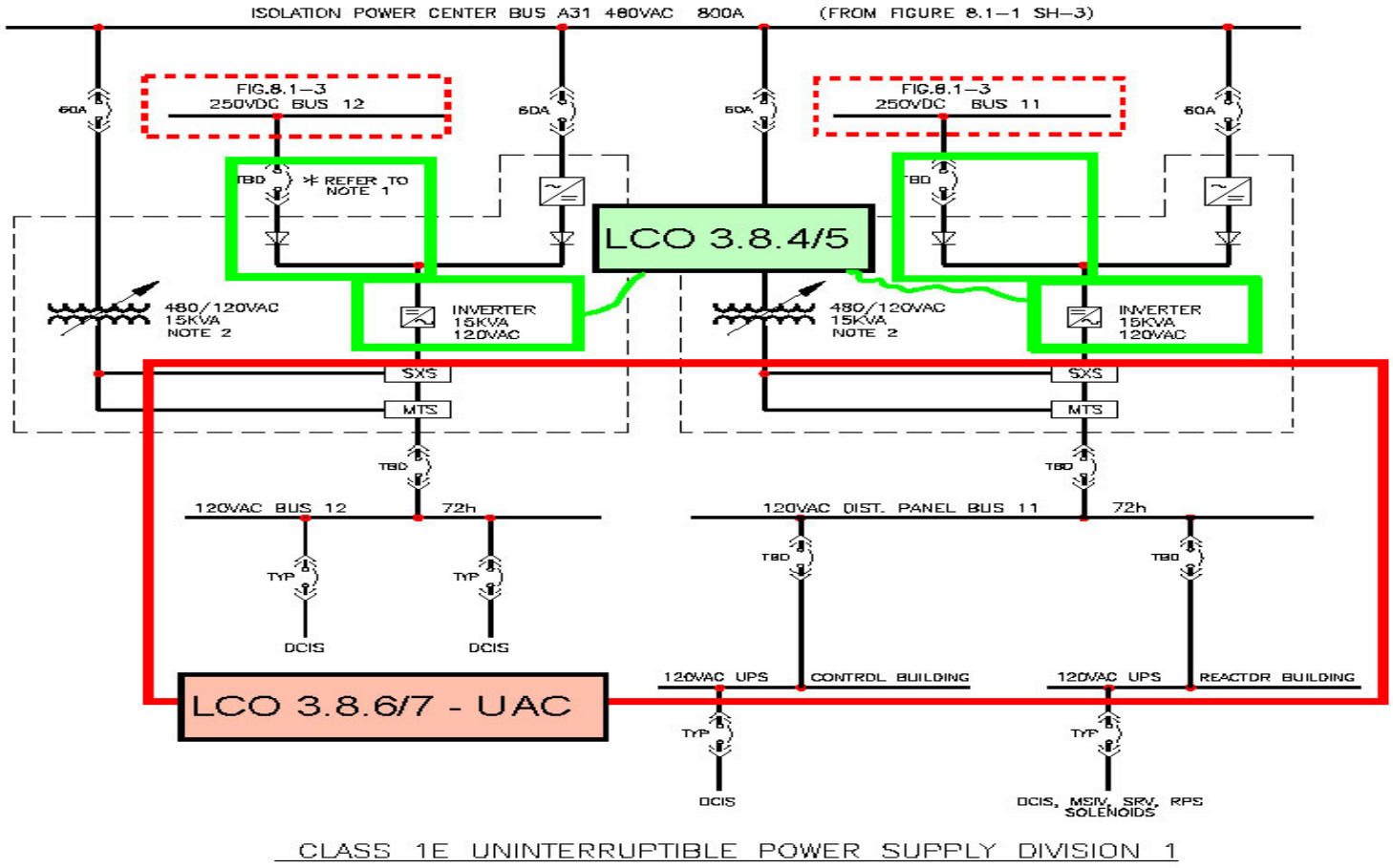
ESBWR Instrumentation & Controls - NRC Audit

LCO "N-2" Statements [Portion of DCD Figure 8.1-3]



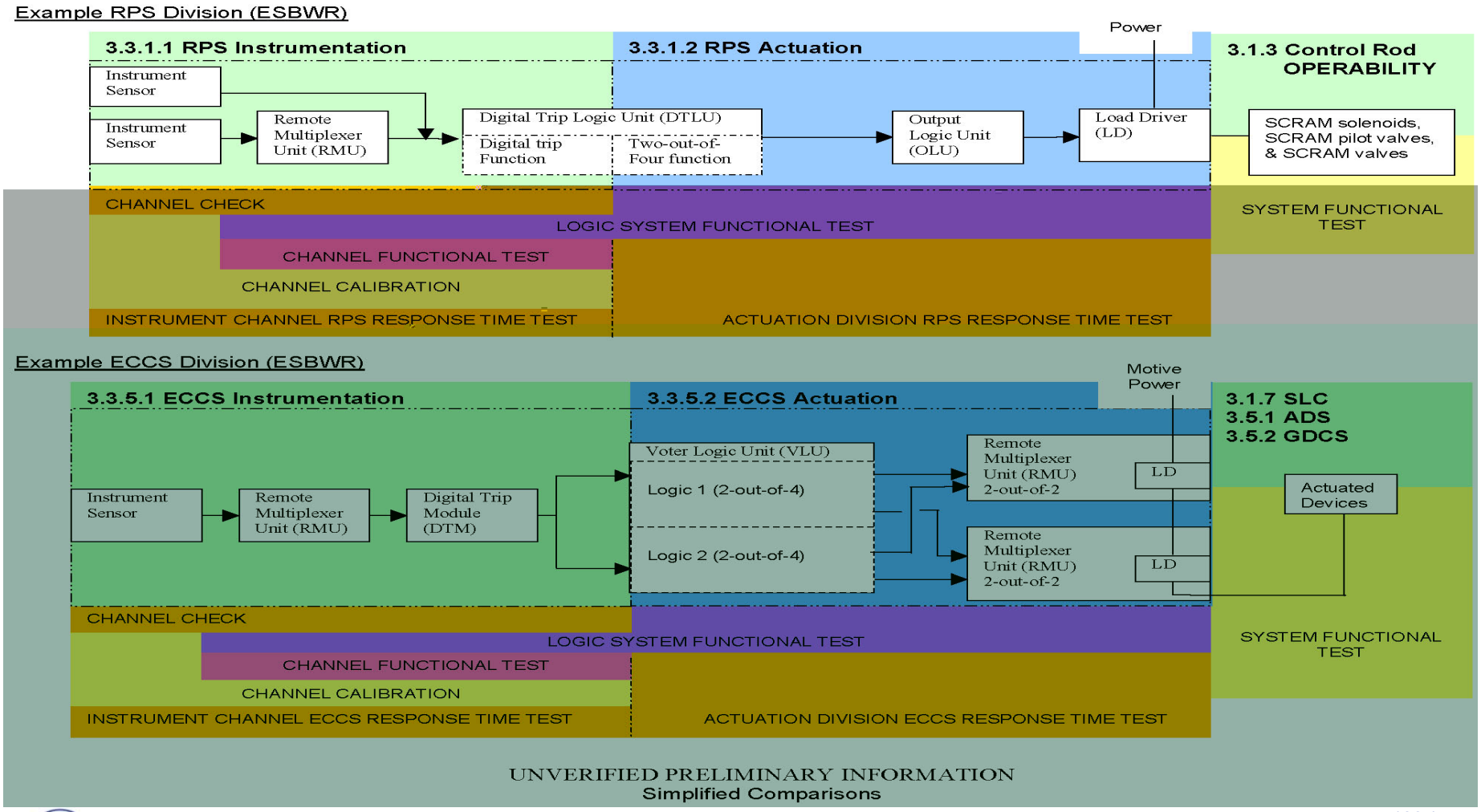
ESBWR Instrumentation & Controls - NRC Audit

LCO "N-2" Statements [Portion of DCD Figure 8.1-4]



ESBWR Instrumentation & Controls - NRC Audit

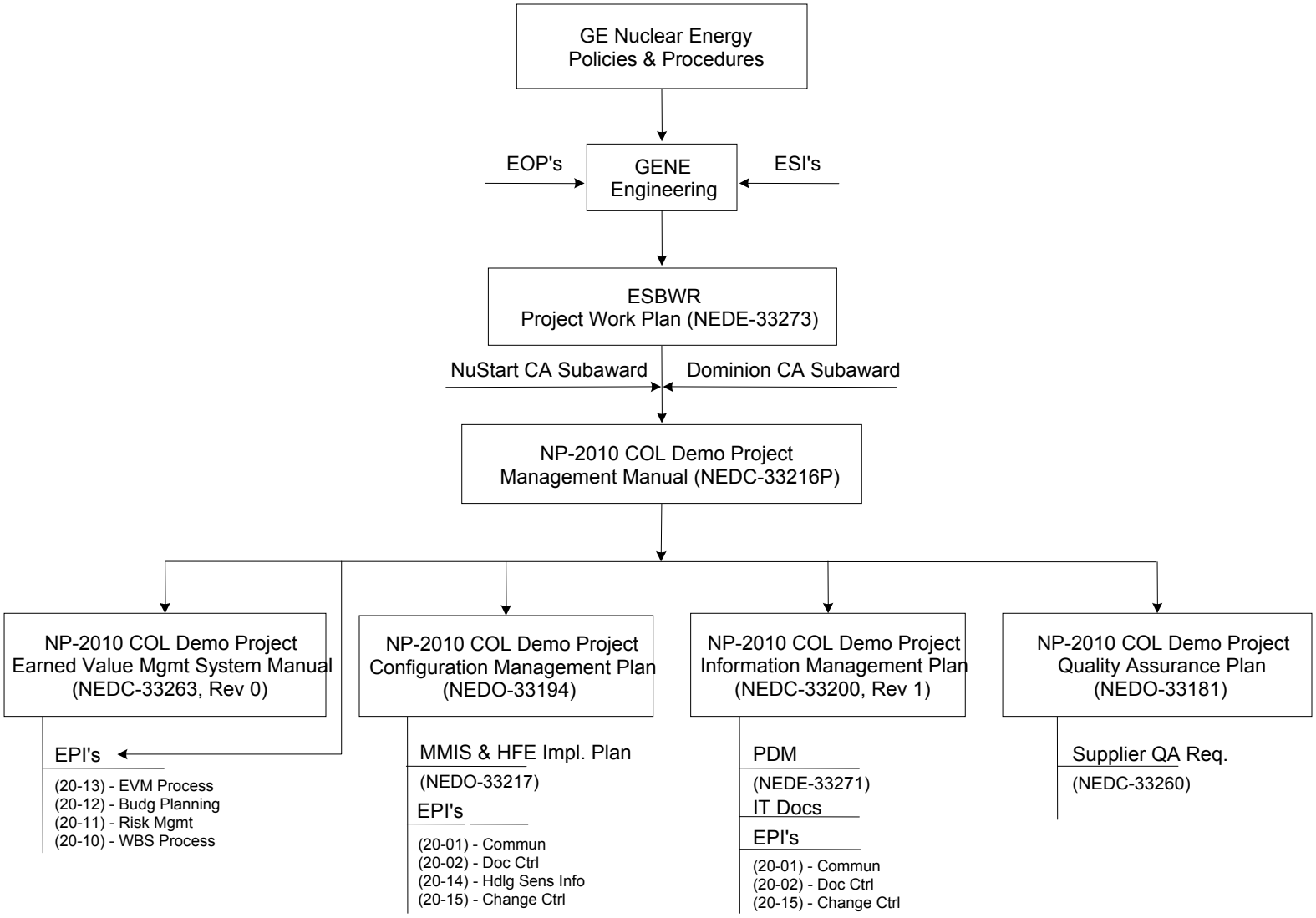
Surveillance Testing – Simplified Example



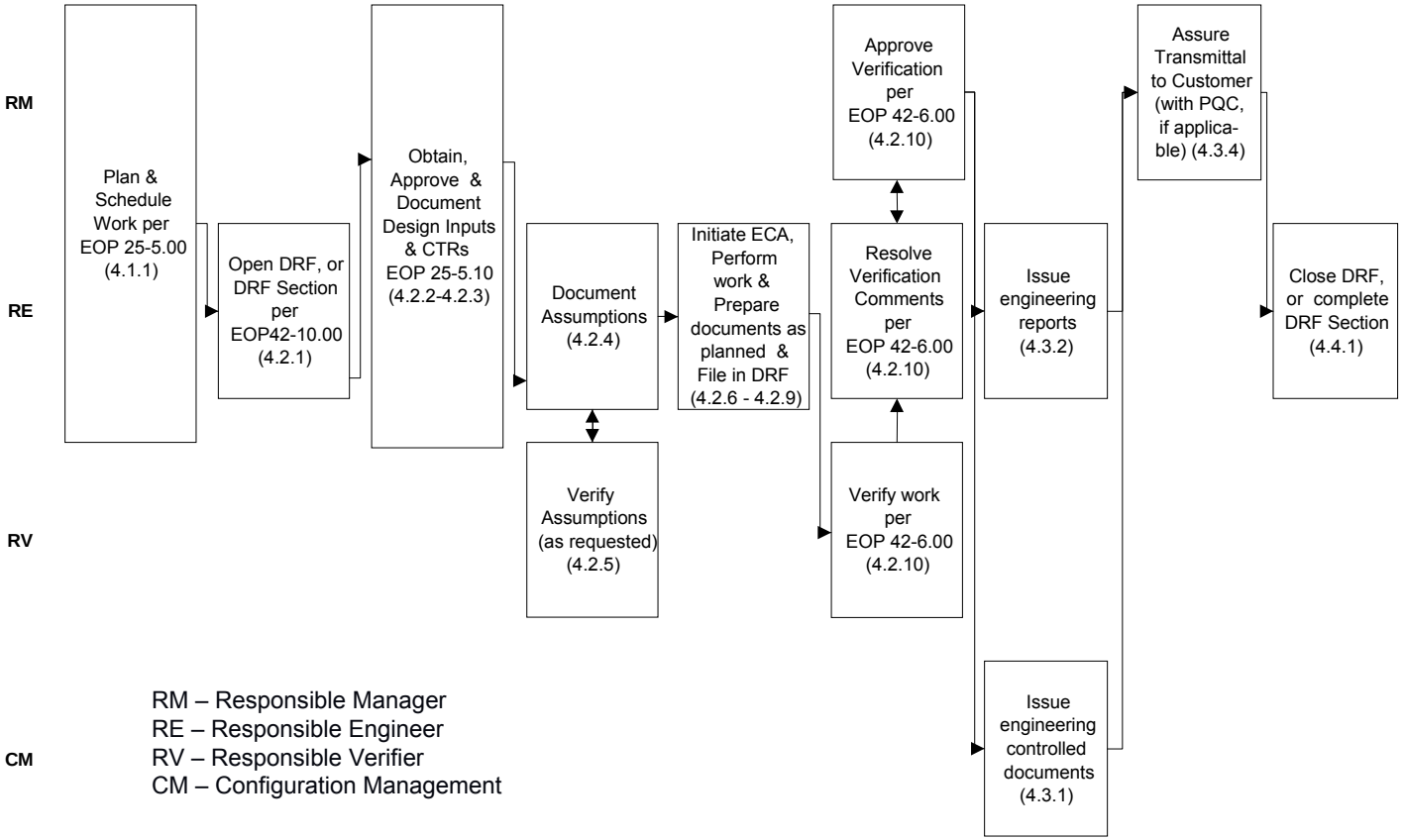
Configuration Management

Allen Dubberley

ESBWR
Project Management Document Hierarchy



GE Energy – Nuclear
Design Process



Work Planning & Scheduling

EOP 25- 5.00

Work Performance

EOP 25 - 5.10
EOP 40 - 3.00
EOP 40 - 9.00
EOP 40 - 9.20
EOP 40 -12.00
EOP 40 -17.00
EOP 42 - 6.00
EOP 42 - 6.10
EOP 42 -10.00
EOP 55 - 2.00
EOP 65 - 2.00
EOP 65 - 2.10

Independent Verification

Deferred verification

Supplier Eng Services

Issue/Deliver Output Documents

EOP 30 - 5.00
EOP 42 - 1.00
EOP 42 - 4.00
EOP 42 - 5.00
EOP 42 - 8.00
EOP 45 - 4.00
EOP 60 - 3.10

ERM/ECN

Supplier Documents

Work Completion

EOP 42 -10.00

imagination at work

Draft Unverified

Independent Verification Requirements and eMatrix (eIV)

Randy Gonzales

ERM/ECN Document Requirements and eMatrix (ERM/ECN and eDRF)

Randy Gonzales

GE Infrastructure - Nuclear

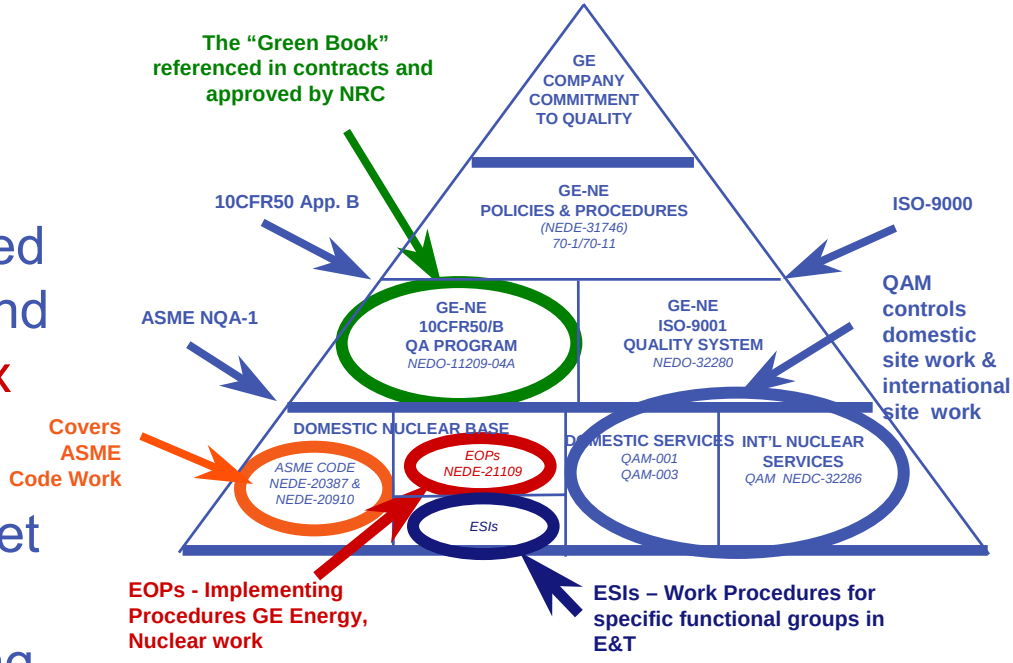
eMatrix Overview

Rev 0. – Q4-2006

imagination at work

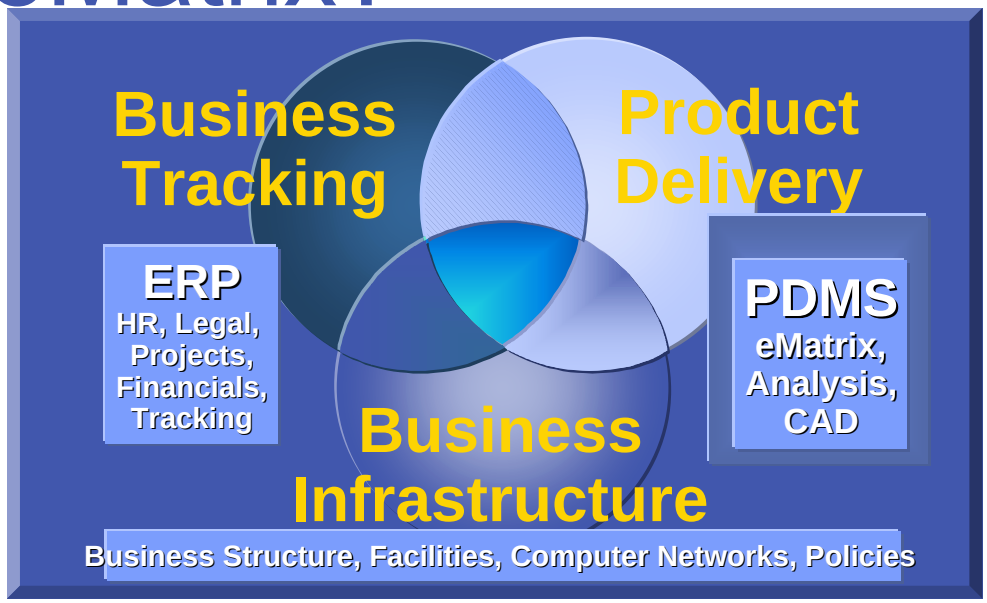
Nuclear Product Requirements

- GE Nuclear is required to establish and maintain a QA program that establishes design basis and configuration control.
- The program must be documented by written policies, procedures and instructions. (10CFR50 Appendix B, NQA1,"Green Book")
- As part of our requirement to meet the regulation we follow an industry standard for documenting designs.



The establishment of a Configuration Management System is part of our industry standard - including Document Control, Design and Change Process and Design Basis Methodology.

What is eMatrix?



Product Data Management System

- **Product** related engineering, services, manufacturing data related to delivery, business documents and enterprise processes
- **Data** stored in a regulatory compliant, web-based, secure vault
- **Management** that allows us to create, store, link, control, approve and retrieve all product related data using a standardized process
- **System** involves a global, integrated network that makes our workflow and information available 24x7

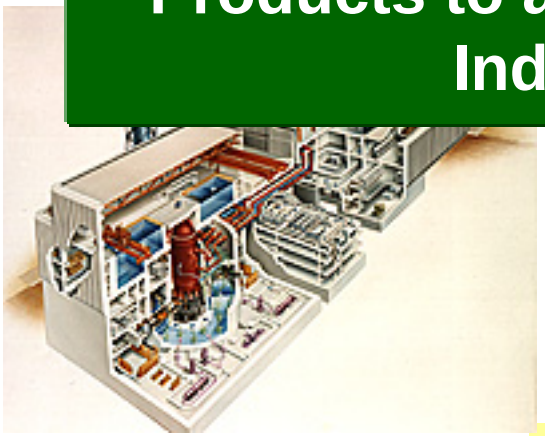
eMatrix in the Nuclear Business

- **Three main groups in GE Nuclear/Global Nuclear Fuels**
  - **Nuclear New Plants Business - Engineering and Construction**
  - **Nuclear Industry Services - Parts, Services and Training**
  - **Nuclear Fuel Manufacturing - Manufacturing, Delivery, Maintenance**

GENE/GNF

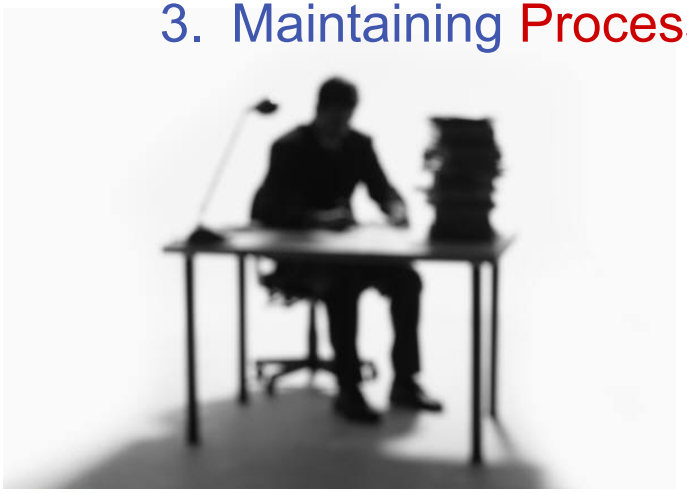
A diverse, global $Billion+ business

eMatrix is the Engineering Tool that enables our People to deliver Integrated Quality Products to a Global Energy Industry

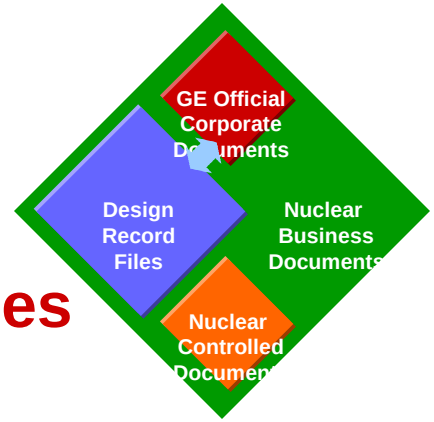


What is eMatrix

- eMatrix is the regulatory compliant electronic vault for general engineering information and company intellectual property
- The eMatrix environment is a PDMS system that includes:
  1. Storing Documents in a controlled environment
  2. Organizing Relationships between the documents based on how we do business
  3. Maintaining Processes to enable and control workflow



What is eMatrix - Documents



GE Corporate Documents

- Drawings
- Specifications
- Parts Lists
- Change Records (RMCN)

Design Record Files

- Design Basis
- Verification
- Design Review
- Audit Management

Nuclear Controlled Documents

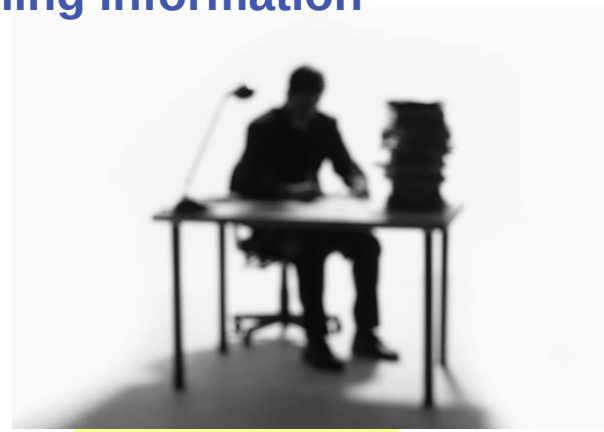
- NEDx Documents
- Field/Customer Notifications
- Instructions/Manuals/Procedures
- Controlled Reports
- Transmittals/Letters
- Procurement
- QA Records
- Vendor Information
- Outside Party Information
- Certifications/Calibrations
- Manufacturing Records

Nuclear Business Documents

- Presentations
- General Business Information
- Marketing documents
- Training Information

Each Document is controlled by

Type
Name
Revision



imagination at work

What is eMatrix - Relationships

Security
- Security Class
- Applications
- Vaults
- Families (OPI,etc)

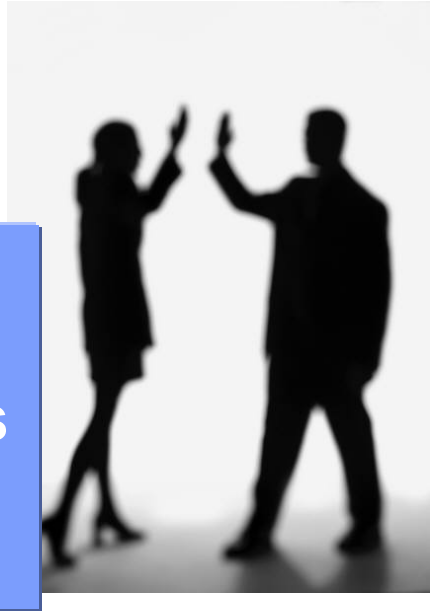
Approvals
- Account/Profile Changes
- Verification e-Signature
- Manager e-Signature

Supporting
- Supporting DRF's
- Supporting RMCN
- Supporting Procurement

Sub-group
- DRF Section
- File Objects

Process
- Promotion
- Rules for Approval
- Upload/Download/Checkout

Average of over 25 Relationships per eMatrix Object



What is eMatrix - System Processes

Security/Access Processes

- Corporate Security Enforcement
- Can't See What You Can't Access
- Separate Business Vaults
- Document Families and Linking

Approval Processes

- RE/RV/RM Roles Assigned
- Profile Change Approvals
- Verifications and Manager Approvals

Promotion/Release

- Verification Signature locks Access
- Delegates and Escalation
- Flex in Unincorporated Change
- Fully Compliant Revision Process

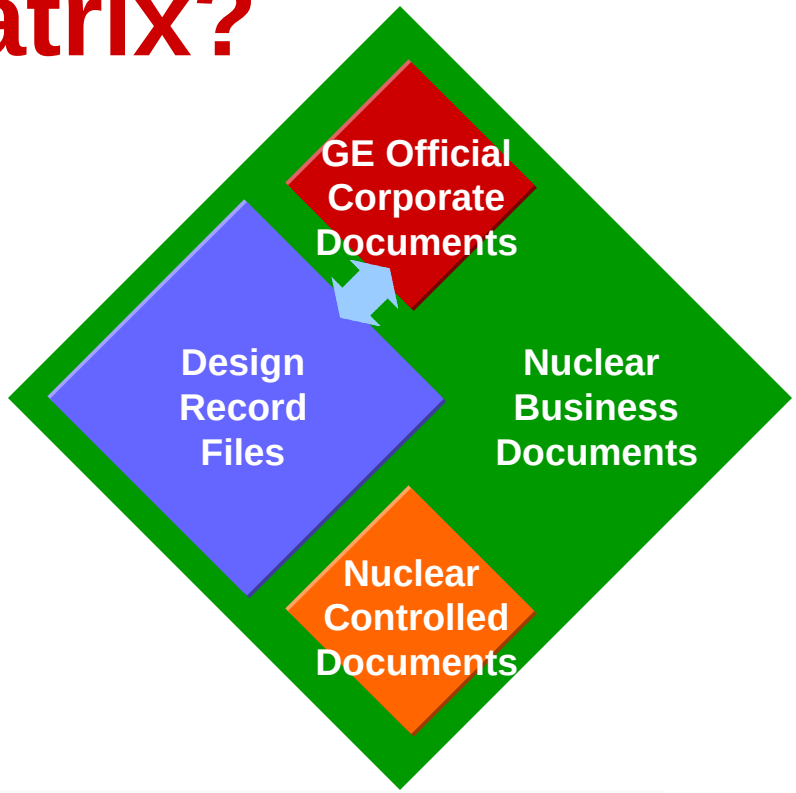
Review/Verification Processes

- Independent Verification Enforcement
- Flex in Changing Verifiers/Reviewers

Key Process Policies

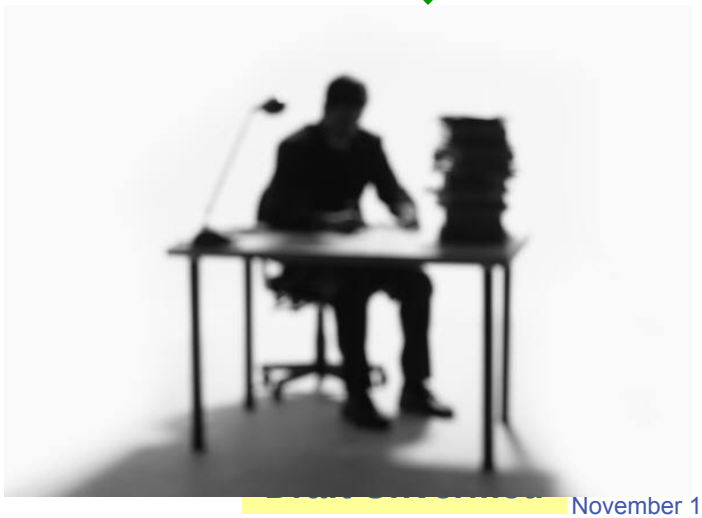
- P&P 70-50 - GE-NE Handling and Storage of Quality Assurance Records
- P&P 100-17 - Records Storage
- P&P 100-33 - Identification & Handling of GE Trade Secrets
- EOP 40-2.00 - Quality Information Systems
- EOP 42-1.00 - Design Process
- EOP 42-6.00 - Independent Design Verification
- EOP 42-8.00 - Document Initiation or Change by ERMECN
- EOP 42-10.00 - Design Record File
- EOP 75-6.00 - Quality Assurance Records
- NEDO 11209 - QA Program Description

What data is in eMatrix?

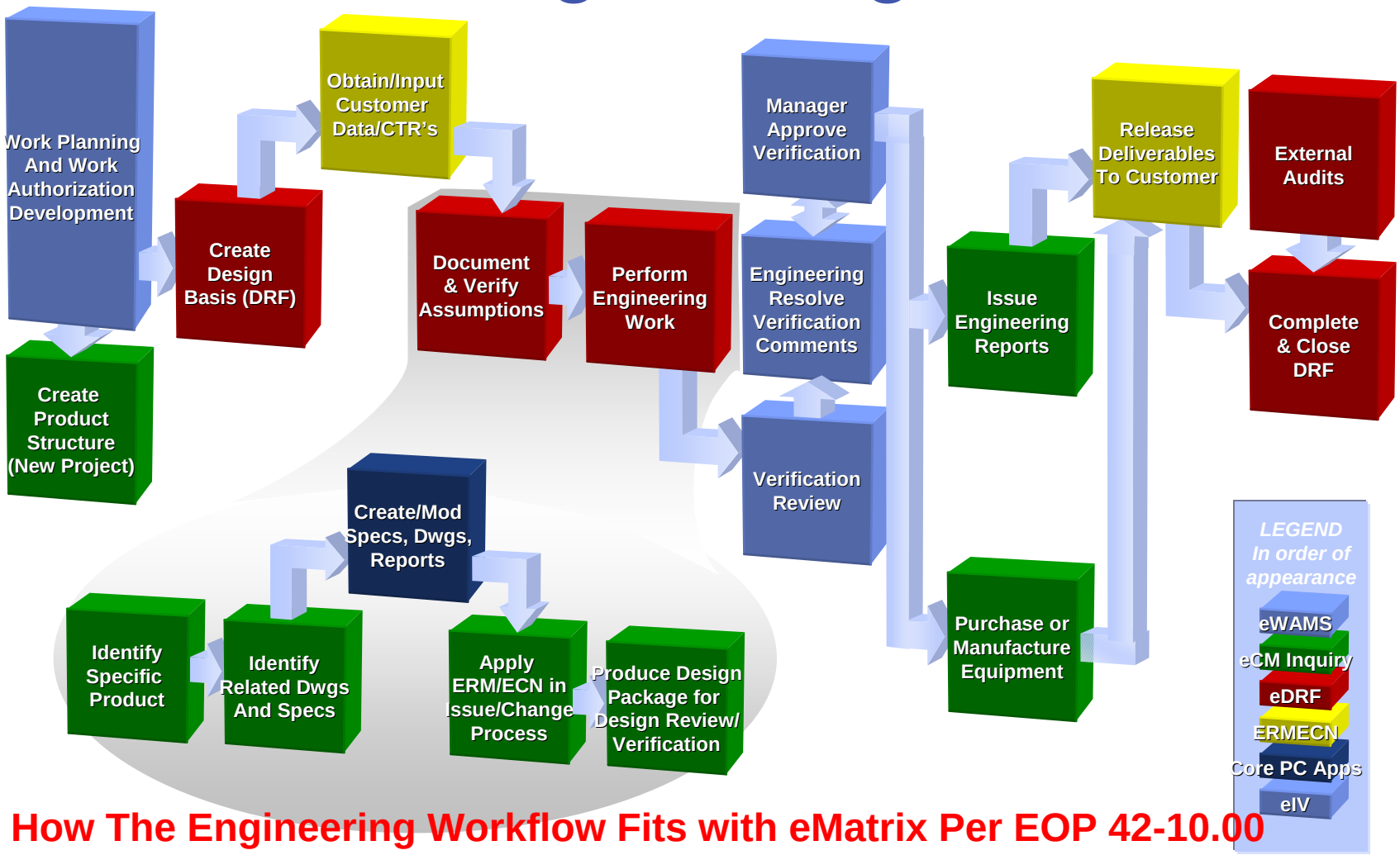


A few examples of the larger data sets in eMatrix

- Drawings, P/L, Specs 90,865
- Change Documents 10,863
- DRF/Legacy DRF 52,870
- DRF Sections 66,902
- Customer Order Docs 48,694
- GEK type Manuals 14,585



The eMatrix Engineering Process



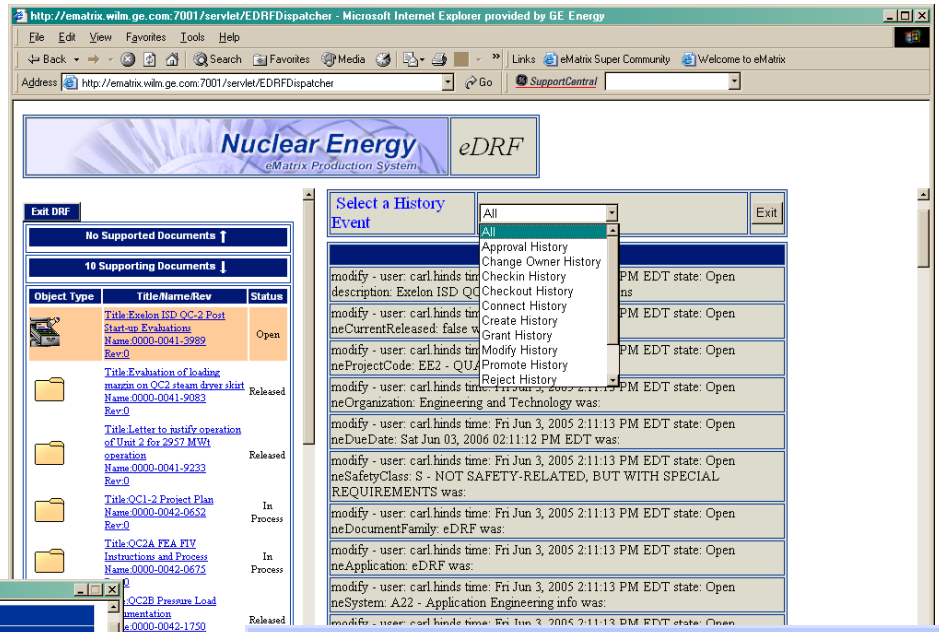
How The Engineering Workflow Fits with eMatrix Per EOP 42-10.00

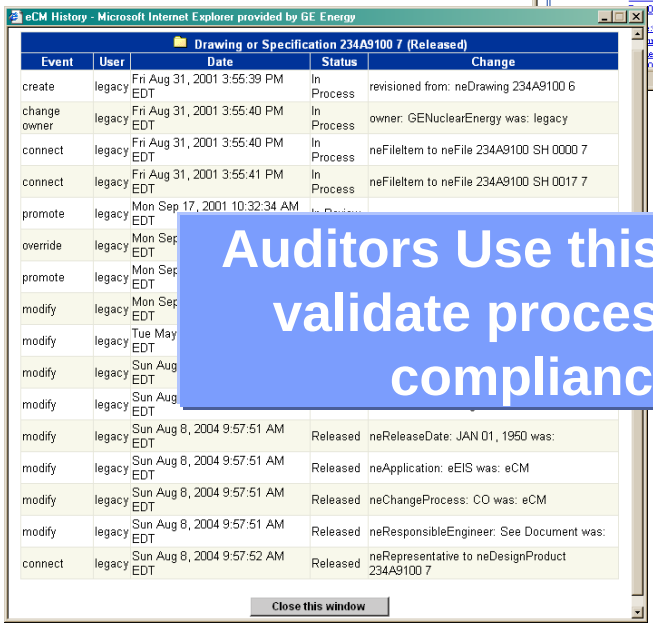
The Engineering Process involves **ALL** eMatrix Modules

eMatrix Audit History

All eMatrix Applications record EVERY action performed on an object, including:

- Date/Time Stamp
- Who Performed the Action
- Before and After condition
- Change Description





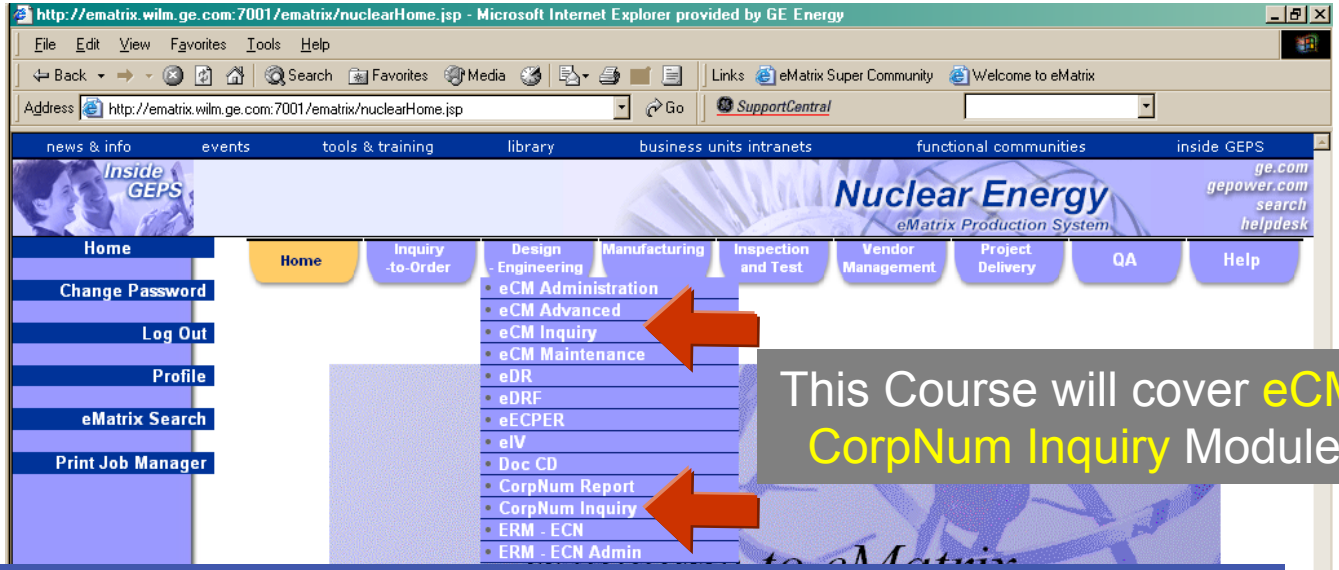
eMatrix Support Team Uses this data to resolve your questions

Auditors Use this data to validate process and compliance

imagination at work

Draft Unverified

Business Documents



This Course will cover eCM Inquiry and CorpNum Inquiry Modules in eMatrix

What we will cover:

Search, Attributes, Incorporated/UnIncorporated Changes, Prod Structure

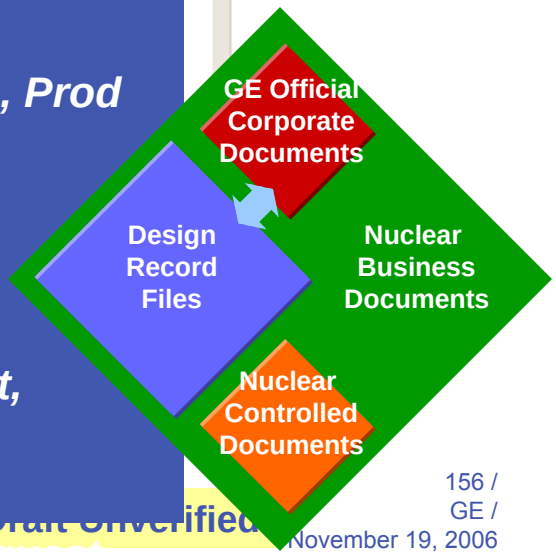
Nuclear Controlled Documents

Search, Families, View Attributes, Print, Batch Request

Design Record Files

Search in eCM, Navigator, Attributes, Print, Batch Request, Legacy

General Business Documents



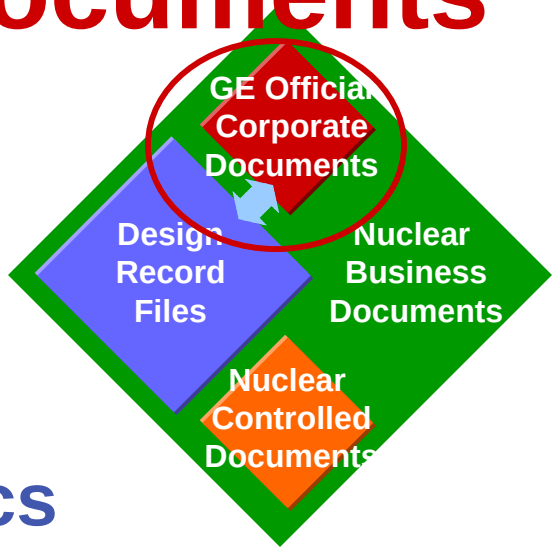
Corporate Controlled Documents

GE Corporate Documents

- Drawings
- Specifications
- Parts Lists

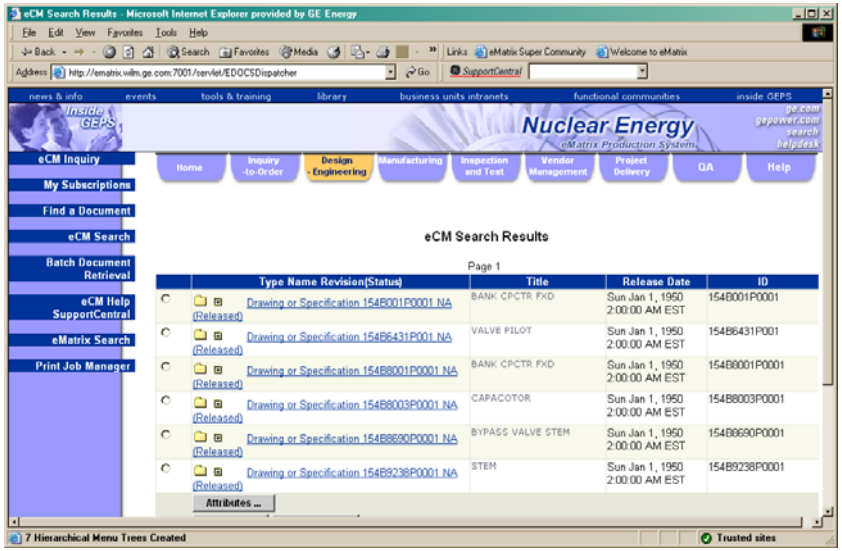
Documents

- Change Records (RMCN) ***Meta-data***



Characteristics

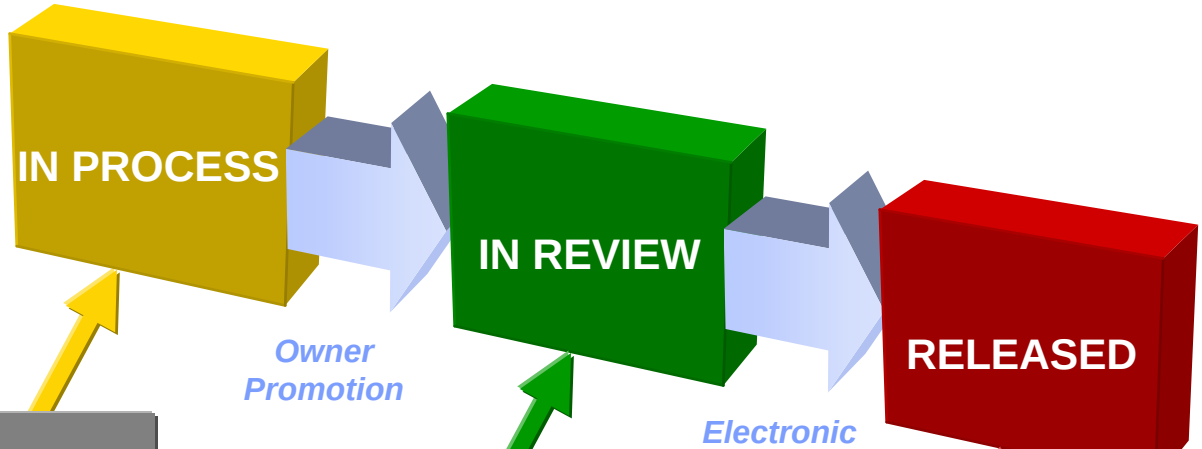
- Customer Deliverable - Our Product!
- Intellectual Property for GE
- All documents must be “issued” before delivery - full engineering process
- Must be applied to Plant and System
- Under full Regulatory Compliance in eMatrix
  - Optical Drive Storage
  - Independent Verification
  - Plant Life Retention/Retrievable
  - All Changes Controlled and Tracked



imagination at work

Draft Unverified

General and Issued Document States



In-Process
- In Process Section - PRIVATE
- Edit capability restricted to Owner/RE
- Only RE can promote to In-Review.

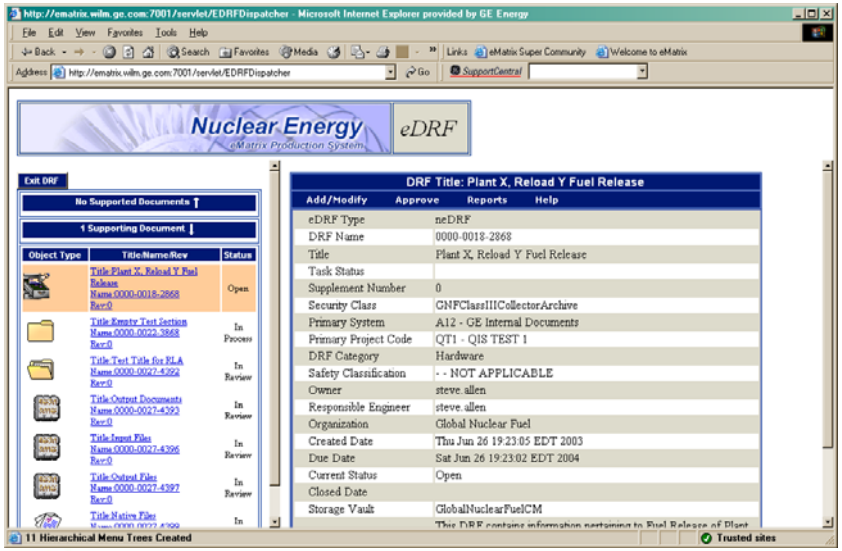
In-Review
- In Review Section - SHARED
- Collaborative object lets workgroup load documents, review data
- If no Verification required, RE can promote to Released.

Released
- LOCKED – changes made by Revision only
- Archive Objects to Optical Storage (TIFF,PDF,ASCII only)
- All Closed Documents are View Only and under Rev Control

Nuclear Controlled Documents

Design Record Files

- Design Basis
- Verification
- Design Review
- Audit Management

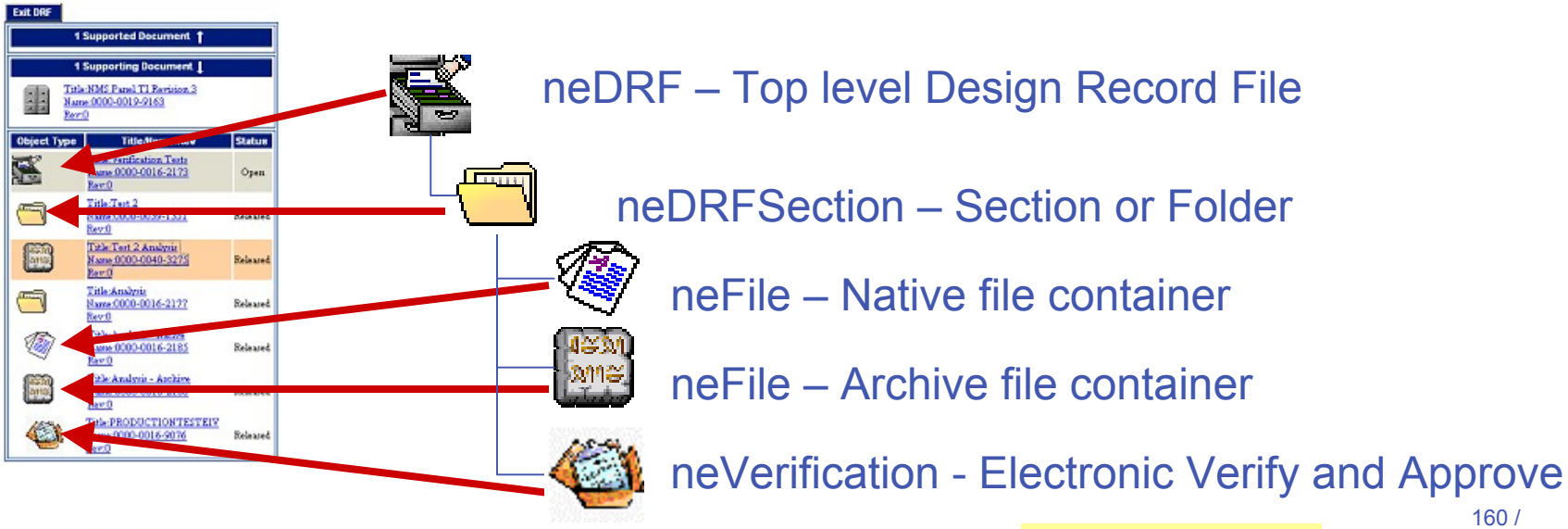


Characteristics

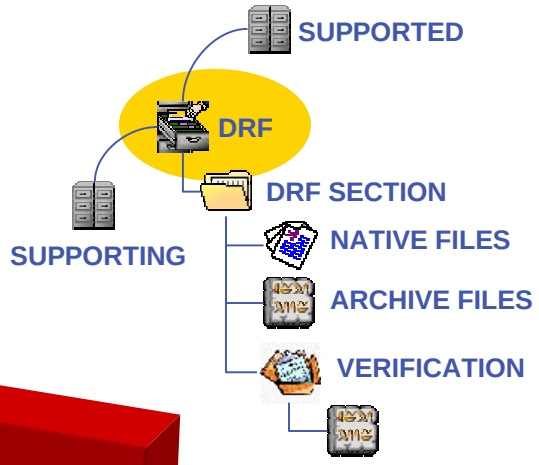
- Design Basis - without recourse to the originator
- Data Collector for ongoing work
- Under full Regulatory Compliance in eMatrix
- Independent Verification or Design Review linked
- Proof of Design to auditors and quality review

What is a DRF?

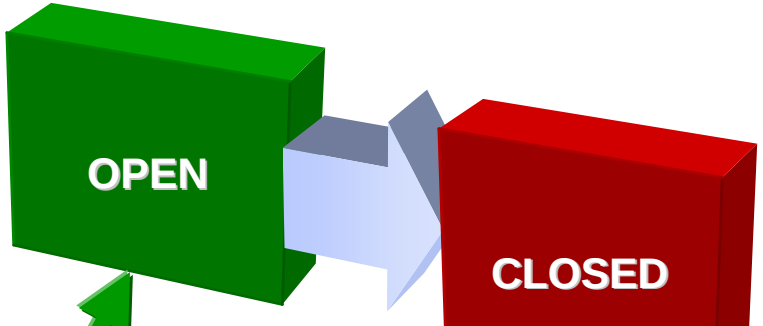
- Capture the Design Process as you do your work
- Obtain Electronic Verification and approvals
- Collector for regulatory compliant deliverable design data (Archive)
- Convenient and traceable Storage for work in progress (Native)
- Link to Issued Documents and Reference Work
- Regulatory Record of your Completed Design



DRF Data States



Top Level DRF's are only "Open" or "Closed"



Electronic Approval

In-Review = OPEN DRF
- Open DRF - SHARED
- Like In Review State for Issued docs
- Promotion to Closed State requires Reviewer/Manager electronic approval

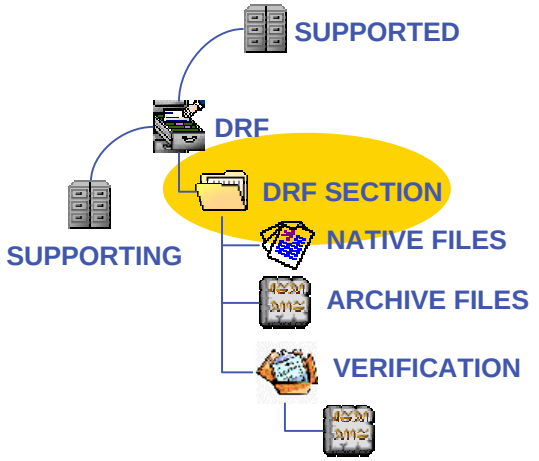
Released = CLOSED DRF
- LOCKED – changes made by Supplement only
- Archived to Optical (TIFF,PDF,ASCII)
- All Closed DRF Objects are View Only and under Rev Control

eMatrix Issued Documents and DRF Sections have 3 Data States – Top Level DRF's have only 2

DRF Section States
includes File Objects

DRF Sections are "In Process", "In Review" or

Electronic Approval



In-Process
- In Process Section - PRIVATE
- Edit capability restricted to Owner/RE
- If eIV Verification required set switch to Yes, then create eIV and connect to Section before promotion to In-Review
- If no eIV Verification required, RE can promote to In-Review.

In-Review
- In Review Section - SHARED
- Promotion to Released State requires eIV object (if switch set to Yes) and Verifier/Manager electronic approval
- If no Verification required, RE can promote to Released.

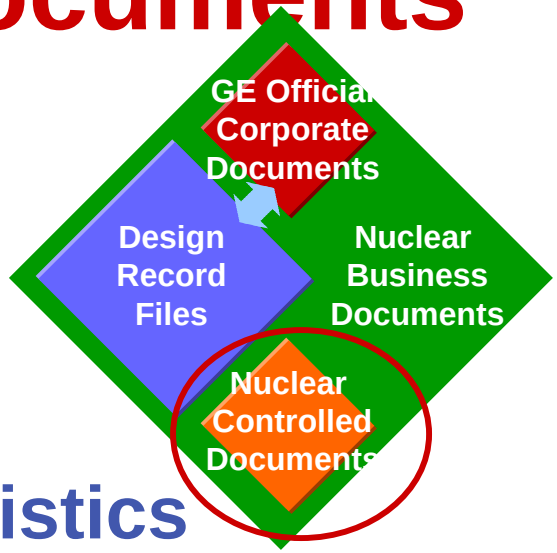
Released
- LOCKED – changes made by Revision only
- Archived to Optical (TIFF,PDF,ASCII only)
- All Closed DRF Sections are View Only and under Rev Control

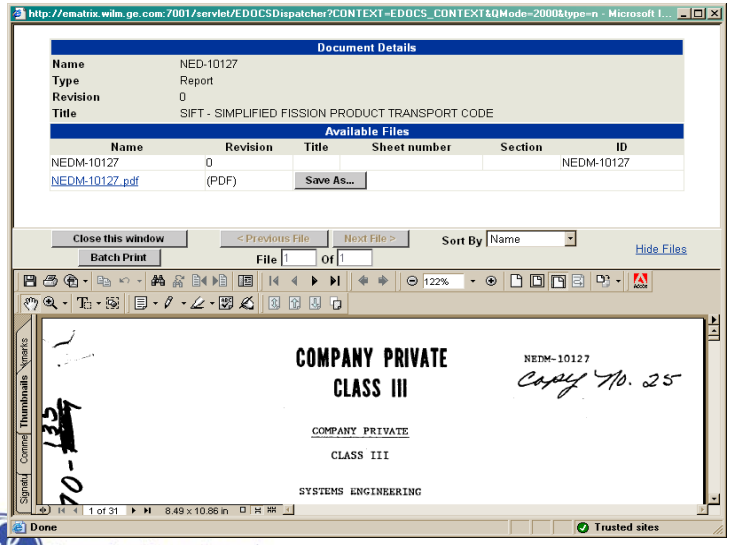
Note: An eIV signature Locks the associated In-Review Section
(See Promotion Training Module)

Nuclear Controlled Documents

Nuclear Controlled Documents

- NEDx Documents
- Field/Customer Notifications
- Instructions/Manuals/Procedures
- Controlled Reports
- Transmittals/Letters
- Procurement/Vendor Information
- QA Records
- Outside Party Information
- Certifications/Calibrations
- Manufacturing Records

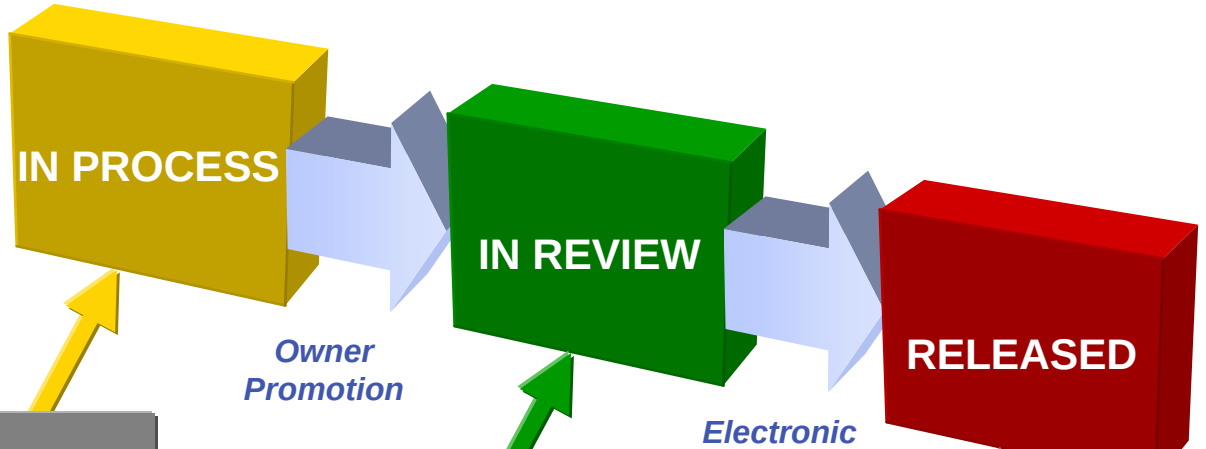




Characteristics

- Maintain a GENE Tracking Number
- Intellectual Property for GE Nuclear
- Referenced for Engineering, Manufacturing or Order Fulfillment
- Require a secure storage and accountable medium beyond shared drive -all actions stored in history file

General Document States



In-Process
- In Process Section - PRIVATE
- Edit capability restricted to Owner/RE
- Only RE can promote to In-Review.

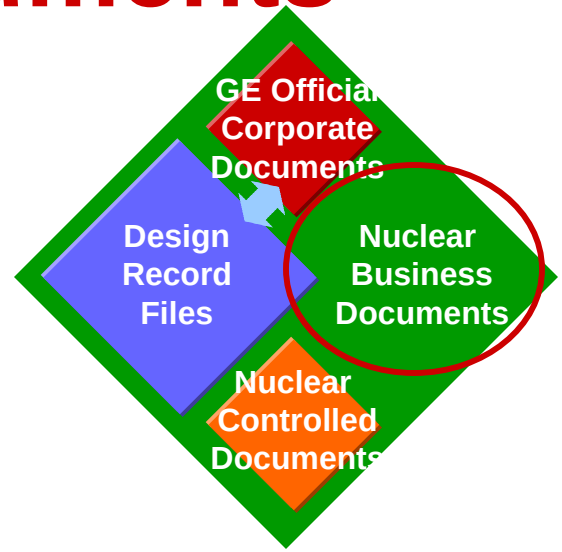
In-Review
- In Review Section - SHARED
- Collaborative object lets workgroup load documents, review data
- If no Verification required, RE can promote to Released.

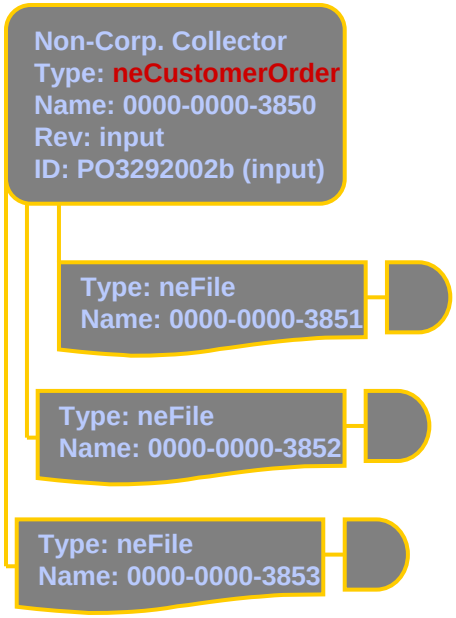
Released
- LOCKED – changes made by Revision only
- Archive Objects to Optical Storage (TIFF,PDF,ASCII only)
- All Closed Documents are View Only and under Rev Control

Nuclear Business Documents

Nuclear Business Documents

- Third Party or Outside Party Information
- General Secure Business Documents
- Marketing documents
- Training Information/Curriculum

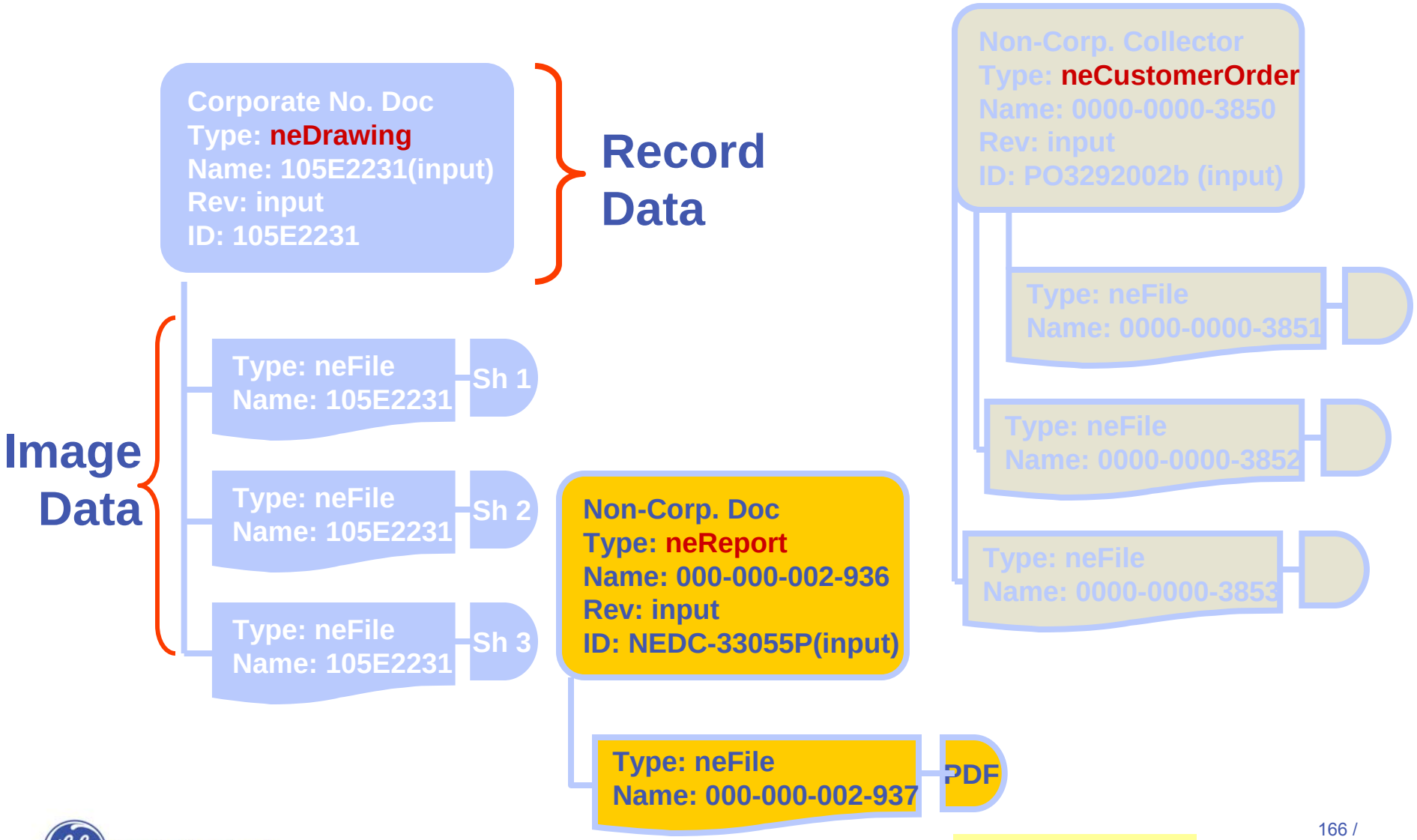




Characteristics

- Requires secure storage beyond shared drive folders with limited access (named user access per folder)
- Must fit in a document family for creation/ building and tracking
- Storage recommended by policy/procedure for QA retention over 5 years (100-33, 70-50)
- Third Party or Outside Part Info of proprietary nature

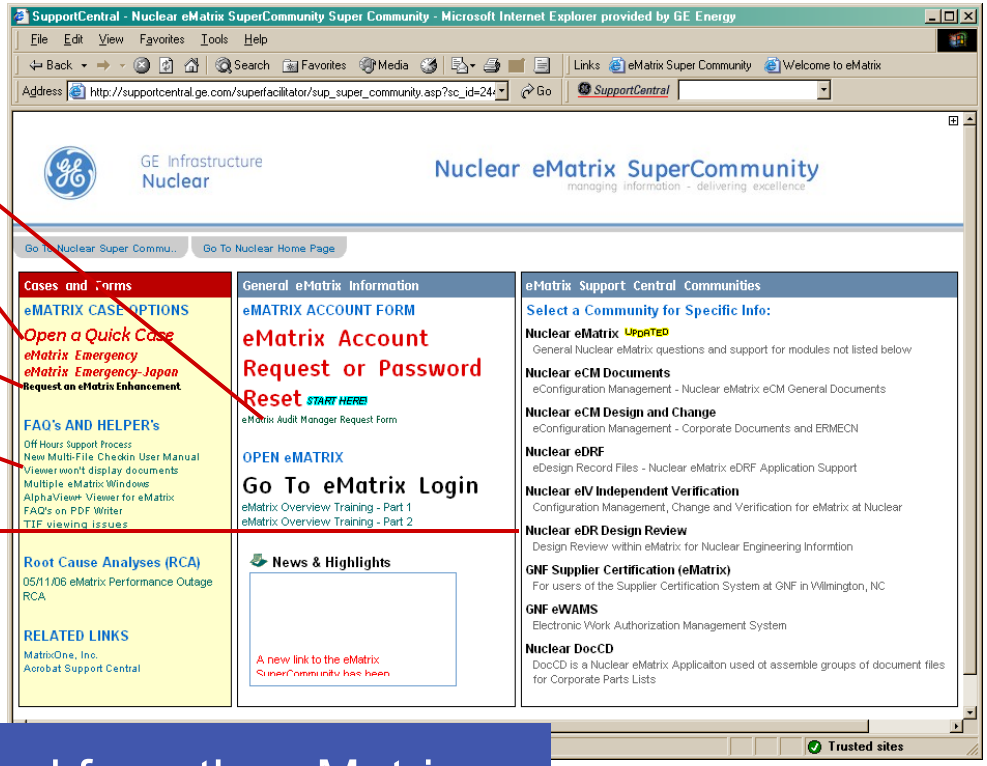
eCM Maintenance Document Diversity



eMatrix SuperCommunity - A word about support

Key Features:

- **Automated Account Requests**
- **QuickCases for local response**
- **Escalate emergencies**
- **FAQ and Helps**
  - Viewer Problems
  - PDF Questions
  - Multi-file Checkin
- **Detailed Sub-communities**
  - Nuclear eMatrix - Overall
  - eCM Documents
  - ERMECN
  - eDRF
  - eIV/eDR
  - Supplier Cert
  - eWAMS
  - DocCD



Linked from the eMatrix Login Page as a Centralized starting point for all eMatrix

Nuclear eMatrix - The "Business Backbone"

eMatrix is the regulatory compliant electronic vault and process enabler for engineering information and company intellectual

Regulatory Vault storage for Documents

- Secure 5 terabytes available 24x7 globally

Engineering Relationships between Functions

- Role-based Business Model defines document relationships

Guided and Rule-Based Embedded Processes

- Helping people implement their responsibility

The way we do engineering…

- Integrated ideas, design basis, analysis, specification, verification, approvals, promotion, vaulting and change

imagination at work

GE Infrastructure - Nuclear

Your Turn…

QUESTIONS?

imagination at work

GE Infrastructure - Nuclear

Remember: eMatrix is a tool - it is still our people who deliver the best products to our customers!

THANK YOU!

imagination at work

Software Overview

Rich Miller and Tom Jenkins

High Quality Software Development Process

- Completeness
- Consistency
- Correctness
- Style
- Traceability
- Unambiguity
- Verifiability

High Quality Software Development Process

Completeness

Those attributes of the planning documents, implementation process documents and design outputs that provide full implementation of the functions required of the software. The functions which the software is required to perform are derived from the general functional requirements of the safety system, and the assignment of functional requirements to the software in the overall system design.

Improvements

- Requirements documented in the plans
- Standards re-evaluated
- Top Down Traceability from DCD and Regulatory Bases shall be performed

High Quality Software Development Process

Consistency

The degree of freedom from contradiction among the different documents and components of a software system. There are two aspects to consistency. Internal consistency denotes the consistency within the different parts of a component for example, a software design is internally consistent if no set of design elements are mutually contradictory. External consistency denotes the consistency between one component and another for example, software requirements and the resulting code are consistent with one another if there are no contradictions between the requirements and the code.

Improvements

- **Spec references corrected,**
- **Document titles corrected,**
- **Adherence to BTP Structure**

High Quality Software Development Process

Correctness

The degree to which a design output is free from faults in its specification, design, and implementation. There is considerable overlap between correctness properties and properties of other characteristics such as accuracy and completeness.

Improvements

- **Document titles corrected**
- **Organizational correctness**
- **Standards mapped/applied**

High Quality Software Development Process

Style

The form and structure of a planning document, implementation process document or design output. Document style refers to the structure and form of a document. This has connotations of understandability, readability, and modifiability. Programming style refers to the programming language characteristics of the software and programming techniques which are mandated, encouraged, discouraged, or prohibited in a given implementation.

Improvements

- **GEEN standard document style and ESBWR DCD Writer's guide applied to LTRs**
- **GEEN references do not have revisions numbers inside the documents. eMATRIX captures revision numbers.**

High Quality Software Development Process

Traceability

The degree to which each element of one life cycle product can be traced forward to one or more elements of a successor life cycle product, and can be traced backwards to one or more elements of a predecessor life cycle product.

Improvements

- **Traceability Matrix of plans to DCD requirements, reg guides, and IEEE standards,**
- **Independent Verification of Results**

High Quality Software Development Process

Unambiguity

The degree to which each element of a product, and of all elements taken together, have only one interpretation.

Improvements

- **Common definition of “requirements” and “traceability”,**
- **Organization clarification**
- **Document Titles**

High Quality Software Development Process

Verifiability

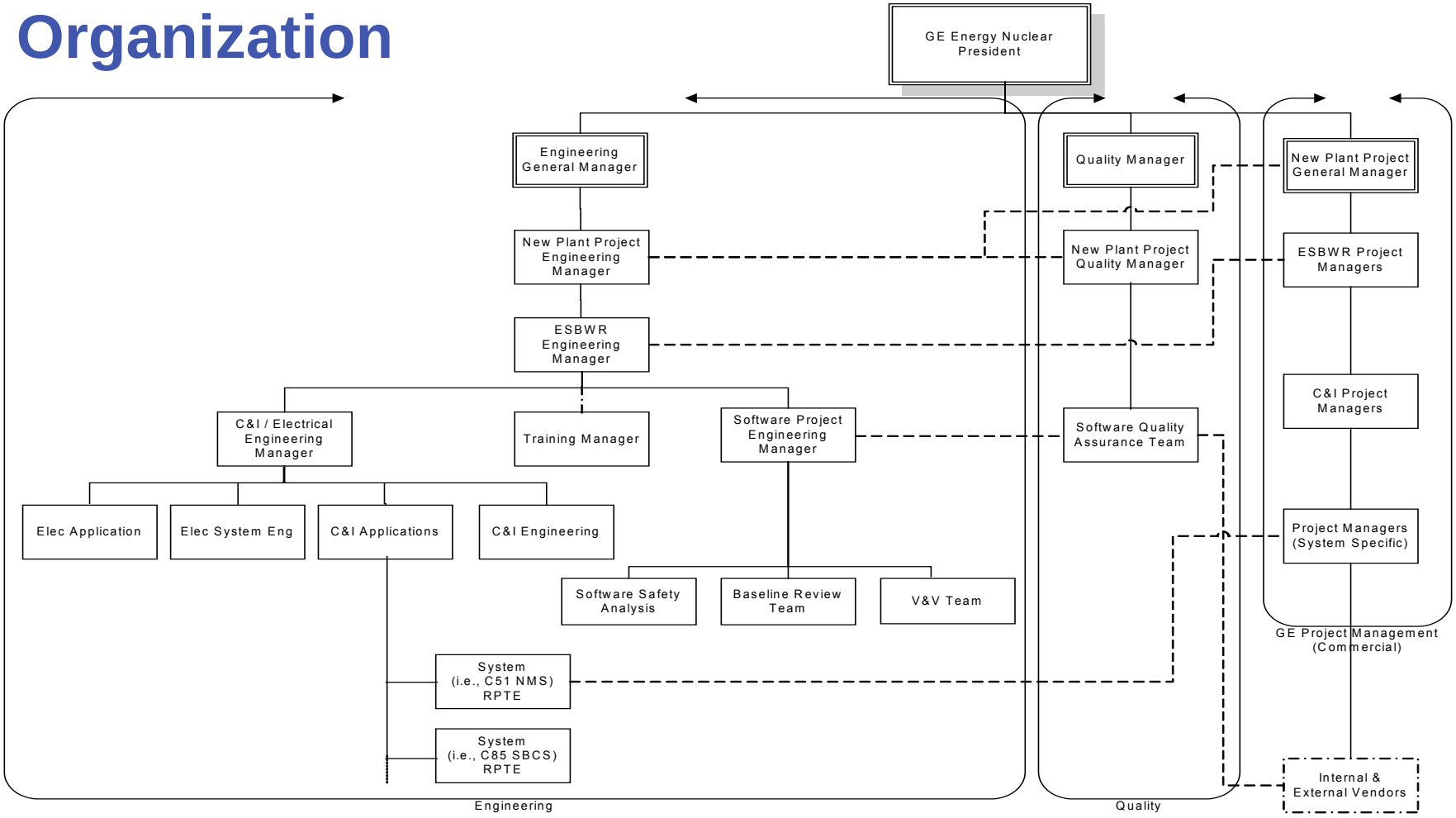
The degree to which a software planning document, implementation process document or design output is stated or provided in such a way as to facilitate the establishment of verification criteria and the performance of analyses, reviews, or tests to determine whether those criteria have been met.

Improvements

- **Independent verification of the plans**
- **QA oversight of SQA activities**

ESBWR Instrumentation & Controls - NRC Audit

Organization



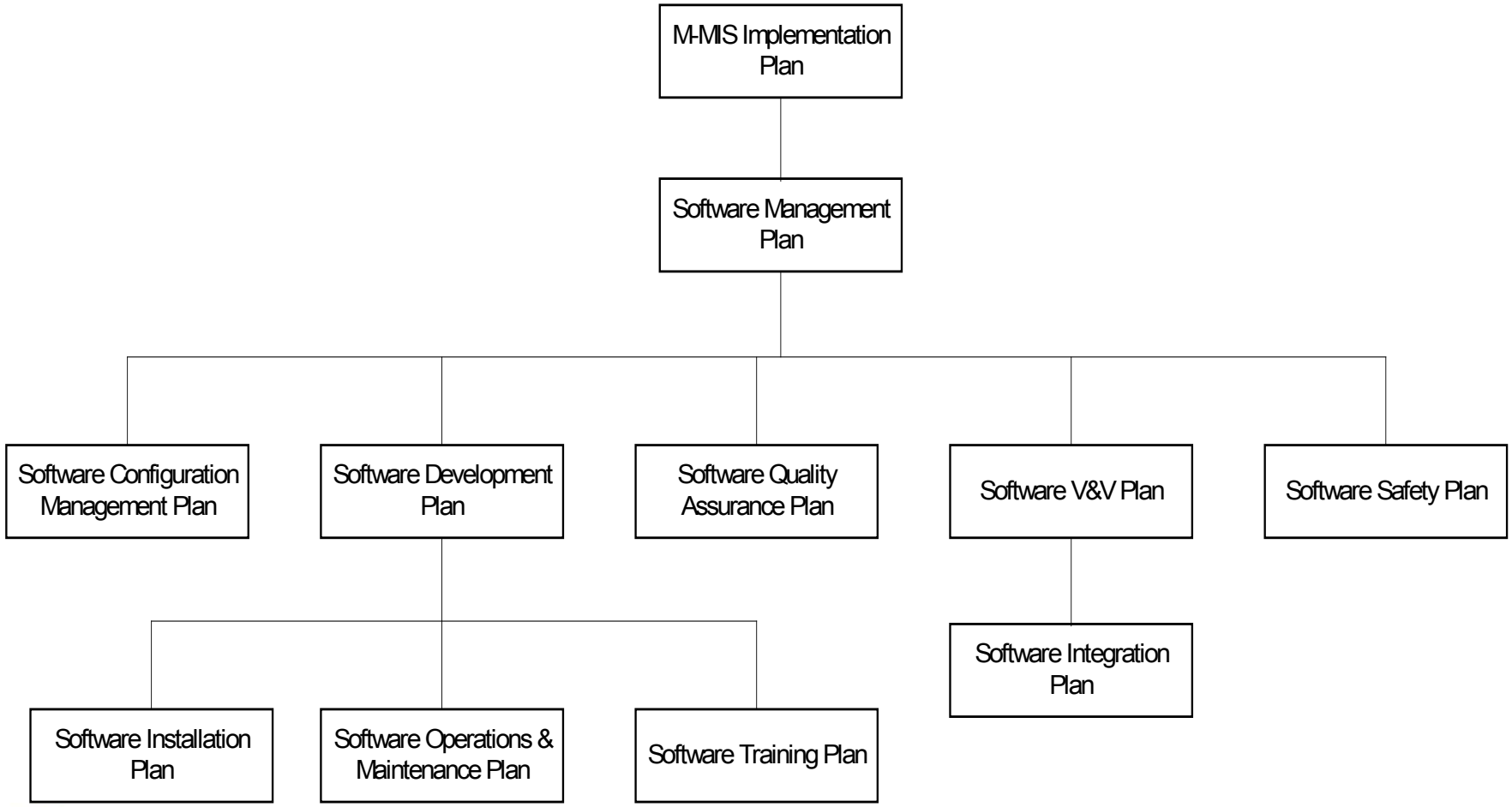
ESBWR Instrumentation & Controls - NRC Audit

High Quality Software Development Process

Summary

GE is extensively rewriting the plans to clarify fundamental concepts and requirements. The plans are in draft unverified form but available for proprietary session inspection during this visit. Proprietary verified releases are expected in December ’06 and February ‘07. QA engaged in oversight.

ESBWR I&C Software Plan Structure



ESBWR Instrumentation & Controls - NRC Audit

Sample from SQA Plan

Software Life Cycle Activities	Design Outputs	Responsible Organization	SQA Activities	Procedure / Process	V&V Organization	SQA Output
Implementation Phase	Source Code	Design Team	Module Testing	SIntP [2.1.2(7)]	Q - Design Team & VVT N - Design Team	Module Test Report
	Module Test Report		Independent Verification	Q - SVVP N - EOP 42-6.00 [2.1.2(6a)]	Q - VVT N - Design Team	Q - Verification Package and V&V Review Report N - Verification Package
	If applicable, Support Software/Tool and Third Party Software and its documentation package					
	If applicable, Previously Developed Software Evaluation Report and supplemental documentation					
			Software Safety Analysis	SSP [2.1.2(5)]	SST	Q - Software Safety Analysis Report
			Baseline Review	SVVP [2.1.2(3)] & SCMP [2.1.2(2)]	BRT	Baseline Review Record

Sample Traceability of Plans

Diverse Protection Systems

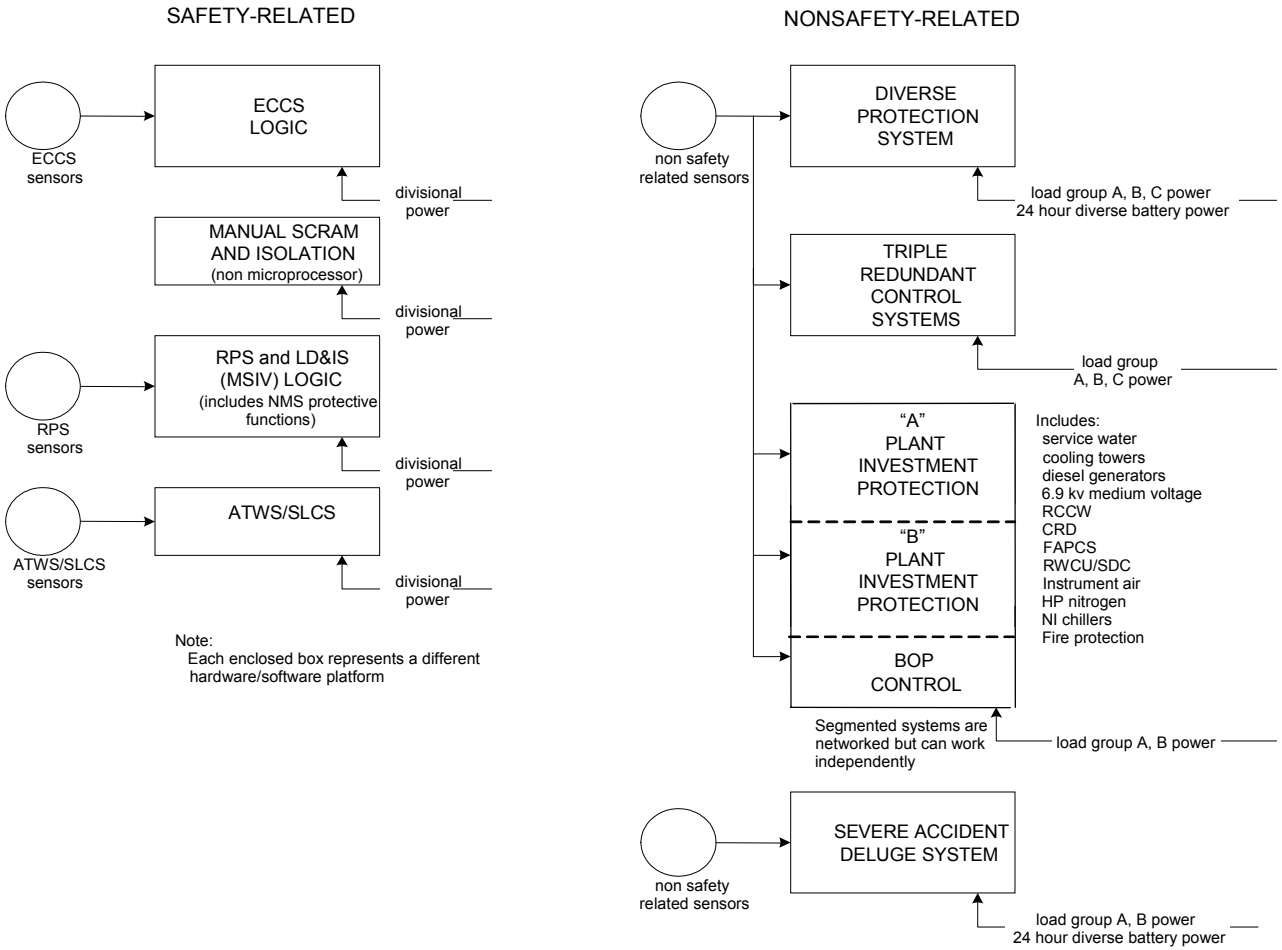
ESBWR Instrumentation & Controls - NRC Audit

ESBWR Diverse Protection System

- Can obtain any safety data from dedicated gateway data links
- Can obtain any nonsafety data using its own RMUs or the plant nonsafety network
- Provides backup scram and MSIV isolation functions
- Provides backup non-MSIV isolation functions
- Provides backup ADS and GDCS functions
- Can initiate SLCS
- Can initiate SCRRI, all control rod run in, feedwater runback
- Initiates level 8 turbine trip and FW runback
- Initiates level 9 FW pump trip
- Triply redundant reliable against inadvertent actuation
- Non fail safe logic
- On GENE network and can be controlled by GENE control room displays

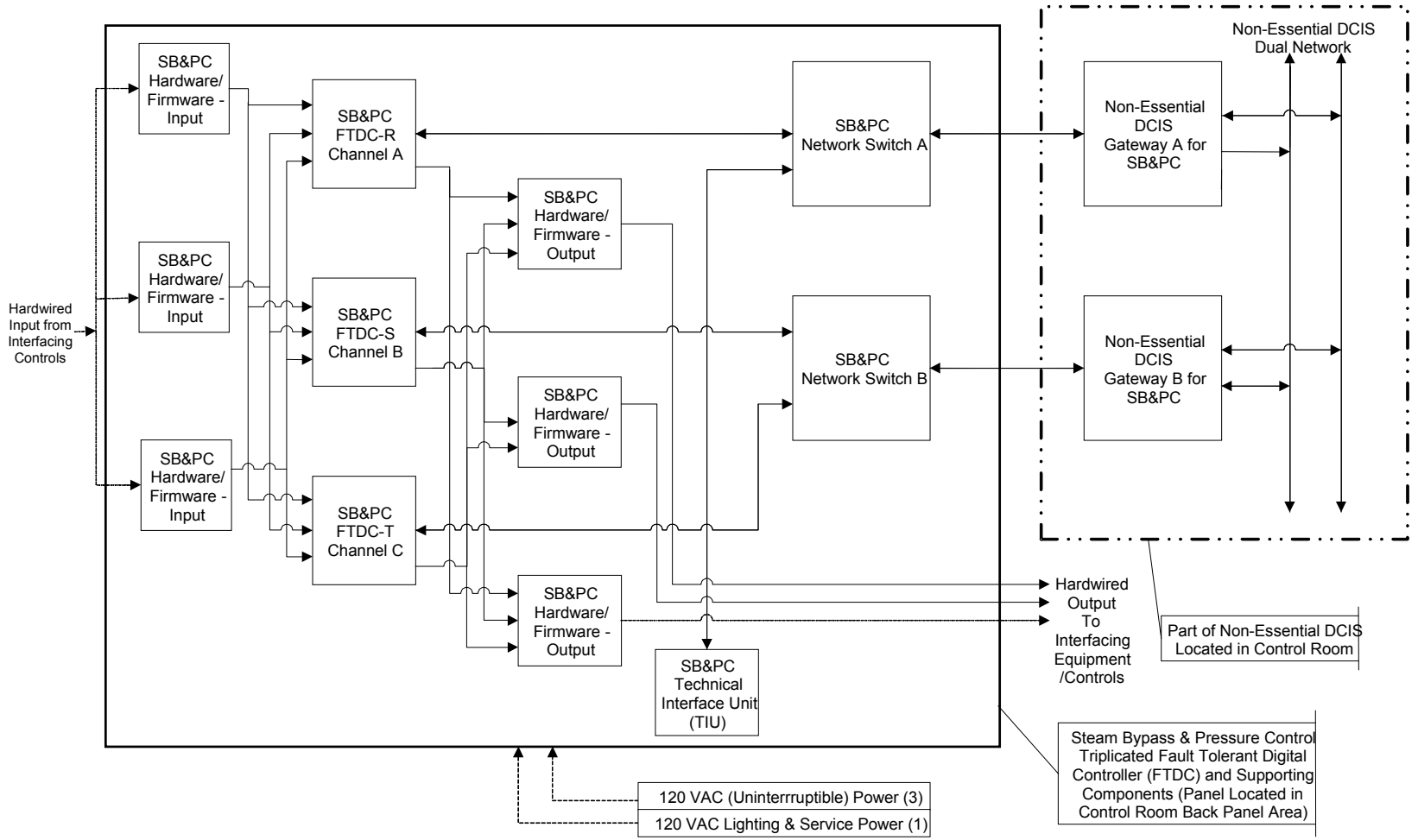
ESBWR Instrumentation & Controls - NRC Audit

DCIS Power & Sensor Diversity



ESBWR Instrumentation & Controls - NRC Audit

Fault Tolerant Digital Control System – Mark VIe



ESBWR Plant Investment Protection

- Plant investment protection takes advantage of network switch capability by segmenting specific DCIS functions
- "A" and "B" PIP functions are segregated to different controllers
- PIP A controllers are connected to PIP A network switch
- PIP B controllers are connected to PIP A network switch
- Main control room displays segregated into PIP A, PIP B, BOP and GENE network switches
- Individual segments are still dual redundant
- Result is that normally all nonsafety controllers and displays can do all functions but any network switch group can be lost without affecting operation of the other groups
  - > i.e. Diesel generator A can be monitored, alarmed and controlled separately from diesel generator B

COL Participation in IC Design Process Life Cycle Activities

Ray Reith

ESBWR Instrumentation & Controls - NRC Audit

- Review and Comment of Draft Revisions of Design Control Documents
- Review and Comment of NRC Request for Information and GE responses
- Detailed Draft COL presentations to discuss potential COL Actions
- Assignment of COL Holder Operating personnel (SRO Type) to GE Human Factors Organization
- Periodic Technical Overviews
- Monthly DCWG Interactions with NRC on ESBWR COLs

ITAAC Update

Rich Miller, Steve Zander and Steve Kimura

ESBWR Instrumentation & Controls - NRC Audit

- Background
- Identify I&C systems to be included in Design Acceptance Criteria (DAC) process with ITAAC in DCD Tier 1 document
- Discuss the DAC selection criteria
- Discuss the I&C systems design process ITAAC
- Discuss other I&C system-specific ITAAC issues

Background

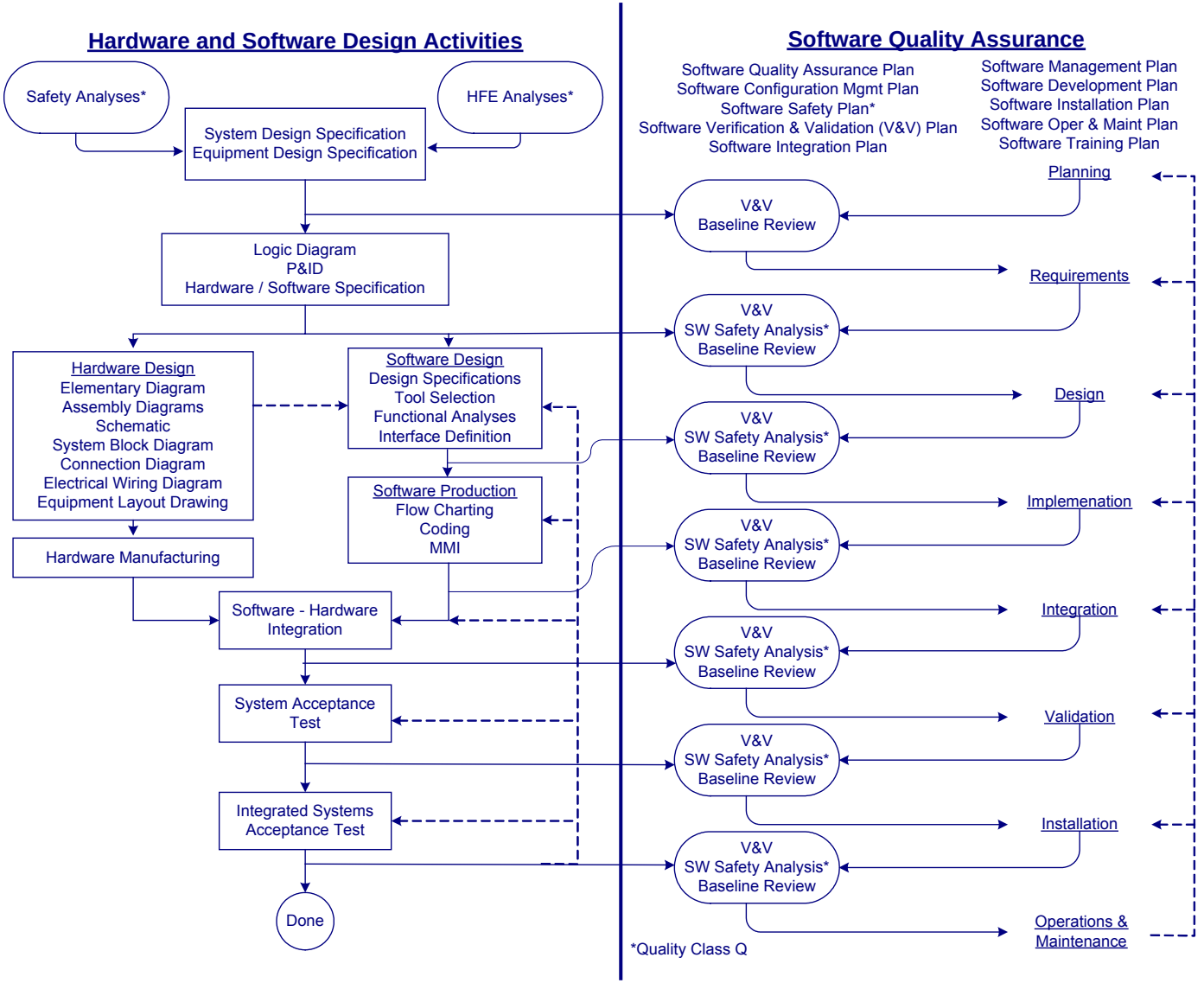
ESBWR Instrumentation & Controls - NRC Audit

- E-DCIS (safety-related)
  - SSLC/RTIF
    - RPS
    - LDIS (MSIV only)
  - SSLC/NMS
    - SRNM
    - APRM
    - LPRM
    - OPRM
  - SSLC/ESF
    - ECCS (ADS, GDCS)
    - PCCS (mechanical only)
    - LDIS (non MSIV)
  - ATWS
    - FWRB
    - SLCS
  - ICS
  - PRNM
- NE-DCIS (nonsafety-related)
  - RTNSS (Graded approach - Presented separately)

ESBWR Instrumentation & Controls - NRC Audit

- Safety-related or RTNSS and not previously Certified
- Rapidly changing technology based hardware
  - Microprocessor-based
  - Software intensive
  - Electronic component sensitive
  - Emerging industry standard based
- HFE driven
- Software

ESBWR Instrumentation & Controls - NRC Audit



ESBWR Instrumentation & Controls - NRC Audit

- IEEE Std. 603 Updates (DG1145)
  - Creating a set of standard ITAACs that can be applied to all I&C safety-related and/or RTNSS systems
  - Reviewing/updating existing DCD/Tier 1 ITAAC for conformance to IEEE Std. 603 requirements
    (with possible exception to channel separation and independence rules based on PRA evaluation showing the normal IEEE Std. 603 approach is less reliable)
  - Reviewing/updating DCD/Tier 2 for conformance to IEEE Std. 603 requirements
    (with possible exception to channel separation and independence rules based on PRA evaluation showing the normal IEEE Std. 603 approach is less reliable)

Commercial-Grade Dedication Process Per GE EOPs 45-1.00 and 65-2.20

Rich Miller and Bishara Kakunda

Equipment Qualification Process for Multiple Vendors and Configuration Control

Rich Miller, Wayne Marquino and Bishara Kakunda

ESBWR Instrumentation & Controls - NRC Audit

Requirements – Regulations, Codes and Standards

- 10 CFR 50 Appendix B
- 10 CFR 50.49
- Reg. Guide 1.100 - 6/88
- SRP 3.10 Seismic Qualification
- SRP 3.11 Environmental Qualification
- NUREG 0588 7/81
- IEEE 323-2003
- IEEE 344-1987

GE Program – Environmental Qualification – DCD Section 3.11

Environmental design conditions:

- Normal Operating Conditions
- Abnormal Operating Conditions
- Test Conditions
- Accident Conditions
- Post-Accident Conditions

Environmental Qualification

- GE Specification 24A7006 EQ
  - > 60 years
  - > Verified using methods and procedures of qualification as stated in IEEE 323
  - > The supplier shall specify qualified life, shelf life and activities of maintenance surveillance, periodic testing and any parts replacement required to maintain qualification of equipment provided.

Environmental Qualification

- Qualification Plan
- Specified Values - specified per location
  - > T max – Example – See Figure 1
  - > T min – Example – See Figure 1
  - > Qualified integrated dose
  - > Max pressure
  - > Qualified life
  - > Humidity
  - > Spray
  - > Qualification Report

ESBWR Instrumentation & Controls - NRC Audit

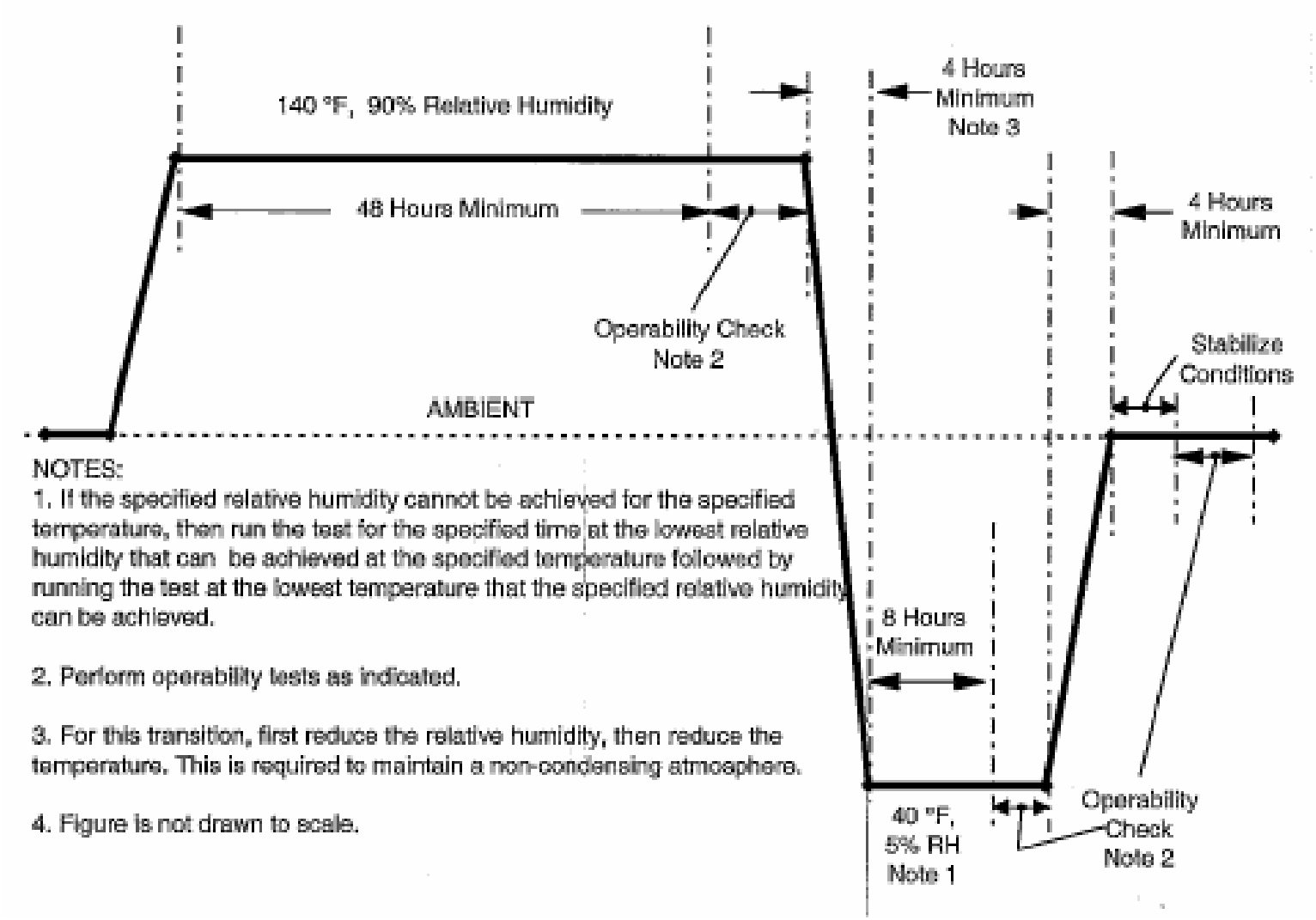


Figure 1

ESBWR Instrumentation & Controls - NRC Audit

Seismic Qualification

- IEEE Std 344
- Resonance Search
- Simulated Seismic Event
  - –SSE spectrum bounds ESBWR sites
- Test Response Spectrum
  - – example 10g @ 5% DAMPING
- Test Frequencies
  - – 1 TO 100 Hz
- Tri-Axial Vibration
- Monitor Specimen, Relay Contacts
- Post-Seismic Testing

Electromagnetic Qualification

- EPRI TR-102323 and Reg. Guide 1.180
  - "Guideline for Electromagnetic Interference Testing in Power Plants"
- EMI/RFI
  - Conducted Emissions
  - Radiated Emissions
  - Conducted Susceptibility
  - Radiated Susceptibility
  - High Frequency Transients
- Surge Withstand (Destructive) (as applicable)
- 1E/Non 1E Isolation (Destructive) (as applicable)

ESBWR Instrumentation & Controls - NRC Audit

Requests for Additional Information

- RAI 7.1-12 – IEEE 603 Safety System Criterion 5.4 Equipment Qualification
- RAI 7.3-4 - Instrument location and EQ requirements of the reactor vessel level and drywell pressure instrumentation

System Review / Audit Preliminary Simplified Logic Diagrams

Rich Miller, Dean Toukatly and Peter Yandow

ESBWR Instrumentation & Controls - NRC Audit

Primary Logics Package

System Number	System Name	Number of Simplified Logic Sheets
A10	Simplified Logic Standard	8
B21	Nuclear Boiler System (NBS)	16
B32	Isolation Condenser System (ICS)	4
C11	Rod Control and Information System (RC&IS)	14
C12	Control Rod Drive System (CRD)	6
C21	Leak Detection and Isolation System (LD&IS)	20
C51	Neutron Monitoring System (NMS)	15
C74	Safety System Logic and Control System (SSLC)	8
C85	Steam Bypass and Pressure Control System (SB&PC)	9
E50	Gravity-Driven Cooling System (GDCS)	10
T62	Containment Atmosphere Monitoring System (CMS)	9

Secondary Logics Package

System Number	System Name	Number of Simplified Logic Sheets
C31	Feedwater Control System (FWCS)	19
C71	Reactor Protection System (RPS)	16
G31	Reactor Water Cleanup / Shutdown Cooling System (RWCU / SCS)	15

RAIs in Process - I&C

Rich Miller, Peter Yandow and RAI Assigned Engineers (Backup)

ESBWR Instrumentation & Controls - NRC Audit

Outline

>Subject Areas

>Overall status

>RAI's

ESBWR Instrumentation & Controls - NRC Audit

Subject Areas

>DCIS Architecture/ FMEA

>Cyber Security

>Regulatory Requirements Applicability Matrix including IEEE 603

>Design Specifics including Soft control, SR/NSR Communications, Logic Diagrams, Testing

>Gamma Thermometer Design

>Communications – Physical and Software

>Software Controls

>DCD Clarifications

ESBWR Instrumentation & Controls - NRC Audit

Overall Status as of 11/15/06

>Completed design review - 38

>In Design review - 68

>Draft - 61

ESBWR Instrumentation & Controls - NRC Audit

Handouts

Samples

ESBWR Instrumentation & Controls - NRC Audit

RAI 7.1-12

How is the ESBWR design in conformance with IEEE-603 Safety System Criterion 5.4, Equipment Qualification?

IEEE-603-1991, Safety System Criterion 5.4, Equipment Qualification:

The application document (DCD, Tier 2) should confirm that the safety system equipment is designed to meet the functional performance requirements over the range of normal and worst case (e.g., any transient, accident or anticipated operational occurrence) environmental conditions where the equipment is expected to operate. The DCD,Tier 2, should address mild environment qualification and electromagnetic interference (EMI) qualification of safety system I&C equipment. The DCD should confirm that there is independence between environmental control systems and sensing systems that would indicate the failure or malfunctioning of environmental control systems. The application also should include confirmation that the environmental protection for instrument sensing lines conforms with the guidance of RG 1.151-07/1983, "Instrument Sensing Lines" and EMI qualification conforms with the guidance of RG 1.180, Rev.1,"Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation Control Systems." If some of the activities will be performed beyond the design certification stage, then the DCD should identify the COL action requirements. Appropriate ITAAC acceptance criteria should be proposed to verify the commitment.

ESBWR Instrumentation & Controls - NRC Audit

RAI 7.1-12 - Response

GE Response

The ESBWR utilizes safety-related system equipment designed to meet certain functional performance requirements including environmental conditions over the entire range during normal operations, transient, and accident conditions (includes both abnormal events and abnormal operational occurrences) for the area in which it is located.

The safety-related system equipment qualifications include electromagnetic interference qualification, seismic qualification, and other environmental condition qualification such as temperature, humidity, radiation, and pressure. Normal and accident environmental conditions under which safety-related equipment are required to perform, are identified in ESBWR DCD Tier 2 Table 3.2-1. To that extent, the ESBWR safety-related I&C systems are designed to meet all equipment qualification requirements as enveloped by the requirements of DCD Tier 2 Chapter 3 consistent with the requirements of IEEE Std. 603 which will be defined in NEDO-33294 Rev 0, "*ESBWR Instrumentation & Control Criteria for Safety-Related Control Systems*."

Currently the need for sensing line environmental control systems (freeze protection) is not anticipated in the ESBWR design. However, as site specific designs progress, if the need should arise where freeze protection is required, then electrical independence between the environmental control systems (freeze protection) and sensing systems will be provided in compliance with RG 1.151-07/1983 "*Instrument Sensing Lines"* as currently described in the DCD Tier 2 Chapter 8, Subsection 8A.3.1 "*Electric Heat Tracing."*

Electrical and electronic components in the I&C safety-related systems shall be qualified for anticipated levels of electromagnetic interference at the location for which it is to be installed. Electromagnetic compatibility (EMC) of I&C equipment will be verified through factory testing and site specific testing for both individual equipment and interconnected systems to meet EMC requirements for protection against:

- Electromagnetic Interference
- Radio Frequency Interference
- Electrostatic Discharge
- Electrical Surge Withstand Capability

In the ESBWR design, EMI qualifications follow the requirements as defined in Mil-Std-462D, Mil Std. 461D, and IEC Standard 801. The ESBWR safety-related I&C equipment is qualified to perform within specified ranges continuously even while exposed to EMI environmental limits at the hardware mounting location. EPRI Report TR-102323 "*Guidelines for Electromagnetic Interference Testing in Power Plants"* is used to define the envelope limits. To that end, EMI qualification for all safety related systems in the ESBWR design are consistent with the requirements of RG1.180, Rev 1 *"Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation Control Systems."*

EMC qualification requirements will be defined in the Licensing Topical Reports associated with the specific safety related system platforms scheduled for submittal to the NRC by December 30, 2006. The overall I&C development and qualification process, which includes a program to assess and mitigate the effects of electromagnetic interference, will be included as part of the DAC process to be included in DCD Tier 1 Revision 3 as addressed in RAI 7.2-28.

ESBWR Instrumentation & Controls - NRC Audit

RAI 7.3-4

Identify the instrument location and equipment qualification requirement of the reactor vessel level and drywell pressure instrumentation.

DCD, Tier 2, Revision 1, Section 7.3.1.1.3, "Safety Evaluation," stated that ECCS initiating instrumentation must respond to the potential inadequacy of core cooling regardless of the location of the breach in the reactor coolant pressure boundary. Identify the instrument location and the equipment qualification requirement of the reactor vessel level and drywell pressure instrumentation that will perform the mitigation function. Are these sensors qualified to function in harsh environment? Discuss the response time of these instrument channels in response to various pipe break locations.

GE Response

DCD, Tier 2, Revision 2, Section 7.3.1.1.3 has been revised to remove any reference to drywell pressure as ECCS initiating instrumentation. ECA SR3-2006-0002 was approved and changed the ECCS initiating parameter to RPV water level (L1) only. The RPV level L1.5 in conjunction with high drywell pressure initiation parameters are no longer applicable.

RPV level instruments are located outside containment as stated in Section 7.3.1.1.3.4, “Regulatory Guides (RGs)”, under the bullet for RG 1.118 of DCD, Tier 2, Revision 2.

Safety-related RPV level instruments are qualified for the environment in which they must perform their safety function as stated in Section 7.7.1.1.1, “Safety (10 CRF 50.2) Design Basis”, and Section 7.7.1.3, “Safety Evaluation”, of DCD, Tier 2, Revision 2.

The response times for the level channels are in the order of magnitude of hundreds of milliseconds, much faster than a change in the reactor level due to a pipe break in any location. The response of the ECCS to design basis LOCA is discussed in Sections 6.3.3.4 and 6.3.3.7.4 of DCD, Tier 2, Revision 2. Additionally, there is a 10 second delay following receipt of a voted L1 signal to confirm the ECCS initiation signal as noted in Table 6.3-1 of DCD, Tier 2, Revision 2. This delay is very large in comparison to the level instruments response time regardless of the instrument locations.

Simulated Assisted Engineering (SAE) Modeling Demo - RWCU

Steve Priete and Tom Jenkins

Open Item Discussion

Various

Public Meeting - Audit Results

Various