PMSTPCOL PEmails

From: Cook, James W [jwcook@STPEGS.COM]
Sent: Friday, January 28, 2011 4:02 PM
To: Muniz, Adrian
Subject: STP 3 & 4 Ch 7 presentation slides for 08Feb
Attachments: ACRS Presentation Ch 07 FSE (draft) 1-26(ccc).pdf

Attached are draft slides for our ACRS presentation on 08Feb.

James Cook

Licensing Engineer STP 3 & 4
jwcook@stpegs.com
(409)504-0337

Hearing Identifier: SouthTexas34Public_EX
Email Number: 2576

Mail Envelope Properties (C7F098E3C31A0141A02043F0B8E656EE26B628209F)

Subject: STP 3 & 4 Ch 7 presentation slides for 08Feb
Sent Date: 1/28/2011 4:01:45 PM
Received Date: 1/28/2011 4:01:52 PM
From: Cook, James W

Created By: jwcook@STPEGS.COM

Recipients:
"Muniz, Adrian" <Adrian.Muniz@nrc.gov>
Tracking Status: None

Post Office: exgmb1.CORP.STPEGS.NET

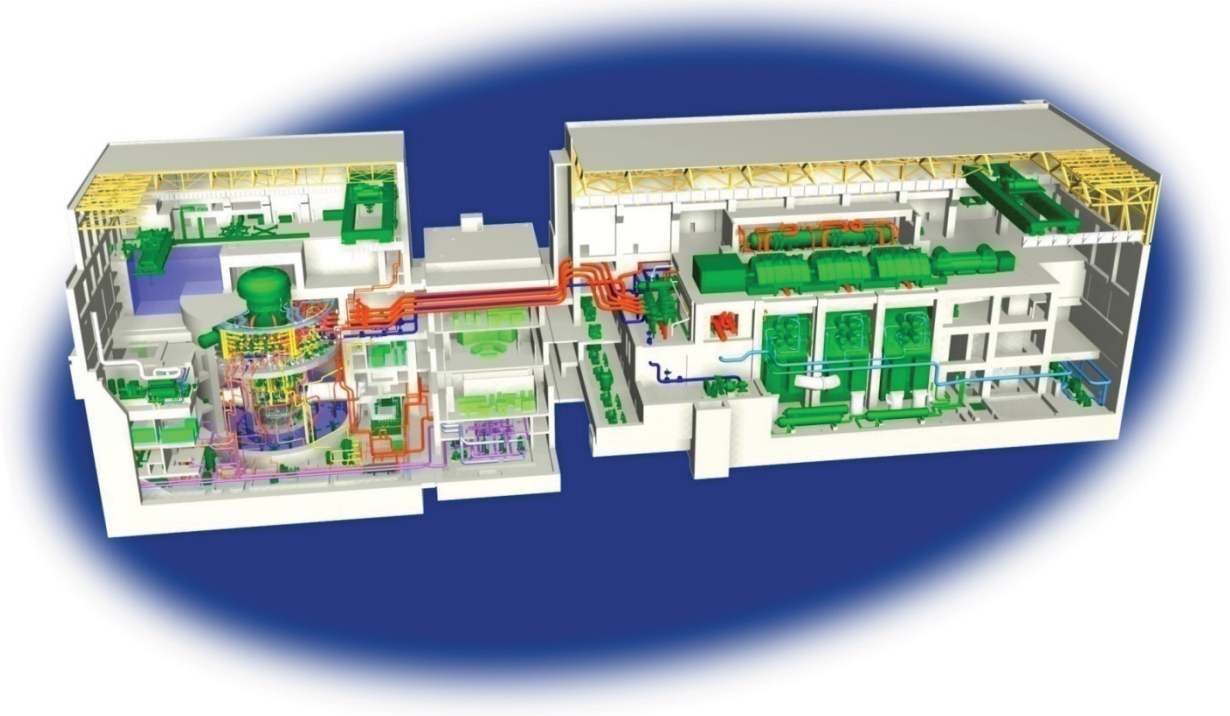
Files	**Size**	**Date & Time**
MESSAGE	188	1/28/2011 4:01:52 PM
ACRS Presentation Ch 07 FSE (draft) 1-26(ccc).pdf	731664	

Options
Priority: Standard
Return Notification: No
Reply Requested: No
Sensitivity: Normal
Expiration Date:
Recipients Received:

DRAFT

South Texas Project Units 3 & 4 Presentation to ACRS Subcommittee

Chapter 7
Instrumentation and Control Systems



DRAFT

DRAFT

Agenda

Chapter 7 was discussed at ACRS ABWR Subcommittee on May 20. No Open Items were identified in the draft SER.

Other Issues:

- Setpoint Methodology
- Current RGs and Codes and Standards applied to Common Q Platform
- Appendix 7DS
  - Four Design Principles
  - Simplicity

DRAFT

DRAFT

Attendees

DRAFT

Instrument Setpoint Methodology

- RAI 07.01-16
- WCAP-17119-P Revision 2, “Methodology for South Texas Project Units 3 & 4 ABWR Technical Specification Setpoints” submitted on July 29, 2010
- Included a summary of methodology application and typical setpoints for the OPRM trip function

DRAFT

DRAFT

Current RGs and Codes and Standards applied to Common Q Platform

- RAI 07.01-14
- Westinghouse Common Q Platform (WCAP-16097) approved applying RGs and industry codes and standards in effect at the time
- STPNOC has committed to apply the RGs and codes and standards in effect 6 months prior to submittal of the COLA for all safety related DI&C platforms including Common Q

DRAFT

DRAFT

FSAR Appendix 7DS

- Includes no new design changes or departures
- Consolidates information from various parts of COLA and applicable technical reports regarding
  - Four Design Principles (redundancy, independence, determinism & diversity)
  - Simplicity
- Scope includes safety-related digital instrumentation & control (DI&C)
  - Reactor Trip and Isolation System (RTIS) & safety-related Neutron Monitoring System (NMS) using Field Programmable Gate Array (FPGA) based platform
  - Engineered Safety Features Logic & Control System (ELCS) using Common Q based platform
- Maps Design Principles to applicable ITAAC and DAC

DRAFT

DRAFT

RTIS/NMS Platform Overview

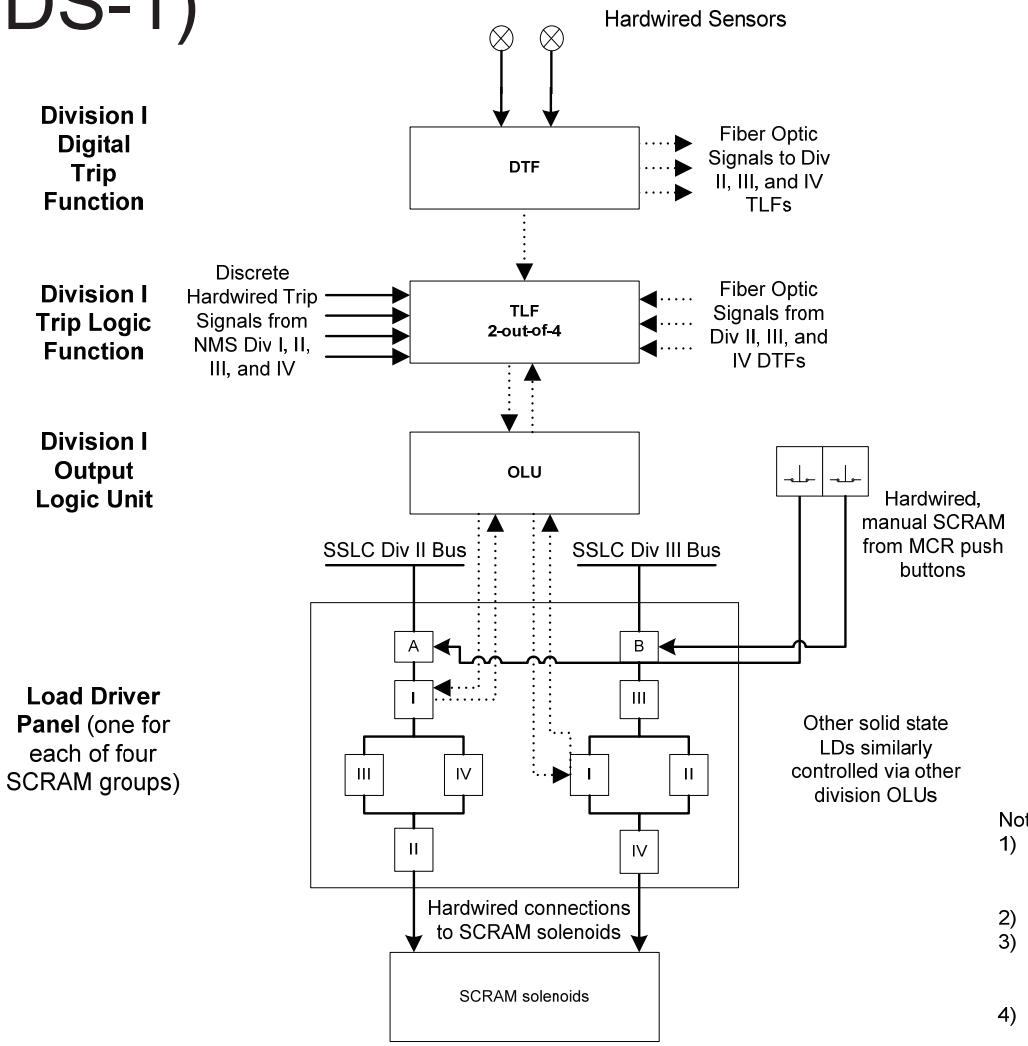
- Digital Trip Function (DTF)
  - Digitizes hardwired sensor input
  - Compares signal values to setpoints to determine sensor division trip status
- Trip Logic Function (TLF)
  - Receives sensor division trip status information from four redundant DTFs
  - Performs 2-out-of-4 voting to determine automatic divisional trip
  - Sends divisional trip status to Output Logic Unit
- Output Logic Unit (OLU)
  - Receives automatic divisional trip status from its divisional TLF
  - OLU distributes trip outputs to Load Drivers (LDs) for reactor trip and Main Steam Isolation Valve (MSIV) closure

DRAFT

DRAFT

RTIS/NMS Platform Overview

(Figure 7DS-1)



Notes:
1) RTIS-RPS Division I shown; other divisions typical. RTIS-MSIV equipment similar.
2) Not all communication links shown.
3) Figure 7DS-1 derived from Tier 1 Figures 2.2.7b and 3.4b and Tier 2 Figures 7.2-8 through 10.
4) Fiber Optic communication is denoted by dotted lines and hardwired communication is denoted by solid lines.

DRAFT

DRAFT

RTIS/NMS Platform Redundancy

- NMS has four independent & redundant divisions that provide trip status to RTIS
- RTIS has four independent & redundant divisions
  - Each division includes a DTF, a TLF, and an OLU
  - Division-of-Sensors bypass
  - Trip-Logic-Output bypass
- Four independent & redundant power supplies
  - Designed redundancy satisfies Single Failure Criterion (IEEE-603 Criterion 5.1)

DRAFT

DRAFT

RTIS/NMS Platform Independence

- Four independent power sources
- Independence from non-safety systems
  - Communications isolation and independence
  - Electrical isolation and physical separation
- Four independent RTIS/NMS sensor divisions to determine divisional sensor trips
  - No communication across sensor divisions
- Four independent RPS and MSIV TLF and OLU divisions
  - Only communication across division boundary is to support 2-out-of-4 voting function
  - Communication isolation and independence
  - Electrical isolation and physical separation

DRAFT

DRAFT

RTIS/NMS Platform Independence – Communication

- Communication Across Divisions
  - Only discrete information of fixed format and fixed length
  - Qualified, isolated, point-to-point, unidirectional fiber optic communication links
  - Each communication link has its own independent buffer
- Communication to Other Systems
  - Qualified, isolated, point-to-point, unidirectional fiber optic communication links
  - Each communication link has its own independent buffer
- All communications include Self-Diagnostics functions
  - Continuously monitor proper communication performance
  - Upon detection of failure, division marked as inoperable (i.e., tripped) and operator is alerted

DRAFT

DRAFT

RTIS/NMS Platform Determinism

- Each FPGA is a synchronous, clocked sequential circuit
  - Each FPGA only starts processing data when data is transferred into that FPGA, and sends data to the next FPGA or module when processing is complete
  - Changes of state occur only at selected times, controlled by a timing signal
  - Sequential processing FPGAs are monitored by watchdog timer
  - Failure of signal processing will result in module marked as inoperable
- Timing is verified by analysis and simulation during design

DRAFT

DRAFT

RTIS/NMS Platform Diversity

- RTIS and NMS platforms diverse from the Engineered Safety Features (ESF) Control and Logic System (ELCS) which actuates ESF functions
- RTIS and NMS diverse from non-safety and balance of plant I&C systems
- RTIS diverse from Anticipated Transient Without Scram (ATWS) mitigation equipment
- STP 3&4 diversity strategies summarized in FSAR Tier 1 Subsection 3.4C and Tier 2 Appendix 7C

DRAFT

DRAFT

RTIS/NMS Platform Simplicity

- Separation of Safety and Non-Safety Functions
  - Non-safety functions are not performed in safety-related equipment
  - Complex activities (e.g. cross channel checks and historian functions) are performed in non-safety equipment
- Non Re-Writable (NRW) FPGA
  - Functionality implemented in fixed gates with deterministic timing that cannot be changed
- Minimization of Interdivision Communication
  - Communication across division boundaries limited to trip status information for 2-out-of-4 coincidence logic

DRAFT

DRAFT

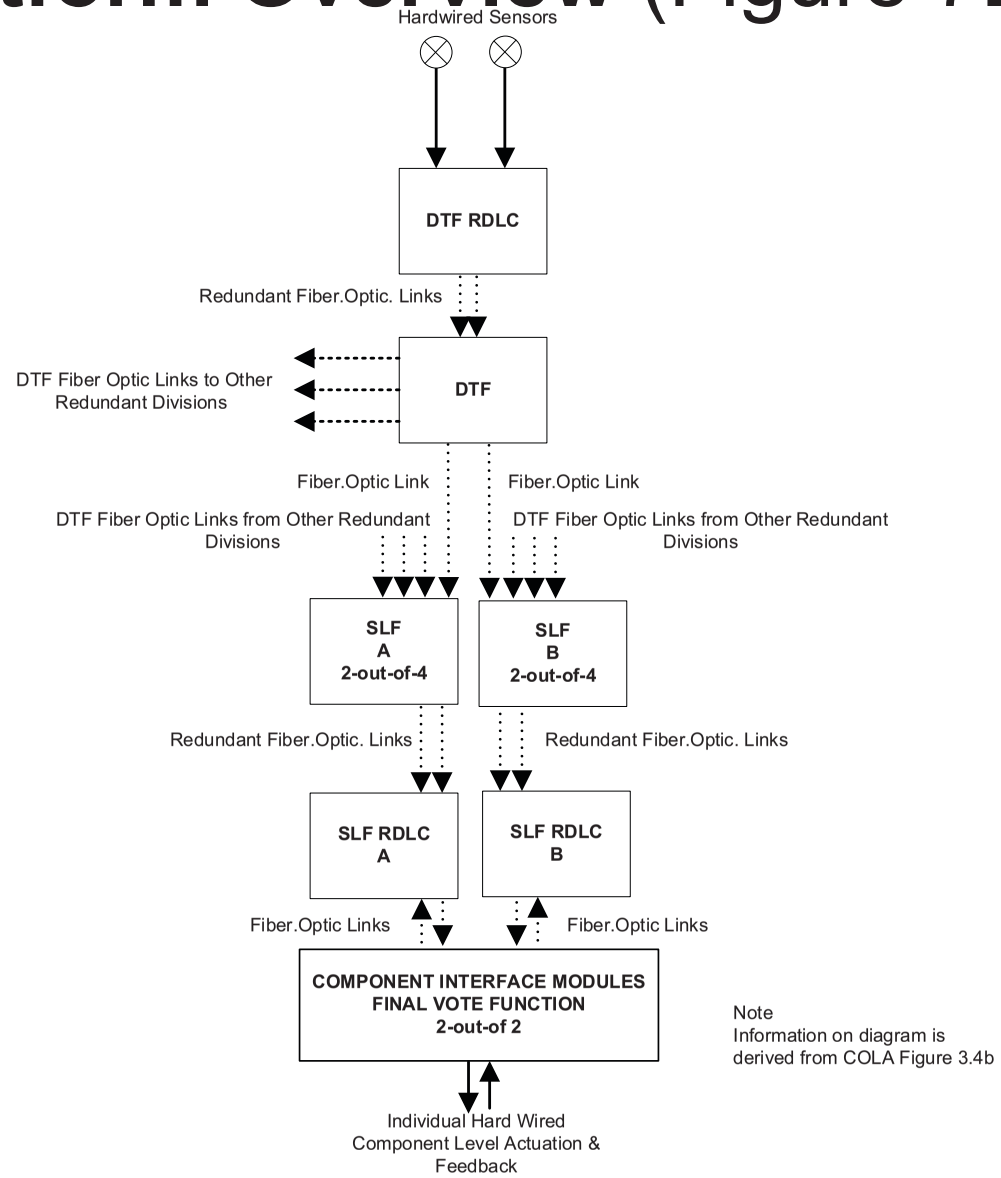
ELCS Overview

- Digital Trip Function Remote Digital Logic Controller (DTF RDLC)
  - Remote data acquisition of Engineered Safety Feature (ESF) sensor signals
- Digital Trip Function (DTF)
  - Compares signal values to setpoints to determine division ESF safety function initiation status for one division
- Safety Logic Function (SLF)
  - Performs 2-out-of 4 coincidence logic to determine system level automatic initiation status
- Safety Logic Function Remote Digital Logic Controller (SLF RDLC)
  - Receives system level automatic and manual system level actuation signals from SLFs
  - Provides logic to determine component actuation and control commands to Final Vote Function
- Final Vote Function
  - Receives individual component actuation and control commands
  - Performs 2-out-of 2 coincidence logic for component actuation and control

DRAFT

DRAFT

ELCS Platform Overview (Figure 7DS-3)



Note
Information on diagram is derived from COLA Figure 3.4b

DRAFT

DRAFT

ELCS Redundancy

- Four independent & redundant sensor divisions
- Three independent & redundant ESF Safety Function Actuation divisions
  - ESF safety function system level initiation
  - ESF component actuation and control
- Four independent & redundant power sources

DRAFT

DRAFT

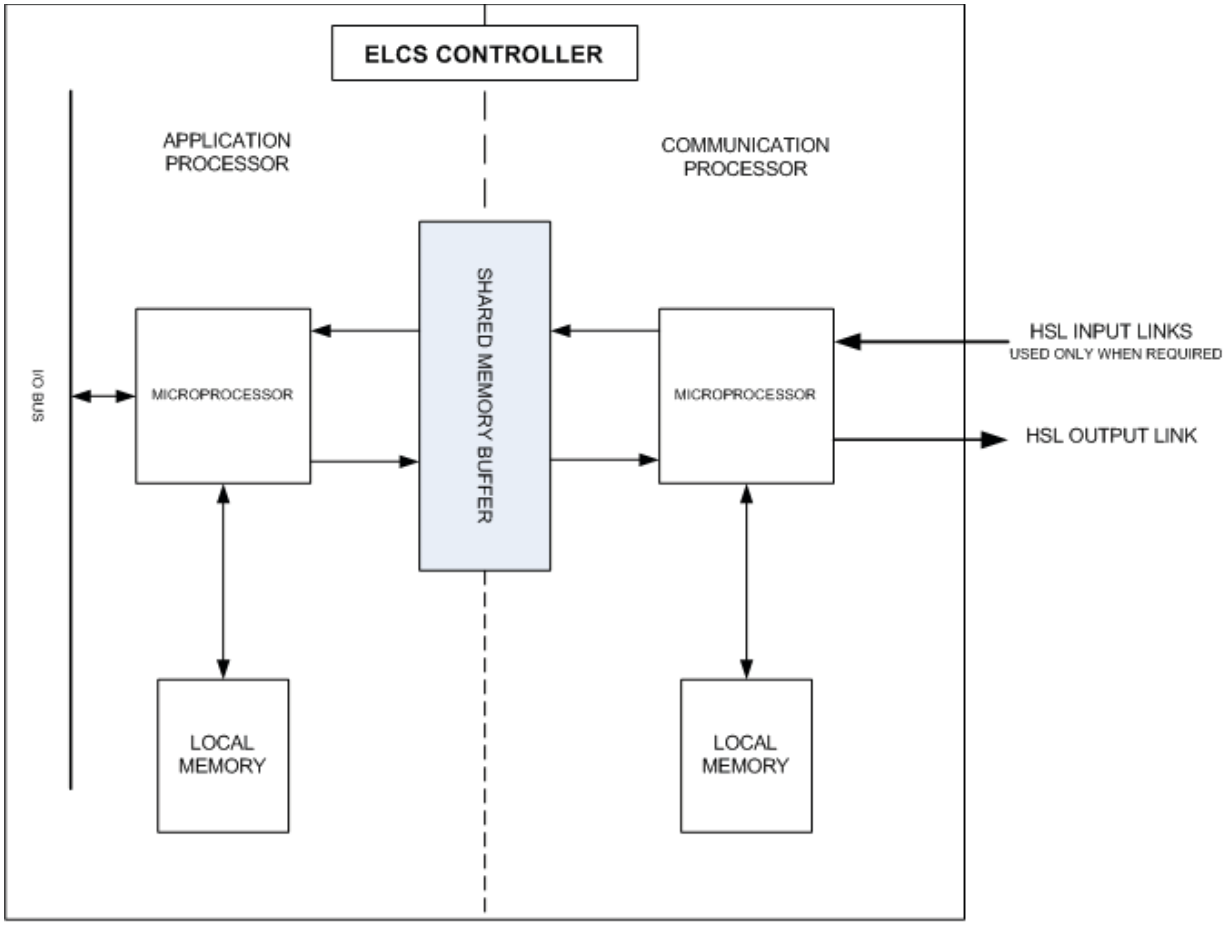
ELCS Independence

- Four independent power sources
- Independence from non-safety systems
  - Electrical isolation and physical separation
- Four independent ESF sensor divisions
- Three independent ESF Safety Function Actuation divisions
  - Electrical isolation and physical separation
- Communications Independence
  - Safety related communications are isolated and independent
  - Non-safety related communications are isolated and independent

DRAFT

DRAFT

ELCS Controller Simplified Diagram



NON-PROPRIETARY VERSION OF FUNCTIONAL ARCHITECTURE FIGURE, SECTION 6.2.1.2.1.2 OF COMMON Q TOPICAL REPORT WCAP-16097-P-A

DRAFT

DRAFT

ELCS Independence

Inter-division Communication

- DTF to SLF Communication
  - DTF transmits trip status to SLFs
    - Unidirectional Serial Link with fiber optic isolation
    - Fixed periodicity of transmission
    - All data transmitted, even if none has changed
    - Fixed length, fixed format message
      - Fixed data mapping – same data point in same position
      - Data redundancy provided in message
      - Cyclic redundancy check (CRC) data provided in message
    - Supports detection of corrupt data

DRAFT

DRAFT

ELCS Independence

Inter-division Communication (cont'd)

- DTF to SLF Communication (cont'd)
  - SLF receives DTF communication
    - SLF has a communication processor and an application processor that communicate through shared memory
    - Communication processor receives message
      - Link failure diagnostic detects failed link
        - Provides error status
      - CRC diagnostic provides error status for bad message
      - Data redundancy diagnostic provides error status
      - Stores message in a unique location in shared memory
    - Application processor reads message
      - Diagnostic error status causes the message data to be replaced with predetermined value
      - Alarm message sent to operator

DRAFT

DRAFT

ELCS Determinism

- ELCS Application Processor
  - No external interrupts
  - Internal clock uses precision interval timer
  - Application software modules
    - Scheduled execution based on precision interval timer
    - Predetermined fixed execution cycle
    - Predetermined fixed time allowance provided for background diagnostics
  - Diagnostics
    - Watchdog timer – annunciation to operator
    - Monitor of application software execution and loading - annunciation
    - Application processor monitors communication processor error status and substitutes predetermined value for bad data
      - Loss of all communication links will cause all ESF safety functions, except LDS, to remain in their “as is” state
      - Leak Detection System is fail-safe and will provide isolation actuation and annunciation

DRAFT

DRAFT

ELCS Determinism

- ELCS Communication Processor
  - Deterministic Protocol
  - All data transmitted, even if none has changed
  - Fixed length, fixed format message
    - Fixed data mapping – same data point in same position
    - Data redundancy provided in message
    - Cyclic redundancy check (CRC) data provided in message
  - Deterministic Transmission Intervals
    - Based on fixed intervals of application processor requests to send messages
  - Deterministic Reception Intervals
    - Based on fixed message reception intervals from transmitting controllers
  - Communication process is buffered from application processor by shared memory
  - Diagnostics
    - Watchdog timer
    - Loss of communication
    - Message Diagnostics – CRC and data redundancy

DRAFT

DRAFT

ELCS Determinism

- Response Time Analysis
  - Criteria based on Safety Analysis requirements
  - Includes all delay elements
  - Determines criteria for response time validation testing
  - Documented in a report
- Validation Testing
  - Validates analysis
  - Documented in a report

DRAFT

DRAFT

ELCS Diversity

- Diverse from equipment credited to mitigate ELCS failure
  - Diverse equipment is hard wired (See FSAR Tier 1 Subsection 3.4C and Tier 2 Appendix 7C)
- Diverse from RTIS and NMS
  - ELCS is microprocessor based
  - RTIS and NMS are FPGA based
- Diverse from non-safety control systems
  - Different microprocessor and software
  - Different communications technology and equipment

DRAFT

DRAFT

ELCS Simplicity

- Separation of Safety and Non-Safety
  - ELCS control is performed within ELCS
  - No non-safety digital control communication links
- Simplicity of Communication
  - Unidirectional serial links for automatic and manual initiation of ESF safety functions simplify architecture
- Minimization of Interdivision Digital Communication
  - Only system level coincidence logic function uses interdivisional digital communication links

DRAFT

ACRS Action Item Summary

ACRS May 20, 2011 Meeting

- ACRS suggested additional discussion was needed for their conclusion of:
  - ELCS determinism
  - Impact of data corruption on ELCS communications independence
- ELCS Presentation Information
  - Supports that data corruption does not compromise communication independence
  - Supports inter-division communication compliance to independence and determinism requirements
  - Supports the compliance to determinism requirements
- Additional Questions?

DRAFT

DRAFT

Chapter 7

Questions and Comments

DRAFT