U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Planning the Future for I&C Safety Systems

Richard Stattel
Instrumentation and Controls Branch (EICB)
December 3-4, 2012

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Objectives

- Recent Licensing Experiences
  - Oconee Digital Reactor Protection / Engineered Safety Protection System (RPS/ESPS) and automatic diverse safety actuation system
  - Watts Bar Unit 2 Post Accident Monitoring System (PAMS)
  - Diablo Canyon Power Plant (DCPP) Process Protection System (PPS) upgrade
  - Crystal River – Fast Cool down Safety Function (Analog Implementation)
- Digital I&C Licensing Processes ISG-06
- Factors of Managing I&C Safety system performance
  - Barriers
  - Competing Objectives

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Licensing Process Overview

- DI&C Licensing Process Overview
- Format of ISG-6
  - Tiers of Complexity
  - Phases of Process
  - Areas of Review
- Lessons learned / Process Improvement Suggestions

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Oconee RPS/ESPS Safety Evaluation

- Issued on January 28, 2010 (ML100130944)
- Scope includes Reactor Protection System (RPS) and Engineered Safety Protection System (ESPS) systems for all three units
- Modification included a Diverse Actuation system which provided a backup actuation for HP and LP Safety Injection. NSR
- Replaces Analog equipment with Teleperm TXS based digital equipment
- Extensive Safety Evaluation (Conducted over a two year period)
- Inspections performed during site testing and installation

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Unit One Inspections Performed

- Range of Inspection: January through September, 2011
- Team Composition: 5 inspectors from Region 2, Resident Insp.
  HQ support (NRR,NRO)
- Estimated Level of Effort: 240 hrs Off-site preparation and review
  100 hrs On-site Inspection
- Notable Inspection Activities
  - Review of Operating Procedures
  - Review of Surveillance Test Procedures to ensure that system operability assumptions were maintained during test evolutions
  - Confirm usage requirements for Key Switches
  - Confirmation that physical security measures had been implemented.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Watts Bar 2
Safety Related
Monitoring Systems

- Containment High Range Radiation monitoring system
- Common Q – Post Accident Monitoring System (PAMS)

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Watts Bar 2 Safety Related Monitoring Systems

- Containment High Range Radiation monitors
  - Changed to Sorrento digital RM-1000 monitors
  - No digital communications to other systems

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Watts Bar 2 Safety Related Monitoring Systems

- Common Q – Post Accident Monitoring System (PAMS)
  - New system replaces Unit 1 ICCM-86 (Functionally equivalent to Unit 1)
  - Based on ABB-AC160 platform
  - Includes Two Independent Trains Consisting Of:
    - RVLIS
    - Core Exit Thermal Couples
    - Saturation Monitor
  - Digital Communications is Uni-Directional Via Two Barriers
    - Maintenance Test Panel
    - Data Diode

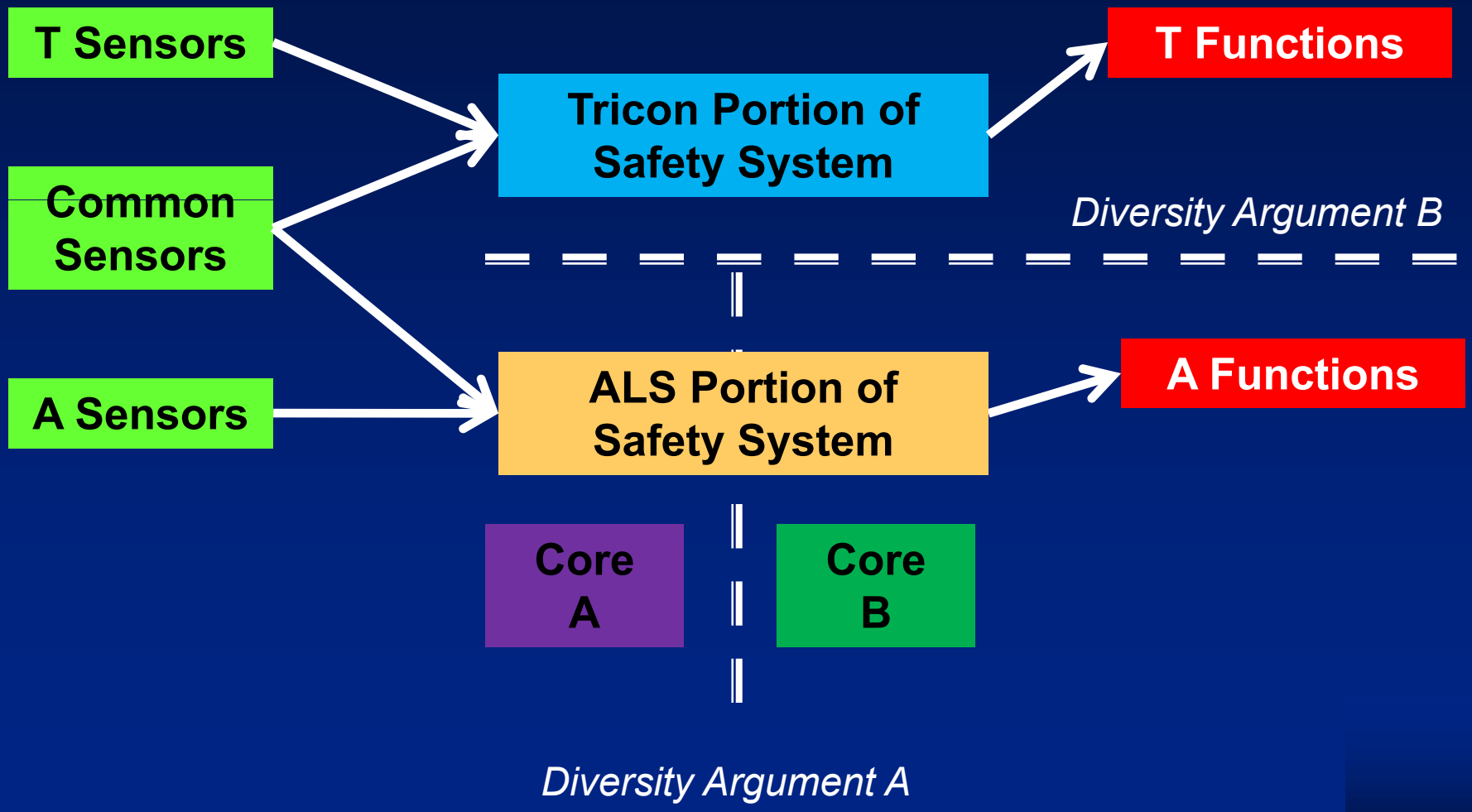
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Diablo Canyon Process Protection System (PPS) Replacement

- License Amendment Request (LAR) received - October 2011
- Replaces Eagle 21 digital equipment with Tricon and ALS based digital equipment.
- Scope includes Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS) processing functions for both units.
- Safety Evaluation scope is similar to the Oconee SE with some key exceptions:
  - Voting Logic performed by SSPS system is not affected.
  - Automatic diverse actuation is being implemented via ALS sub-system instead of implementing a separate diverse NSR system.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Diablo Canyon Diversity



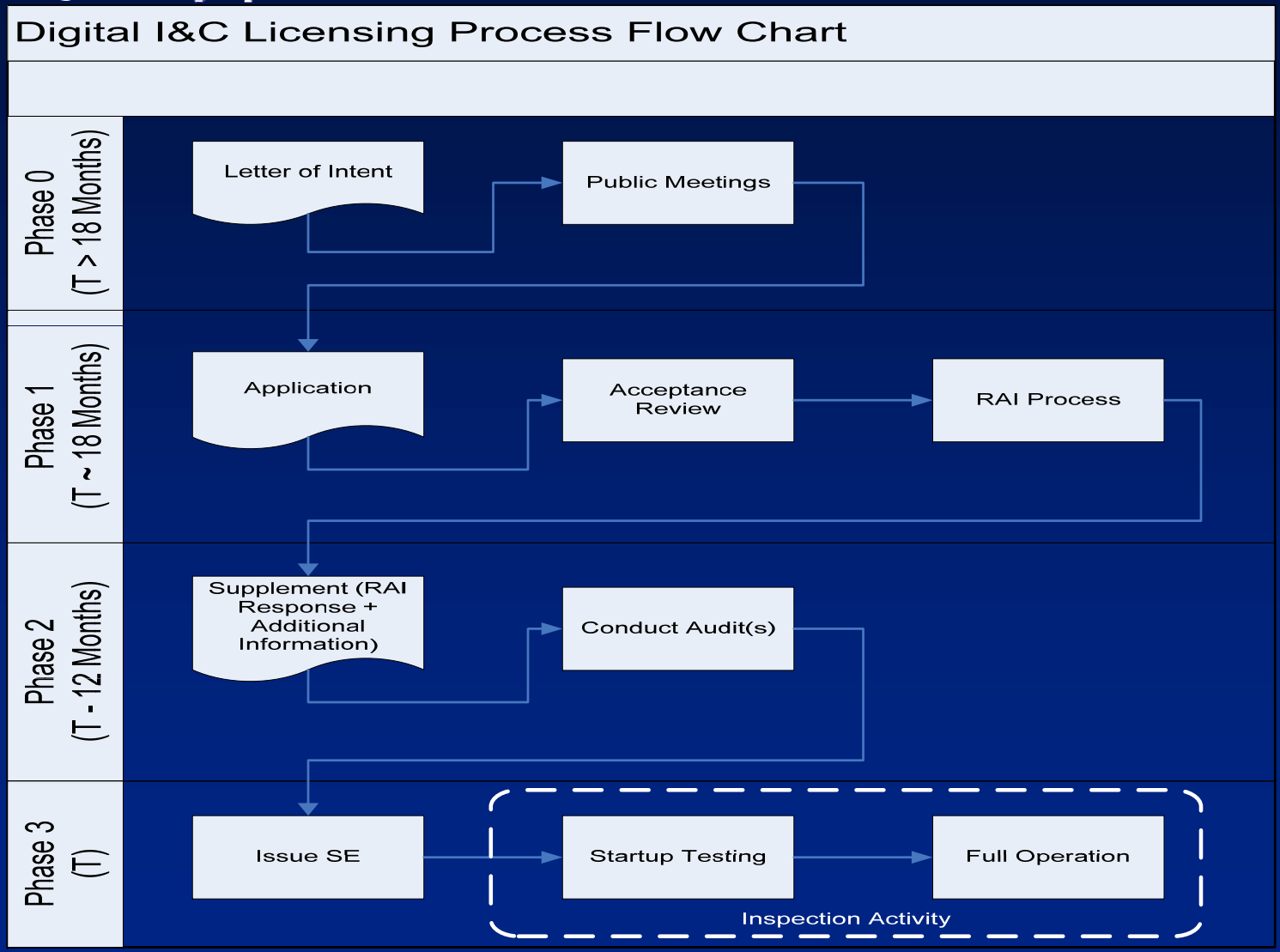
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Crystal River Fast Cooldown System

- EPU Application Submitted June 2011
- Crystal River is the first B&W plant to apply for an EPU.
- Scope includes addition of a new Fast Cooldown safety function to be actuated on low safety injection flow rate.
- Licensee has chosen to implement this function using an Analog Safety system.
  - The Analog Platform used has not been reviewed by the NRC before.
  - The NRC is reviewing for compliance with the criteria of IEEE 603-1991.
  - Because the system is not digital, software CCF concerns that would require a D3 analysis do not need to be considered.

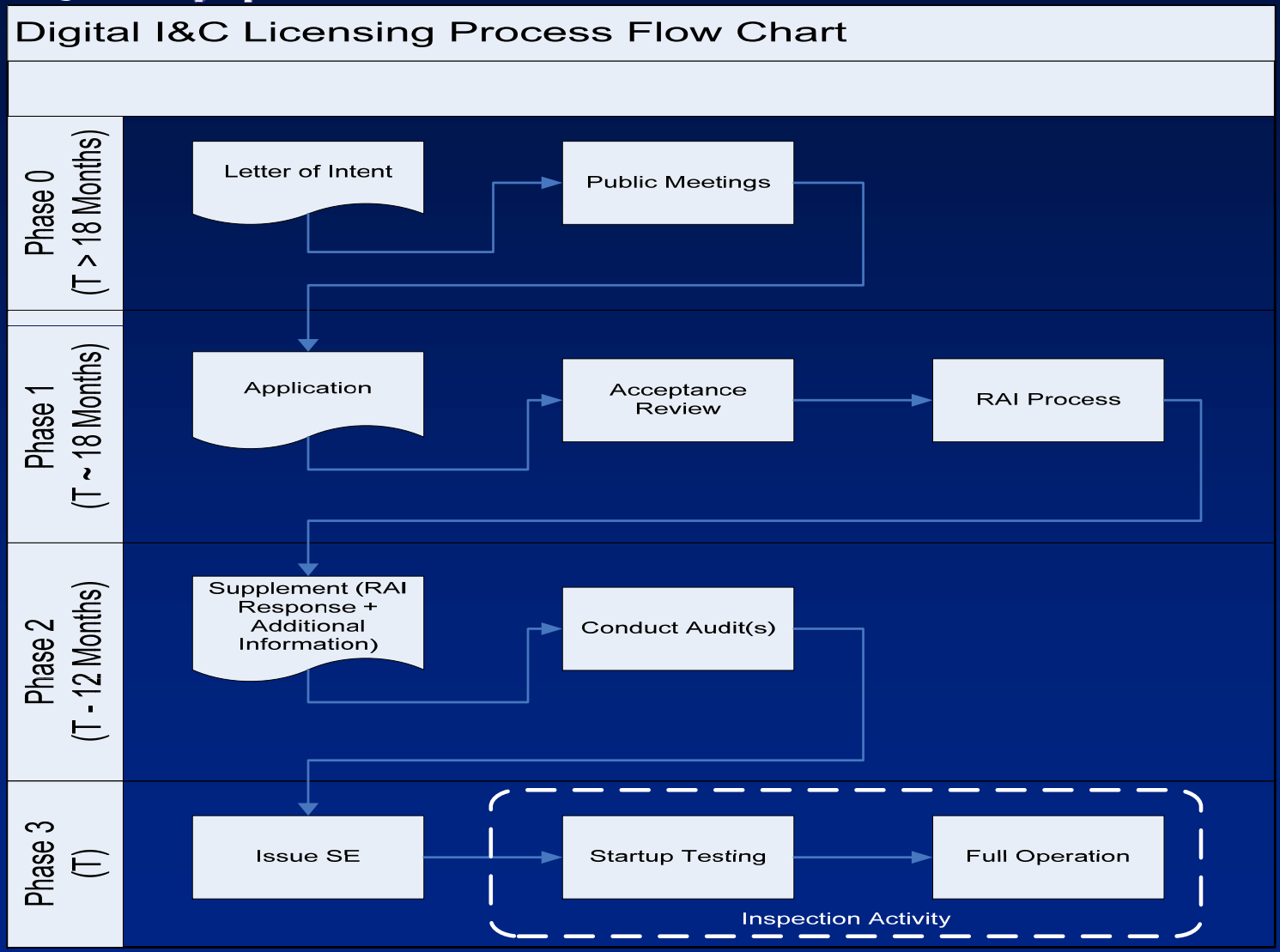
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Process Overview



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Process Overview



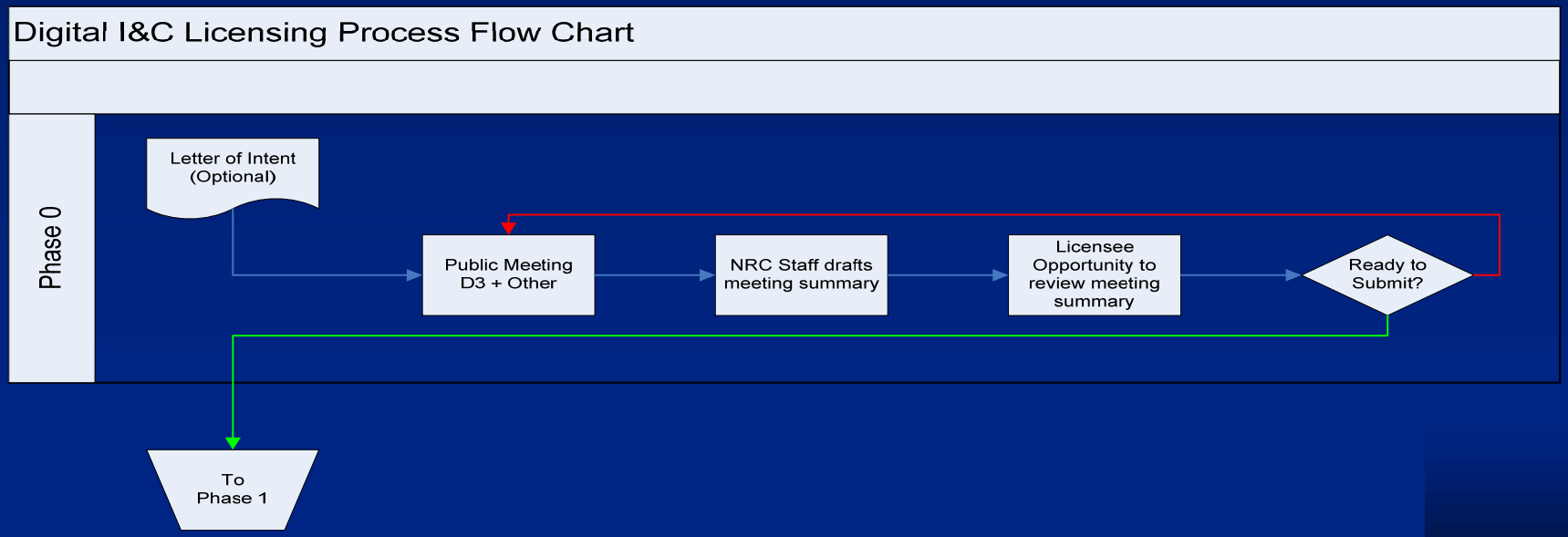
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Licensing Process Tiers of Review

- Each Tier corresponds to an expected review complexity:
  - Tier 1: Previously approved system, no deviations from topical report, review to focus on plant specific aspects, least review effort expected.
  - Tier 2: Previously approved system, with deviations, moderate review effort expected.
  - Tier 3: Totally new system, extensive review effort expected. Thorough review of all technical areas.

ISG-06 Phase 0

- **Minimum Information (Documentation):**
  - Assumes Entire Safety System Replacement
  - No provision for reducing based on scope
  - Provides a forum for determining what documentation from Enclosure B should be submitted with the LAR



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Licensing Process

- A Phase 1 documentation matrix is used to identify documentation needed to perform the safety evaluation.
- For Diablo Canyon, a Matrix was developed based on the guidance provided in Interim Staff Guide (ISG)-06.

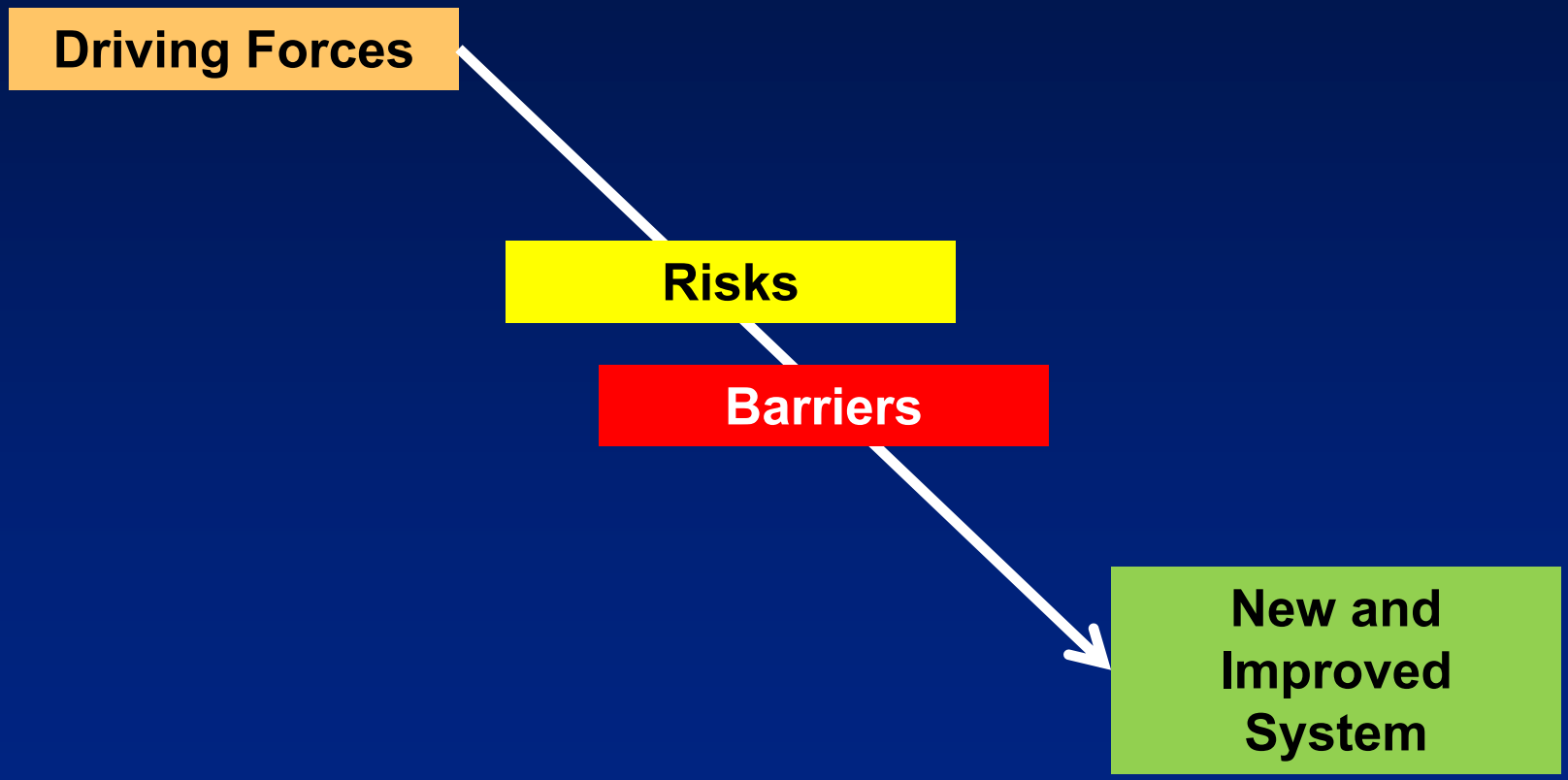
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Diablo Canyon PPS Enclosure B Phase 1 Compliance Matrix

	Tier			Enclose B Documentation (Phase 1)	PG&E information Submitted with LAR	W/ALS Tier 3 Platform documents	W/ALS Doc. Submitted with LAR	Tricon Tier 2 Platform documents	Triconex Documents Submitted with LAR
	1	2	3						
1.1	X	X	X	**Hardware Architecture Descriptions** (D.1.2)	**4.2 System Description (4.2.1 - 4.2.11)**	**ALS Platform Specification (Rev 8 10/31/11) 6002-00011 ML11320A101**	**6116-00011 Diablo Canyon PPS ALS System Design Specification**	**V10 Platform Document (s): - 9100042-002 (P) [ML101110707] - 6200152-002 (P) [ML101110707]**	**993754-1-914 Diablo Canyon Triconex PPS System Architecture Description (incl Hardware and Software)**
1.2			X	**Quality Assurance Plan for Digital Hardware** (D.2.2)	**4.3 Hardware Development Process**	**CSI Quality Assurance Manual (Rev 6 11/11/11) (Related to Appendix B Program) ML11320A102**	**9000-00000 QA Manual**	**Not Applicable for Tier 2**	**Not Applicable for Tier 2**
1.3	X	X	X	**Software Architecture Descriptions** (D.3.2, D.4.4.3.2)	**4.4 Software Architecture**	**ALS Platform Specification (Rev 8 10/31/11) 6002-00011 ML11320A101**	**6116-10201 Diablo Canyon PPS ALS FPGA Requirements Specification**	**V10 Platform Document(s): - 6200106-001 (P) [ML101110707]**	**993754-1-914 Diablo Canyon Triconex PPS System Architecture Description (incl Hardware and Software)**

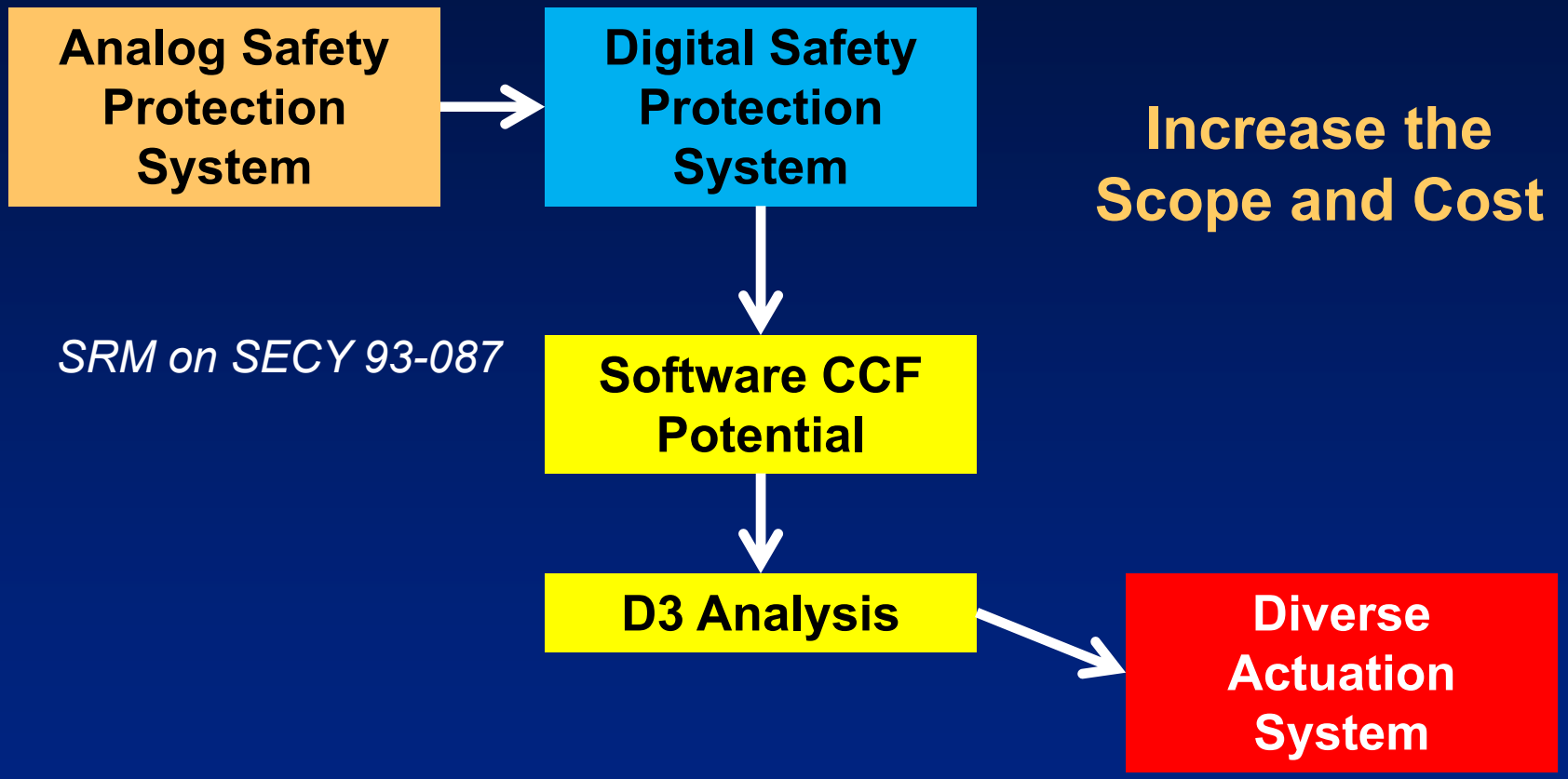
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

I&C System Upgrade Factors



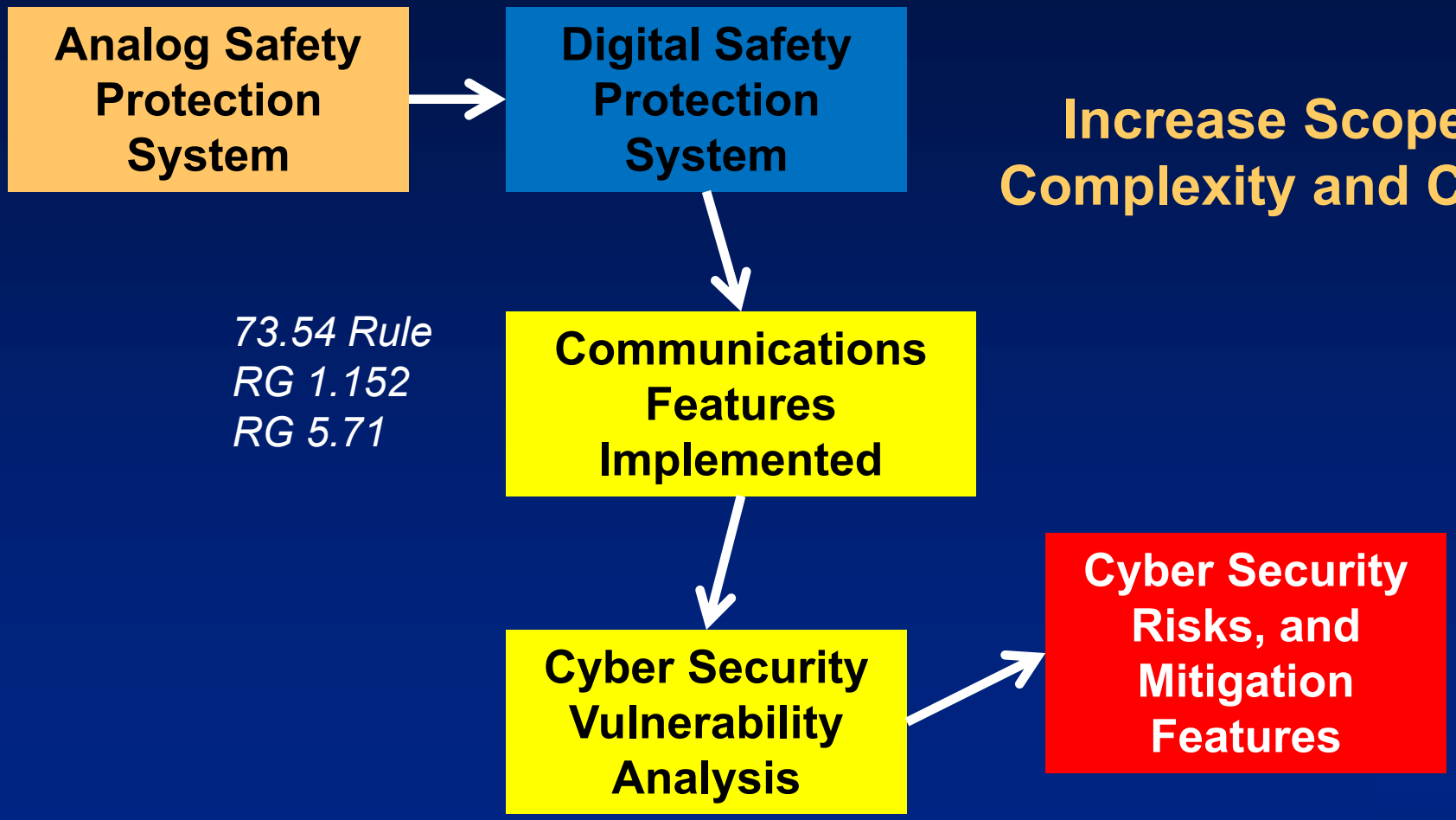
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Barriers to I&C System Upgrades Diversity Requirements



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Barriers to I&C System Upgrades Cyber Security Requirements



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Factors

- Driving Forces (Meeting System Safety Objectives)
  - Continued performance of aging systems into the future
  - Reliability Improvements
  - Improvements in System Monitoring and Diagnostic Capabilities
  - Reduced Surveillance burden
  - Reduced Maintenance costs
- Barriers to Performing System Upgrades
  - Diverse Actuation System Requirements
  - Communications Independence / Cyber Security
  - Software Development Processes
  - Software Tools
  - System Integration
- Competing Objectives
  - Including Cyber Security Features
  - Minimizing System Complexity

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Summary

- Phase 0 meetings were successful in facilitating a high quality LAR for the DCPP Process Protection System
- Enclosure B was effective in providing the information needed by the staff to start its technical review of the LAR. The LAR appears to adequately address all applicable regulatory requirements
- SG-06, Enclosure B should be enhanced to provide the required information for a platform LTR submittal.
- The DCPP PPS implements diversity within the design. This shows that alternative diversity strategies to duplicating safety functions in DAS are possible.
- Carefully coordinate submittal of the safety system LAR with completion of the referenced platform development and testing. NRC review of Platforms referenced in LAR should be well underway, and all platform testing completed.
- Deviations from staff guidance may be acceptable but will result in staff spending significant additional time and resources to review and determine acceptability.
- A Digital Safety System must be tested in its fully integrated configuration before approval.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Questions?

U.S. Nuclear Regulatory Commission

Nuclear Energy Institute Presentation

Region II Inspection Lessons Learned

Shakur Walker

Tuesday December 4, 2012

Washington, DC

Oconee RPS Inspection

- Pilot Inspection Procedure IP52003, Digital Instrumentation and Control Modification Inspection
- Confirmatory review of licensing basis outlined in approved Safety Evaluation Report
- U1 inspection conducted in Spring 2011; U3 conducted in Spring 2012

Oconee RPS Inspection

Lessons Learned:

- The Inspection Follow-up Items listed in the SER were essential to focusing inspectors on what items were important
- Having NRR personnel (Safety Evaluation Reviewers) on the team was very beneficial
- Maintained constant communications with NRR and licensee
- Having a SharePoint site set up by the licensee to provide information requested by the inspectors proved helpful (info. included procedures, test results, corrective action documents)

Oconee RPS Inspection

Lessons Learned (cont'd):

- Licensee should finalize as many documents as possible prior to installation and inspection.
- Inspection is more of a confirmatory review of licensing basis as approved in the SER.
- The scope of this inspection effort was large and challenging. Be cognizant of potential ancillary non-safety systems that could be affected

Oconee RPS Inspection

Lessons Learned (cont'd):

- IFIs documented in SER were for all three units
- Unit 3 inspection was more limited in scope
- U3 inspection was focused more on lessons learned; corrective actions
- Important to note most issues that arise are "work-in-progress"

Questions and Comments

U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

New Construction DI&C Inspection

Overview and Lessons Learned

T. Fredette (NRO/CIPB)
W. Roggenbrodt (NRO/DE)
K. Mott (NRO/DE)

December 4, 2012

Background

- DI&C inspection infrastructure for Part 52 new reactors in development since Nov 2009 (new procedure and framework); structured to align w/ DI&C development life cycle
- Initial focus was STP 3&4 DI&C ITAAC; abbreviated inspection efforts completed in 2010 (Project-level DI&C life cycle Planning Phase)
- Staff commenced compiling inspection lessons learned as process "burned in"

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Additional Inspection Activities

- **Series of inspections for MOX process control system software development (Triconex PLC); life cycle planning phase through FAT (2010 – present)**
- **AP1000 Protection & Safety Monitoring System (PMS) ITAAC; initial inspection completed early 2012 (life cycle requirements phase); *more inspections for PMS planned through 2013***

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Initial AP1000 DI&C Inspection

- PMS System Definition (aka Requirements) Phase Inspection Findings
  - Independent V&V
  - Life Cycle Process Compliance
  - Completeness of Design Output (Software Requirement Specification)

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Planned 2013 Inspections

- Follow up to Planning Documents (~2/2013)
- Component Interface Module Planning Phase (~ 3/2013)
- Follow up to PMS System Definition Phase (~6/2013)
- Diverse Actuation System (initial inspection) TBD

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

DI&C Inspection Lessons Learned

- **Interpretation of ITAAC; staff and licensees must agree on language and intent in order to solidify inspection scope**
- **Inspection planning; use of risk insights to inform inspection sample (e.g. requirements traceability)**
- **Inspection team model; use of tech staff SMEs in inspection role; staff addressed associated challenges internally**
  - **new inspection primer**
  - **just-in-time training conducted as needed**

Lessons Learned (cont.)

- Make use of all available inspection tools, inspection insights, internal DI&C experience, etc.
- ID and address inspection procedure enhancements
- Continuous licensee/staff interaction:
  - inspection scheduling/logistics
  - inspection pre-brief (DI&C development organization and doc hierarchy) if practical
  - virtual reading room (e.g. sharepoint site)
  - engagement with cognizant DI&C mgmt
  - Part 52 licensing POC (licensee) for inspection support and C2LB

Documents of Interest

- STP Inspection Report (ML102110291)
- MOX Inspection Reports (ML103060343)
  (ML11318A279)
  (ML110410628)
  (ML12319A431)
- AP1000
  Inspection Report (ML12171A058)

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Acronyms

- **STP** – South Texas Project
- **MOX** – Mixed Oxide Fuel Fabrication Facility
- **PLC** – Programmable Logic Controller
- **FAT** – Factory Acceptance Test
- **ITAAC** – Inspections, Tests, Analyses, and Acceptance Criteria
- **POC** – Point of Contact
- **CL2B** – Construction to Licensing Basis
- **PMS** – Protection & Safety Monitoring System

Digital Modifications and 50.59 – a Regional Perspective

U.S.NRC
United States Nuclear Regulatory Commission
Protecting people and the environment

Mod/50.59 Inspection Potential Issues with Digital Modifications

U.S.NRC
United States Nuclear Regulatory Commission
Protecting people and the environment

Cyber Security

- Is the system susceptible to outsider intrusion?
- Does access to important to safety systems go beyond the plant boundaries?

Fire Protection

U.S.NRC
United States Nuclear Regulatory Commission
Protecting people and the environment

- How close together are the digital controllers?
- What if area heats up due to a fire?
- How are the digital components affected by smoke?

Important To Safety

U.S.NRC
United States Nuclear Regulatory Commission
Protecting people and the environment

- Used in a number of regulations:
  - Maintenance Rule, 10 CFR 50.65
  - Cyber Security Rule, 10 CFR 73.54
  - 10 CFR 50.59
- Primary Importance:

  Malfunction of an SSC Important to Safety

Important To Safety

U.S.NRC
United States Nuclear Regulatory Commission
Protecting people and the environment

- Discussed in NEI 96-07

  "Malfunction of SSCs important to safety means the failure of SSCs to perform their intended design function described in the UFSAR(whether or not classified as ***safety-related*** in accordance with 10 CFR 50, Appendix B)."

- Rule:
  - "Does the activity result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety?"

IN 2010-10
Implementation of a Digital Control Under 10 CFR 50.59

U.S.NRC
United States Nuclear Regulatory Commission
Protecting people and the environment

- "Highly Safety Significant" systems
  - Ability to cope with software common-cause failure vulnerabilities.
  - Software quality is not enough to justify that failure is not credible.
  - RCMS, . . .

U.S.NRC
United States Nuclear Regulatory Commission
Protecting people and the environment

- Million Dollar Question:

  How does Highly Safety Significant relate to Important to Safety?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting people and the environment

QUESTIONS?

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Lessons-Learned using ISGs for Licensing Actions: ISG-04, Communications-HICR

Bill Kemper
Instrumentation and Controls Branch (EICB)
December 4, 2012

NRC Digital I&C Website: http://www.nrc.gov/about-nrc/regulatory/research/digital.html

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Agenda

- ISG-04 Scope/Background
- Licensing Actions Reviewed
  - Wolf Creek MSFIS
  - Oconee RPS/ESPS Upgrade (TELEPERM XS)
  - Diablo Canyon PPS Replacement (Tricon V10/ALS FPGA System)
  - Platform LTRs
    - Tricon V10
    - HFC-6000
    - Common Q Update
- Lessons learned / Process Improvement Suggestions

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Background

- ISG 4 guidance specifically addresses issues related to interactions among safety divisions and between safety-related divisions and equipment/systems that are not safety-related.
- ISG-04 is not applicable to interactions among equipment that are all within the same safety division or that do not involve anything that is safety-related.
- ISG-04 does address certain aspects of digital control systems that are not safety-related but which may affect the plant conformance to its safety analyses (accident analyses, transient analyses, etc.).
- The guidance provided in ISG-04 adheres to the principles set forth in IEEE 603-1991 and IEEE 7-4.3.2-2003 by describing means for ensuring independence among redundant safety channels/divisions while permitting some degree of interconnection and commonality among those independent channels.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Background

- ISG-04 is divided into three Staff Positions:
  - Position 1 - Interdivisional Communications – This section provides 20 Points concerning interdivisional communications, which includes bidirectional transmission of data and information among components in different electrical safety divisions and bidirectional communications between a safety division and equipment that is not safety-related.
  - Position 2 - Command Prioritization – This section provides 10 Points related to combining safety-related and non-safety actuation signals to control a safety-related actuation device via a prioritization device or software function block referred to as a “priority module.”
  - Position 3 - Multidivisional Control And Display Stations – This section provides 7 Points concerning safety-related and non-safety operator workstations, used for the control of plant equipment in more than one safety division and for display of information from sources in more than one safety division.

Application of ISG 4 to Licensing Applications

Staff Position 1 – Interdivisional Communications

Point 1: states that the safety channel should not be dependent upon any information or resource originating or residing outside its own safety division to accomplish its safety function.

- Nearly all license applications reviewed do not invoke cross-divisional communications or require input from other external sources to perform a division's safety function--and therefore comply with this Point.
- However, in the Oconee system, each safety channel/processor received sensor data and status from the other three safety channels (2^{nd} Min / 2^{nd} Max function).
  - Application proposed bidirectional interchannel data communications.
- The staff had to review the 2^{nd} Min / 2^{nd} Max function block and coding of that function block to determine the impact on the channel safety functions if the data communications was lost or malfunctioned, and verified that each safety channel was capable of accomplishing its safety function without this interchannel communication. The Oconee RPS/ESPS complied with Point 1.

Lessons Learned

1) Digital Safety Systems utilizing cross-channel communications will take significantly more effort to review and extend the time required for this review.
2) Significant design details will need to be provided with the LAR, and additional audits will be required to demonstrate conformance with this criteria.

Slide 5

Application of ISG 4 to Licensing Applications

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Staff Position 1 – Interdivisional Communications

Point 3: States that a safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function, that safety systems should be as simple as possible, and that functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system.

- Again, with exception of Oconee, all license applications reviewed do not receive inputs into a SR channel/div. directly from other redundant channels/divisions to implement the safety function.
- However, most license applications provide inputs to/from the safety channels from external sources via Maintenance Work Station/Service Units (MWS) intended to support or enhance performance of a division's safety function.
- The staff determined that the Oconee RPS/ESPS system did not comply with Point 3, but did meet the regulatory requirements for Independence of 10 CFR 50 App. A, GDC 24, and 10 CFR 50.55a(h).
- In the case of MWS interchannel communications, the staff had to verify that this communication did support/enhance the safety function, while ascertaining these non-safety MWS could not cause the safety system to fail, or another system could perform the safety function (e.g., DAS).

Lessons Learned

1) Deviations from staff guidance may be acceptable but will require significantly more effort to review and extended the time required for this review. Channel based MWS are more conducive to conforming with this guidance.
2) Sufficient detail should be provided with the LAR to demonstrate that communications from outside a safety division does in fact support or enhance the performance of the safety functions.

Slide 6

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Application of ISG 4 to Licensing Applications

Staff Position 1 – Interdivisional Communications

Point 10: States that on-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment, and that a keylock switch either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic.

- Most license applications utilize continuously connected external Maintenance Work Stations/Service Units (MWS) to change the safety system software, monitor system operations, and testing.
- These safety system designs utilize a keylock switch to address this criteria. However, in most cases these keylock switches set a software bit, does not open or interrupt a physical connection, and therefore does not comply with Point 10.
- In most cases, the staff determined that the system still complied with the regulatory requirements for Independence of 10 CFR 50 App. A, GDC 24, and 10 CFR 50.55a(h).
- However, CCF of all 4 channel keylock switches had to be resolved by crediting a diverse back up system (DAS) for the safety systems.

Lessons Learned

1) Continuous connectivity of MWS's with the safety systems that use software solutions for data isolation will require significantly more effort to review and extended the time required for this review.
2) A DAS will likely be required to address CCF of software based keyswitch disconnects if no other means of physical disconnects are invoked.

Slide 7

Application of ISG 4 to Licensing Applications

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Staff Position 1 – Interdivisional Communications

Point 11: States that provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service…

- Some Digital Safety System Processors enable changing certain parameters and operational modes, or bypassing specific trip functions within a channel of the safety system without the affected channel/division being in bypass or tripped. This would not be in compliance with Point 11.
- In those cases, the staff determined that the system could be approved pursuant to this criteria utilizing administrative controls (procedures) by the licensee to place the affected channel in bypass or trip whenever the keyswitch for the safety processor or trip function is taken out of the "Run" or "Operate" position.

Lessons Learned

1) Safety System Processor designs that physically bypass or trip all channel/division safety functions when not in Run is more conducive to approval.
2) Administrative controls are a viable alternative if platform design does not facilitate meeting this criteria.

Slide 8

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Application of ISG 4 to Licensing Applications

- Staff Position 2 – **Command Prioritization**

  Provides guidance applicable to a prioritization device or software function block, referred to simply as a "priority module." A priority module receives device actuation commands from multiple safety and non-safety sources, and sends the command having highest priority on to the actuated device. The actuated device is a safety-related component such as a motor actuated valve, a pump motor, a solenoid operated valve, etc. The priority module must also be safety-related.

  - To date, no license applications for operating reactors have proposed utilizing Priority Modules for safety system design.
  - Priority Modules have been proposed for new reactor designs and are still under review.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Application of ISG 4 to Licensing Applications

- Staff Position 3 – **Multidivisional Control and Display Stations (MCDS)**

  This section provides guidance concerning operator workstations used for the control of plant equipment in more than one safety division and for display of information from sources in more than one safety division. This guidance also applies to workstations that are used to program, modify, monitor, or maintain safety systems that are not in the same safety division as the workstation.

  - To date, no license applications for operating reactors have proposed utilizing MCDS for control of plant equipment , or display of information from sources in more than one safety division.
  - The Oconee Service Unit did have the capability to program, modify, monitor, or maintain safety systems that are not in the same safety division as the workstation.
  - The Oconee Service Unit was found to be in compliance with this criteria.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Summary

- ISG-04 has been utilized effectively to review and approve data communications designs pertaining to Digital Safety System license applications.
- Invoking interdivisional communications complicates a license application review considerably, which results in additional NRC staff resources, time, and system design information to review and approved the design.
- Using a Channel/processor Mode Change Keyswitch that uses software to isolate the processor from the MWS will likely require a Diverse Actuation System to compensate for CCF of the software based switch.
- Utilizing channelized MWS are a better solution than an interchannel MWS from a regulatory approval perspective. Safety related MWS are even better.
- Continuously connected MWS must support or enhance performance of the safety function; otherwise, it should not be in service/connected while the safety channel/division is on-line.
- Deviations from staff guidance may be acceptable but will result in staff spending significant additional time and resources to review and determine acceptability.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Application of ISG 4 to Licensing Applications

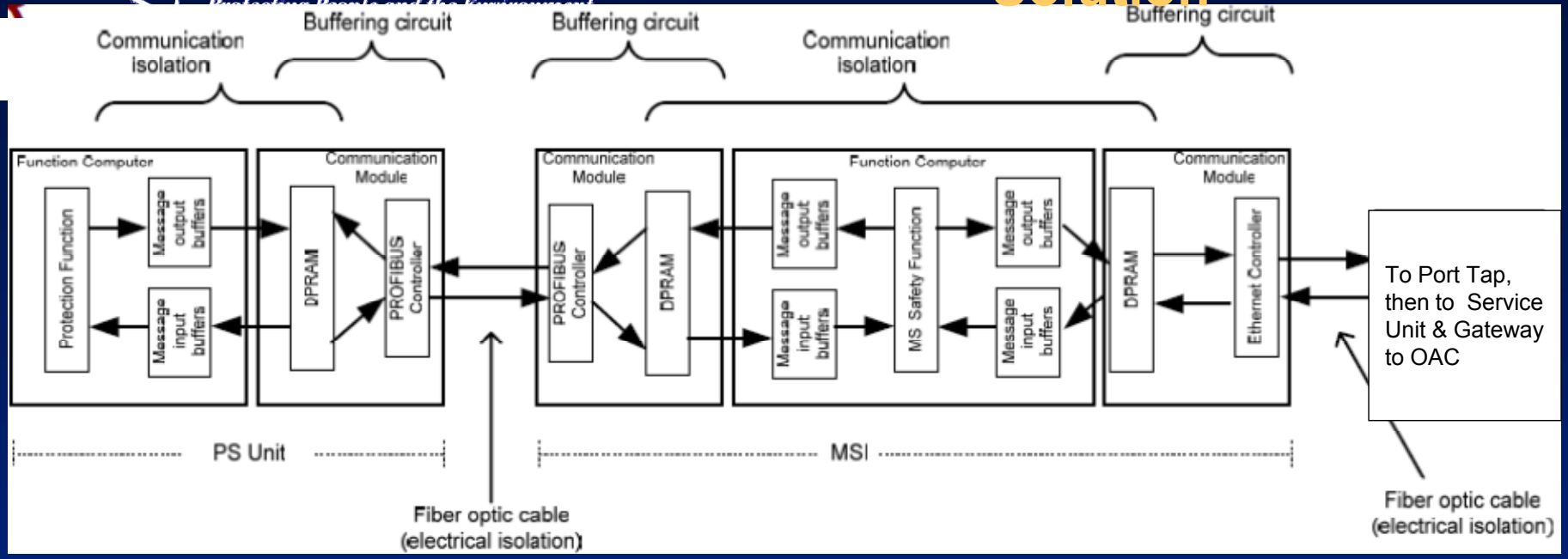
- Questions??

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Application of ISG 4 to Licensing Applications

Back up Slides

Safety to Non-Safety Communications Oconee Solution



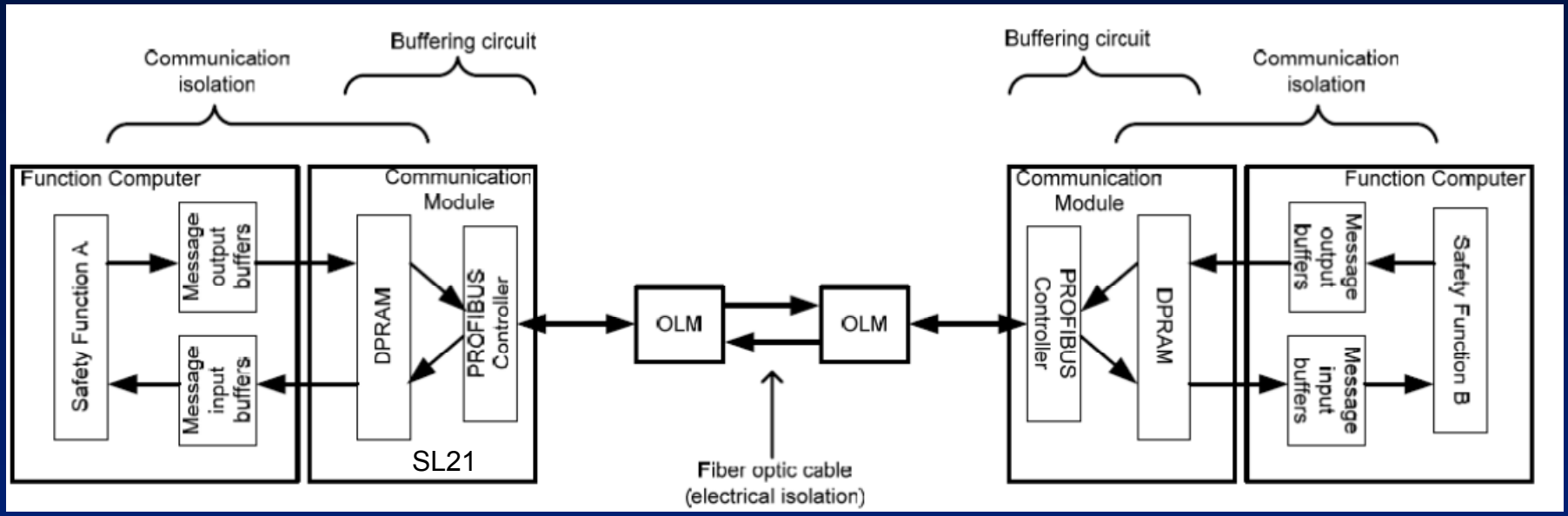
One Way Communications pathway to the OAC

Two Way Communications to the Service Unit

- Provides electrical isolation between Safety and Non-Safety Systems
- Provides communication isolation between Safety and Non-Safety Systems
- The MSI serves as a Safety to Non-Safety Boundary
- Deterministic in nature

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Inter-Channel Communications Oconee Solution

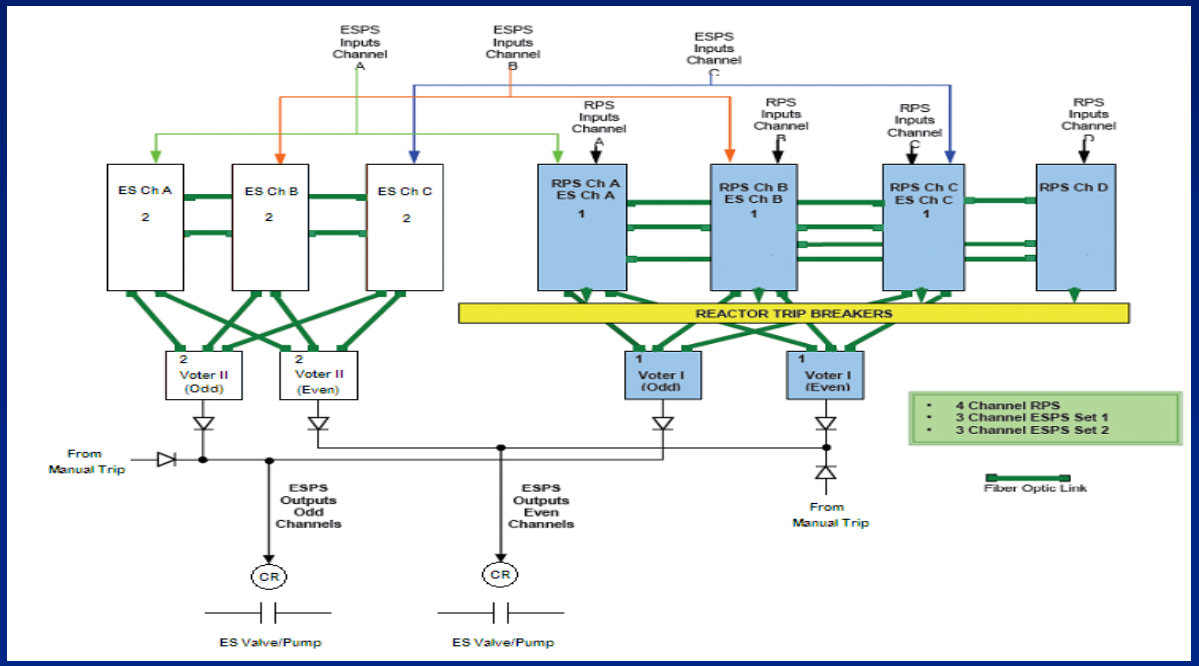


- Provides electrical isolation between Safety Channels
- Provides communication isolation between Safety Channels
- Deterministic in nature

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Oconee Reactor Protection System / Engineered Safety Protection System (RPS/ESPS)

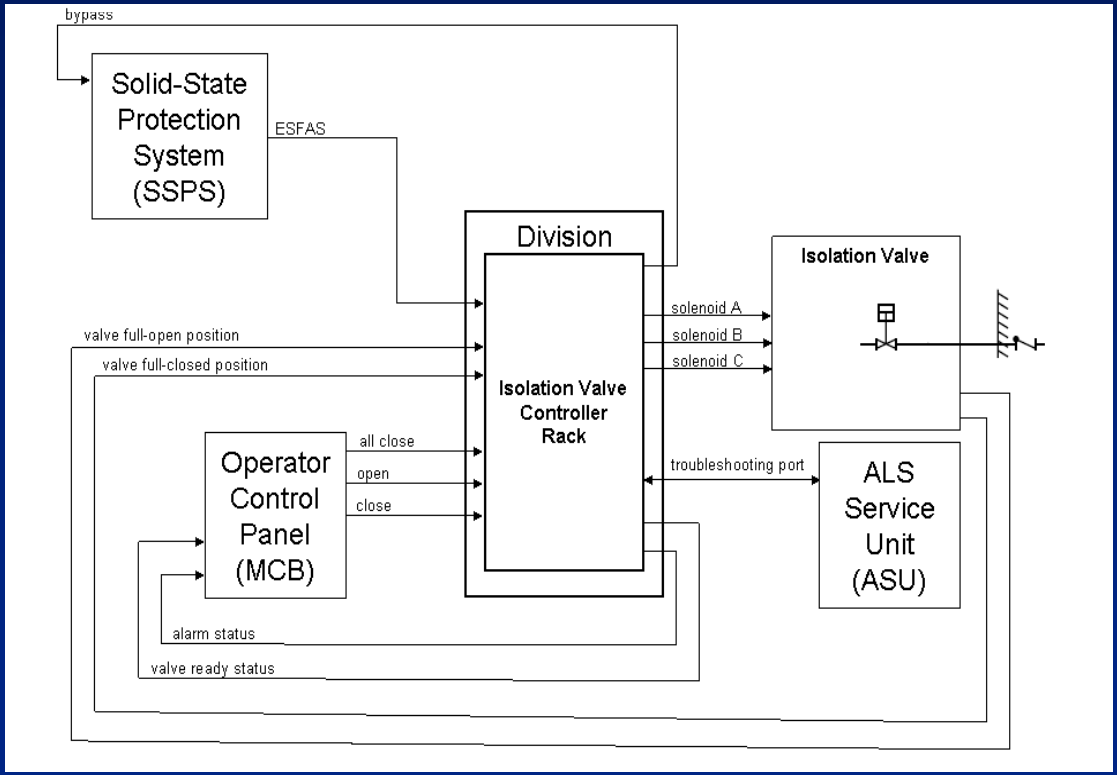
- System Design
  - Combined Reactor Trip System (RTS) and Engineered Safety Features Actuation System (ESFAS)
  - References approved platform topical report
    - Micro-processor based Areva TXS platform
    - Changes to referenced platform
  - Diverse actuation systems



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Wolf Creek Main Steam and Feedwater Isolation System

- System Design
  - Main Steam and Feedwater Isolation System (MSFIS)
    - Part of Reactor Protection System (Safety-Related)
  - Uses new digital technology (i.e., FPGA)



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

NRC Perspectives on SDOE & Cyber Security

Tim Mossman, NRR Electronics Engineer
Tung Truong, NRO Electronics Engineer
Eric Lee, NSIR Sr. Security Specialist (Cyber)
Perry Pederson, NSIR Security Specialist (Cyber)

Prepared for
NEI Digital I&C Meeting – Lessons Learned

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

NRC Regulatory Framework

- Licensing reviews against the requirements of 10 CFR 50 and 52 specifically address safety
  - NRR & NRO will evaluate digital safety systems for a Secure Development and Operational Environment
- 10 CFR 73 covers security and protection from malicious activity, including cyber security
  - NSIR will evaluate licensees' cyber programs and protections of Critical Digital Assets (CDAs)
  - CDAs include safety, important-to-safety, security and emergency preparedness functions, as well as digital support systems for any of the above

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Part 50 / 52 SDOE

- Regulation
  - 10 CFR 50.55a(h), IEEE Std. 603-1991
    - Clauses 5.6.3 (Independence) and 5.9 (Access Control)
  - 10 CFR Part 50, Appendix A, GDC 21, “Reliability”
  - 10 CFR Part 50, Appendix B, Criterion III, “Design Control”
- Guidance
  - Regulatory Guide 1.152, Rev. 3 (2011)
  - IEEE Std. 7-4.3.2-2003

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Regulatory Guide 1.152 Rev. 3

- Secure Development Environment
  - Develop safety systems in a secure environment (e.g. verification and validation of requirements, design, coding phases; configuration management)
- Secure Operational Environment
  - Establish an operational environment to ensure reliable system operation

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

"Secure Development Environment"

- At the conclusion of a successful review, staff will be able to conclude that a Secure Development Environment has been established for the digital safety system such that there is reasonable assurance that superfluous features and code was not incorporated into the system.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

What is Unnecessary Code?

- For digital safety systems, staff considers simpler systems to be better
  - Simpler systems should result in more predictable, deterministic behavior
- Unnecessary code in a system is considered to be a potential source of unpredictable behavior such that the reliable operation of the digital safety system could be affected
  - The regulatory guide specifically calls out unwanted, unneeded and undocumented code

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Cyber features in safety systems?

- If licensees choose to incorporate cyber controls within a digital safety system, staff would want to ensure that such features do not adversely affect the reliable operation of the safety function
- Note, RG 5.71 states: "*A security control should not be applied if the control adversely impacts [Safety, Security or Emergency Preparedness] functions or performance (e.g., unacceptable change in system response time, undesirable increase in system complexity). When a security control is determined to have an adverse affect, alternate controls should be used by the licensee to protect the CDA from cyber attack up to and including the DBT consistent with the process described above. Any residual vulnerability in a CDA as a result of not implementing a security control for concern over its impact to CDA function or performance should be eliminated or mitigated by alternate controls.*"

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

What controls have been credited?

- For single-vendor developments, a large percentage of the secure development environment can be addressed by the high-quality software processes used in digital safety system development
- Of particular emphasis:
  - V&V of all key outputs of each development phase
  - Configuration management of code, key design basis documentation, test configurations
  - Requirements traceability (!!!)
  - Control of test environment – isolation
- [*Note: RG 5.71, Appendix C, Section 12 contains guidance on supply chain cyber controls.*]

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Secure Operational Environment

- At the conclusion of a successful review, staff will be able to conclude that a Secure Operational Environment has been established for the digital safety system such that it can be demonstrated that reasonable measures have been taken to prevent inadvertent access to the system and prevent undesirable behavior from connected systems from affecting its reliable operation.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Inadvertent Access?

- As previously stated, intentional, malicious activity is addressed under 10 CFR 73.54 programs
- Inadvertent access is postulated to be an event involving plant personnel (or an on-site contractor) with no nefarious motive
  - Physical points of access include open communication ports on the system that someone from the licensee's workforce may mistakenly attempt to connect into
  - Logical points of access include any points of human interface on systems connected to the same network on which the digital safety system resides

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Undesirable behavior?

- Term carefully chosen, as not all situations of concern are necessarily the result of "failures"
  - i.e., Connected systems may be capable of behaviors – considered to be within their design – that safety systems cannot handle

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Cyber Controls for SOE?

- Licensees can credit controls in their approved cyber security plans (submitted per 10 CFR 73.54) as part of their secure operational environment story
  - However, NRR / NRO will only make findings relative to Part 50 / 52
  - Suitability and effectiveness of controls for cyber purposes are evaluated by NSIR / Regional inspection

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Inadvertent access protections?

- Staff has seen and been able to credit:
  - "Barriers" and alarms protecting physical access to digital safety systems
  - Logical access controls on any equipment designed to interface with the digital safety system
    - Area of synergy with cyber security controls

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Undesirable Behavior Protections?

- Staff has seen and been able to credit:
  - Isolation of the digital safety system (!!!)
  - Hardware-based (and software-based) devices that enforce one-way communication
  - ISG#4 communication controls
  - CRC checks on software code
  - CRC checks on messages
  - Out-of-range checks on data
  - “White lists” of acceptable messages

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

What about SDOE for Licensing Topical Reports?

- A vendor must be able to substantiate that it has a secure development environment
- For topical reports, no operational environment exists to assess
  - However, to the extent that a vendor's platform has features that would support a secure operational environment, staff would want to review those to enable reference of those controls in a license application (if applicable)

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

10 CFR 73.54

Title: Protection of digital computer and communication systems and networks

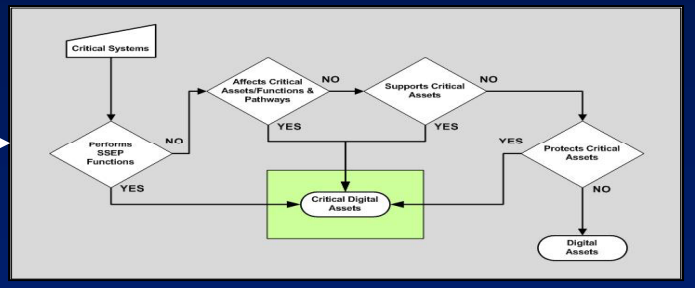
- Performance-Based, Programmatic (< 2 pages)
  - Provide high assurance against cyber attack
  - Integrated with Physical Security Program (10 CFR 73.55)
- Basic Requirements
  - Critical digital assets must be protected
  - Safety, important-to-safety, security, and emergency preparedness functions and support systems that can impact those functions
  - Defense-in-depth protective strategy
  - Records maintained for duration of license

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

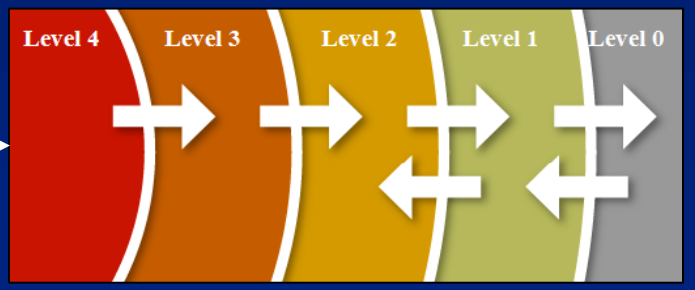
Regulatory Guide 5.71

Form Cyber Security Team

Identify Critical Digital Assets



Apply Defensive Architecture



Address Security Controls

1. Address each control for each CDA, or
2. Apply alternative measures, or
3. Explain why a control is N/A

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Cyber Security Plans (CSP)

- Licensing document / required by regulation
  - incorporated into plant operating license
- Describes how cyber security program is established and maintained
- Essential elements – Plan must:
  - describe roles and responsibilities of a multi-disciplinary Cyber Security Team
  - describe the process for identifying Critical Digital Assets
  - describe the defensive model (protective strategy)
  - reference comprehensive security controls
  - describe the process for addressing controls
  - commit to maintaining adequate documentation

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

CSP Implementation

- Interim Milestones 1-7 (12/31/2012)
  - address key threat vectors for all Critical Digital Assets
  - Emphasis on target set equipment
- Milestone 8 (site specific date)
  - full cyber security program implementation
  - policies and procedures: training, attack mitigation, incident response, continuity of operations, etc.
  - completion of all design remediation actions, including those that require a refuel outage for implementation

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

FERC / NERC Interactions

- Energy Policy Act of 2005
- NRC Authority
- FERC Order 706/706B
  - recognizes potential for overlap
- NRC/FERC Memorandum of Agreement
- NRC/NERC Memorandum of Understanding
- SECY-10-0153: Implementation of the Commission's determination of systems and equipment within the scope of 10 CFR 73.54

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Cyber Security Roadmap

- Provides an update to the Commission on the status of the implementation of cyber security requirements for power reactor licensees and Combined License applicants.
- The paper outlines the approach for evaluating the need for cyber security requirements for the following four categories of the NRC licensees and facilities:
  - Fuel cycle facilities
  - Non-power reactors
  - Independent Spent Fuel Storage Installations
  - Byproduct materials licensees

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Oversight Development

- Interim Implementation Inspections
  - Begin January 2013
- Full Implementation Inspections
  - Begin late 2014
- Inspection Program Development
  - Inspection Procedure (Temporary Instruction)
  - Pilot of inspection process August 2012
  - Significance Determination Process (SDP)
  - Inspector training
  - Contractor training

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Fuel Cycle Facilities

- Working group established in 2011 by NMSS and NSIR
  - Developed a questionnaire;
  - Licensees responded to questionnaire via teleconference;
  - Staff performed selected site visits; and
  - Staff issued a final report (February 2012).
- Working group determined:
  - short-term goal would be to work with Industry (NEI and FCF) on a voluntary industry initiative;
  - long-term, a rulemaking using a graded, risk-informed approach should be considered.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Fuel Cycle Facilities

- Since 2011, the working group:
  - briefed industry on the threat and recommendations in the report;
  - worked extensively with Industry to obtain a voluntary agreement and implementation of six measures
- Staff and Industry could not reach a consensus on the adoption of all six measures
- Staff is writing a Commission paper to seek approval for issuing Security Orders to address the six measures and go forward with a follow-on rulemaking

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Future Activities

- SDOE
  - Revision to RG 1.152
    - ISG04 => IEEE 7-4.3.2 - 2010
- Cyber Security
  - Additional Guidance Development
  - Cyber Security Roadmap Implementation
  - Interagency and International Support

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Summary

- Regulatory infrastructure for SDOE and Cyber security has been put in place
  - More work remains to refine guidance, gain experience with reviews and inspections, and establish precedence
- NRR / NRO / NSIR are working to establish roles and responsibilities to ensure effective and efficient regulation

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Back-up Slides

NRC Regulatory Framework

Requirements

- 10 CFR 73.1 (Design Basis Threat)
- 10 CFR 73.54 (Cyber Security)

Regulatory Objective

PREVENT RADIOLOGICAL SABOTAGE

Scope

Systems that provide:
- **Safety, Important-to-Safety** functions
- **Security** functions
- **Emergency Preparedness** functions
- Support Systems whose failure would have an *Adverse Impact** on one of the above functions

*Adverse Impact** = Compromise of support system impairs/defeats the functionality of a safety system, important-to-safety system, security system, or emergency response system

Approach

Programmatic
Defense-in-Depth
Risk-informed

Guidance

RG 5.71 & Appendices
NEI 08-09 (Generic Cyber Security Plan Template)

Implementation

Oper. Rx Cyber Security Plan (10 CFR 50.34)
COLA Cyber Security Plan (10 CFR Part 52)

NRC Licensing

NSIR Safety Evaluation (Chapter 13)
NRR/NRO Issue License Condition

Support Systems whose failure would not have an *Adverse Impact** on a safety, important-to-safety, security, or EP function fall under **FERC** regulations (i.e., **NERC** cyber security standards)

MOA with **FERC**
and
MOU with **NERC**

NRC Oversight

Inspection Procedures
ITAAC [no programmatic ITAAC]
Inspector Training
Significance Determination Process

Requirements

- 10 CFR 50.55a (IEEE Std. 603-1991)
- 10 CFR 50 Appendix A (General Design Criteria)
- 10 CFR 50 Appendix B (Quality Assurance)
- 10 CFR 52.4

Regulatory Objective

SYSTEM FUNCTIONALITY & RELIABILITY

Scope

Systems that are:
- **Safety-Related**

Approach

System-level design features
Diversity and Defense-in-Depth
Deterministic

Guidance

IEEE Std. 7-4.3.2 - 2003
RG 1.152 Rev 3
Design Acceptance Criteria [Part 52]

Implementation

Licensing (10 CFR 50 / 52)
Amendment Request (10 CFR 50.90)
DC Application (10 CFR Part 52)

NRC Licensing

NRR/NRO Safety Evaluation (Chapter 7)
NRR/NRO Issue License Amendment

Evolution of Cyber Security

RG 1.152 Rev. 2

Section 2.1-2.5:

- Secure development environment
- Security Features to enhance reliable operation of safety systems.

RG 1.152 Rev. 3

Section 2.1-2.5:

Secure Development and Operational Environment

Consistent with RG 1.168, RG 1.169 and BTP14

10 CFR 73.54 + RG 5.71

Sections A.4.1.2, A.4.2.2 A.4.2.6 and Section C.12

•Perform cyber security impact analysis to identify security features to be incorporate into the systems and inherit from its environment.

• Security at development facilities and process

Security from System's and Program's

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Background

- Security of digital systems was initially covered in Regulatory Guide 1.152, Revision 2
  - Design aspects of digital computer-based systems were addressed in IEEE 7-4.3.2 – 2003; however, treatment of security aspects was deferred
- Nine regulatory positions cover the nine phases of a software life-cycle (from development through retirement)
  - Built upon provisions of 10 CFR 50, Appendix B (Criterion III) and 10 CFR 50.55a(h) (IEEE Std 603, Clauses 5.6.3 and 5.9)
  - Included coverage of cyber security

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Background (continued)

- New Rule 10 CFR 73.54 was issued in 2009 to specifically cover cyber security
  - Regulatory Guide 5.71 was issued in 2010 to supplement the implementation of the regulation
- With cyber security protections discussed under Part 50 (via RG 1.152, Rev 2) and under the new regulations in Part 73, NRC staff revisited its regulatory approach to cyber security

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Cyber Security Background

- 2001 to 2004: Advisories, Orders and Guidance
- 2005: Endorsement of NEI 04-04, “Cyber Security Program for Power Reactors”
- 2006 to 2007: Further guidance for use of computers in safety systems and software reviews for digital instrumentation and control systems (e.g., RG 1.152, Revision 2)
- Current Regulation
  - 10 CFR 73.54 “Protection of digital computer and communication systems and networks”

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

RG 1.152, Revision 3

- Regulatory Guide 1.152, Revision 3 was released in July 2011
- The revision reflects that cyber security and protection from malicious acts is covered under 10 CFR 73.54
  - No regulatory findings or conclusions relative to cyber protections will be made under Part 50/52 licensing actions
- However, the need existed to ensure appropriate controls were still in place during development and operation of digital safety systems to ensure their reliable operation

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

RG 1.152, Revision 3 (continued)

- RG 1.152 Revision 3 provided clarification on:
  - Protection of the development environment from inclusion of undocumented, unneeded, and unwanted code
  - Controls to prevent inadvertent access to systems
  - Protection against undesirable behavior of connected systems
- This collection of controls is now terms as establishment of a “secure development and operational environment”