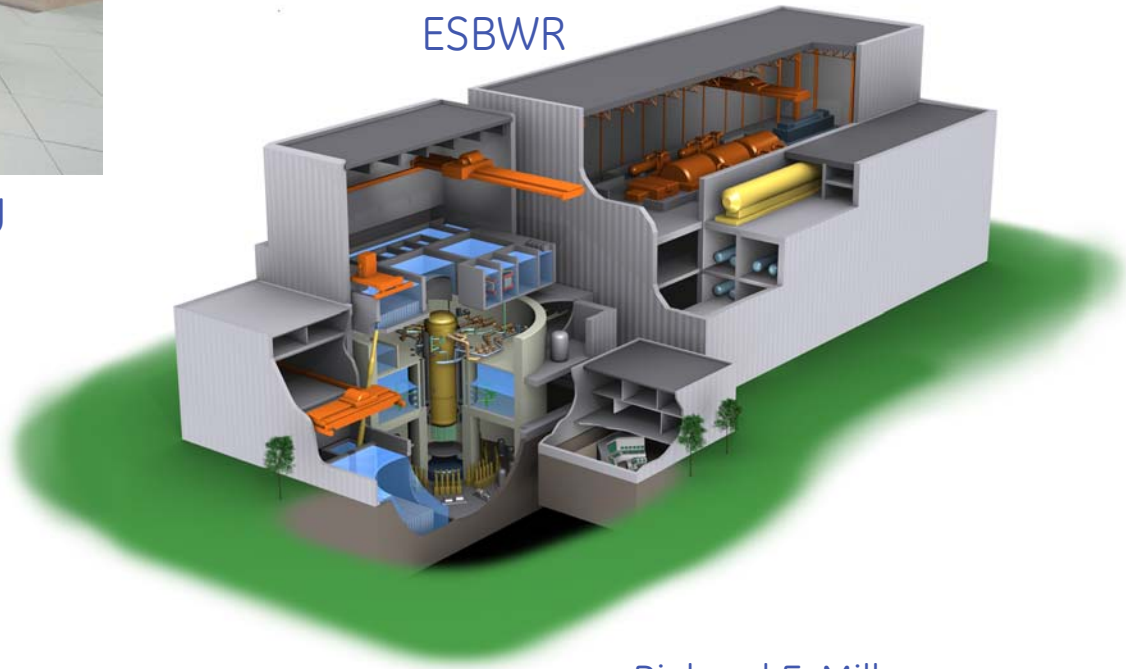
ESBWR Instrumentation & Controls - Update

April 25 - 26, 2007

ESBWR MCR Phase 1 Rendering

ESBWR



imagination at work

Richard E. Miller

ESBWR Instrumentation & Controls - Update
Agenda

Wednesday, April 25th

0830 Introductions/Agenda Overview

0900 ESBWR DCIS

- DCIS Architecture Overview Update
- Overview of Plant Physical Locations

1100 NUMAC Architecture Update

- Architecture Update
- Communications

1200 Lunch

ESBWR Instrumentation & Controls - Update
Agenda (continued)

Wednesday, April 25th - Continued

1300 SSLC/ESF DCIS

- Selection Criteria
- Architecture Overview
- Communications
- QNX Operating System

1645 Daily Summary, Readjust Agenda

1700 Adjourn

ESBWR Instrumentation & Controls - Update
Agenda (continued)

Thursday, April 26th

0830 RAI 7.1-48 / Plant Specific SER Items

0930 IEEE 603 Lifecycle

1030 ITAACs Related to IEEE 603

1130 Equipment Qualification – RG 1.209

1200 Lunch

ESBWR Instrumentation & Controls - Update
Agenda (continued)

Thursday, April 26th (continued)

1300 November 2006 I&C Audit Open Items

1330 DCD Changes from Rev. 2 to Rev. 3

1400 Status of RAIs

1430 Discussion on RAIs

1530 Summary / Action Items

1600 Public Comments

1630 Adjourn

ESBWR DCIS

DCIS Architecture Overview Update

Overview of Plant Physical Locations

Rich Miller / Ira Poppel

DCIS Architecture Overview Update

Safety Category	Safety-Related		Nonsafety-Related				
	Q-DCIS		N-DCIS				
System Families	RPS	SSLC/ESF	DPS	CORE SYSTEMS	Balance of any N-DCIS Systems	PCF	Severe Accident
Architecture	Divisional	Divisional	Triple Redundant	Triple Redundant	Dual Redundant	Workstations **	PLCs
Systems/ Subsystems	RPS LD&IS (MSIV) NMS ATWS/SLC* CMS+	ICS ADS (SRV/DPV) GDCS SLC LD&IS (Non-MSIV) CRHS CMS+	RPS ECCS Backup	FWCS, PAS (Automation) SB&PC, TGCS	PIP A, PIP B Balance Of Plant (Power Generation)	HMI, Alarms, SPDF, Historian, 3D Monicore	Deluge System (GDCS Subsystem)
Vendor	GE-NUMAC	GE/INVENSYS-TRICON	GE-MARK VIe				GE-FANUC

* Diverse (Discrete Programmable Logic)
\+ Diverse Sensor Inputs
** Dual redundant as necessary

Diversity Strategy

Note: Crosshatching denotes different hardware/software platforms.
Shading is for readability only.

ESBWR SSLC/ESF Architecture Overview Update

- ESBWR Q-DCIS is composed of
  - RPS, LD&IS (MSIV), NMS, ATWS/SLC*, CMS
  - SSLC/ESF
    - ICS, ADS (SRV/DPV), GDCS, SLC, LD&IS (non-MSIV), CRHS, CMS, safety-related monitoring and control (VDUs)

* Diverse sensor inputs, non programmable logic

Proposed Suppliers for Primary DCIS Families

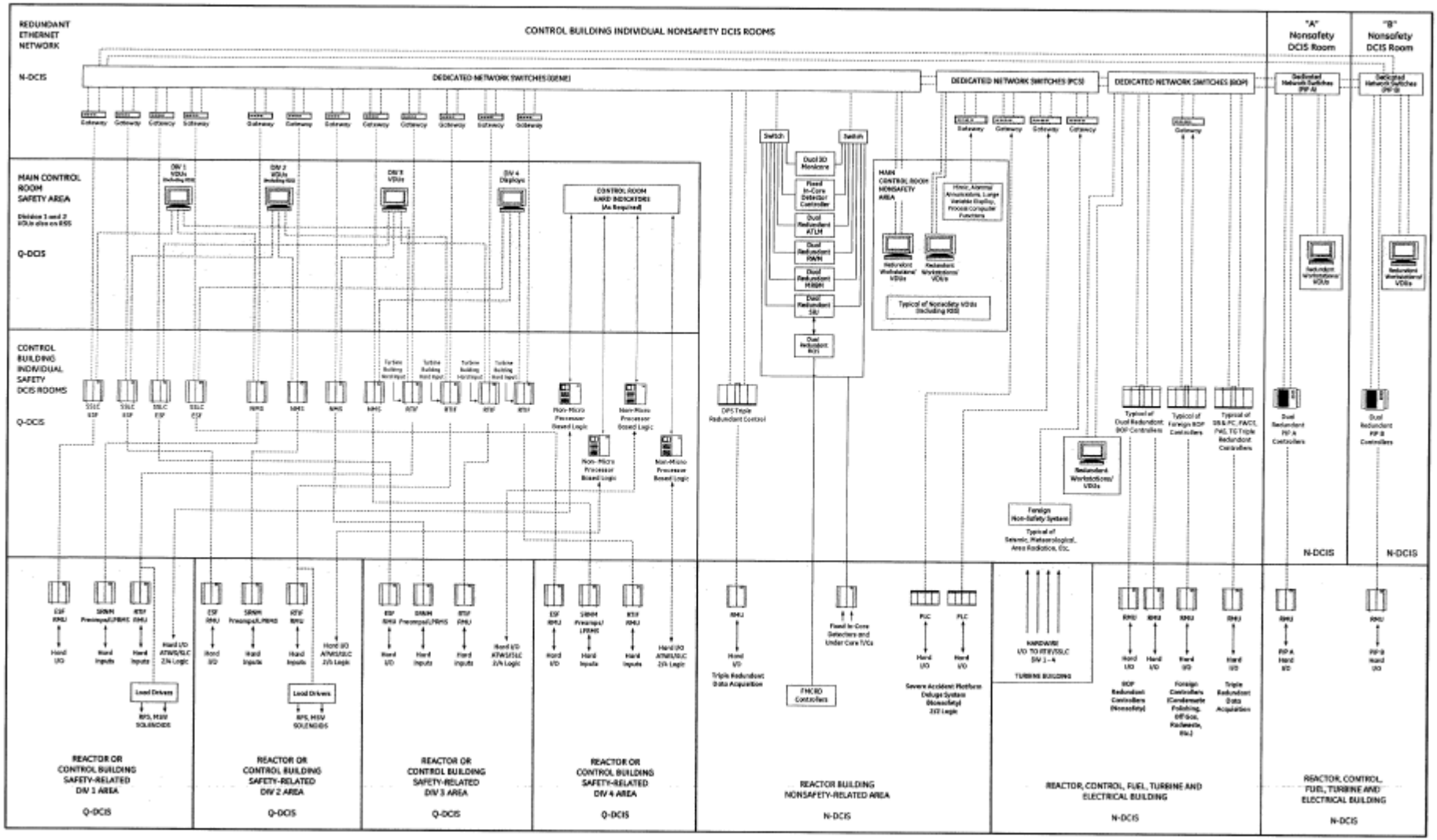
- NMS/RPS > GE (NUMAC)
- ECCS/ESF > Invensys (TRICON) (primary), DS&S (SPINLINE3) (secondary), or DRS (PLUS32) (backup)
- DPS > GE (Mark VIe)
- Nuclear Control Systems > GE (Mark VIe) and Hitachi
- Balance of Any Nonsafety-Related Systems > GE (Mark VIe)
- Plant Computer Functions > (GE-Mark VIe / DS-S (SAIPMS/Win) or Scientech (R*TIME)
- Severe Accident > Quality Diverse PLC Supplier such as GE-FANUC
- 3rd Party DCIS Suppliers > Various

ESBWR Instrumentation & Controls - Update

- No changes in overall DCIS concept
  - DCIS block diagram unchanged
- No changes in main control room functionality

ESBWR Instrumentation & Controls - Update

ESBWR Distributed Control and Information System (DCIS) Functional Network Diagram



ESBWR DCIS Equipment Location Overview and Control Room Panel Layout

ESBWR DCIS Locations

- DCIS locations include:
  - Main control room (control building)
  - Two N-DCIS rooms (control building)
    - Rooms separate PIP A and PIP B
  - Four Q-DCIS rooms (control building)
    - Rooms separate safety divisions
  - All buildings/many rooms for RMUs
    - Acquire/output data

ESBWR DCIS Locations (cont.)

- Most DCIS cabinets have been located to specific rooms in the various buildings
  - Rooms and cabinets must have compatible environmental ratings
- Some DCIS locations/rooms are plant specific
  - Circ water pumphouse, PSW cooling towers

ESBWR Safety-related / Nonsafety-related DCIS Rooms

N-DCIS

(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 SSLC/SLC 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

N-DCIS

(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 SSLC/SLC 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 control 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

Q-DCIS

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 SSLC/ESF 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 SSLC/ESF RMU

CB room 3130
(div 3 E-DCIS)

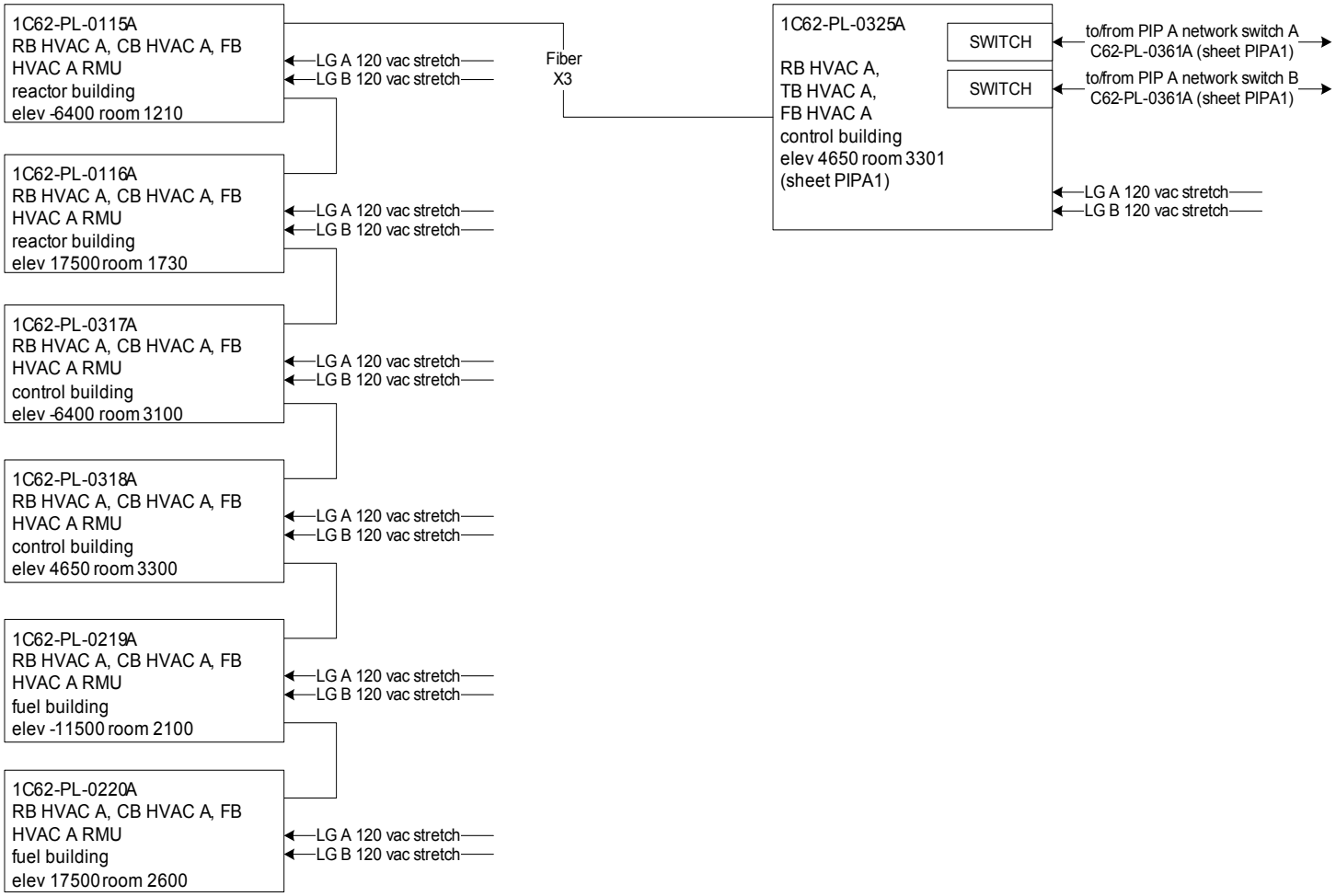
1C63-PL-3301 NMS
1C63-PL-3302 RTIF
1C63-PL-3303 PRM
1C63-PL-3305 SSLC
1C63-PL-3306 test/gateway
1C63-PL-3307 SSLC/ESF RMU

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 SSLC/ESF RMU

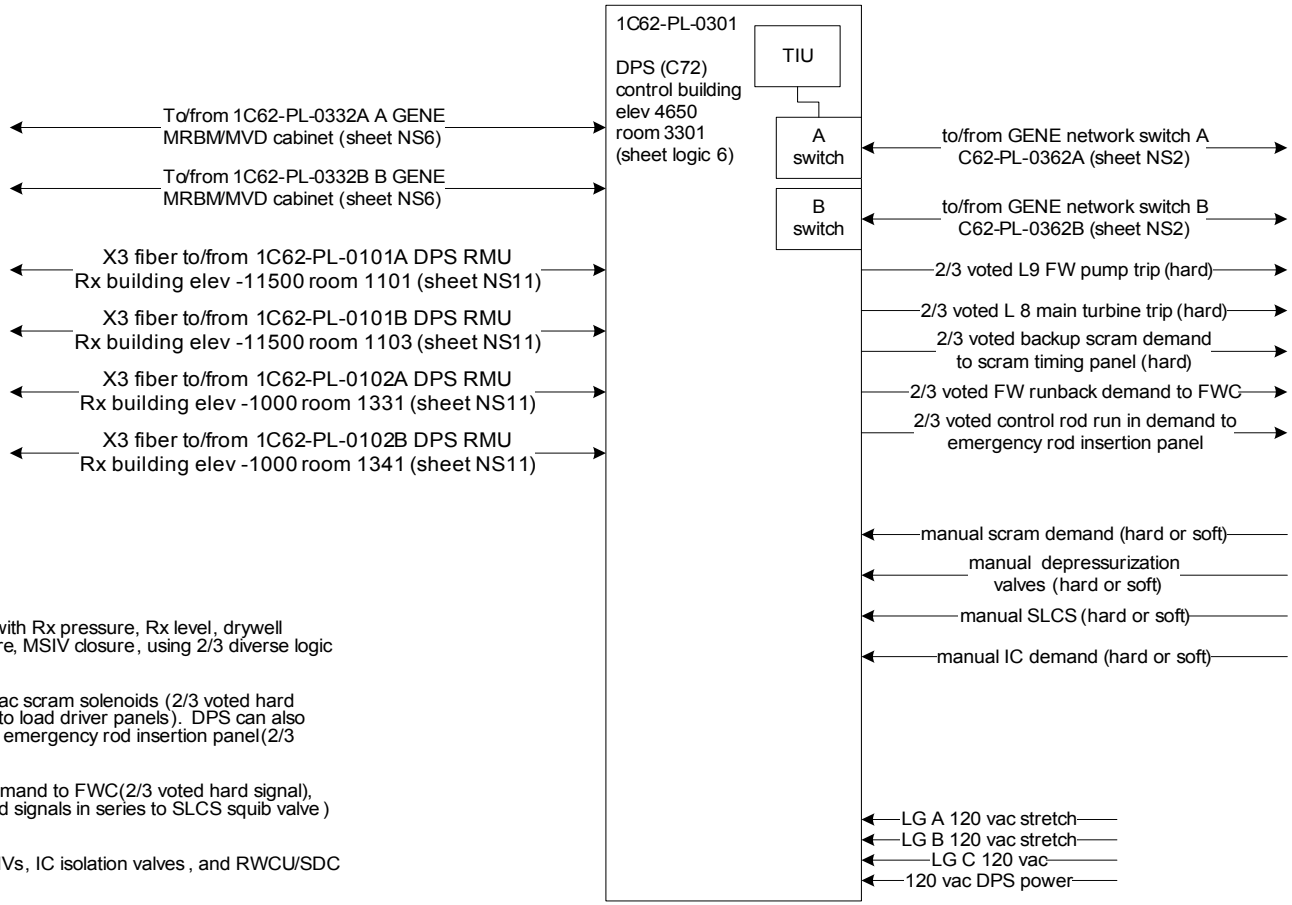
ESBWR PIP A Room Location Example

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



ESBWR GENE Room Location Example

ESBWR 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.

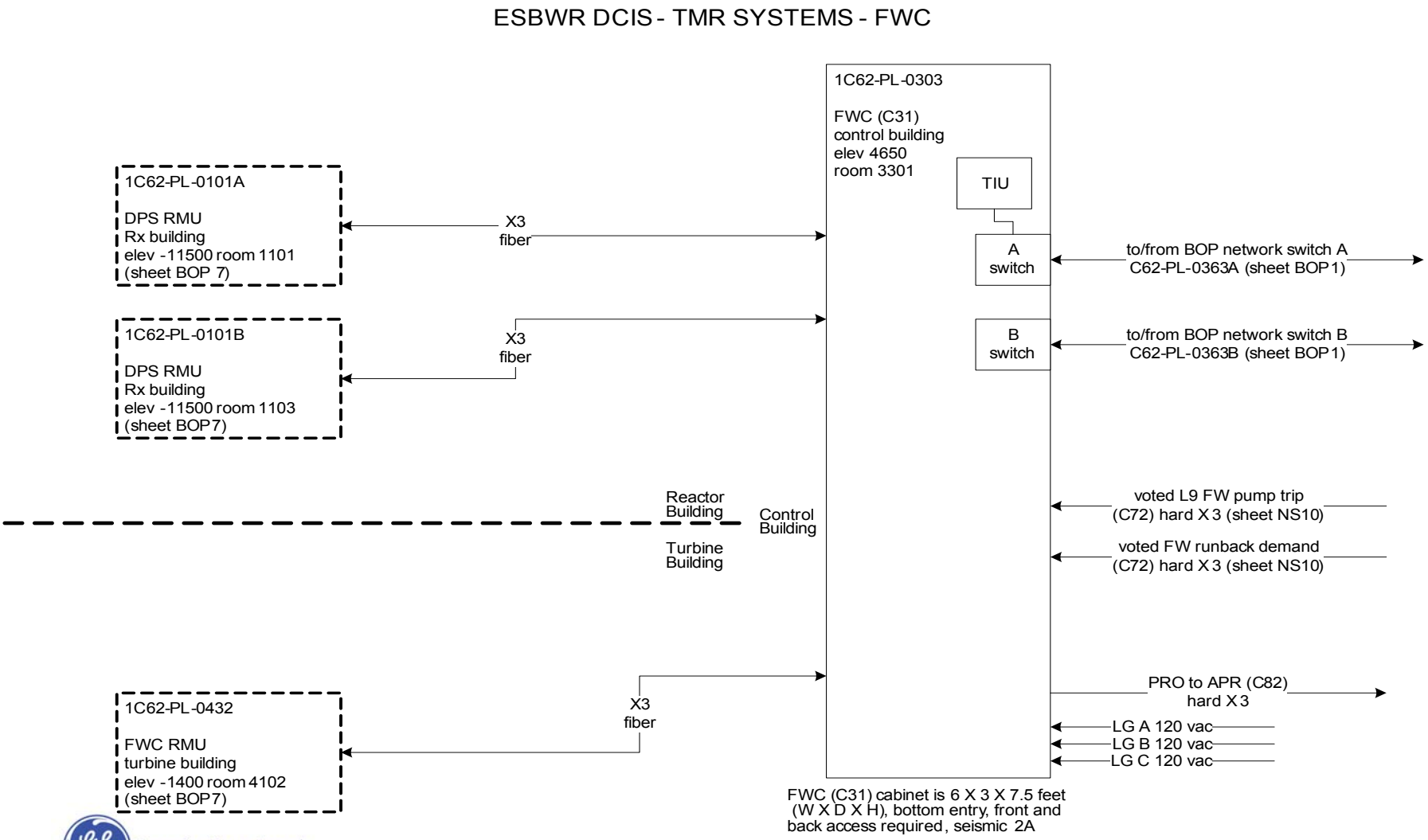
DPS provides diverse actuation to MSIVs, IC isolation valves, and RWCU/SDC isolation valves.

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

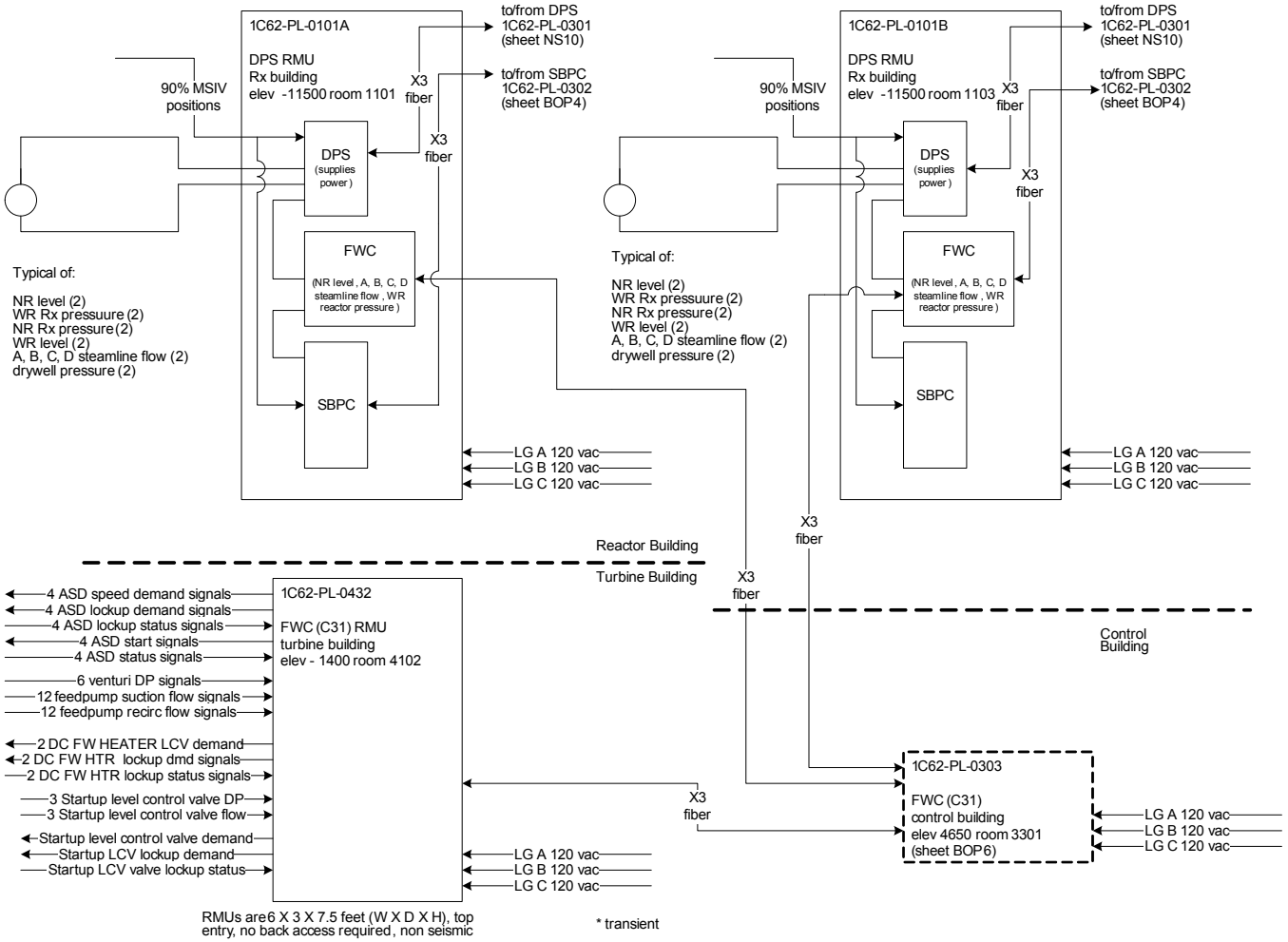


imagination at work

Unverified Draft

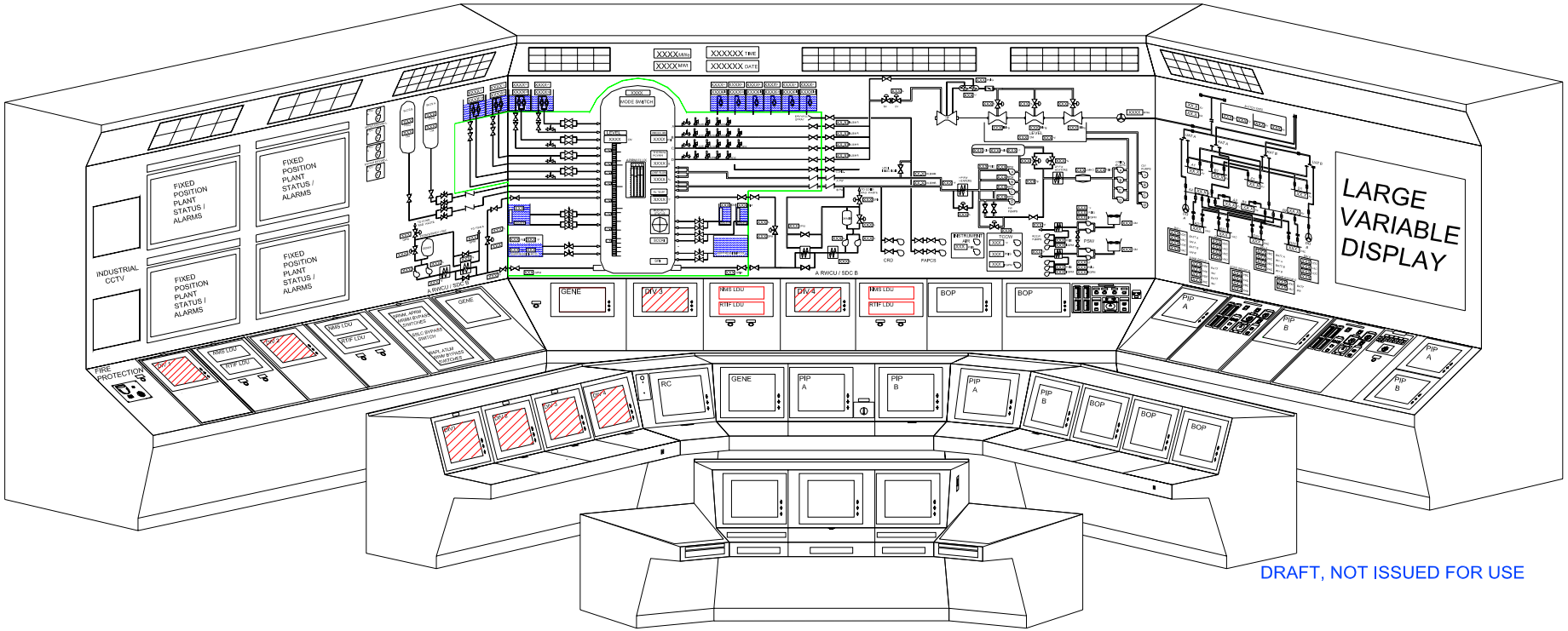
ESBWR GENE Room Location Example (cont.)

ESBWR DCIS - TMR SYSTEMS - FWC RMUs



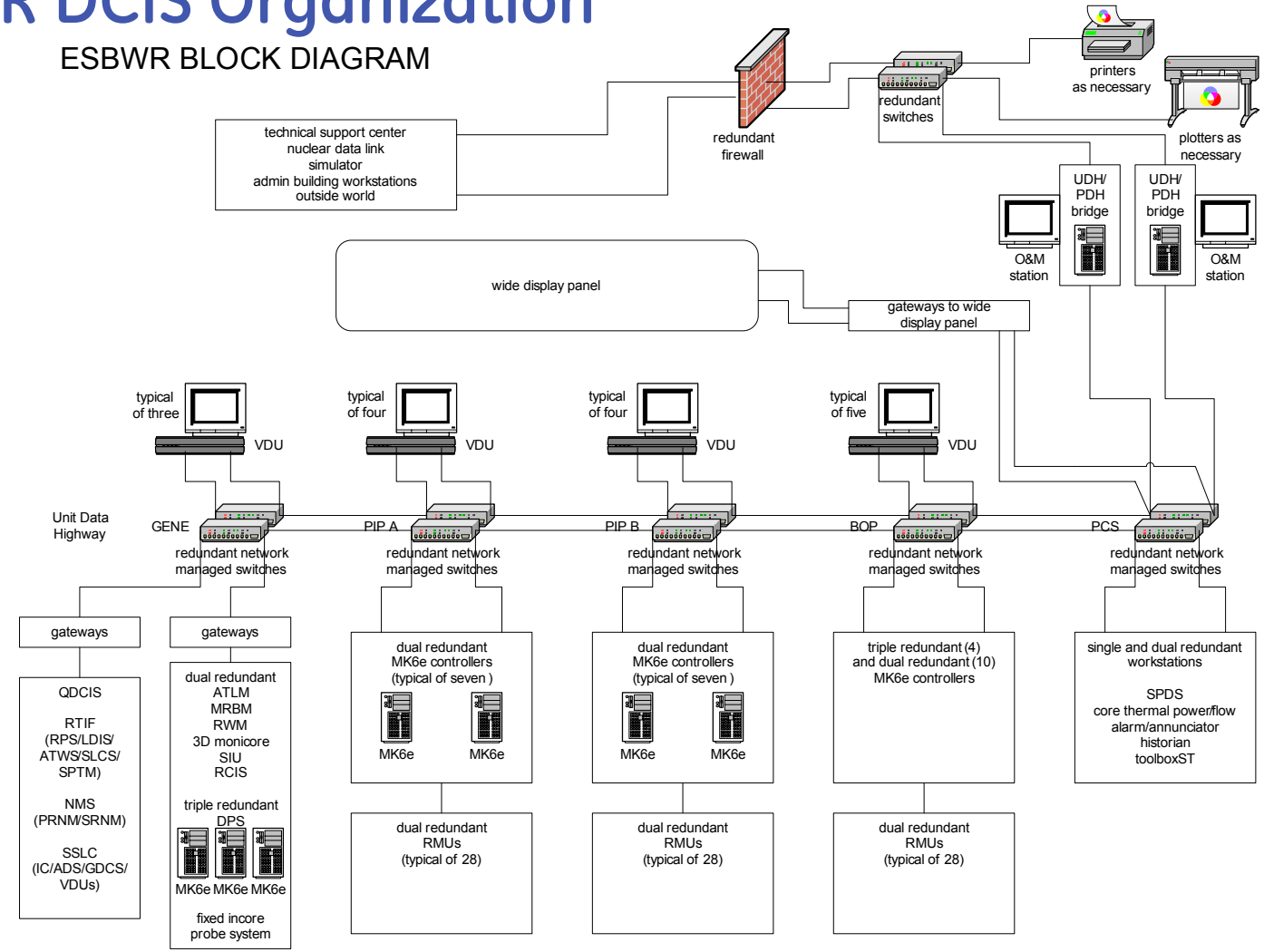
ESBWR Control Room Panels

DRAFT ESBWR CONTROL PANEL



ESBWR DCIS Organization

ESBWR BLOCK DIAGRAM



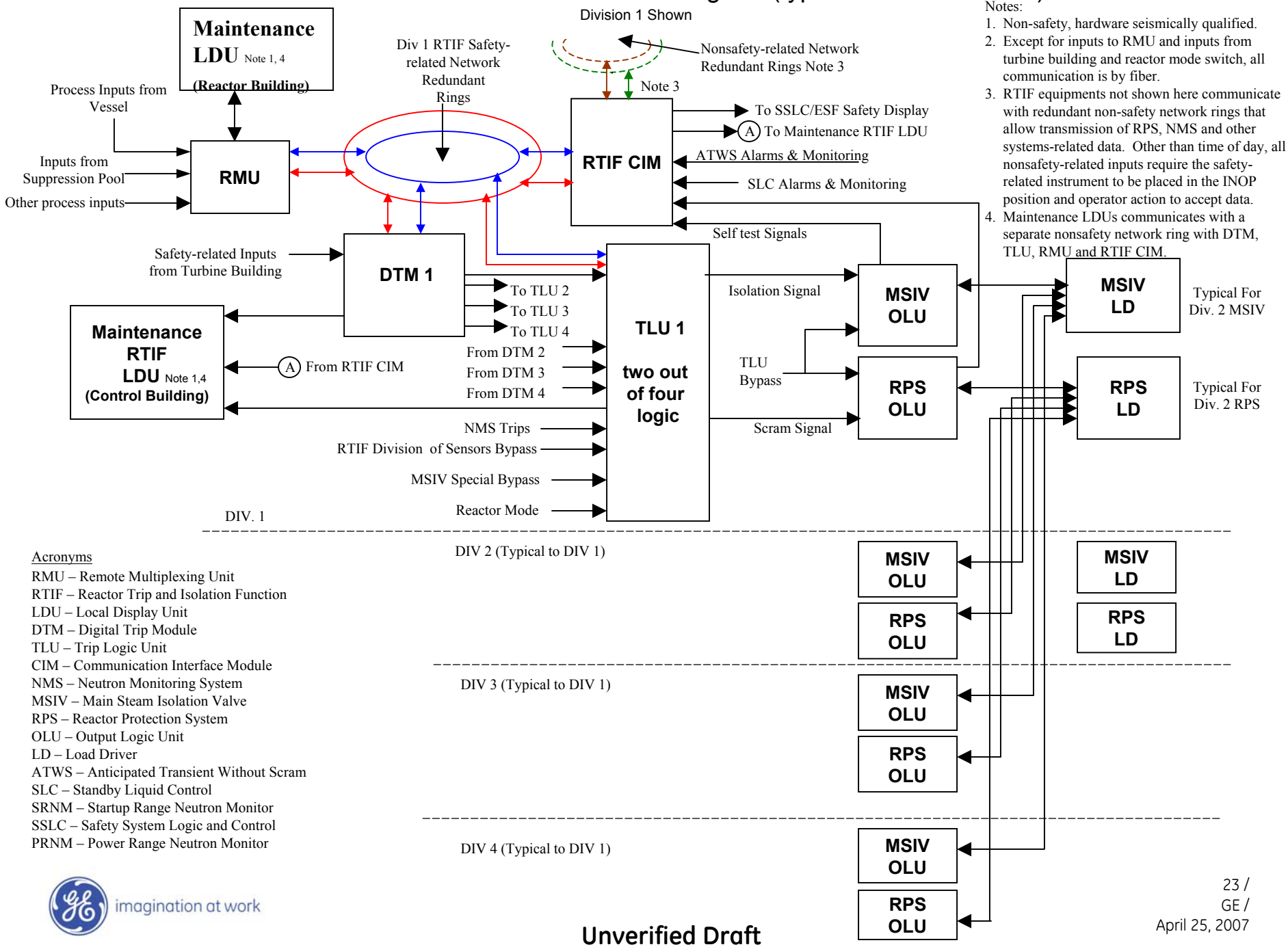
NUMAC Architecture Update

Architecture Update

Communications

Bishara Kakunda / Rich Miller

NUMAC RTIF Functional Block Diagram (typical of four divisions)



Notes:

1. Non-safety, hardware seismically qualified.
2. Except for inputs to RMU and inputs from turbine building and reactor mode switch, all communication is by fiber.
3. RTIF equipments not shown here communicate with redundant non-safety network rings that allow transmission of RPS, NMS and other systems-related data. Other than time of day, all nonsafety-related inputs require the safety-related instrument to be placed in the INOP position and operator action to accept data.
4. Maintenance LDUs communicates with a separate nonsafety network ring with DTM, TLU, RMU and RTIF CIM.

Acronyms

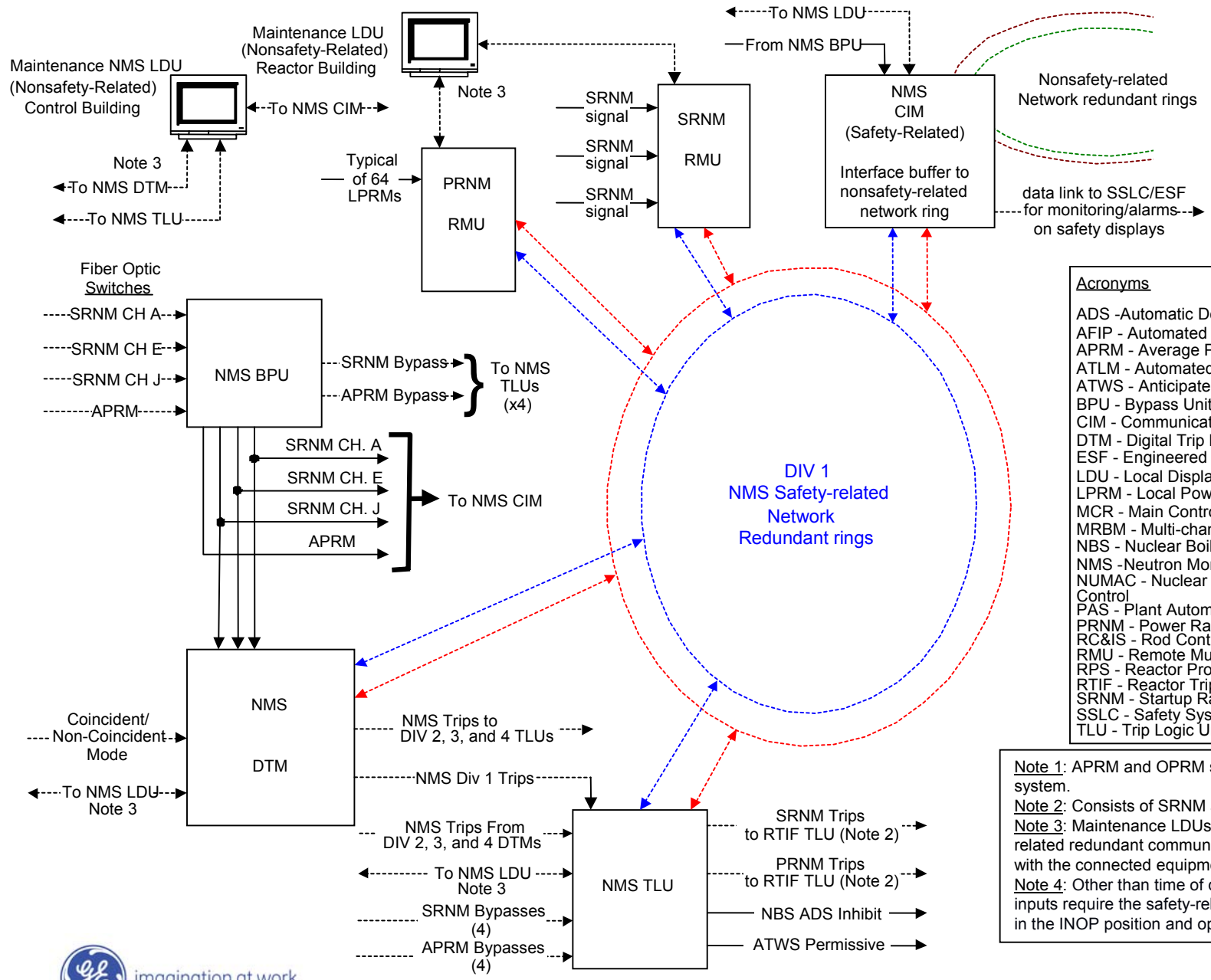
RMU – Remote Multiplexing Unit
RTIF – Reactor Trip and Isolation Function
LDU – Local Display Unit
DTM – Digital Trip Module
TLU – Trip Logic Unit
CIM – Communication Interface Module
NMS – Neutron Monitoring System
MSIV – Main Steam Isolation Valve
RPS – Reactor Protection System
OLU – Output Logic Unit
LD – Load Driver
ATWS – Anticipated Transient Without Scram
SLC – Standby Liquid Control
SRNM – Startup Range Neutron Monitor
SSLC – Safety System Logic and Control
PRNM – Power Range Neutron Monitor

imagination at work

Unverified Draft

NUMAC NMS Functional Block Diagram (typical of four divisions)

Division 1 Shown



Acronyms

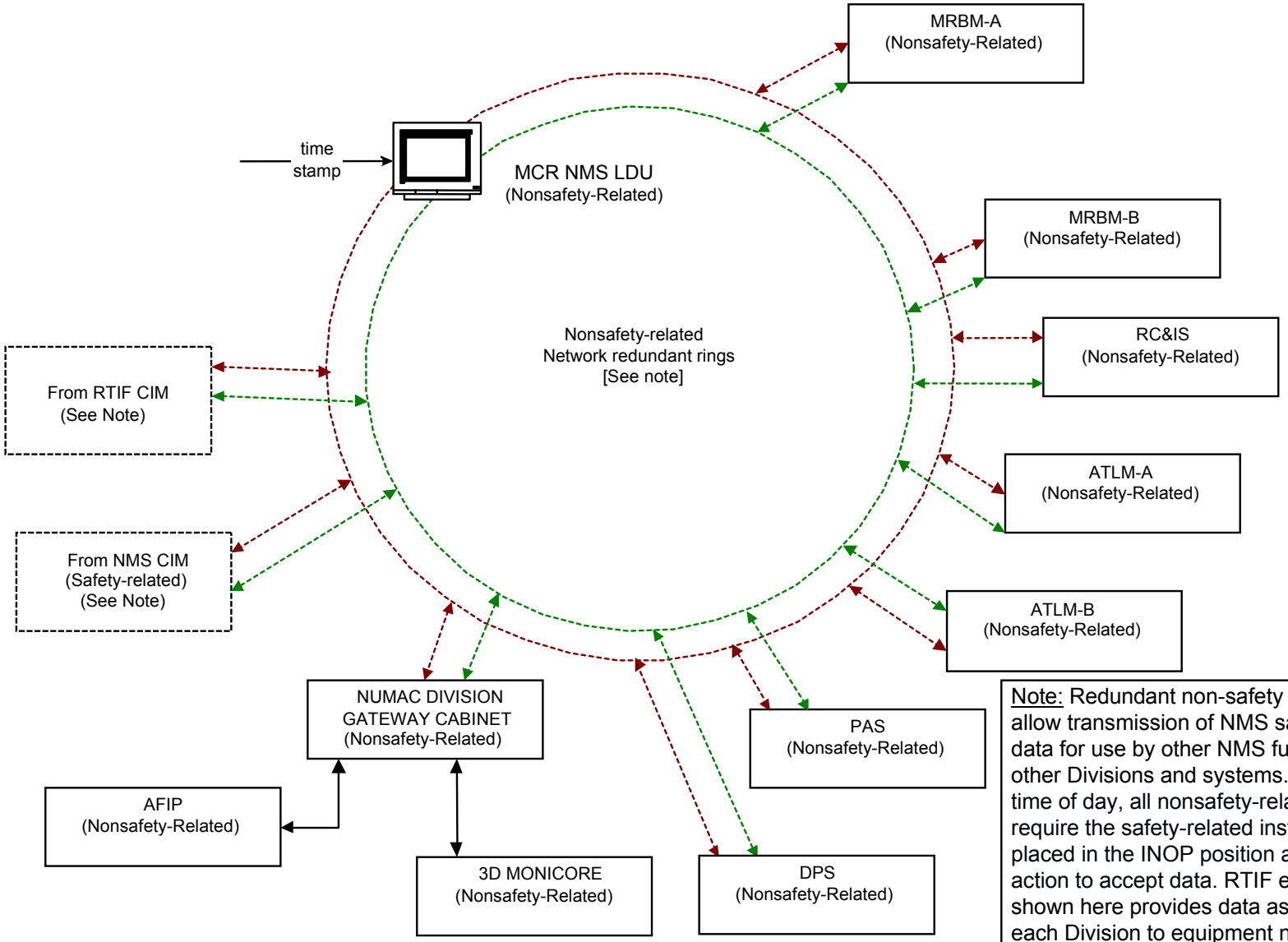
ADS -Automatic Depressurization System
AFIP - Automated Fixed In-core Probes
APRM - Average Power Range Monitor
ATLM - Automated Thermal Limit Monitor
ATWS - Anticipated Transient Without Scram
BPU - Bypass Unit
CIM - Communications Interface Module
DTM - Digital Trip Module
ESF - Engineered Safety Features
LDU - Local Display Unit
LPRM - Local Power Range Monitor
MCR - Main Control Room
MRBM - Multi-channel Rod Block Monitor
NBS - Nuclear Boiler System
NMS -Neutron Monitoring System
NUMAC - Nuclear Measurement Analysis and Control
PAS - Plant Automation System
PRNM - Power Range Neutron Monitor
RC&IS - Rod Control and Information System
RMU - Remote Multiplexing Unit
RPS - Reactor Protection System
RTIF - Reactor Trip and Isolation Function
SRNM - Startup Range Neutron Monitor
SSLC - Safety System Logic and Control
TLU - Trip Logic Unit

Note 1: APRM and OPRM systems are part of PRNM system.
Note 2: Consists of SRNM and PRNM Voted Trips
Note 3: Maintenance LDUs are on separate nonsafety-related redundant communications rings associated with the connected equipment.
Note 4: Other than time of day, all nonsafety-related inputs require the safety-related instrument to be placed in the INOP position and operator action to accept data.

imagination at work

Unverified Draft

NMS & RTIF Interface with Nonsafety-Related Network Rings



Note: Redundant non-safety network rings allow transmission of NMS safety-related data for use by other NMS functions and by other Divisions and systems. Other than time of day, all nonsafety-related inputs require the safety-related instrument to be placed in the INOP position and operator action to accept data. RTIF equipment not shown here provides data associated with each Division to equipment not depicted here.

NUMAC Communications

Bishara Kakunda / Rich Miller

ESBWR Instrumentation & Controls - Update

Key Features:

- Safety-related communications within a division are accomplished by pairs of reflective memory counter rotating rings

- Safety-related inputs from turbine building are sent directly to the DTM

- Trip signals are sent point to point via fiber with continuous error checks (from DTM to TLU). There are separate NMS and RTIF TLUs

- Loss of (or incorrect) communication defaults to a trip condition

Communications

- Safety-related function is not time dependent (does not use time of day) and is asynchronous with other divisions. Loss of, or invalid, data from any division defaults into a trip at the receiving division

- NMS and RTIF architectures are similar. NMS trip signals sent from NMS TLU to RTIF TLU within a division are OR'd within NMS DTM logic first

- Communication from safety to non-safety is through a Communication Interface Module

Communications

- Communication of data from nonsafety-related to safety-related is also through a Communication Interface Module but is limited to maintenance/calibration data, APRM and LPRM calibration data and time of day

- Other than the time of day, all non-safety inputs require the safety-related instrument to be placed in the INOP position and operator action to accept the data

- The data received are buffered until the safety-related device reads, validates, and then uses them appropriately with operator action

SSLC/ESF DCIS

Selection Criteria

Architecture Overview

Communications

QNX Operating System

RAI 7.1-48 / Plant Specific SER Items

Rich Miller / Ira Poppel / Joe Murray

SSLC/ESF Selection Criteria

Ira Poppel

ESBWR SSLC/ESF Selection Criteria

- The ESBWR requires safety-related DCIS for ECCS functions (SSLC/ESF) to be highly reliable to initiate ESF when required:
  - Manually and automatically
- The ESBWR incorporates depressurization via one-shot explosive squib valves so it is equally important to have high confidence that inadvertent actuation will be avoided
- The ESBWR SSLC/ESF must provide a highly reliable operator interface for monitoring functions (including NMS and RPS/LDIS) as well as for ECCS functions

ESBWR SSLC/ESF Selection Criteria (cont.)

- The ESBWR SSLC/ESF must provide highly reliable interdivisional communication for the two out of four initiation logic
- The ESBWR SSLC/ESF must provide highly reliable and isolated safety-related (SR) / nonsafety-related (NSR) communications while accepting NSR time of day signals for display and data time tagging
- Support N-2

ESBWR SSLC/ESF Selection Criteria (cont.)

- Important supporting selection criteria include:
  - > Fiber optic communication
  - > Redundant communication
  - > Redundant power supplies
  - > Appropriate collection of input/output capability
  - > Maximum self diagnostic coverage
  - > Wide customer support base/historic support capability

ESBWR SSLC/ESF Vendor Selection

- ESBWR SSLC/ESF primary vendor is the Invensys TRICON system
  - > Triple Modular Redundant
  - > No single point of failure
  - > Full internal diagnostics, self testing and self calibration
  - > Designed to maintain operation with multiple failures, properly report failures, and allow on-line repairs
  - > Extensive existing application
    - – 7000 systems in service
    - – 400,000,000 hours without a failure to perform on demand
    - – Same platform for safety-related system

SSLC/ESF Architecture Overview

Ira Poppel / Joe Murray

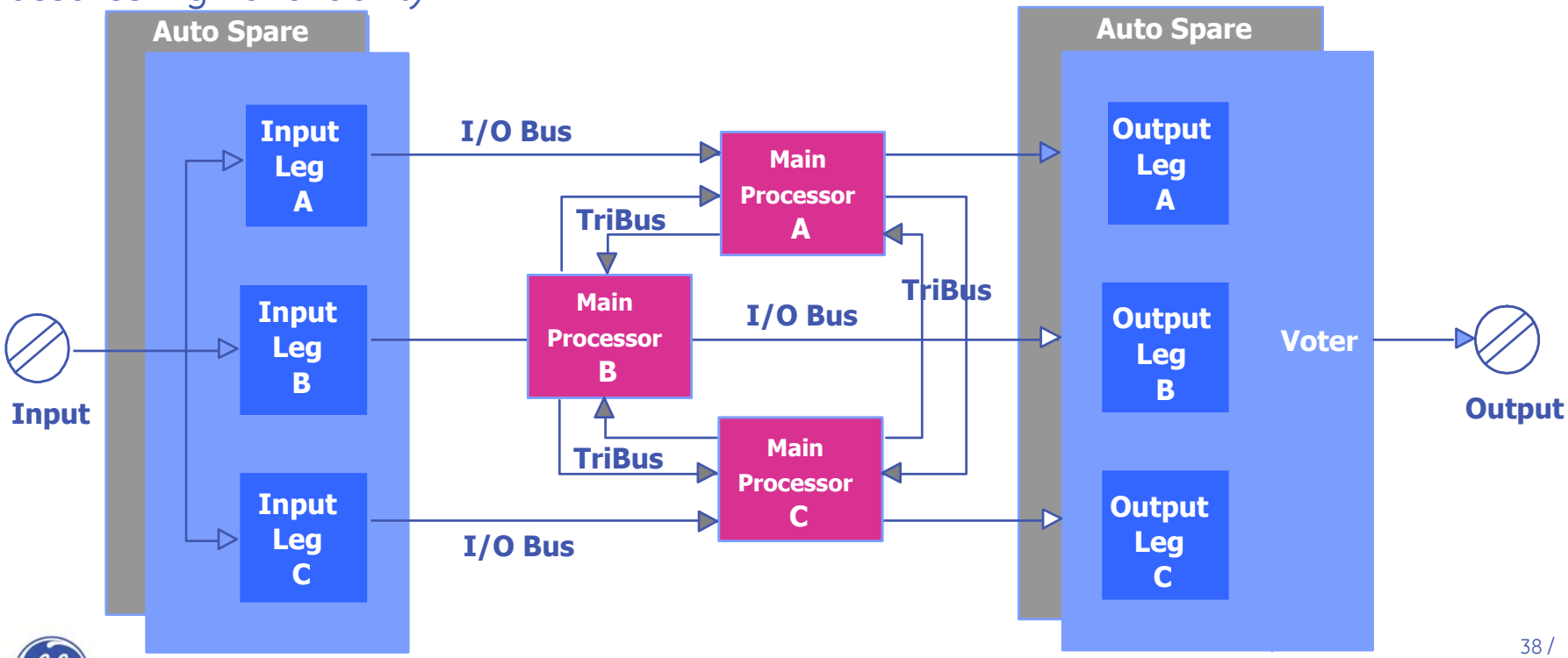
TRICON Reliability

- Per division, the TRICON is designed to avoid inadvertent actuation. However, the overall four division design provides sufficient availability when actuation is required

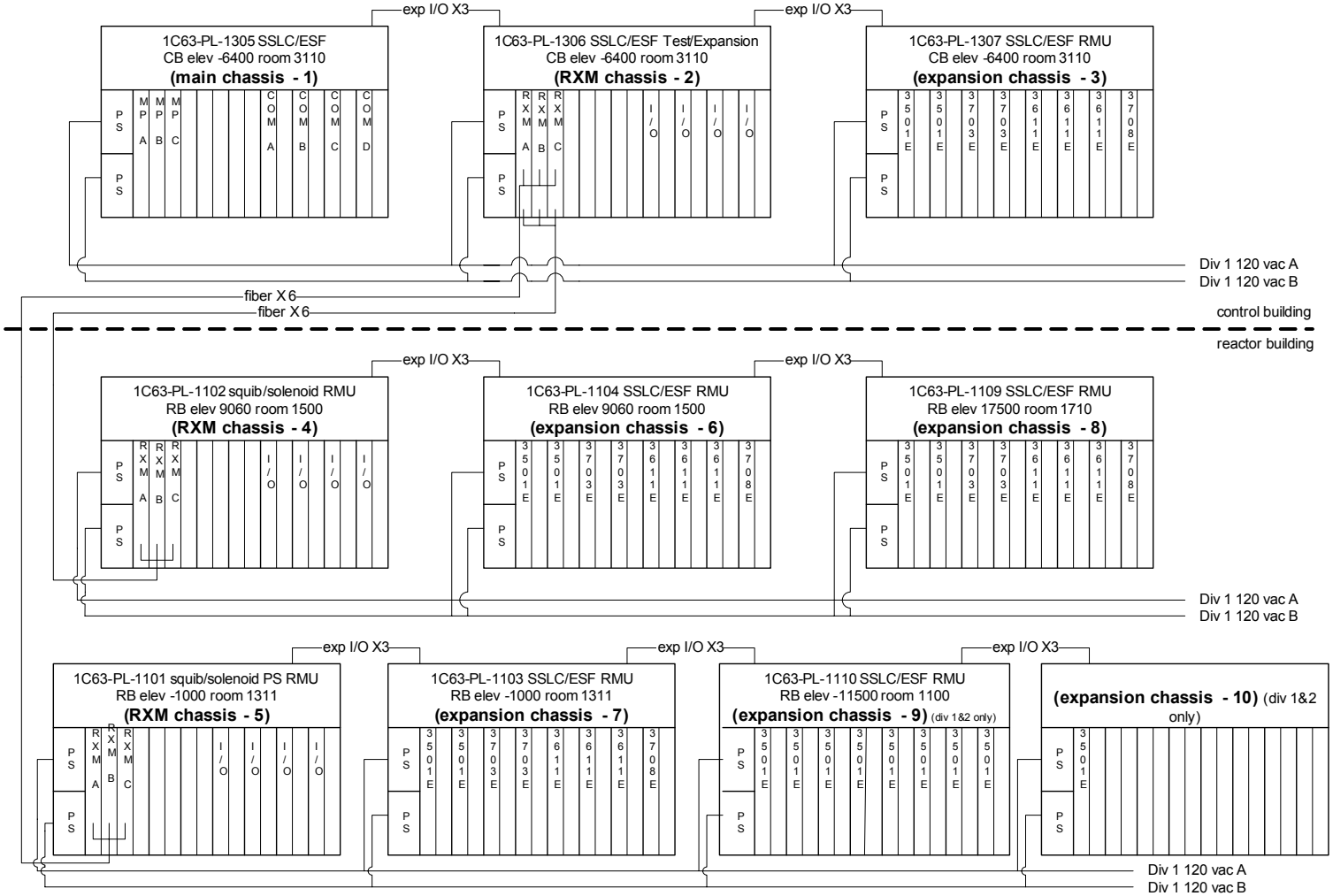
- Sufficient reliability for actuation is assured by
  - > ESBWR N-2 design (any two SSLC/ESF divisions can fail and SR functions can still be available)
  - > Diverse hardware/software DPS system
  - > TRICON reliability

TRICON Architecture

- Triply redundant architecture assures per division SSLC/ESF reliability despite measures taken to avoid inadvertent actuation
- Extensive self diagnostics, on-line processor and I/O card replacement capability assures high availability



ESBWR TRICON Architecture (typical of four divisions)



TRICON Squib/Solenoid Inadvertent Actuation

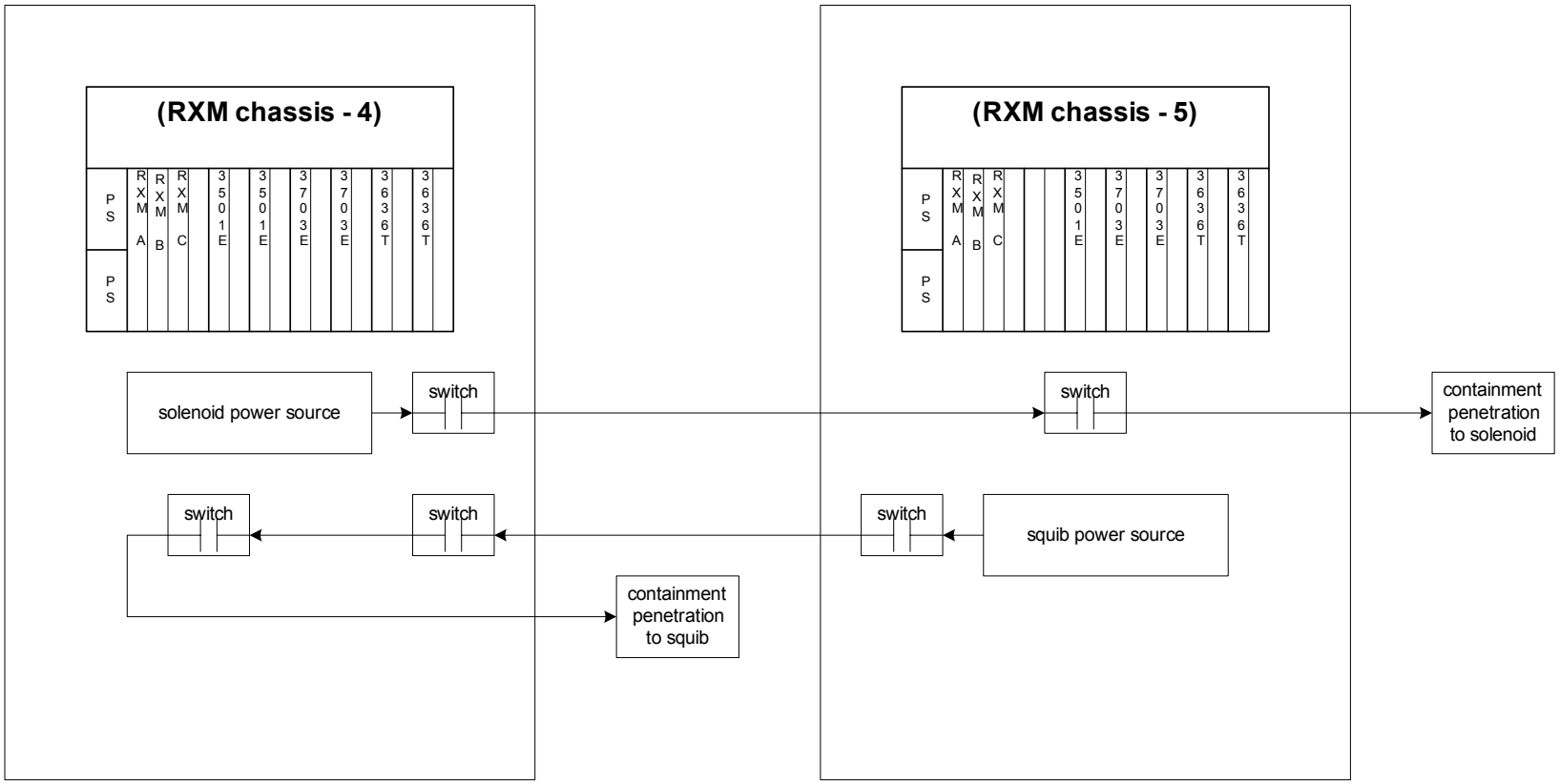
- Inadvertent actuation of any squib valve (DPV, GDCS) requires the simultaneous failure of three processors or three independent discrete outputs

- Inadvertent actuation of any SRV solenoid valve requires the simultaneous failure of three processors or two independent discrete outputs

TRICON Squib/Solenoid Inadvertent Actuation (cont.)

- Discrete outputs per division are within two widely separated cabinets
  - > Eliminates hot short consideration
  - > Eliminates fire consideration
- Squib/solenoid power is grounded (not floating) and will use shielded power cable

TRICON Squib/Solenoid Detail



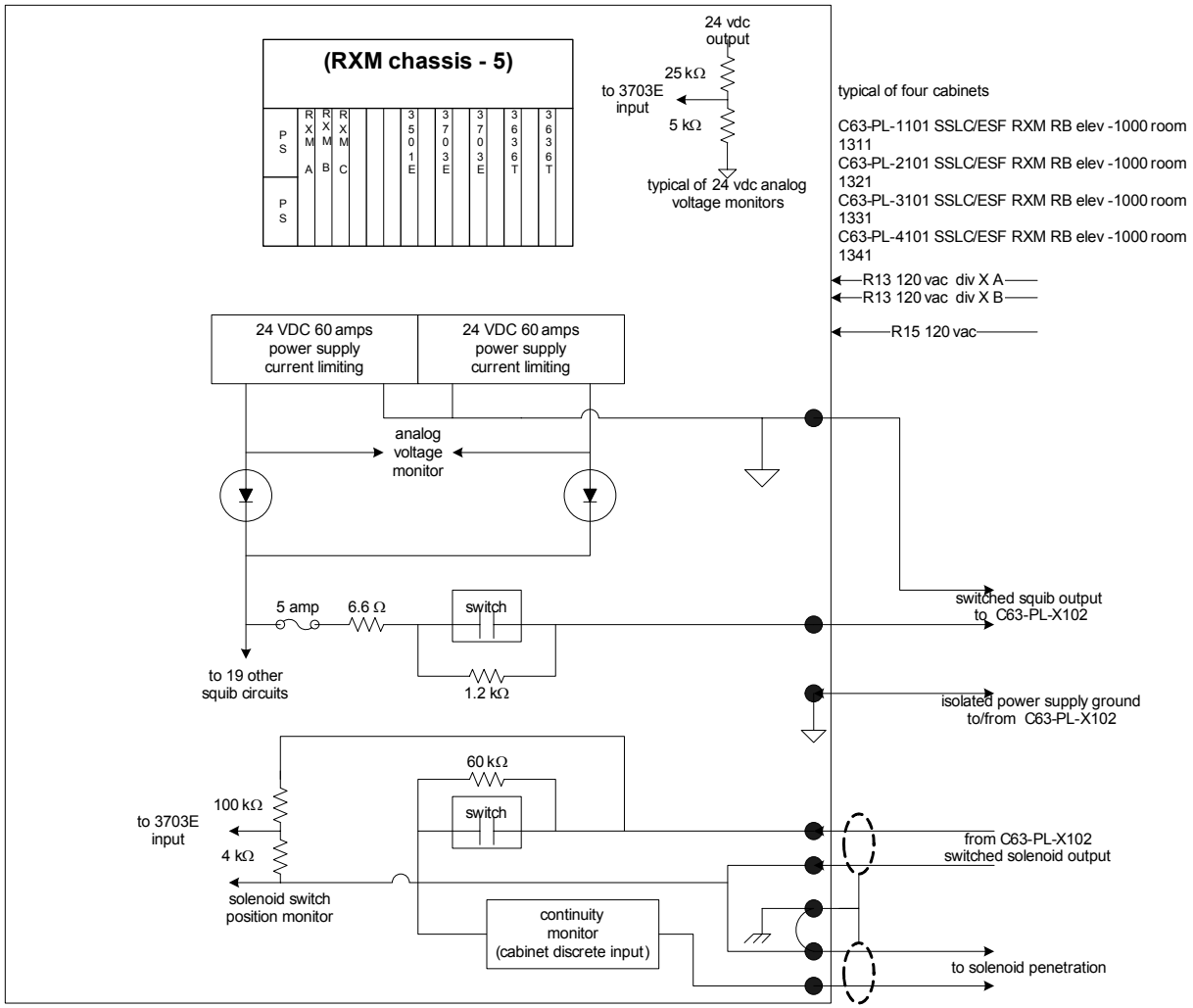
typical of four cabinets

C63-PL-1102 SSLC/ESF RXM RB elev 9060 room 1500
C63-PL-2102 SSLC/ESF RXM RB elev 9060 room 1502
C63-PL-3102 SSLC/ESF RXM RB elev 9060 room 1501
C63-PL-4102 SSLC/ESF RXM RB elev 9060 room 1503

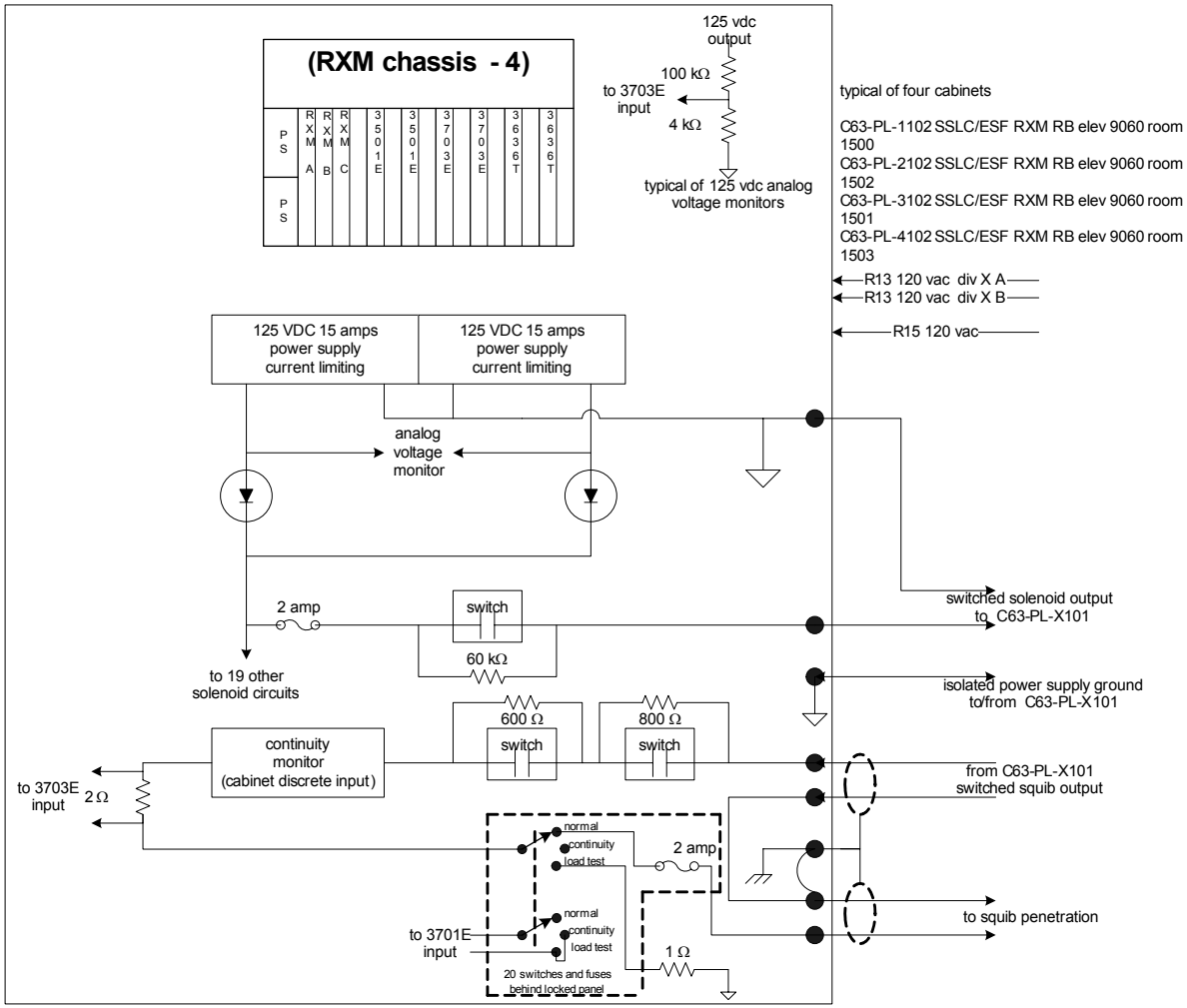
typical of four cabinets

C63-PL-1101 SSLC/ESF RXM RB elev -1000 room 1311
C63-PL-2101 SSLC/ESF RXM RB elev -1000 room 1321
C63-PL-3101 SSLC/ESF RXM RB elev -1000 room 1331
C63-PL-4101 SSLC/ESF RXM RB elev -1000 room 1341

TRICON Squib/Solenoid Detail (cont.)



TRICON Squib/Solenoid Detail (cont.)



TRICON Squib/Solenoid Reliability

- Squib/solenoids have redundant, monitored power supplies
- Discrete outputs (3 squib/2 solenoid) can be individually closed and positions monitored without operating squib/solenoid
- Squib/solenoid continuity is continuously monitored
- Squib firing (power supply/current) capability can be monitored without operating squib

SSLC/ESF Communications

Ira Poppel / Joe Murray

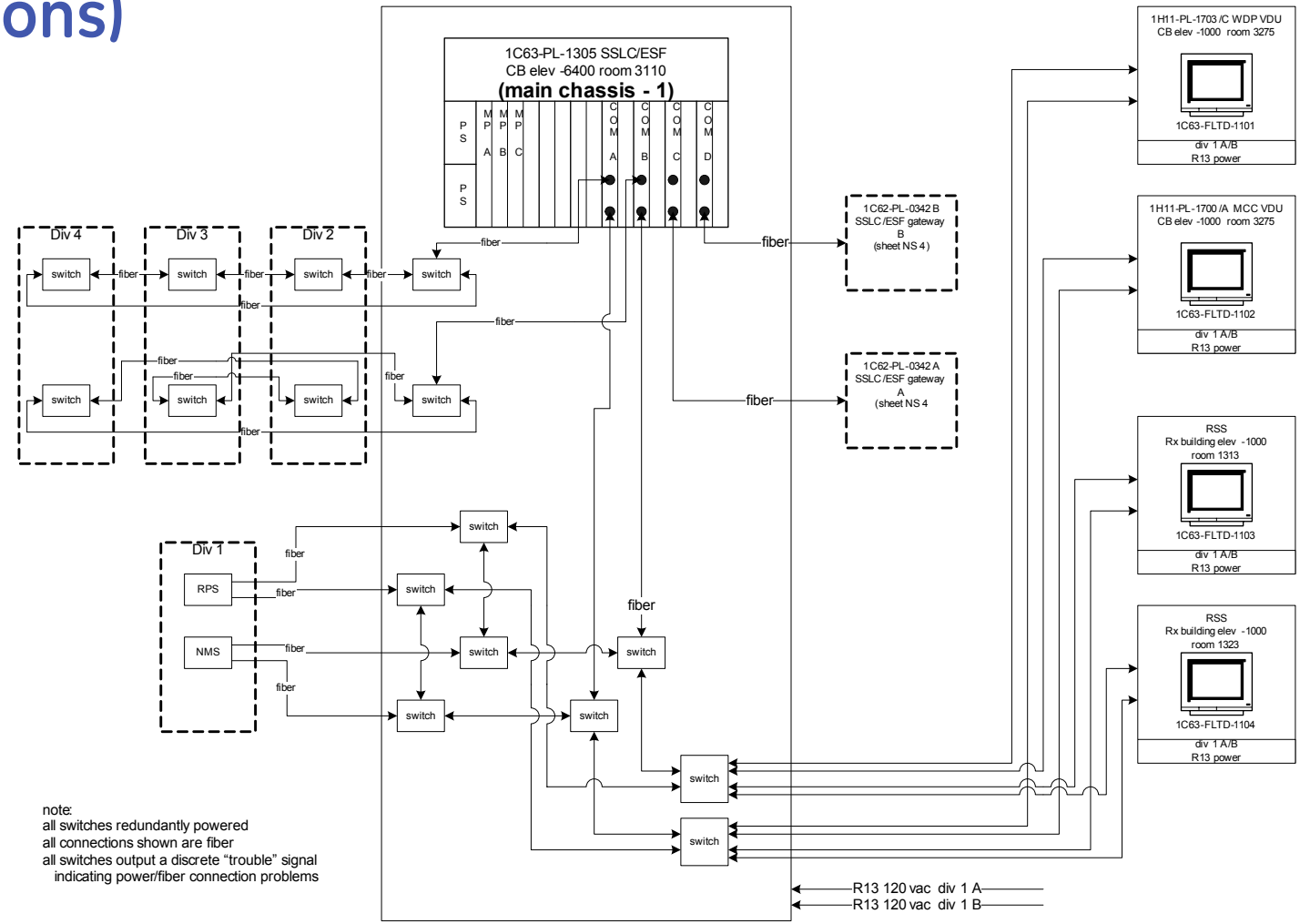
TRICON Communication

- TRICON communication
  - > Per division to VDUs
  - > Per division to N-DCIS
  - > Per division RPS/NMS to VDU
  - > Between divisions for two out of four initiation logic

TRICON Communication

- TRICON communication
  - Must never corrupt another division
  - Must never depend on any NSR communication or data
  - Must never allow NSR communication or data to corrupt SR functions
- Governed by IEEE 603 data isolation and independence

TRICON Communication Configuration (typical of four divisions)



note:
all switches redundantly powered
all connections shown are fiber
all switches output a discrete "trouble" signal
indicating power/fiber connection problems

imagination at work

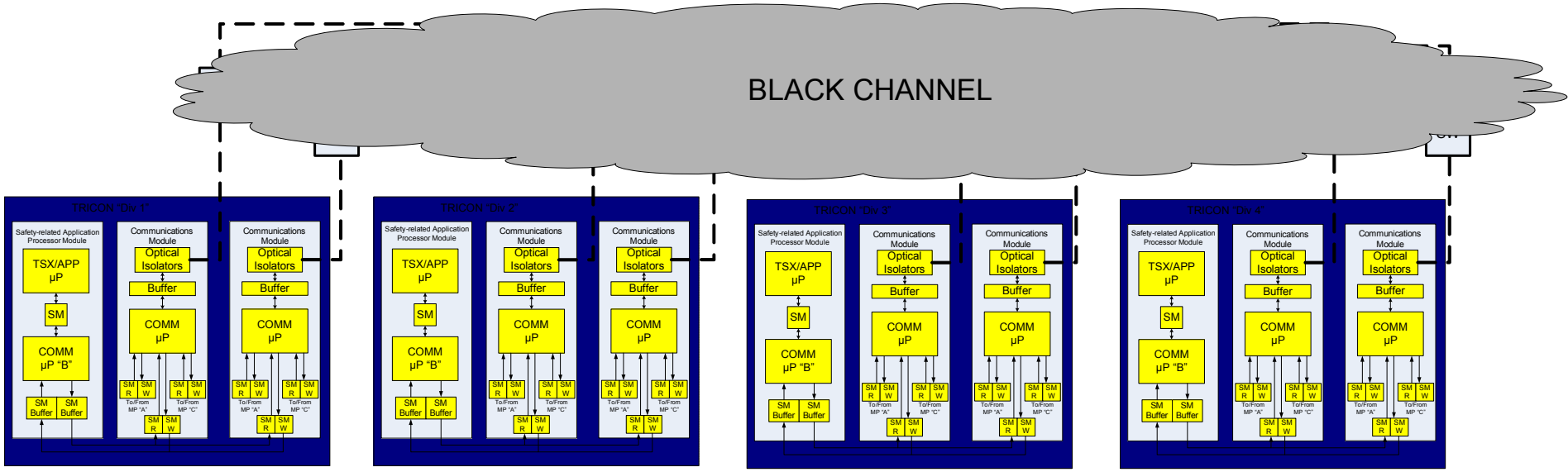
Unverified Draft

TRICON Communication Description

- TRICON is designed via "Black Channel" definition
  - Black Channel means that everything outside of the TRICON is considered an unknown
  - All design criteria to meet independence / isolation and maintain data integrity is contained within the SR TRICON
    - Point to point or network communication choice is irrelevant since it does not matter how the data gets to the TRICON
  - No credit is taken for external devices
- Full electrical isolation
  - Optical-Isolators and fiber optics
- Communications isolation from SR application processor

TRICON Independent of Network Topology

- All design features to ensures data independence, isolation, and integrity reside in TRICON



TRICON Communication Description

- Main processor modules have separate application and communication processors
- Separate communication card with its own processors
- Asynchronous processors
- All data writes (i.e. to the TRICON) must be in the proper format, have the proper source and destination address, and be within a given range
  - No writes allowed to any points not pre-assigned as writeable
  - Those pre-assigned points must also be programmed into sending TRICON

TRICON Communication Description (cont.)

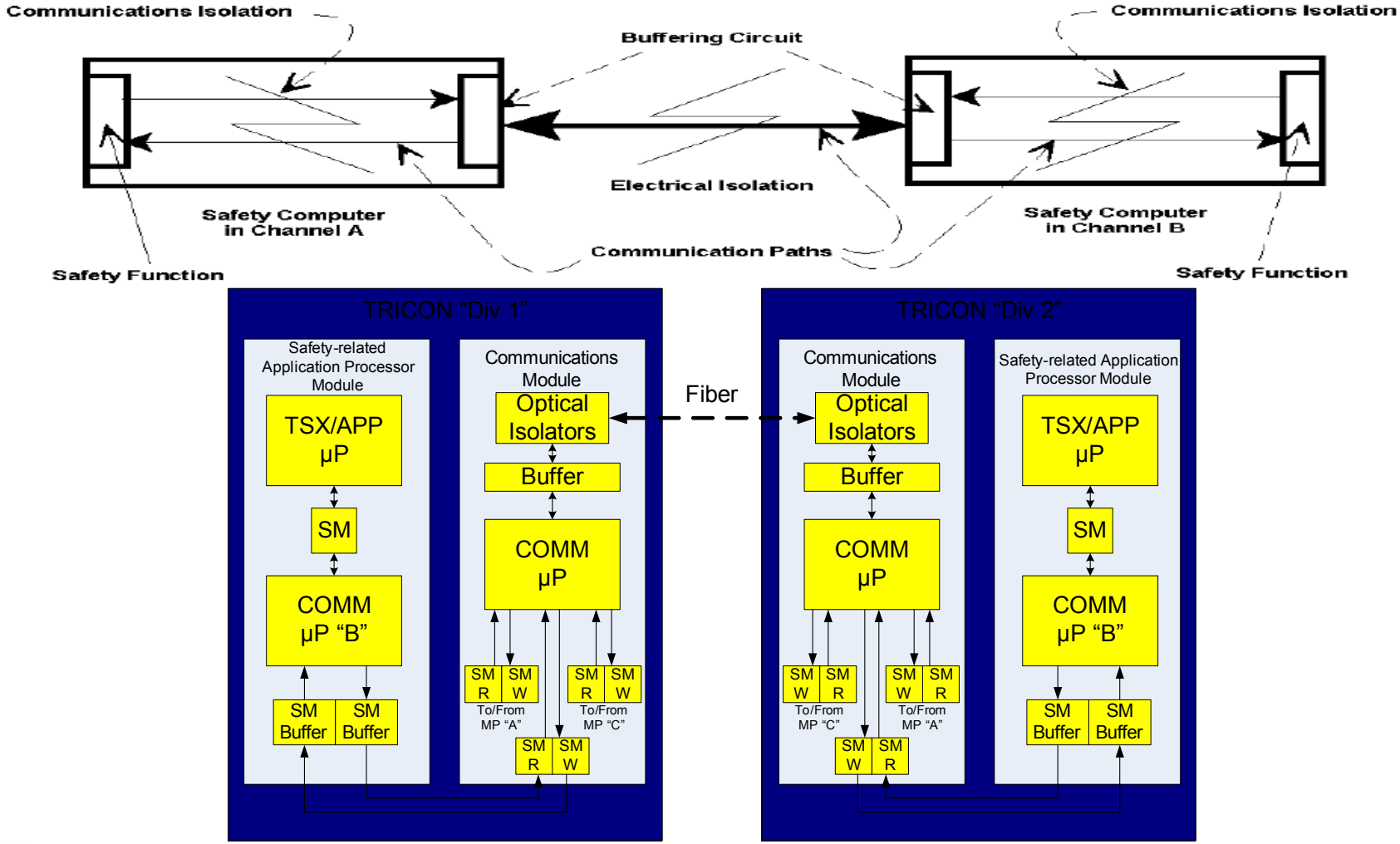
- The SR application processor never handles “read” (i.e. from the TRICON) requests
  - > Full data dump every scan of all user predefined (programmed) readable points and all diagnostics values
- Individual communications cards can be configured for “Read Only”
- TRICON to TRICON Peer-to-Peer is a proprietary protocol that is essentially a point to point UDP/IP non-request transmission with an additional safety communication layer on top of the standard communication layers

TRICON Communication Hardware

TRICON SR to SR Communication

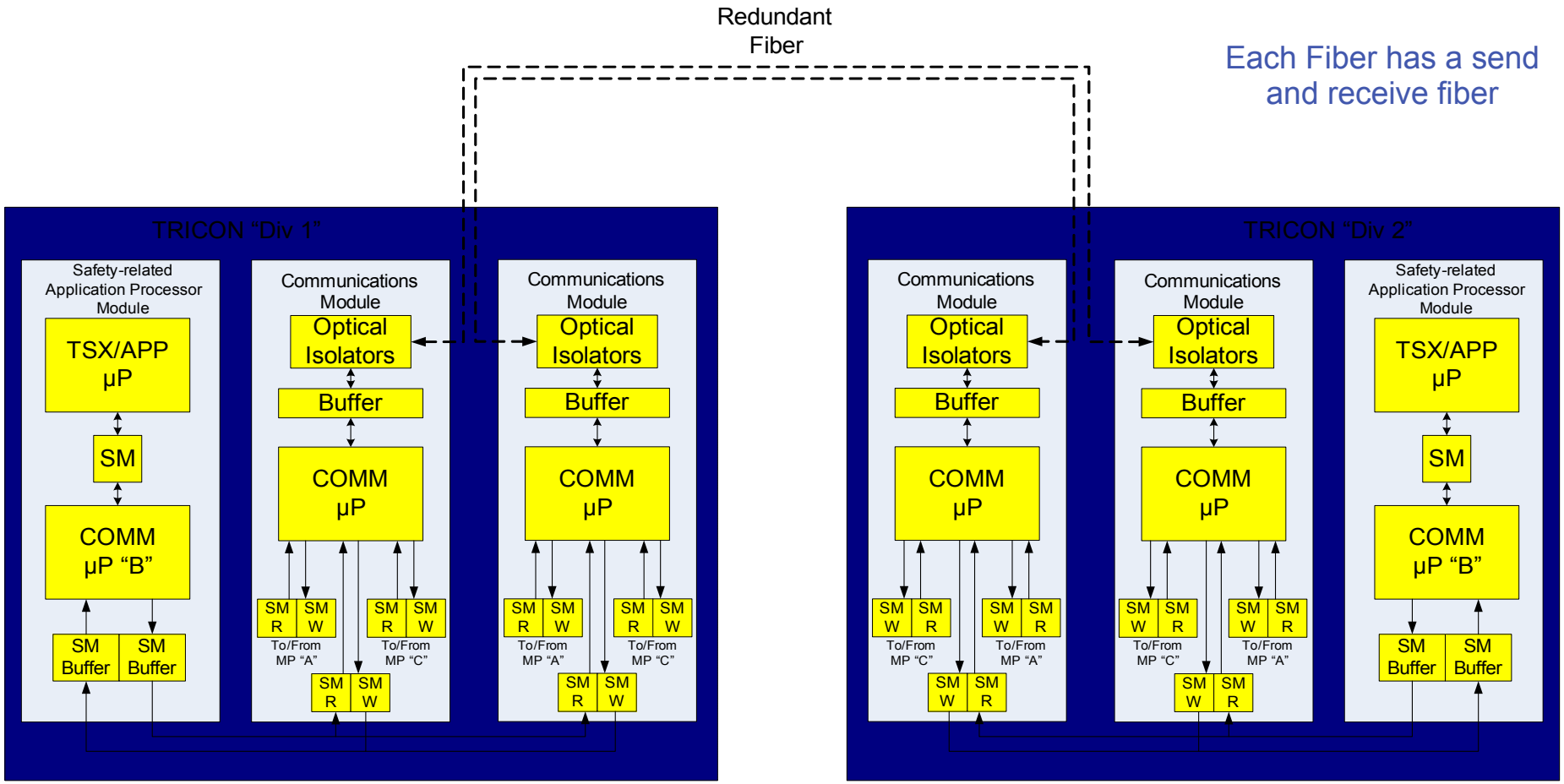
- Sends parameter trip decisions and bypass status from each division to all other divisions for two out of four initiation logic
- Dual Redundant Self Healing Ring Fiber Network
  - > Multiple fault tolerant
  - > COTS dedicated network switches, data integrity independent of switches
- Configuration is N-2

TRICON SR to SR Communication

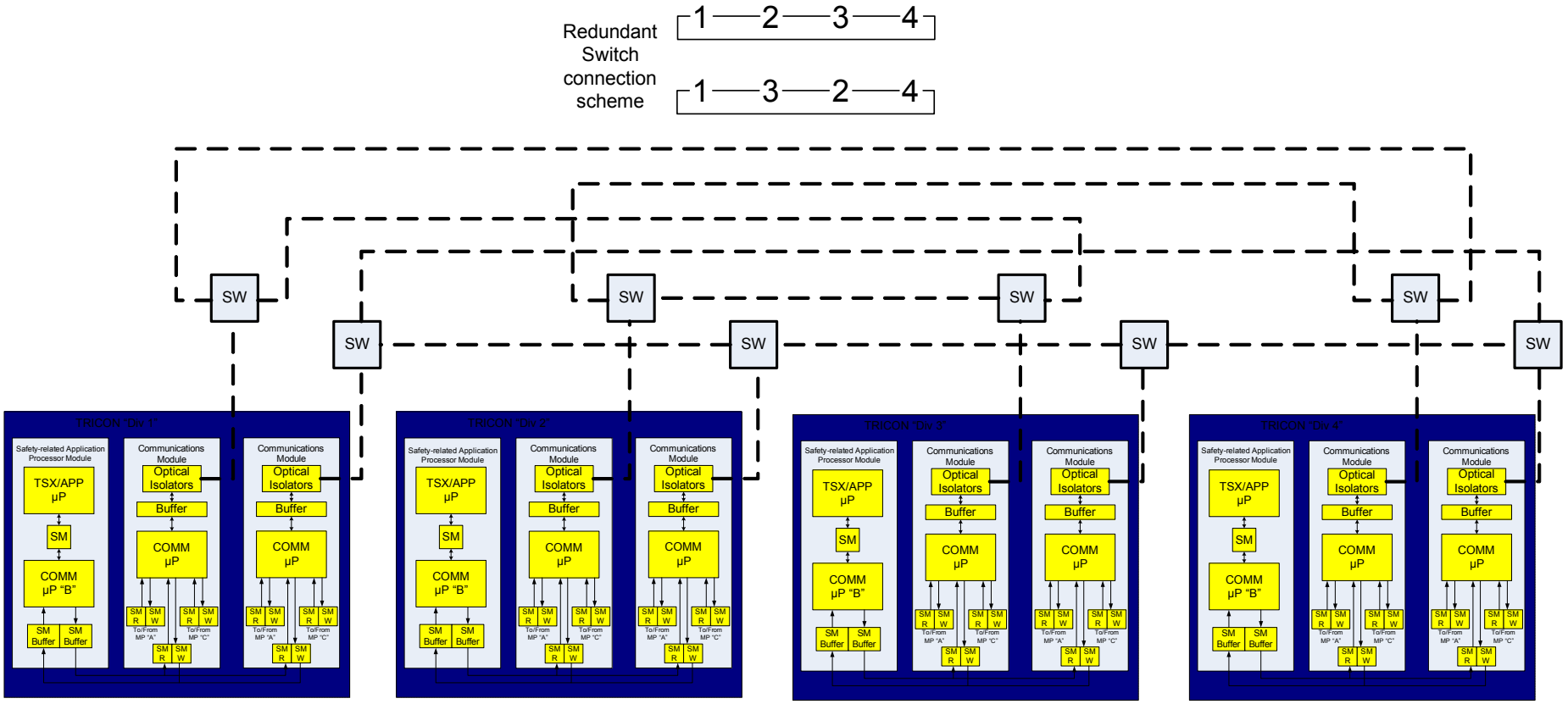


TRICON Redundant SR to SR Communication

Each Fiber has a send and receive fiber



TRICON SR to SR Communication (cont.)



TRICON SR to NSR Communication

- Sends essentially all divisional process, calculated and diagnostic data to N-DCIS for further monitoring, alarming and recording via isolation device(s)
- Communication is through redundant and isolated optical fiber
- SR to SR communication cards are separate from SR to NSR communication cards
- NSR communication card is configured as “Read Only.” All write functions are disabled; all write requests ignored

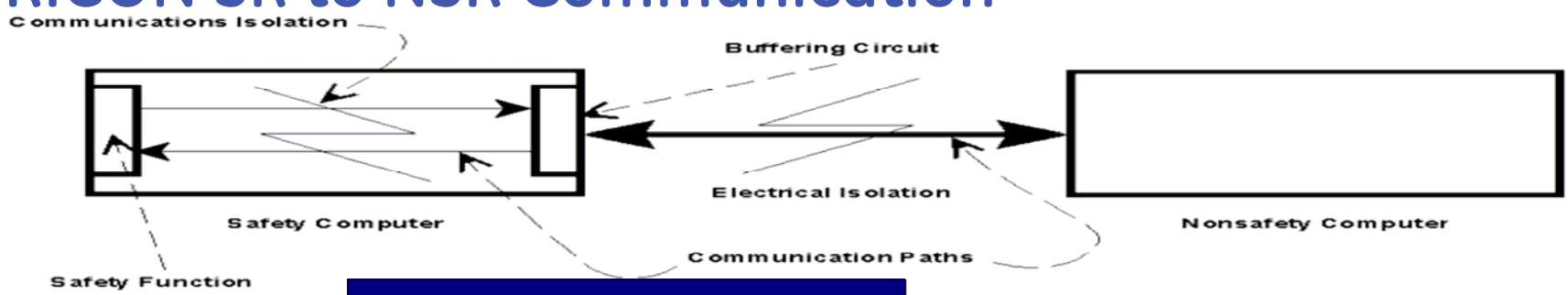
TRICON SR to NSR Communication

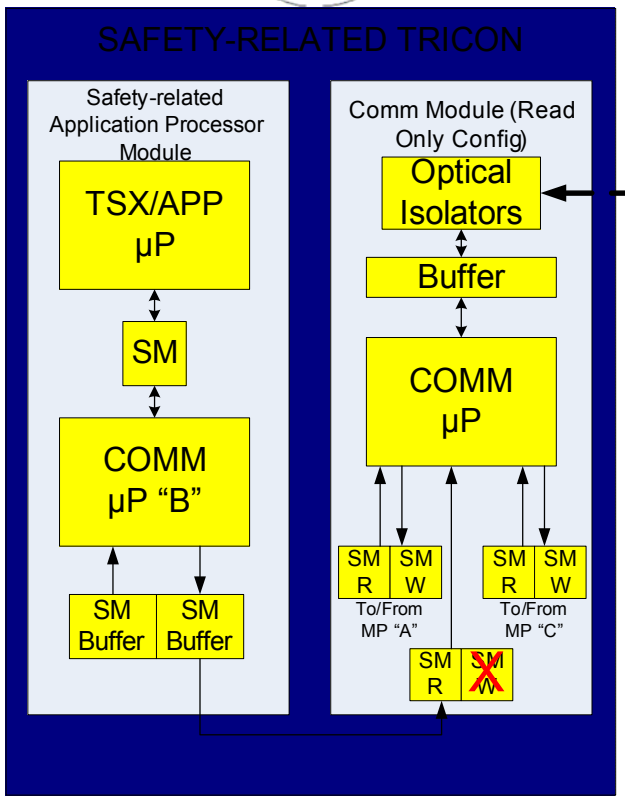
- At the end of every SR application processor scan, all data preprogrammed as “Read” or “Read-Write” and all diagnostics are automatically dumped to communication card memory; not by request

Then:

- A request for data comes into communication card
- The communication card looks only to it’s own memory for available data on a read request
- Acceptable read requests can only be for the listed “read” points or the request is ignored
- Only then are data transmitted out to service the read request

TRICON SR to NSR Communication



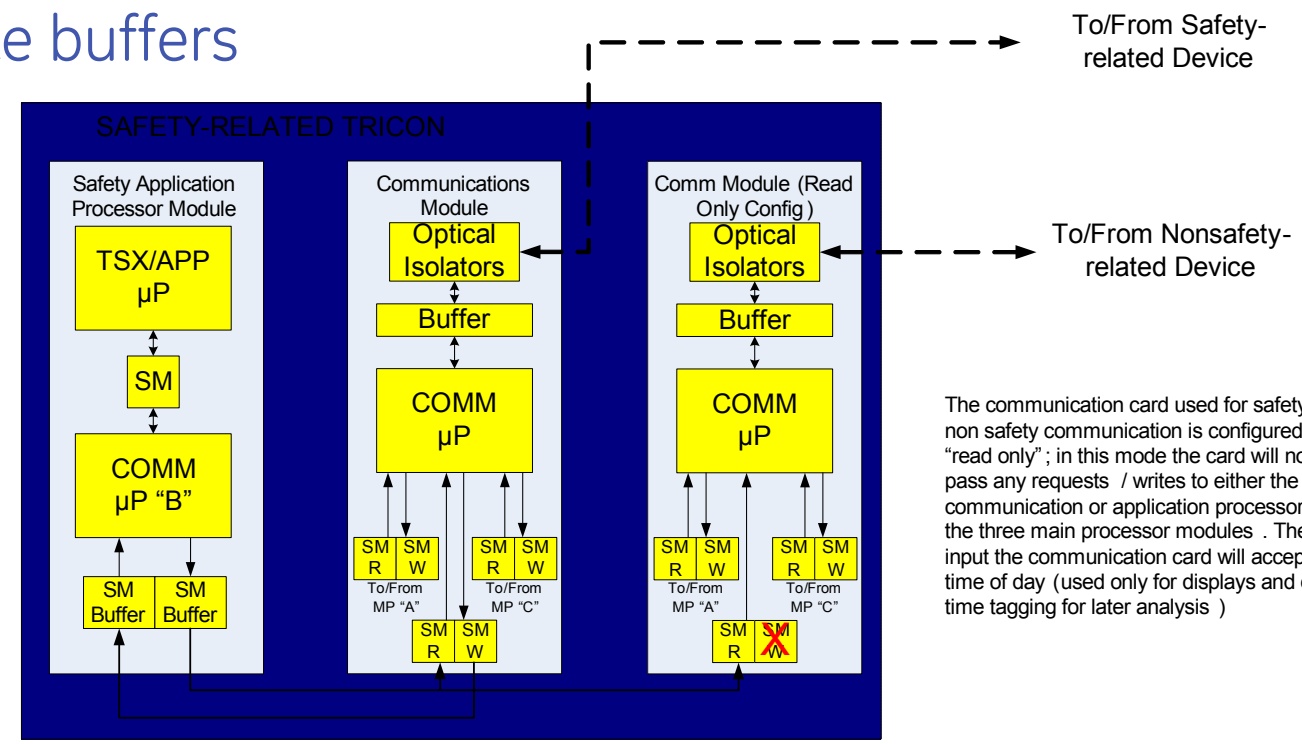


To/From Nonsafety-related Device

The communication card used for safety to non safety communication is configured as "read only"; in this mode the card will not pass any requests / writes to either the communication or application processors in the three main processor modules . The only input the communication card will accept is time of day (used only for displays and data time tagging for later analysis)

TRICON with SR to SR and SR to NR Communications

- SR / SR and SR / NSR communication cards are separate
  - > Separate communications processors
  - > Separate buffers



The communication card used for safety to non safety communication is configured as "read only"; in this mode the card will not pass any requests / writes to either the communication or application processors in the three main processor modules. The only input the communication card will accept is time of day (used only for displays and data time tagging for later analysis)

TRICON Hardware Communications Summary

- TRICON system maintains multiple barriers between the SR application processor and the communication process to external devices
  - > Shared Memory
  - > Buffers
  - > Two barrier processors between the SR application processor and the "outside" world
  - > Capability to disable write functions per communications card
  - > "Read" methodology that ensures no requests go further than the communication card
  - > Isolation / Data Independence is independent of external devices and is controlled fully within the TRICON System

TRICON Communication Data Integrity

Communication Data Integrity

- Physical independence, hardware isolation, redundancy and hardware reliability assure delivery of data with reasonable assurance of integrity

- Data integrity (cyber security) must be further assured by meeting additional requirements:
  - > Investigation of credible faults in communications
  - > Application of acceptable remedial measures

Communication Data Integrity (cont.)

- Specifically:
  - > Know when a message is good

  AND
  - > Know when a message is bad and take specific pre-analyzed actions

Credible Communications Failures

- Corruption
  - > Messages may be corrupted due to errors within a connected participant, errors on the transmission medium, or due to message interference
- Unintended Repetition
  - > Due to an error, fault or interference, old (not updated) messages are repeated at an incorrect point in time
- Incorrect Sequence
  - > Due to an error, fault or interference, the predefined sequence (e.g. natural numbers, time references) associated with messages from a particular source is incorrect

Credible Communications Failures (cont.)

- Loss
  - Due to an error, fault or interference, a message is not received or not acknowledged
- Unacceptable Delay
  - Messages may be delayed beyond their permitted arrival time window. Examples include errors in the transmission medium, congested transmission lines, interference, or due to connected participants sending messages in such a manner that services are delayed or denied (for example First In First Outs in switches, bridges, routers)

Credible Communications Failures (cont.)

- Insertion
  - Due to a fault or interference, a message is inserted that relates to an unexpected or unknown source entity
- Masquerade
  - Due to a fault or interference, a message is inserted that relates to an apparently valid source entity, so a NSR relevant message may be received by a SR relevant participant, which then treats it as SR relevant

Credible Communications Failures (cont.)

- Addressing
  - > Due to a fault or interference, a SR relevant message is sent to the wrong SR relevant participant, which then treats reception as correct

Deterministic Remedial Measures

- Sequence Number
  - > A sequence number is integrated into messages exchanged between message source and message receiver. It may be realised as an additional data field with a number that changes from one message to the next in a predetermined way
- Time Stamp
  - > In most cases the content of a message is only valid at a particular point in time. The time stamp may be a time, or time and date, included in a message by the sender

Deterministic Remedial Measures (cont.)

- Time Expectation
  - During the transmission of a message, the message receiver whether the delay between two consecutively received messages exceeds a predetermined value. In this case, an error has to be assumed
- Connection Authentication
  - Messages may have a unique source and/or destination identifier that describes the logical address of the safety relevant participant

Deterministic Remedial Measures (cont.)

- Feedback Message
  - > The message sink returns a feedback message to the source to confirm reception of the original message. This feedback message has to be processed by the SR communication layers

Deterministic Remedial Measures (cont.)

- Data Integrity Assurance
  - The SR application process does not trust that the incoming data's transmission integrity is assured by the sender, instead redundant data is included in the message to permit data corruptions to be detected by methods used by the receiver of the data
    - CRC (cyclic redundancy checks)
    - Hash functions

Data Integrity Summary

	Safety Measures					
Communication Errors	Sequence Number	Time Stamp	Time Expectation	Connection Authentication	Feedback Message	Data Integrity Assurance
Corruption					X	X
Unintended Repetition	X	X				
Incorrect Sequence	X	X				
Loss	X				X	
Unacceptable Delay		X	X			
Insertion	X			X	X	
Masquerade				X	X	
Addressing				X		

Message Authentication Techniques

- Hash function
  - > A hash function is used for digital signatures, data protection and message authentication. Hash functions take a message of variable length as input and produce a fixed-length string as output, referred to as hash-code or simply hash of the input message. More specifically a hash function is used to create a digital signature which can identify and authenticate both the sender and message of a digitally distributed message

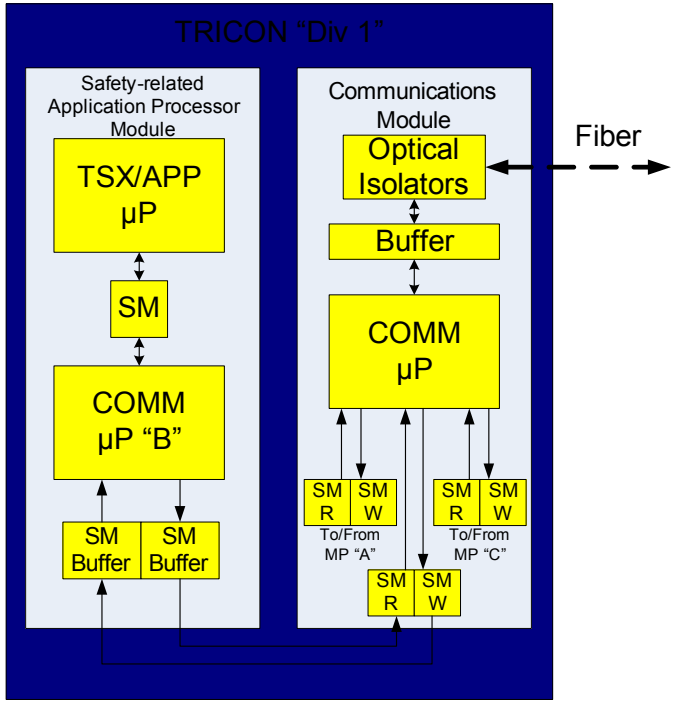
Message Authentication Techniques (cont.)

- CRC (cyclic redundancy check)
  - > Cyclic Redundancy Check is a technique used for detecting data transmission errors. Transmitted messages are divided by the sending processor into predetermined lengths that are then divided by a fixed divisor. The remainder result of that division is appended onto and sent with the message. When the message is received, the receiving processor recalculates the remainder and compares it to the transmitted remainder. If the numbers do not match, an error is detected

TRICON Communication Implementation

Function	Dest. Address & internal address	Source Address & internal address	Seq. #	Data	Hash Function	CRC-64

Assembled in Safety -related App Processor — Appended in Comm Card

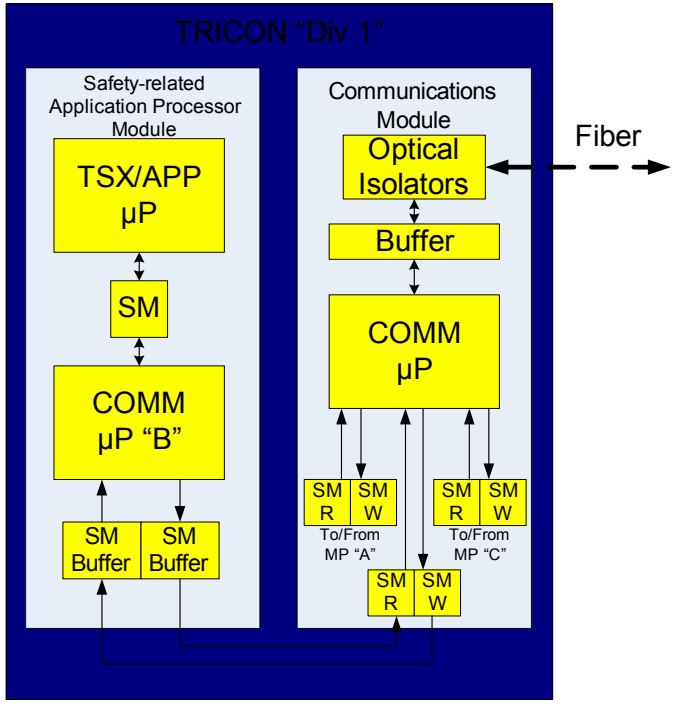


- TRICON expects a feedback message for every transmission. If the message is lost (non-validated), the sending unit will take action (alarm) and the receiving unit will take action as defined in the application program
- All remedial safety measures are taken within the SR application processor to ensure integrity of all internal communication links
- The user defines actions taken on loss of validated data/communication in the application program

TRICON Communication Implementation

Function	Dest. Address & internal address	Source Address & internal address	Seq. #	Data	Hash Function	CRC-64

Assembled in Safety -related App Processor — Appended in Comm Card



- Non-responsiveness will cause TRICONs to reset sequence numbers. Sequence numbers are not skipped
- CRC-64 added by communications card for extra security
- Addresses, internal addresses, data formats and ranges, data point ID's are all preprogrammed in each TRICON system. Messages that do not follow proper format are rejected
- Receiving TRICON verifies message and sends feedback response to Source TRICON

QNX Operating System

Ira Poppel / Joe Murray

Application and VDU Operating Systems Block Diagram

	Q-DCIS		N-DCIS
	Safety-related		Nonsafety-related
	RPS / NMS	SSLC/ESF	Mark VIe Nonsafety-related systems
VDU Functions	Monitoring and alarm only	Control, monitoring and alarm	Control, monitoring and alarm
VDU Operating System	VDU supplied by SSLC/ESF supplier	QNX	Cimplicity
Application Operating System	Custom NUMAC	Custom Tricon	QNX Mark VIe

Background

- QNX attributes
  - > Open operating system (OS)
  - > High operating experience
  - > Only open OS approved by NRC in VDU application

- ESBWR / QNX Application
  - > QNX OS used in ESBWR in safety-related VDU for control and monitoring of SSLC/ESF and for monitoring (only) of RPS / NMS
  - > Nonsafety-related logic processors

Regulatory Requirements (Safety-Related)

Review of some applicable standards

- 10 CFR 50.55a(h); IEEE Std 603-1991
  - 5.1 A single failure shall not prevent the proper operation of the protective function
  - 5.2 and 7.3 Once the protective actuation has been initiated, the actuation proceeds to completion (*unless purposefully stopped by operator action*)

Regulatory Requirements (Safety-Related)

Review of some applicable standards (cont.)

> NUREG 0800, Section 7, BTP HICB-19 Rev. 5, March 2007

- Section B.3, Acceptance Criteria (in part)
  - 5. "No failure of monitoring or display systems should influence the functioning of the reactor trip system or the ESFAS

Postulated Failure Mode in Regulatory Space

- Assume credible software common mode failures (SCMF) of the nonsafety-related logic processors and the safety-related VDU system

- Regulatory Requirement
  - SSLC/ESF safety-related system remains operable, will start actuation when required, and will take actuation to completion

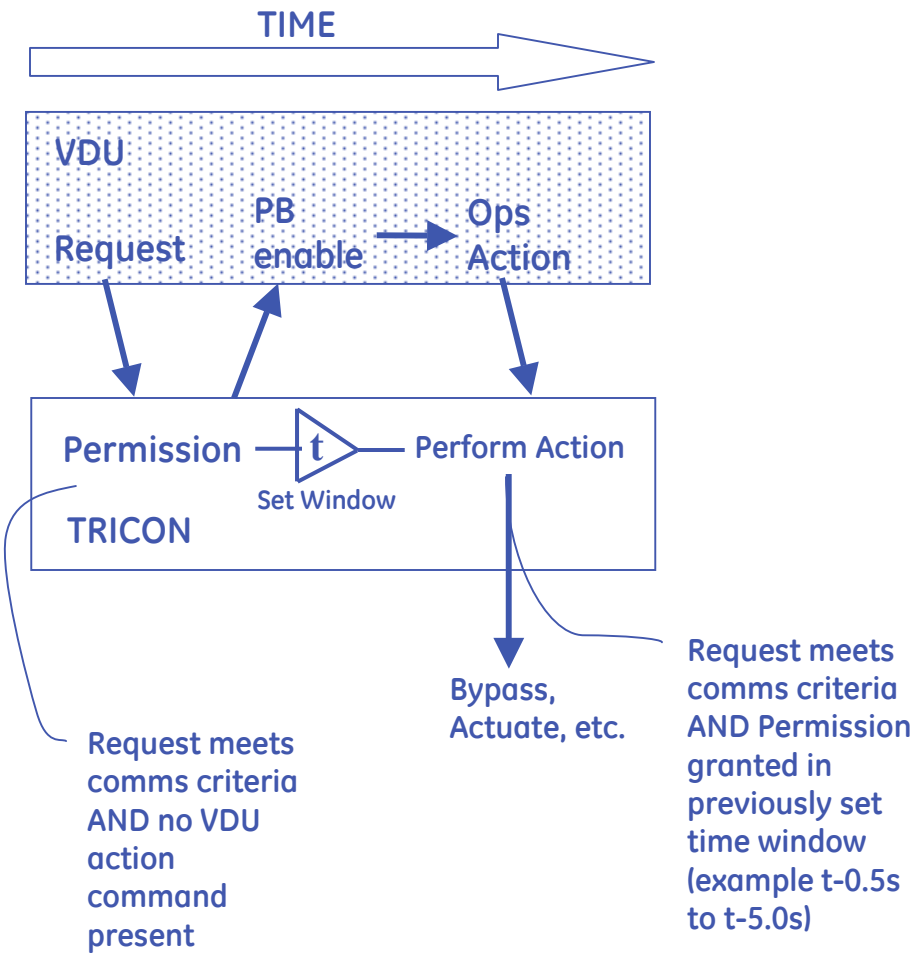
- Verify that design will not allow for credible failure of the safety-related VDU to prevent SSLC/ESF operability

Design for SSLC/ESF operability with failed VDU OS

- VDU failure must not be able to stop SSLC/ESF actions
- VDU / SSLC/ESF TRICON design requirement
  - > Sequential interchange actions by both
  - > Proper sequential commands by VDU in SCMF state – not credible
- VDU must perform two distinct actions to change plant parameter
- VDU Failure that would send proper sequential commands and acknowledge safety-related permissives is not credible

VDU / SSLC/ESF action sequence

- Design places SCMF of QNX into "incredible" failure mode
- OS failure mode would have to disable Diverse System AND cause VDU to start issuing proper sequentially timed commands
- This mitigating design also supports Investment Protection
- Inadvertent actuations are not caused by failed VDU



ESBWR Instrumentation & Controls - Update

Recap

- QNX OS has two paths on ESBWR; VDU (safety-related) and Logic Processor (nonsafety-related)

- Regulatory path requires showing that failure mode will not prevent SSLC/ESF from performing its safety function
  - > Mitigating design methodologies in place

- Non-regulatory "Investment Protection" path requires assurance that failure mode will not cause inadvertent actuations
  - > Mitigating design methodologies in place

RAI 7.1-48 / Plant Specific SER Items

Rich Miller / Joe Murray

Item #1: Qualification for Temperature and Humidity Conditions

"Licensees will be responsible for analysis of the plant-specific environment, and the determination that the Tricon PLC system is suitable for that particular plant usage"

- Temperature and Humidity testing of the TRICON PLC was satisfactorily performed
- Environmental Qualification for TRICON will be provided in LTR 7286-546, Rev 2 scheduled to be issued ~October, 2007
- GE will evaluate these reports to ensure they envelop GE standard design requirements
- ITAAC - Item 1 in Table 2.2.13-1

Item #2: Qualification for Radiation Exposure Levels

"Licensees will be responsible for analysis of the plant-specific radiation environment, and the determination that the TRICON PLC system is suitable for that particular plant usage"

- Since the original SER was issued, Invensys has repeated a set of qualification tests and analyses to cover updates to the Triconex Nuclear Qualified Equipment List and to cover TRICON design changes
- Radiation exposure equivalent to 1E4 rads over 40 years
- This report will be issued by Invensys ~October, 2007
- GE will evaluate these reports to ensure they envelop GE standard design requirements
- ITAAC - Item 1 in Table 2.2.13-1

Item #3: Qualification for Seismic Levels

"The staff found that the Tricon PLC system did not fully meet the guidance of EPRI TR-107330 for seismic requirements, and before using Tricon PLC system equipment in safety-related systems in a nuclear power plant, licensees must determine that the plant-specific seismic requirements are enveloped by the capabilities of the Tricon PLC system"

- Since the original SER was issued, Invensys has repeated a set of qualification tests and analyses to cover updates to the Triconex Nuclear Qualified Equipment List to cover TRICON design changes
- The system passed these tests with a 14g peak in the test response spectrum
- This test report will be issued by Invensys ~October, 2007
- GE will evaluate these reports to ensure they envelop GE standard design requirements
- ITAAC - Item 1 in Table 2.2.13-1

Item #4: Qualification for EMI/RFI: Conducted or Radiated Emissions

"Since the Tricon PLC system did not satisfy the guidance of EPRI TR-102323, it is the responsibility of the licensees to measure or otherwise determine the worst case EMI/RFI environment that would exist at the time the protective function provided by the Tricon PLC system would be required, and then to ensure that the conducted and radiated EMI/RFI emissions and susceptibility capabilities of the Tricon PLC system envelop this environment, and that the system will not affect surrounding equipment"

- Since the original SER was issued, Invensys has repeated a set of qualification tests (in accordance with RG 1.180, Rev. 1) on TRICON equipment

Item #4: Qualification for EMI/RFI: Conducted or Radiated Emissions (cont.)

- Final test reports with associated mitigating design requirements (filters, ferrites, etc.) will be issued by Invensys ~October, 2007
- GE will evaluate these reports to ensure they envelop GE standard design requirements
- ITAAC - Item 1 in Table 2.2.13-1

Item #5: Surge Withstand Capabilities

"Licensees will be responsible for the analysis of the plant-specific surge environment, and the determination that the Tricon PLC system is suitable for that particular plant usage"

- Since the original SER was issued, Invensys has repeated a set of qualification tests (in accordance with RG 1.180, Rev. 1) on TRICON equipment
- Final test reports with associated mitigating design requirements (filters, ferrites, etc.) will be issued by Invensys ~October, 2007
- GE will evaluate these reports to ensure they envelop GE standard design requirements
- ITAAC - Item 1 in Table 2.2.13-1

Item #6: Electrostatic Discharge (ESD) Withstand Capability

"Before installing and using the Tricon PLC system, licensees must have in place administrative or physical controls to ensure that no activity which would require opening the cabinet can take place while the Tricon PLC system is required to provide its protective function, unless the particular cabinet and all channels within that cabinet are placed in a trip or bypassed condition according to plant procedures. An alternative solution is for licensees to perform sufficient testing and analysis to demonstrate that the ESD withstand capability of the Tricon PLC system envelops the plant-specific requirements"

- Since the original SER was issued, Invensys has repeated a set of qualification tests on TRICON equipment.
- ESD is not included within RG 1.180, Rev. 1 because ESD is not a common mode failure. Invensys will test per the levels of EPRI TR-102323 Rev. 1 to be in keeping with the test requirements of EPRI TR-107330

Item #6: Electrostatic Discharge (ESD) Withstand Capability

- Final test reports will be issued by Invensys ~October, 2007
- GE will evaluate these reports to ensure they envelop GE standard design requirements
- ITAAC - Item 1 in Table 2.2.13-1

Item #7: Safety-Related ("Class 1E") to Nonsafety-related (Non 1E) Isolation from Credible Voltages

"Licensees will be responsible for analysis of the plant-specific maximum credible applied voltages produced by non-1E interfaces, and for ensuring that this value is enveloped by the Tricon PLC system capacity, and that the Tricon PLC system is suitable for that particular plant usage"

- Class 1E to Non-1E isolation testing of the TRICON was performed in accordance with the requirements of EPRI TR-107330 and IEEE Standard 384-1981
- The TRICON met all applicable performance requirements during and after application of the Class 1E to Non-1E isolation test voltages
- GE will evaluate these reports to ensure they envelop GE standard design requirements
- ITAAC - Item 5 in Table 2.2.13-1

Item #8: Software Installation Plan Development

"The staff determined that the software installation plan is the responsibility of the licensee, and must be developed before the Tricon PLC system software can be used for safety-related applications in software maintenance plan before the Tricon PLC system software can be used for safety-related applications in nuclear power plants"

- The IPS software quality development plan complies with the Standard Review Plan, Branch Technical Position (BTP) 14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems"
- After commissioning, any changes to the application itself or the application program are covered by the licensee Software Quality Assurance plan
- GE will evaluate Invensys' plan to ensure it exceeds or is equivalent to that required of the certification
- ITAAC - Item 5 in Table 3.2-1

Item #9: Software Maintenance Plan Development

"Although Triconex has an acceptable software maintenance plan, the staff determined that a plant-specific software maintenance plan is also required, and it is the responsibility of licensees to develop this simple to complex systems. The determination of the response time for the particular system intended for safety-related use for a particular plant application, and the determination that this response time satisfies the plant-specific requirements in the accident analysis in Chapter 15 of the safety analysis report is the responsibility of the licensee"

- Refer to Appendix 7B of DCD Tier 2, 26A6642AW, Rev. 3
- GE will evaluate Invensys' plan to ensure it exceeds or is equivalent to that required of the certification
- Plant-specific setpoint analyses will confirm the acceptability of the control system response time
- ITAAC - Items 6 and 9 in Table 3.2-1

Item #10: Software Operations Plan Development

"The staff determined that licensees will be required to develop a software operations plan before using the Tricon PLC system software for safety-related use in nuclear power plants"

- Refer to Appendix 7B of DCD Tier 2, 26A6642AW, Rev. 3
- GE will evaluate Invensys' plan to ensure it exceeds or is equivalent to that required of the certification
- ITAAC - Item 6 in Table 3.2-1

Item #11: Software Safety Plan Development

"The staff determined that licensees will be required to develop a software safety plan before using the Tricon PLC system software for safety-related applications in nuclear power plants"

- Refer to Appendix 7B of DCD Tier 2, 26A6642AW, Rev. 3
- GE will evaluate Invensys' plan to ensure it exceeds or is equivalent to that required of the certification
- ITAAC - Item 8 in Table 3.2-1

Item #12: Software Verification and Validation

"Although Triconex did not strictly follow guidelines of IEEE Std 1012, the staff determined that the combination of the internal Triconex review, the TÜV certification, and the review by MPR and ProDesCon provided acceptable verification and validation for software that is intended for safety-related use in nuclear power plants. However, the staff noted that a significant portion of its acceptance is predicated upon the independent review by TÜV-Rheinland, and licensees using any Tricon PLC system beyond Version 9.5.3 must ensure that similar or equivalent independent V&V is performed; without this, the Tricon PLC system will not be considered acceptable for safety-related use at nuclear power plants. Should licensees use future Tricon PLC systems beyond Version 9.5.3 which have not received TÜV-Rheinland certification, the staff will review the acceptability of the independent V&V during the plant-specific safety evaluation"

Item #12: Software Verification and Validation (cont.)

- Although listed as a plant-specific requirement, this would appear to be a platform-specific requirement. Triconex utilizes the services of TÜV-Rheinland as the classical, independent, creditable third part reviewer of software development and testing
- TÜV services are now an integral component of Invensys' 10 CFR 50 Appendix B QA program and all changes to the TRICON system undergo internal and TÜV V&V services
- Refer to Appendix 7B of DCD Tier 2, 26A6642AW, Rev. 3
- GE will evaluate Invensys' plan to ensure it exceeds or is equivalent to that required of the certification
- ITAAC - Item 9 in Table 3.2-1

Item #13: Impact of TriStation 1131 Use of Tricon PLC Operability

"That section noted that the Triconex PLC system is designed such that the Tricon PLC system should not be connected to a TriStation PC during safety-related operation. The plant-specific procedures which ensure that the TriStation PC is not connected to the Tricon PLC system during safety-related operation will be reviewed by the staff during the plant-specific safety evaluation. In addition, the testing of the operational software produced by the TriStation 1131, and these test plans, procedures, and results will be reviewed by the staff during the plant-specific safety evaluation"

- While the TRICON is performing safety critical functions, it will not be connected to the TriStation 1131 PC during normal operation

Item #13: Impact of TriStation 1131 Use of Tricon PLC Operability

- The application software programmed for the SSLC/ESF and the associated test plans, procedures, and results will be available for audit and/or inspection by the staff prior to plant-specific use
- Keys to TRICONs will be under administrative control as will be the rooms and cabinets
- ITAAC - Item 6 in Table 3.2-1

Item #14: Plant Specific Application Program

"Section 4.2.4 of this SE discusses the application programs, which are inherently plant specific, and therefore are not included in the scope of this SE"

- The Invensys software quality development plan complies with the Standard Review Plan, Branch Technical Position (BTP) 14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems"
- The application software programmed for the SSLC/ESF and the associated test plans, procedures, and results will be available for audit and/or inspection by the staff prior to plant-specific use
- ITAAC - Item 1 in Table 3.2-1

Item #15: Component Aging Analysis

"Section 4.3.3 of this SE discusses the component aging analysis, which determined that the chassis power supplies and backup batteries are susceptible to significant, undetected aging mechanisms. Before installing Tricon PLC system equipment in a nuclear power plant, licensees must have procedures in place to ensure periodic replacement of these components"

- Aging degradation of these components can be effectively addressed through periodic replacement prior to onset of significant loss of performance
- Replacement procedures are contained in the TRICON Planning and Installation Guide
- The qualified life maintenance process will be prepared to include vendor replacement recommendations as discussed in Section 3.11.2 in the DCD
- ITAAC - Table 3.6-1

Item #16: Response Time Characteristics

"The staff determined that the actual response time for any particular system will depend upon the actual system configuration, and may vary significantly from nuclear power plants"

- The SSLC/ESF platform operating the ESBWR specific application will be tested during factory acceptance testing. The testing will specifically confirm required response times. There is no credible failure mode that can change the system response time
- Plant-specific setpoint analyses confirms the acceptability of the control system response time
- ITAAC - Item 9 in Table 3.2-1

Item # 17: Diversity and Defense-In-Depth (D3)

"A review of the differences between the Tricon PLC system and the non-safety control system implemented at a particular nuclear power plant, and the determination that plant specific required diversity and defense-in- depth continue to be maintained must be addressed in a plant-specific D-in-D&D evaluation"

- Licensing Topical Report NEDO-33251, Rev. 0, "ESBWR I&C Defense-In-Depth and Diversity Report," outlines the diversity and defense-in-depth of the ESBWR safety-related and nonsafety-related systems
- NEDO-33251 will be updated in it's next revision to include vendor specific information for the SSLC/ESF platform
- ITAAC - Table 2.2.14-1

Item # 18: Qualification Summary Report "Applications Guide" Recommendations

"Triconex has made a number of determinations of items and criteria to be considered when applying the Tricon PLC system to a specific plant application. These are contained in the "Applications Guide," provided as Appendix B to the "Qualification Summary Report," Triconex document number 7286-545. A number of these are the same as those discussed above, but the "Applications Guide" goes beyond regulatory compliance to include good engineering practice and applications suitability determinations. It is expected that licensees intending to use the Tricon PLC system will consider each item in this guide, and document the appropriate decisions and required analysis"

- The SSLC/ESF LTR will provide the ESBWR requirements based on the latest qualification testing provided for the TRICON PLC
- The SSLC/ESF LTR is scheduled to be issued ~October, 2007

IEEE 603 Lifecycle

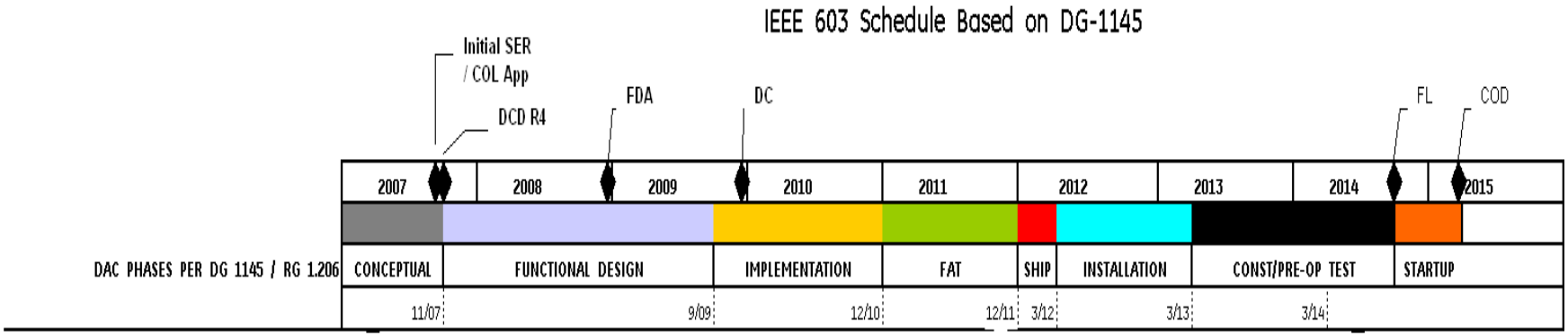
Rich Miller

Typical Lifecycle Phases

- Overview
- Conceptual Design Phase (IEEE 603 Section 4)
- Functional Design Phase (IEEE 603 Section 6/7)
- Physical Design Phase (IEEE 603 Section 5)

ESBWR Instrumentation & Controls - Update

Overview



[1] - In DCD

[2] - ITAAC exists in DCD Tier 1 Revision 3 for RPS, Table 2.2.7-1

▽ Related information available

◬ Data available for partial closure

▼ Firm closure for part or all of data

Acronyms:

Calc	Calculation(s)	EQ	Equipment Qualification	S/U	Startup
COD	Commercial Operation Date	FAT	Factory Acceptance Test	SER	Safety Evaluation Report
COL	Combined Operating License	FDA	Final Design Authority	SLD	Simplified Logic Diagrams
Const/Pre-Op	Construction/Pre-Operational	FL	Fuel Load	Spec	Specification
D3	Defense	FMEA	Failure Modes and Effects Analysis	SQAP	Software Quality Assurance Plan
DC	Design Complete	HFE	Human Factors Engineering	SSA	Software Safety Analysis
DCD	Design Control Document	Insp	Inspection(s)	T.S.	Technical Specifications
DCIS	Distributed Control & Information Syste	PDM	Project Design Manual	TA	Task Analysis
DLD	Detailed Logic Diagram	PO	Purchase Order		
Doc(s)	Document(s)	Prelim	Preliminary		

ESBWR Instrumentation & Controls - Update

Conceptual Design Phase

IEEE 603 Schedule Based on DG-1145

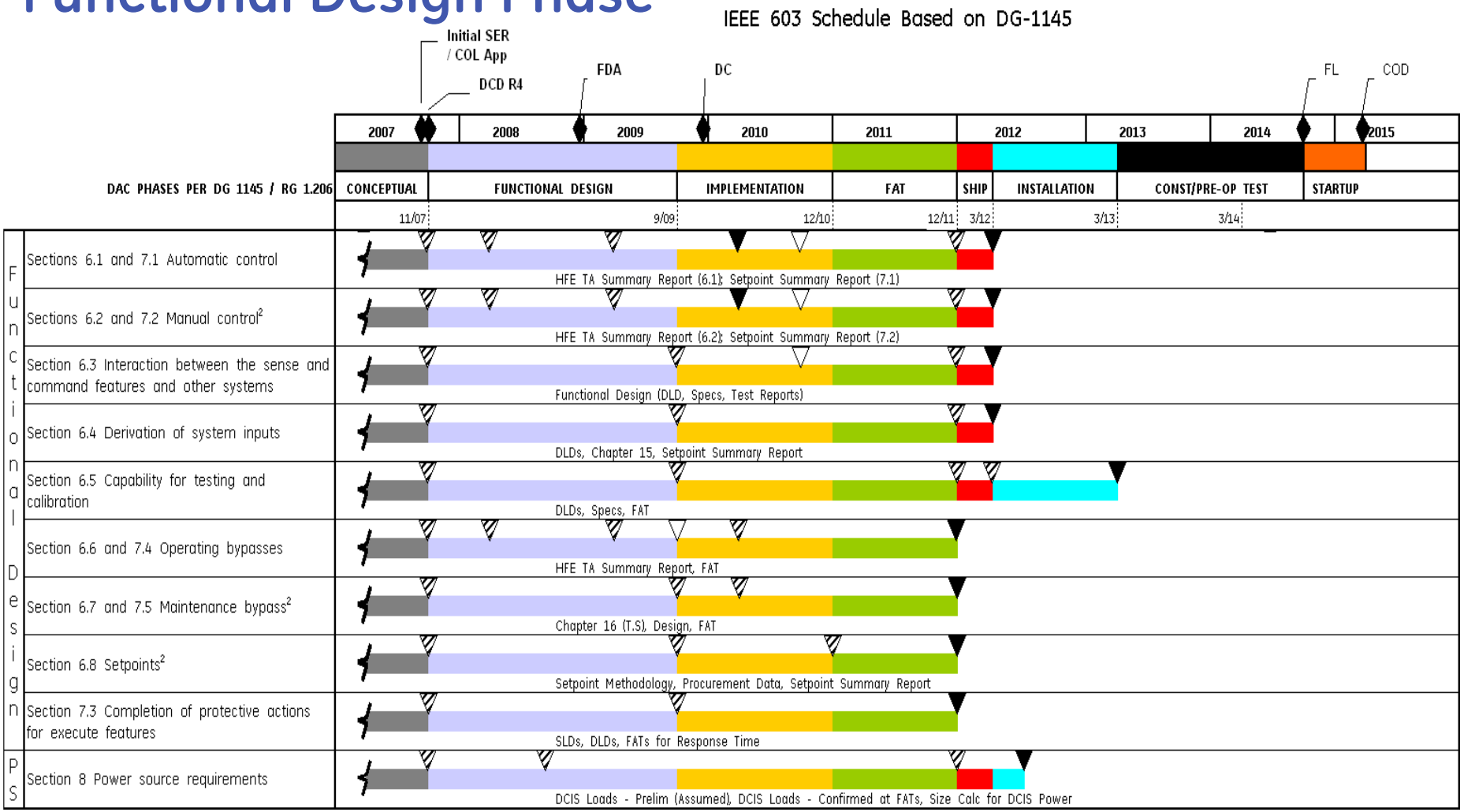
Initial SER / COL App
DCD R4
FDA
DC
FL
COD

DAC PHASES PER DG 1145 / RG 1.206	2007	2008	2009	2010	2011	2012	2013	2014	2015
	CONCEPTUAL	FUNCTIONAL DESIGN		IMPLEMENTATION	FAT	SHIP / INSTALLATION		CONST/PRE-OP TEST	STARTUP
	11/07		9/09	12/10	12/11	3/12	3/13	3/14	

Conceptual Design	Section 4.1 Identification of design-basis events[1]	
	Section 4.2 Identification of safety functions and protective actions of execute features[1]	[Not addressed in DG-1145]
	Section 4.3 Identification of permissive conditions for each operating bypass[1]	[Not addressed in DG-1145]
	Section 4.4 Identification of variables monitored and analytical limits[1]	
	Section 4.5 Minimum criteria for manual initiation of control of protective actions[1]	
	Section 4.6 Identification of minimum number and locations of sensors[1]	
	Section 4.7 Range of transient and steady-state conditions[1]	
	Section 4.8 Identification of conditions that have the potential to cause functional degradation of safety system performance[1]	
	Section 4.9 Identification of the methods used to assess the reliability of the safety system design[1]	
	Section 4.10 Identification of critical points in time after onset of design-basis event[1]	[Not addressed in DG-1145]
	Section 4.11 Identification of protective provisions that prevent safety system functions[1]	[Not addressed in DG-1145]
	Section 4.12 Identification of other special design basis that may be imposed[1]	[Not addressed in DG-1145]

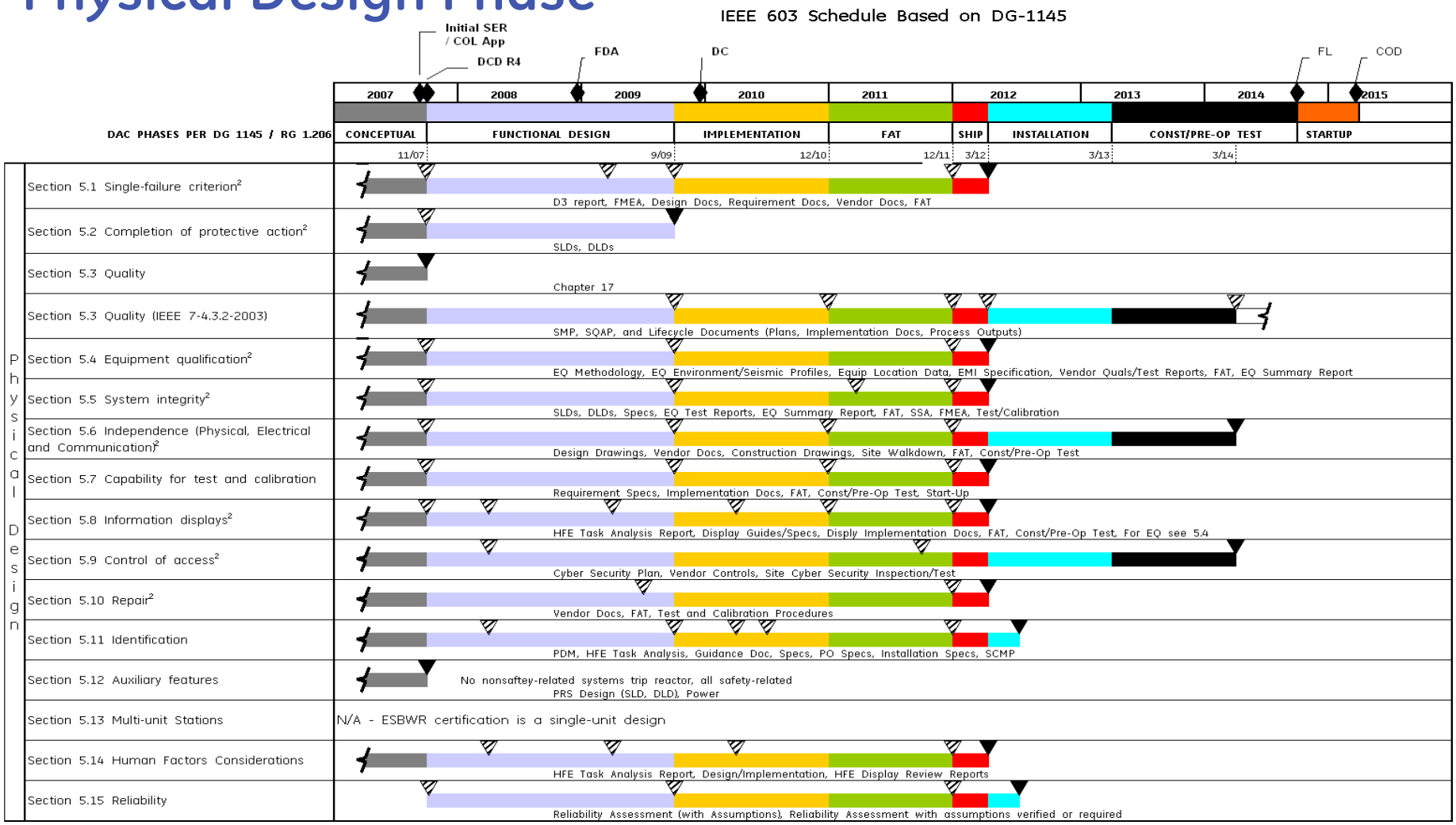
ESBWR Instrumentation & Controls - Update

Functional Design Phase



ESBWR Instrumentation & Controls - Update

Physical Design Phase



imagination at work

Unverified Draft

ITAACs Related to IEEE 603

Peter Yandow / Rich Miller

ESBWR Instrumentation & Controls - Update

Inspections, Tests, Analyses, Acceptance Criteria (ITAAC) Related to IEEE 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"

- Addressed IEEE-603 in DCD Revision 3
- Addressing IEEE-603 in Tier 1, Revision 4
- Example IEEE-603 ITAAC in Tier 1, Revision 4, Table 2.2.15-2
- Lifecycle and ITAAC Closure

ESBWR Instrumentation & Controls - Update

Addressed IEEE 603 in DCD Revision 3

- Addressed IEEE-603 criteria in DCD Tier 2, subsection 7.1.6.6.1
- Added sample IEEE-603 ITAAC to Tier 1, Rev. 3 pending issuance of RG 1.206
- Planned to address remaining criteria via responses to RAIs 7.1-4 through 7.1-30

ESBWR Instrumentation & Controls - Update

Addressing IEEE 603 in Tier 1, DCD Revision 4

- Address all IEEE-603 criteria for evaluating in Tier 1

- Add Tier 1 Subsection 2.2.15 to be a common location for all IEEE-603 ITAAC
  - > Address criteria applicable to each ESBWR system
  - > Include appropriate ITAAC

- Move IEEE-603 related ITAAC from other subsections to new Tier 1, subsection 2.2.15

ESBWR Instrumentation & Controls - Update

Tier 1, Revision 4, Subsection 2.2.15

- Tier 1, Table 2.2.15-1 to identify I&C systems and the IEEE-603 criteria applicable to their design

- Tier 1, Table 2.2.15-2 to identify:
  - > IEEE-603 Design Acceptance Criteria / ITAAC
  - > IEEE-603 post-design ITAAC

- Refer to Handout: Sample Tier 1 Design Descriptions and subsection 2.2.15 tables depicting examples

ESBWR Instrumentation & Controls - Update

Tier 1, Revision 4, Subsection 2.2.15

- Tier 1, Table 2.2.15-1 to identify I&C systems and the IEEE-603 criteria applicable to their design

- Tier 1, Table 2.2.15-2 to identify:
  - > IEEE-603 Design Acceptance Criteria / ITAAC
  - > IEEE-603 post-design ITAAC

- Refer to Handout: Sample Tier 1 Design Descriptions and subsection 2.2.15 tables depicting examples

ESBWR Instrumentation & Controls - Update

Example IEEE 603 ITAAC in Tier 1, Revision 4, Table 2.2.15-2

- Single Failure: Criterion 5.1
  - > DAC-ITAAC only
  - > Generic wording for all applicable I&C systems

- Completion of Protective Actions: Criteria 5.2 & 7.3
  - > DAC and post-design ITAAC
  - > ITAAC specific to system

- System Integrity: Criterion 5.5
  - > Post-design ITAAC Only
  - > Generic wording for all applicable I&C systems

ESBWR Instrumentation & Controls - Update

Example IEEE 603 ITAAC in Tier 1, Revision 4, Table 2.2.15-2 (continued)

- Capability for Test & Calibration: Criteria: 5.7 & 6.5
  - > DAC-ITAAC only
  - > Generic wording for all applicable I&C systems

- Information Displays: Criterion 5.8
  - > Post-design ITAAC only
  - > Generic wording for all applicable I&C systems

ESBWR Instrumentation & Controls - Update

Summary

- Captured IEEE-603 design criteria in DAC-ITAAC
- Consolidate IEEE-603 design criteria ITAAC in single Tier 1 subsection 2.2.15
- Maintain Lifecycle and ITAAC closure schedule

Equipment Qualification – RG 1.209

Jim Gleason

ESBWR Instrumentation & Controls - Update

RG 1.209

- C.1
  - > Type testing is preferred method
  - > Service conditions based on the actual environmental conditions
- C.2
  - > IEEE Std. 323-2003 mild environment qualification
  - > I&C system functioning and representative at specified normal and abnormal service conditions
  - > Test all safety-related functions and ensure no impairment

RG 1.209

- C.2 (continued)
  - Testing:
    - Confirm the response
    - Verify impact of environmental effects
    - Type testing an entire system or parts thereof
    - Dynamic response to the most limiting conditions
- C.3
  - IEEE Std. 323-2003
    - Electromagnetic interference/radio frequency interference (EMI/RFI) and surge as environmental conditions
  - Regulatory Guide 1.180, Rev. 1

RG 1.209

- C.4
  - > IEEE Std. 323-2003
    - – Section 7.2 In lieu of Section 7.1.
    - – Records should be retained at a facility in an auditable and readily accessible form for review and use as necessary
- C.5
  - > Regulatory Guide 1.89 for harsh environment
  - > Regulatory positions of this guide (RG 1.209) supplement the harsh environment qualification practices endorsed in Regulatory Guide 1.89

RG 1.209 - Commitment

- RG 1.209 is being considered for Rev. 4 of DCD
  - DCD Chapter 7 Instrumentation and Control Systems
  - DCD Chapter 3 Design of Structures, Components, Equipment and Systems,
    - 3.11 Environmental Qualification of Mechanical and Electrical Equipment

November 2006 I&C Audit Open Items

DCD Changes from Rev. 2 to Rev. 3

Peter Yandow / Rich Miller

Chapter 7 Revision 2 to Revision 3 Changes

- Re-wrote Section 7.1
  - > Clearly describe operation of I&C system communications (previously in Section 7.9)
  - > Removed Section 7.9

- Changed safety-related and nonsafety-related Distributed Control and Instrumentation System Abbreviations
  - > E-DCIS is now Q-DCIS
  - > NE-DCIS is now N-DCIS

Chapter 7 Revision 2 to Revision 3 Changes

- Updated Tables
  - > Table 7.1-1 includes newer revisions of Standards / Guides
  - > Table 7.1-2 addresses IEEE 603 design criteria

- Addressed new Regulations applicable to ESBWR
  - > Regulatory Guide 1.97 Revision 4
  - > Regulatory Guide 1.204 / Regulatory Guide 1.180
  - > Regulatory Guide 1.153

Chapter 7 Revision 2 to Revision 3 Changes

- Addressed RAI 7.2-34
  - Mode switch positions

- Write-ups Enhanced / Expanded
  - Gravity Driven Cooling System Operational Description
  - Rod Control & Information System Functional Description (to include Diverse Protection System discussion)
  - Turbine Generator Control System Description (to include operator control, automation options and valve controls)

Chapter 7 Revision 2 to Revision 3 Changes

- Items Removed
  - > Information on Post Accident Sampling (NRC SER as basis)
  - > "Class 1E"
  - > Section 7.A (information found in Section 7.7)

- Revised subsections of Section 7.B – Software Plans

Status of RAIs

Jim Kinsey

Status of RAIs – Chapter 7

- RAI's Addressed in DCD Revision 3 - **11**
- RAI's Transmitted in letters after DCD Revision 3 - **40**
- Open RAI's - **67**

Discussion on RAIs

Rich Miller / Peter Yandow