

May 26, 2010 Meeting

Safety System Development

Process and Platform

CN0410046_NP, Rev. 1.0

Withheld information is marked as shown below



“a, b, c, d” indicate the reasons for withholding as defined in the proprietary information affidavit.



Nuclear Systems & Solutions



Top-level Agenda

- **Introduction**
- **Product Development Process**
- **Quality Assurance**
- **Platform Design and Process**
- **Topical Reports**
- **Conclusion**



INTRODUCTION



About Lockheed Martin

- Development and support of products with life-spans measured in decades
- Significant relevant competencies
- Extensive resources in people, labs, manufacturing, tools, and training provides vast amount of “reach back”

People and Places

- 136,000 employees
- 70,000 scientists and engineers
- 25,000 IT professionals
- Operations in 1,000 facilities, 500 cities, 50 states and 75 countries

Major Competencies

- Nuclear I&C
- Systems Engineering
- System Integration and Test
- Digital System Design
- Safety Critical System Design
- ILS and Product Sustainment
- Program Management
- Production Manufacturing
- Logistics
- Virtual Prototyping
- System Simulation/Modeling
- Electronics Packaging
- Reliability/Maintainability
- Advanced Algorithms

Beginning-to-End Product Development and Support



About NS&S

- **NS&S is an established, full-service vendor with:**
 - **Significant domain experience**
 - **World-class engineering and program execution**
 - **Large-scale Systems Integration capabilities and full life cycle support**
 - **Commitment to applying the Corporation's resources**
 - **Mature culture and commitment to safety and quality**

*We Are Committed to the NRC's Mission of Protecting
People and the Environment*

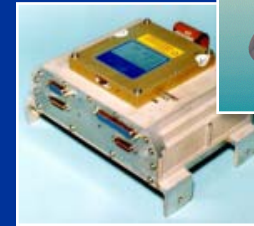
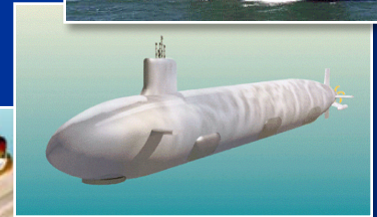
NS&S Within Lockheed Martin



*A Line of Business Dedicated to
Providing Solutions for Nuclear Systems*

Nuclear I&C and Complementary Products

- Largest I&C supplier to the U.S. Navy – systems on ALL nuclear vessels
- Design and manufacturing for GEN3+ reactor systems
 - Contracted and teamed with providers of safety-related equipment and designs
 - Commercial I&C:
 - Clinch River Breeder Reactor
 - Washington Public Power Supply System
 - Safety (Class 1E) and non-safety equipment applications
- Integrated analog and digital designs
- Harsh environment/high reliability
 - Devices qualified to strict military standards (EMI, radiation, shock, temperature)

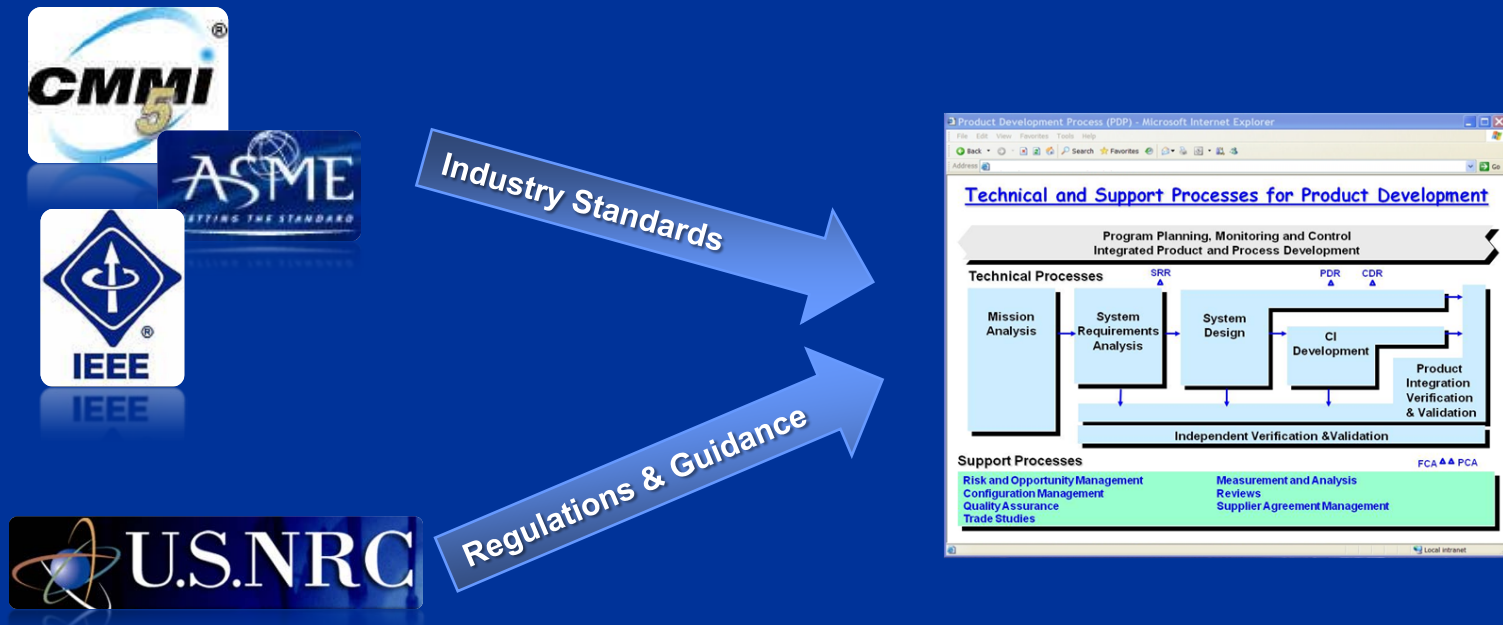


Proven Track Record on Domain-relevant Products

Established, Rigorous Process



- Mature Quality and Safety processes have proven history of building and certifying safety critical systems to our customers



*Mature Process Maps to NRC Requirements
Provides Roadmap to Qualification*



Participants

Lockheed Martin



Background

- **1st Phase 0 meeting w/ NRC on March 17, 2009**
 - **Discussed a new safety system platform**
 - **Discussed plans to submit topical reports for approval of the new platform and the development process**
 - **Discussed early and frequent interaction with regulator to ensure compliance and support regulatory efficiency**
 - **Decision to submit process and platform topical reports together made in November**



Meeting Purpose

- **NS&S plans to request U.S. NRC approval of**
 - **Process for safety-related product development**
 - **Generic platform for safety systems**
- **This meeting provides**
 - **Briefing by applicant on**
 - **Processes, platform, submittal plans**
 - **Staff feedback to applicant**



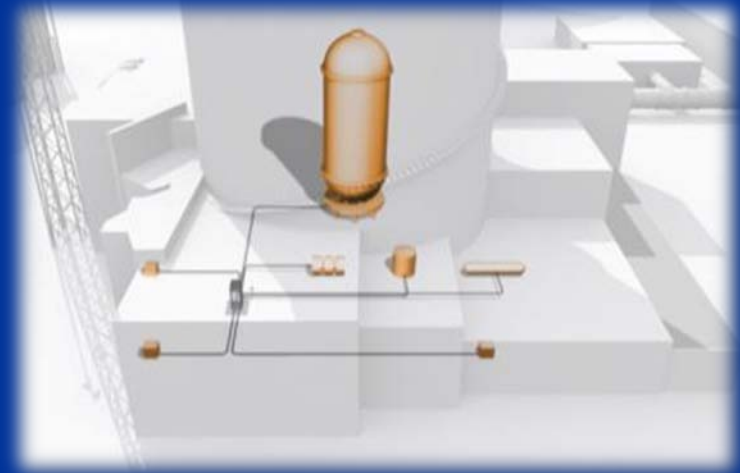
Expected Outcomes

- **NRC understanding of applicants':**
 - **Development process**
 - **Platform design**
 - **Plans for review**
- **LM understanding of NRC staffs':**
 - **Expectations**
 - **High-priority issues**



Motivation

- **The application of digital technology challenges the licensing of I&C safety systems**
- **Key Issues**
 - **Potential software common-cause failures**
 - **Inter-channel communication**
 - **Cyber security**
 - **Communication between non-safety and safety systems**
 - **Dedication of commercial off-the-shelf equipment**





Objective

- **Provide a control system platform for digital I&C safety systems to support the effective design, construction and operation of both existing and new reactors**
- **Key Points:**
 - Digital technologies enhancing safety, reliability and efficiency
 - Technical approach eliminating software common-cause failure vulnerabilities
 - Design, qualification and production under an Appendix B quality assurance program





PRODUCT DEVELOPMENT PROCESS



Agenda – Product Development Process

- **Introduction**
 - **Communications considerations**
- **Process governance**
- **CMMI Level and proof of performance**
 - **Process, audit history, certifications, and registrations**
- **General overview of process**
 - **Overarching instructions**
 - **Technical cross-functional procedures**
 - **Support cross-functional procedures**
 - **How everything works together**



“Secure the Building” or a “Failure to Communicate”

- **It has been claimed that one of the root causes behind the inability of US Armed Services to operate jointly is that the same terms have very different meanings – this is illustrated by a simple order from a Joint Commander to “Secure a Building”**

The response varies by service:

- **The Navy responds by turning off the lights and locking the doors**
 - **The Army responds by occupying the building so no one can enter**
 - **The Marines assaulted the building, captured it, and set up defenses with suppressive fire and amphibious assault vehicles, established reconnaissance and communications channels, and prepares for close hand-to-hand combat should the situation arise**
 - **The Air Force acts most swiftly on the command, they take out a three-year lease with an option to buy**
- **Clearly “What we've got here is (a) failure to communicate” (Cool Hand Luke, 1967)**



Alternative Lexicons (DoD, NUREG, CMMI, Lockheed Martin)

- What do we mean by CDR?
 - DoD, Critical Design Review (MIL-STD-499, 17 July 1969) (CDR) This review shall be conducted by the contractor for each CI when detailed design is essentially complete and fabrication drawings are ready for release. The purpose of this review will be to (1) determine that the detail design of the CI under review satisfies the design requirements established in the CI specification, and (2) establish the exact interface relationships between the CI and other items of equipment and facilities
 - NUREG-0544 – CDR, Conceptual Design Requirement
 - CMMI, Design Review – A formal, documented, comprehensive, and systematic examination of a design to evaluate the design requirements and the capability of the design to meet these requirements, and to identify problems and propose solutions

a, b, d

*MIL-STD-499, CMMI and LMMFC Use DoD Thread
NUREG is Not DoD Alternate Definitions*

Engineering Process Improvement (EPI) Integrated Process Group (IPG)

- **IPG responsibilities are:**

a,
b,
d



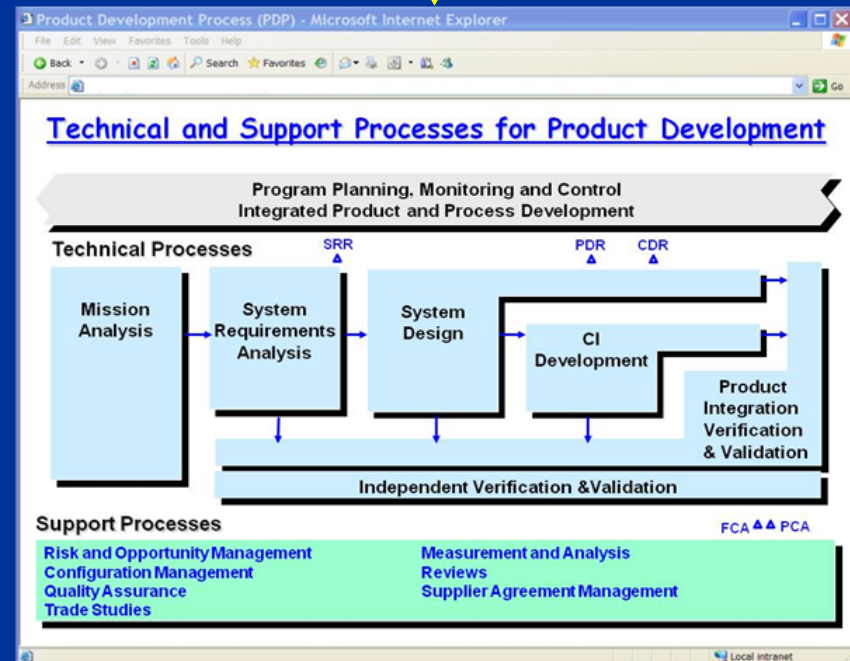
Engineering Process Improvement Integrated Process Group (IPG)

a,
b, d

PDP Flowdown in Command Media



- **External Direction**
 - LM Corporate standard method, CMMI®, AS9100, etc. Implementation
- **MFC Direction**
 - PDP Procedures
 - Process control



Command Media Hierarchy



a, b,
d



PDP Implementation

a, b, d,





What is CMMI® and its Importance?

- **What is it?**
 - **Capability Maturity Model® Integration (CMMI®)**
 - **Industry-wide Process Model sponsored by DoD**
 - **Single integrated process standard for:**
 - **Integrated Product and Process Development (IPPD)**
 - **Systems**
 - **Software**
 - **Supplier Sourcing**
 - **Five defined maturity levels: 1 (lowest) to 5 (highest)**
- **Who wants it?**
 - **The DoD applies CMMI as a discriminator/requirement for major acquisitions**
 - **LM Corporate policy encourages CMMI® rating**
 - **We do because, as companies mature, defined processes provide institutionalization repeatability**
- **What is our status?**
 - **Achieved Level 3 certification in May 2004**
 - **Achieved Level 5 certification in October 2006**



MFC's Process Improvement History

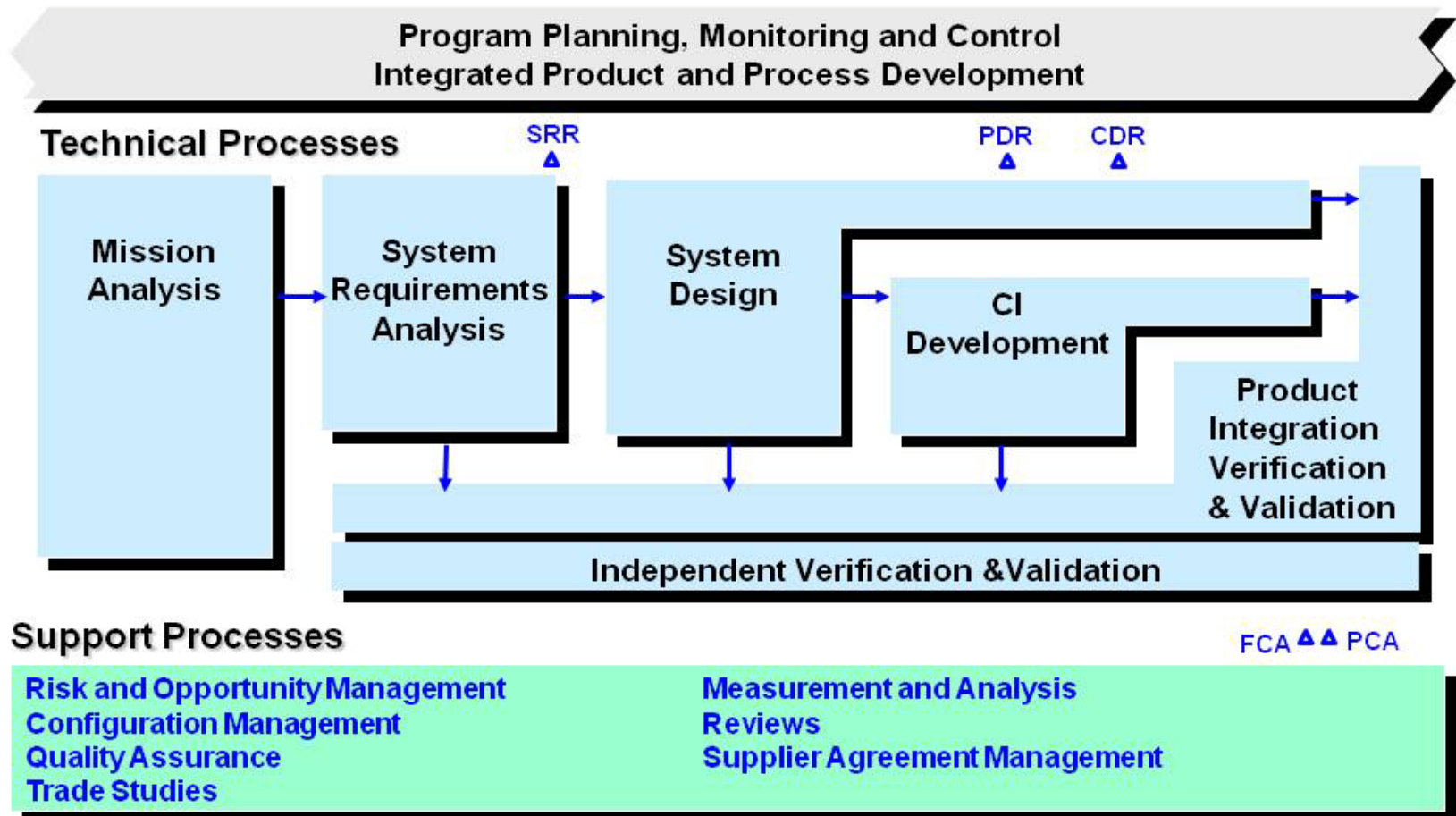
- Our processes are the product of more than 17 years of formal assessment, refinement, and continuous improvement

Year	Event
1992	<ul style="list-style-type: none"> • Internal assessment of EI&M Group • SEI assessment of EI&M Group - meets CMM 1.0 Level 2 for deliverable product software
1993	<ul style="list-style-type: none"> • Government SEI assessment of ASTAMIDS proposal • Government SEI assessment of AFIS proposal (won) • USAF assessment on JDAM proposal (won)
1994	<ul style="list-style-type: none"> • USAF assessment on WCMD proposal (won) • ISO 9000 Certification with Software TickIT • LANTIRN program internal assessment -meets Level 3 Goals
1995	<ul style="list-style-type: none"> • ISO 9000 reassessment certification • Comanche EOSS program internal assessment -meets Level 3 Goals • Longbow FCR program internal assessment -meets Level 3 Goals
1997	<ul style="list-style-type: none"> • SEI CMM (Capability Maturity Model) Level 3 Evaluation
1998	<ul style="list-style-type: none"> • SEI CMM Level 3 Evaluation • SEI CMM Level 3 CBA IPI
1999	<ul style="list-style-type: none"> • SEI CMM Level 3 Evaluation
2001	<ul style="list-style-type: none"> • SEI CMM Level 4 Evaluation
2003	<ul style="list-style-type: none"> • SEI CMMI Level 3 Evaluation – LM CAM (ARC Appraisal Method)
2004	<ul style="list-style-type: none"> • SEI CMMI Level 3 SCAMPI Class A
2005	<ul style="list-style-type: none"> • SEI CMMI Level 4 SCAMPI Class B
2006	<ul style="list-style-type: none"> • SEI CMMI Level 5 SCAMPI Class A
2008	<ul style="list-style-type: none"> • SEI Class C Appraisal
2009	<ul style="list-style-type: none"> • SEI Class C Appraisal
2010	<ul style="list-style-type: none"> • SEI CMMI SCAMPI Class A (Planned)



Product Development Process

Technical and Support Processes for Product Development





PPMC Overview

- Program Planning, Monitoring, and Control (PPMC)
 - PPMC is the overarching controlling process of the PDP

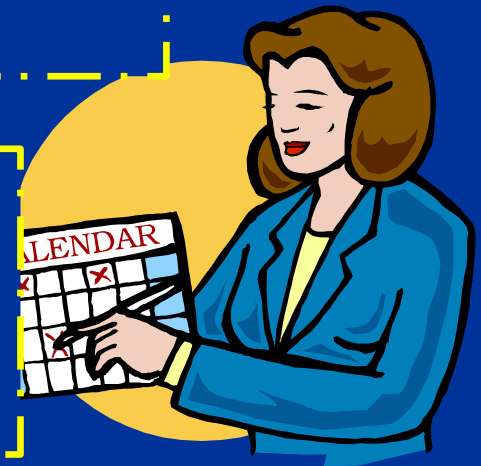
a, b, d

- Planning

a, b, d

- Monitoring & Control

a, b, d





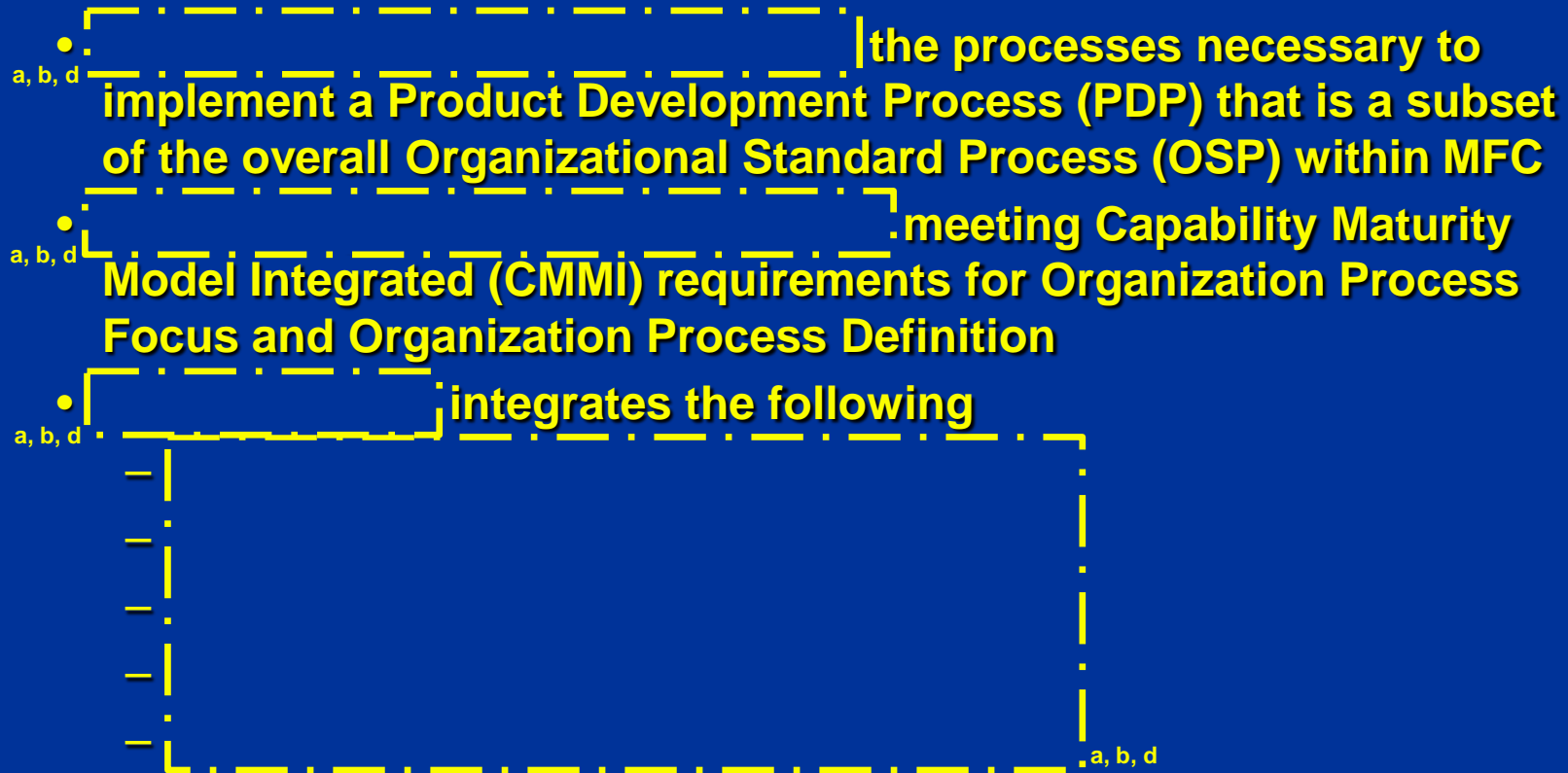
Integrated Product and Process Development (IPPD)

- IPPD is...

a, b, d



Organization Process Focus and Definition





Organizational Innovation and Deployment

- **Organizational Innovation and Deployment**
the process for
evaluation, refinement, replacement, and
insertion of processes and technologies
the CMMI Level 5
process area called **Organizational Innovation
and Deployment**

**Achieve Continuous Process and
Technology Improvements**



Purpose of Mission Analysis

- **The purpose of Mission Analysis is to:**
 - **Determine the needs of the user**
 - **Understand how the product will be used**
 - **Produce the output work products of Mission Analysis**
 -
 -
 -
 -
 -
-

Purpose of System Requirements Analysis



- **The purpose of System Requirements Analysis is to**

a, b, d

a, b, d

*Translate “Customer Speak” into
“Product Developer Speak”*



Purpose of System Design

- The purpose of System Design is to:





Purpose of CI Development

- The purpose of Configuration Item (CI) Development is to design, implement, build, integrate and test a, b, d

a, b, d CIs

- The CI Development process is composed of sub-processes:

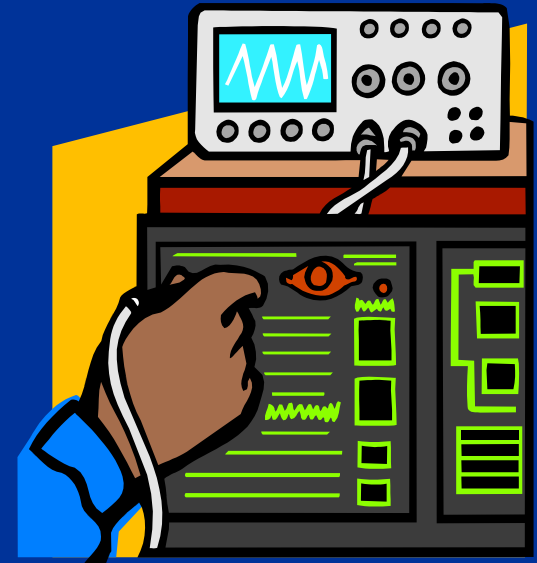
a, b, d



Purpose of PIVV

- **Product Integration, Verification, and Validation (PIVV) is performed to:**

- **Integrate all system elements**
- **Verify that the system was built according to the system requirements in the system specification, i.e., that we built the system right**
- **Validate that the system meets the needs of the users in the intended environment; i.e., that we built the right system**



- **Major work products of PIVV**



- **PIVV procedures**
- **Test reports**

• a, b, d



Product IV&V Definitions

- **Integration:** the process of assembling lower-level configuration items and/or subsystems into a system or unit
- **Verification:** Confirms that work products properly reflect the requirements specified for them. In other words, verification ensures that “you built it right.”
 — Events include Tests, Inspections, Analyses, Demonstrations, etc.
- **Validation:** Confirms that the product, as provided, will fulfill its intended use in the user’s environment. In other words, validation ensures that “you built the right thing.”

Support Process Risk Management Overview

- Proactively identify potential problems and/or opportunities so that appropriate handling/implementation activities may be planned and invoked
- Enhances the overall probability of program success!

- **is** **integral part of program life cycle** ^{a, b, d}



a, b, d=



Purpose of Configuration Management

- **Configuration Management of Work Products:**
 - **Identifies the baseline version(s)**
 - **Provides the ability to obtain the current version**
 - **Provides the ability to retrieve previous versions**
 - **Provides a change history**
 - **Provides a method for CM verification**

a, b, d

CM on Your Program

- Your configuration management process is defined and controlled by _____.

a, b, d

a, b, d

a, b, d

- **participate in the appropriate Program CCBs**



Purpose of Trade Studies

- Trade studies are ^{a, b, d} decision making tool
- They are performed throughout the product development process
- Used to identify, analyze and resolve opportunities or problems
- Alternatives Selection:
 - A trade study where two or more methods of solving a problem exist and you desire to select the appropriate option ^{a, b, d}
- Optimization: ^{a, b, d}
- ^{a, b, d} captures decisions and the rationale

Support Process Trade Study Methodology



a, b, d



Purpose of Measurement and Analysis

- **Develop and sustain a measurement capability that will provide critical information**

a, b, d



Purpose of Reviews

- Provide a means to periodically assess status!
a, b, d
- Requirements for specific reviews are
a, b, d
- There is an emphasis on
a, b, d



Reviews in a “Typical” Product Development Life Cycle

a, b, d



Requirements/Design Reviews

a, b, d

-

- **System Design Review (SDR)**

a, b, d

- **Preliminary Design Review (PDR)**

a, b, d

- **Critical Design Review (CDR)**

a, b, d

Detailed Review Contents Are Described By the Reviews Process



Test Reviews

a, b, d

Supplier Agreement Management

- Our acquisition procedures, including

require:

- Identifying qualified suppliers
- Using qualified products

- Accepting product based on prescribed acceptance criteria

*All to Ensure We Have the Right Materials,
at the Right Price, at the Right Place, at the Right Time*



Causal Analysis and Resolution

- **Causal Analysis and Resolution is a process to identify causes of defects and other problems and take action to prevent them from occurring again**
- **Causal Analysis and Resolution also provides a mechanism for programs to evaluate their processes and look for improvements that can be implemented**

a, b, d

a, b, d



QUALITY ASSURANCE OVERVIEW

Agenda – Quality Assurance



- **Accountability and Authority Flowdown**
- **Organizational “independence”**
- **10 CFR 50 Appendix B compliance**
- **Organization description**
 - **Design, manufacturing, QA, & V&V independence**
- **Vendor endorsement, 10 CFR 50 Appendix B approved supplier**
- **Commercial-grade dedication coverage**
- **Etc.**

Program Accountability and Authority



- **Program implementation of Organizational Standard Process**
 - **Program PDP Tailoring per Command Media Direction**



QUALITY ASSURANCE



a, b, d

- **[REDACTED]** provides leadership for employing Mission Success concepts and philosophies on the activities performed during design, development, procurement, manufacture, delivery, and support of products and services that are provided to meet our Customer's requirements and expectations. This process assures that affected organizations establish documented procedures to provide control of quality throughout all phases of contract performance, beginning during **[REDACTED]** a, b, d
- **[REDACTED]** activities include performing ongoing evaluations to assure conformance to contractual requirements and company procedures, ensuring effective quality management of programs to prevent defective products, analyzing results of measurement and assessment activities, reporting findings, and requiring corrective action and preventive action as necessary

(Cont)

- **_____ organizations perform these activities as an independent function reporting directly to the _____ Senior Executive. Program-level _____ representatives report to Senior _____ Management and are assigned in support of Program Management**
 - It is executed at the program level to perform evaluations of the products and services generated and evaluations of processes performed by the program
 - It is executed at the functional level to perform product and process evaluations on the generation and maintenance of organizational processes and process assets
- **_____ provides an independent evaluation function to assure cross-functional compliance to company policies and procedures**



Development QA Overview

- ^{a, b, d} [] provides leadership in applying Mission Success concepts and philosophies to the activities performed to meet our customer's requirements and expectations
- ^{a, b, d} [] evaluates program processes and products
 - Tells you how you are doing vs. process and plans
 - Identifies possible problems
 - Triggers process improvements and corrective action
- Evaluations are based upon a closed-loop process
 - Checklists based upon the program's tailored processes are used
 - Evaluation results are recorded ^{a, b, d} []
 - Corrective action must be compliant with ^{a, b, d} []
 - Corrective action is tracked to closure



Dev. QA Overview (Cont)

a, b, d

- evaluation data is analyzed and the analysis is documented in a Program Report a, b, d

- **Quality Assurance activities and evaluation results are reviewed with:**
 - Program staff and higher-level management
 - Customer's QA personnel (as appropriate)
- **The PDP Quality Assurance process is followed in addition to other QA command media**

a, b, d

Alternative Lexicons - CMMI



- **Key terms under consideration**
 - **Objectively Evaluate** – To review activities and work products against criteria which minimize subjectivity and bias by the reviewer
 - An example of an objective evaluation is an audit against requirements, standards or procedures by an independent quality assurance function
 - **CMMI Process and Product Quality Assurance** – “Objectivity in process and product quality assurance evaluations is critical to the success of the project. (See the definition of “objectively evaluate” in the glossary)”



Integrated System Manual

- Describes our Quality Management System (QMS)
- References the associated documentation
- Addresses a complete product life cycle

a, b, d

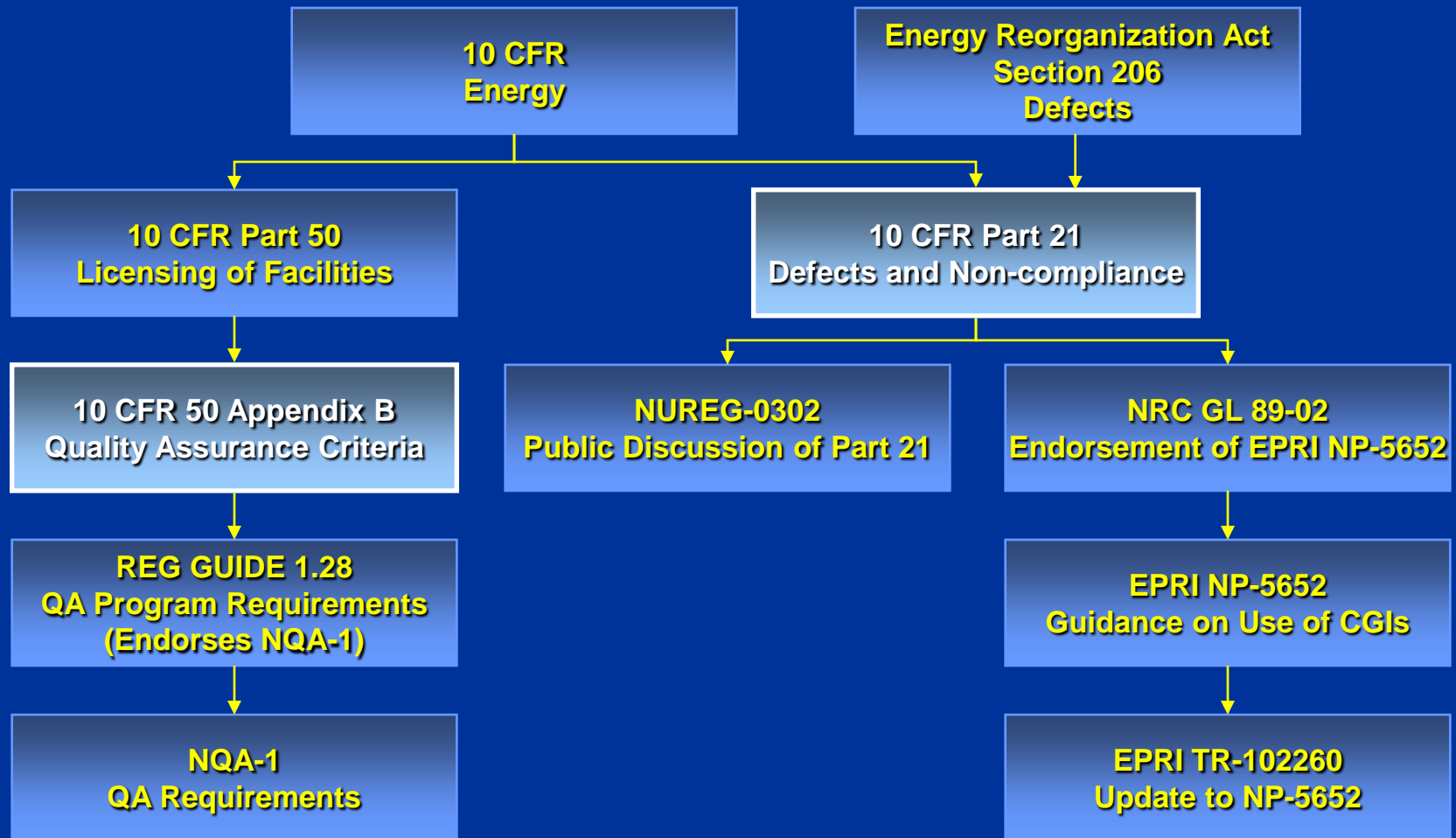


Quality Management History

a, b, d



Nuclear QA Requirements





PL Procedures/Instructions

a, b, d



Quality Assurance

- **Quality Assurance through:**

- **Appendix B of 10 CFR Part 50**

- [Redacted] a, b, d
 - [Redacted] a, b, d

- **Commercial Grade Item Dedication**

- [Redacted] a, b, d
 - **Define critical characteristics**
 - **Acceptance Plan - Ensure critical characteristics are met through special tests, surveillance inspections and analysis**
 - [Redacted] a, b, d



PLD I-V&V Process/Strategy

- Meets the requirements of:
 - IEEE Std. 1012-1998 Software Verification and Validation (NRC endorsed for software)
 - NUREG/CR-7006 Review Guidelines for FPGAs in Nuclear Power Plant Safety Systems (NRC has not endorsed to date)
- Every step in the design path has a corresponding step in the I-V&V path



QMS Compliance Overview

- **10 CFR 50 Appendix B**

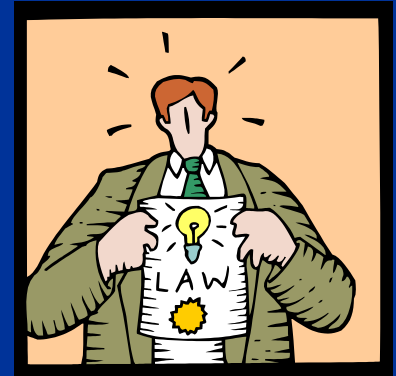
“Quality Assurance Criteria”

- Meeting ASME NQA-1—1994

- **10 CFR 21**

“Reporting of defects and non-compliance”

- **AS9100 non-conformance reporting**
- **Part 21 reporting and accountability**



- **10 CFR 50 Appendix A Criterion 1**

“General Design Criteria, Quality Standards and Records”

- QA program established and implemented
- Quality standards applied based safety function importance
- Appropriate quality records generated for licensees/delegates

Examples of NS&S Quality Controls



a, b, d



Summary

Quality Assurance


- **Well-established Organizational Standard Policies, Procedures and Instructions**
 - **Thoroughly-documented, configuration-managed, and change-controlled**
 - **Compliant with multiple industry standards**



***“Institutionalization” of Quality Assurance
and Quality Control***



Summary

- **Lockheed Martin Missiles and Fire Control**
 - A “Defined Process” organization that tailors its Organizational Standard Processes to the needs of the organization and the customer
- **Nuclear Systems & Solutions**
 - Addresses the requirements of 10CFR50 within its PDP application for safety-related items
 -  a, b, d

*Established, Proven and Compliant
Processes Promote Nuclear Safety*



PLATFORM



Platform

Section Overview

- Program Introduction
- Mission Analysis
- System Requirements Analysis
- System Design
- Configuration Item Development
- Integration, Verification, & Validation
- Specialty Engineering Integration
- Quality Assurance



PLATFORM PROGRAM INTRODUCTION



Program Introduction

➤ Problem Statement

- Nuclear Power Plant (NPP) Instrumentation and Control (I&C) Safety Systems
 - Available platforms challenge (technical, schedule, cost) the licensing of I&C retrofits and new construction due to software common-cause failure vulnerability

➤ Objective

- Offer a **LICENSABLE** digital control system platform for safety-related NPP applications
 - Non-microprocessor/non-software based
 - FPGA-based
 - Designed specifically for the nuclear industry
- Provide **CERTIFIED BUILDING BLOCK(s)**
 - Generically-qualified (with U.S. NRC) modules ready to be configured per customers' application-specific requirements

*NRC Approved – Generic Building Block
(Safety Evaluation Report)*



➤ Current Situation

- Lockheed Martin (LM) is developing a indigenous product, the **DS³**
- Detailed design in progress

➤ Vision

- Leverage LM's proven I&C design and integration expertise with a NRC-approved system and processes to service the domestic and international reactor I&C retrofit and new-build market

***A Premier FPGA-based Platform Designed
Specifically for Use in NPP I&C Safety Systems***



Design Concept Overview

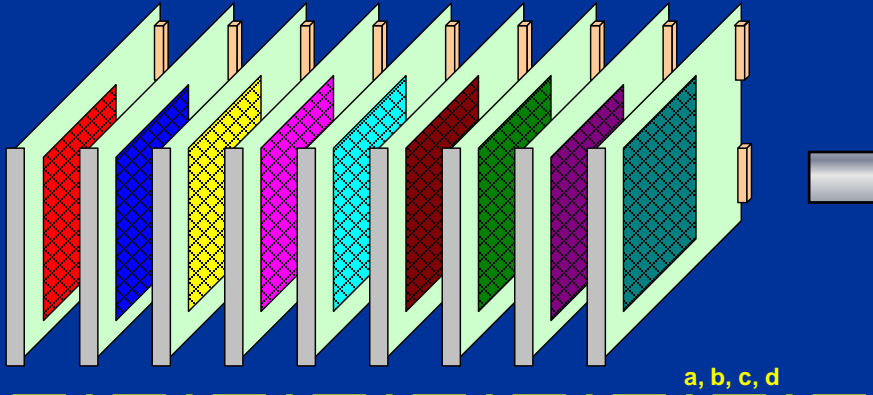
- **A digital platform specifically designed for nuclear I&C safety systems**
 - **Based on functional and physical requirements in EPRI TR-107330**
 - **Design to eliminate software common-cause failure vulnerabilities**
 - No microprocessors, operating systems, or executable software
 - Hardware-based state machine
 - **Design for verifiability**
 - Simple and deterministic
 - Functionally and physically segmented to permit proper verification
 - **Design for supportability**
 - Sustained Integrated Logistics Support (ILS)
 - **Security of an embedded system**



Form, Fit, and Function Similarity to Commercially-available PLCs

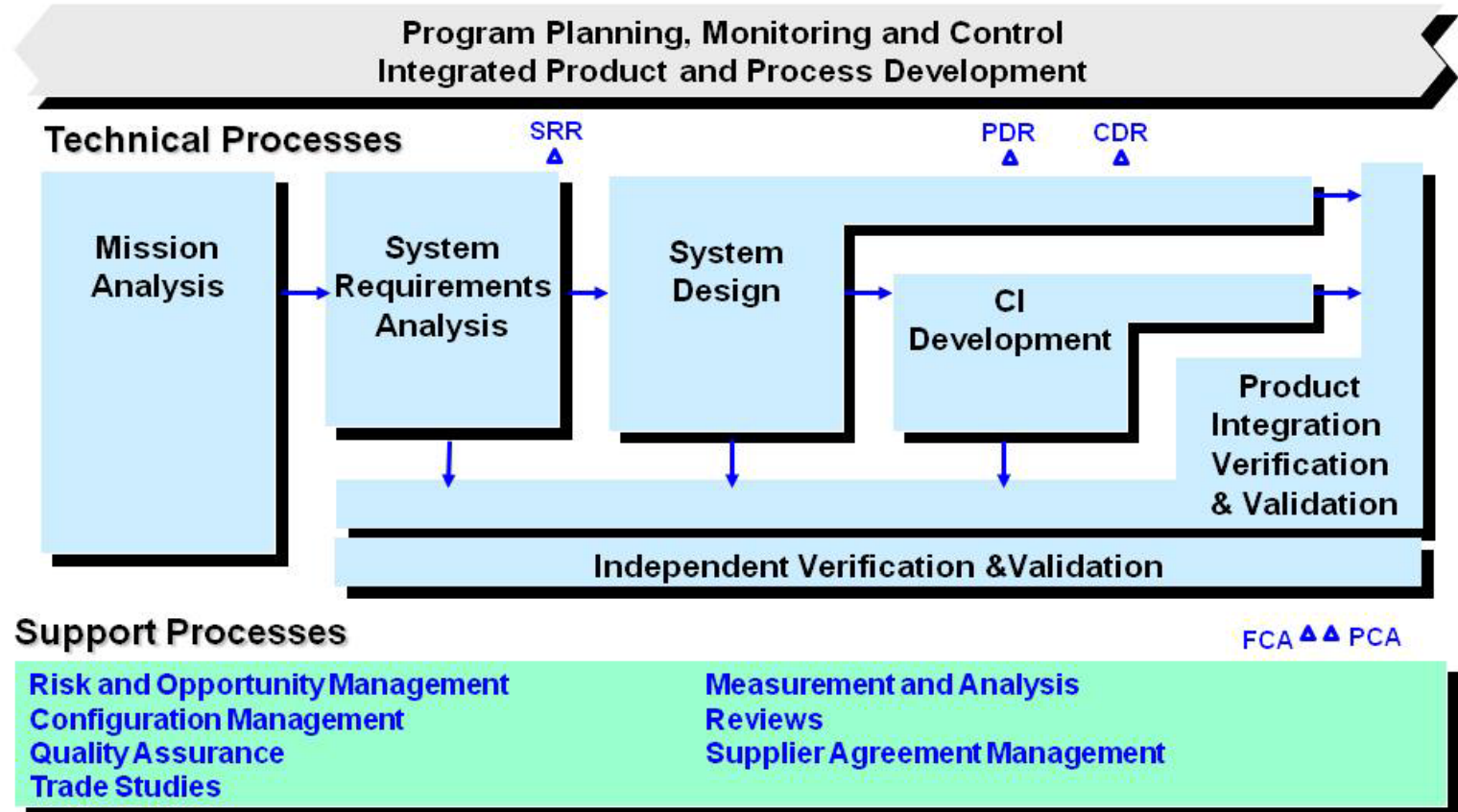
Paradigm

Traditional PLCs (Programmable Logic Controller)



Program Processes

Technical and Support Processes for Product Development



Program Is Following the LM Product Development Process (PDP)



Program Plans

The plans used to manage the specifics of the program

a, b, d

Engineering Practices Manuals



Engineering Practices Manual (EPM) Series – provides policies, design guidance, procedures, and practices that are to be utilized by all personnel unless otherwise directed by the program directives

a, b, d



Roles and Responsibilities

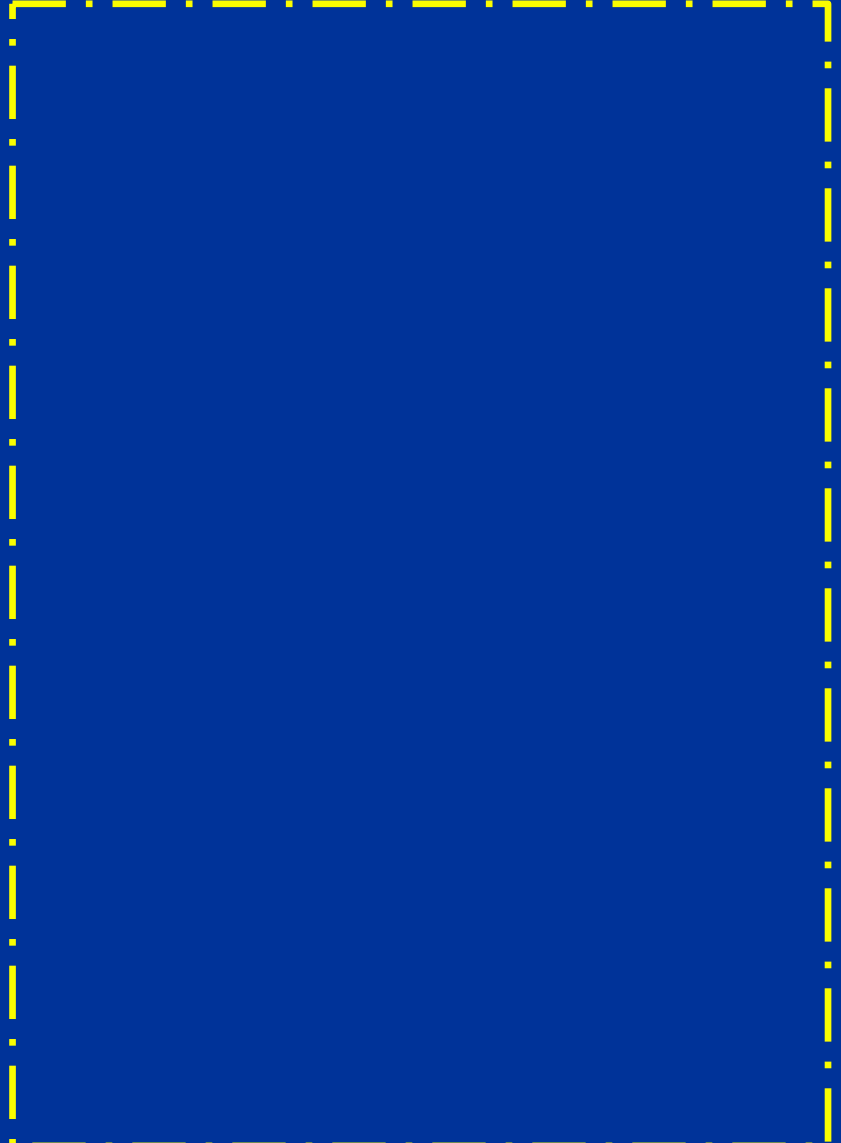
Program Management Plan



Roles Matrix



a, b, d



Program Organization

a, b, d



Program History



a, b, d

Program Plan

a, b, c, d





PLATFORM MISSION ANALYSIS

Mission Analysis

a, b, d



Mission Analysis

a, b, d



Determined Our “Niche” System and Subsystem Functionality



Concept of Operation

➤ System Overview

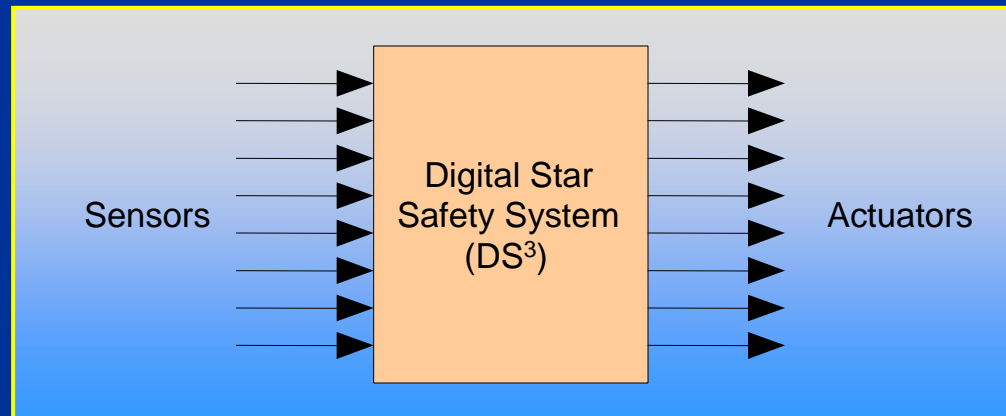
- Function as a computational platform (logic solver) for safety-related nuclear power plant applications
- Continuously monitor the status of the system through signals received from peripheral input devices (sensors)
- Performs computations (solve logic) to calculate control commands
- Converts the control commands to output signals, which are applied to peripheral output devices (actuators)

➤ Operational Environment

- Nuclear Power Plant (NPP) Digital Instrumentation & Control (I&C) Safety Systems

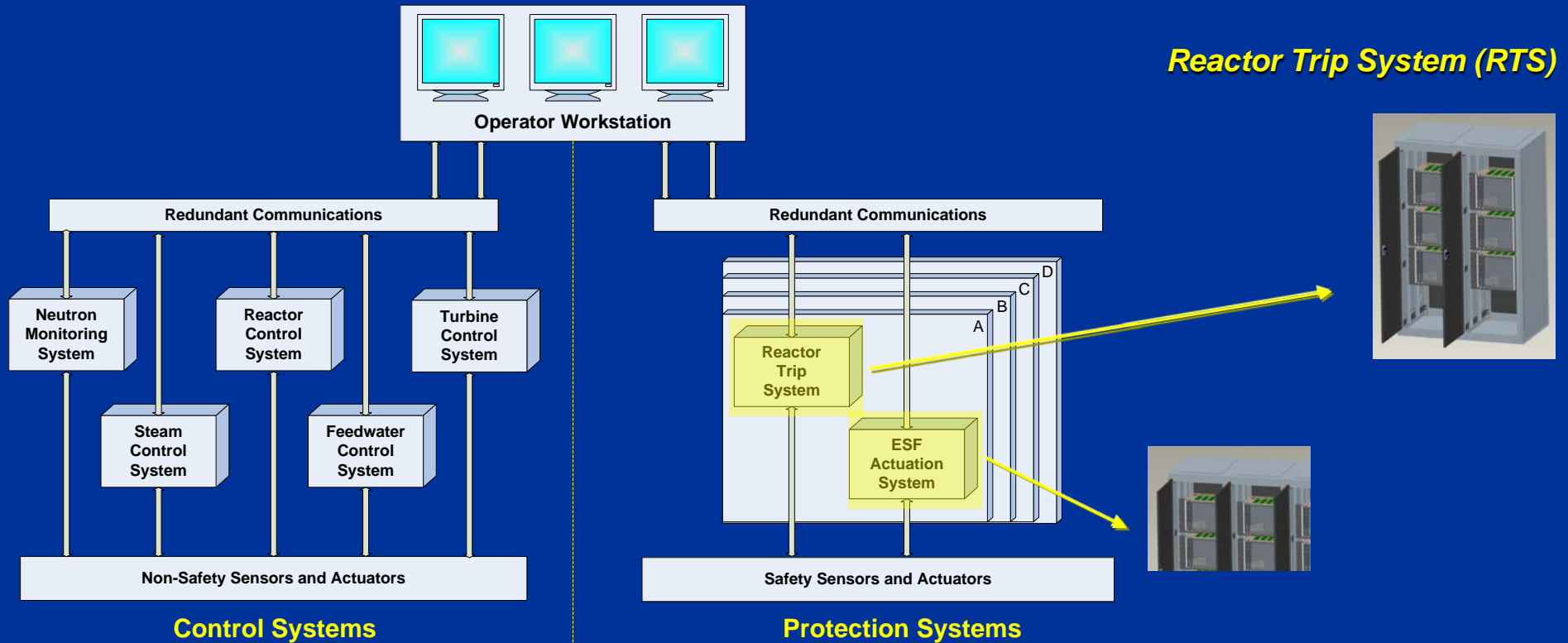
➤ Operational Scenarios

- Reactor Trip System (RTS) sense and command
- Engineered Safety Features Actuation System (ESFAS) sense and command
- Replacement for Analog Systems/Components (e.g. Trip Modules)





Operational Scenario



Simplified Reactor I&C System

Engineered Safety Features (ESF)

A Platform for Reactor Protection Systems



PLATFORM SYSTEM REQUIREMENTS ANALYSIS

System Requirements Analysis

a, b, d



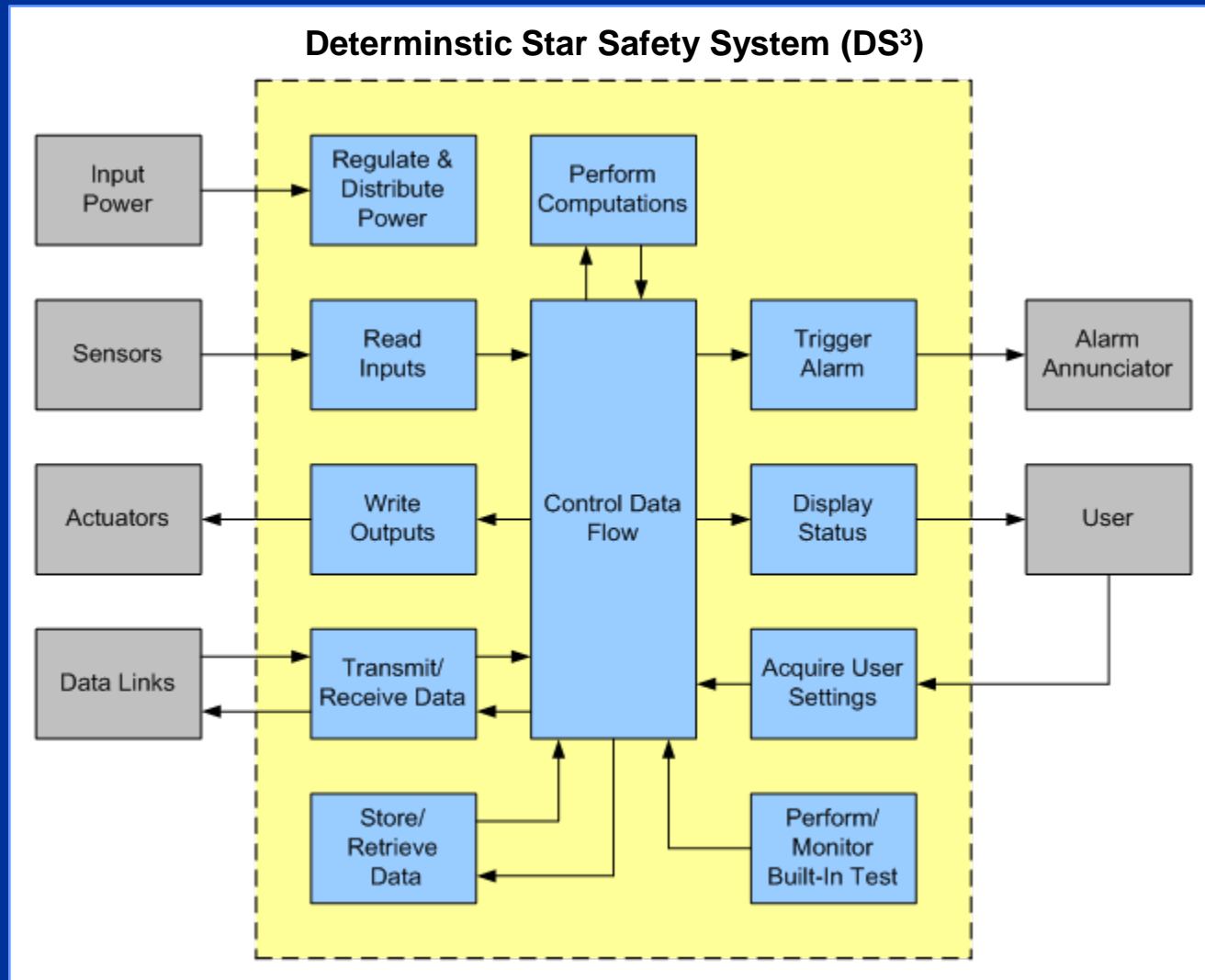
System Requirements Analysis ^{a, b, d}



Requirements Evolution Identified the Best Solution



Functional Architecture



For additional details, reference the Functional Architecture document, FA610000-001

System Specification a, b, d



Starting Point for the System Design Activities



PL Development

a, b, d

PL Requirements

a, b, d



PL Additional Guidance

a, b, d





PL Procedures/Instructions

a, b, d



PLATFORM SYSTEM DESIGN

System Design

a, b, d



System Design

a, b, d



Trade Studies

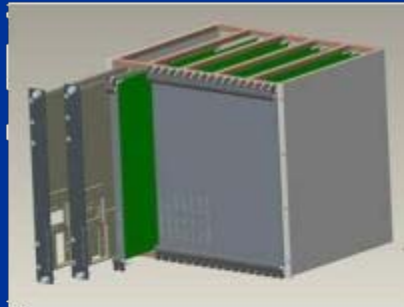
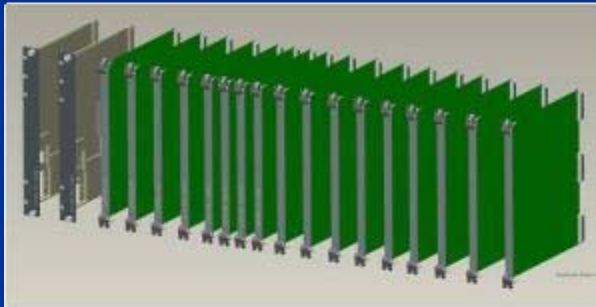
a, b, c, d





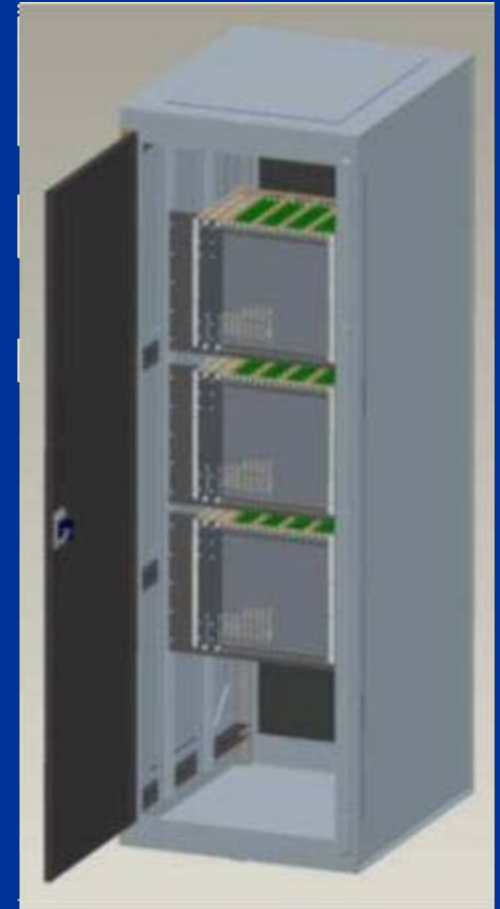
Physical Architecture

- **Generic, modular, scalable**
- **Similar form, fit and function as commercially-available PLCs**



a, b, c, d

- [Redacted]
- Chassis mounted / cabinet installed
- Industry-standard card form factors and chassis
- Suitably rugged for design basis events and long service life
 - Withstand requirements per EPRI TR-107330
 - Environmental, EMI/RFI, ESD, Seismic



Requirements Allocation a, b, d





PLATFORM SYSTEM DESIGN SYSTEM DESIGN DETAILS

System Design Details

a, b, c, d



Generic Logic Module

a, b, c, d

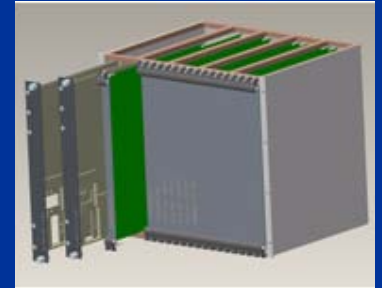
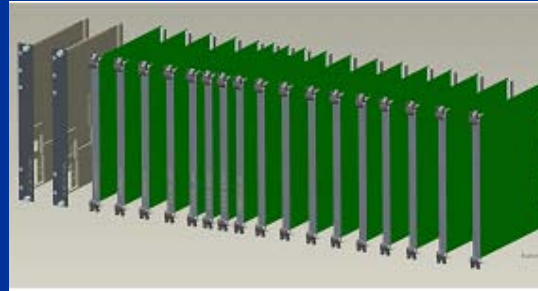




Chassis Configuration

- 21 Slot 9U Chassis
- Dual-redundant Power Supply Slots
- 16 General-purpose Slots
- Dual-redundant Communication Slots

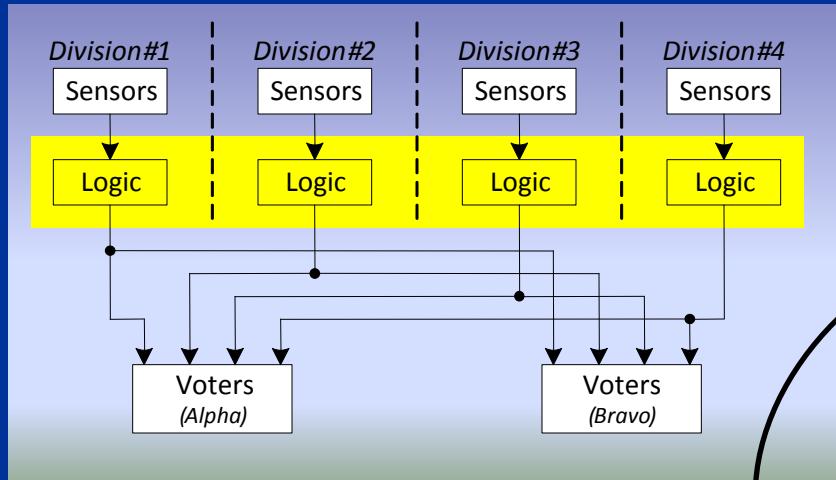
a, b, d



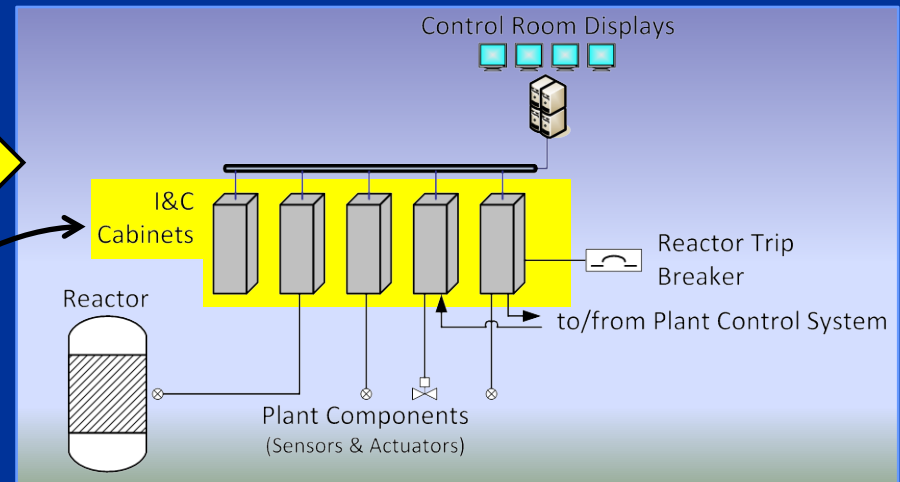


Notional Implementation

Functional Architecture



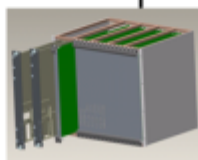
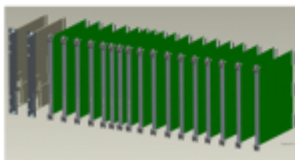
Physical Architecture



Cabinet Suite



LM DS³

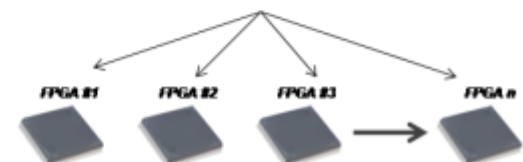
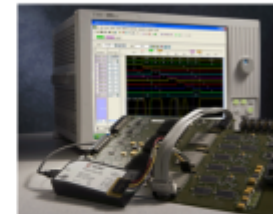


Solution

Cabinets
Power Supplies
Media Converters
Cables
Component Interfaces Circuits

DS³ Control System Platform
Chassis Assemblies
Logic Modules
Programmable Logic
I/O Cabling/Termination

FPGA, Application Specific Logic





PLATFORM CONFIGURATION ITEM DEVELOPMENT

Configuration Item Development

a, b, d





PLATFORM CONFIGURATION ITEM DEVELOPMENT GENERIC LOGIC MODULE (GLM)



PLATFORM CONFIGURATION ITEM DEVELOPMENT GLM - HARDWARE

GLM Circuit Card Assemblies

a, b, d



Carrier Card

a, b, d



Logic Module Card

a, b, d



I/O Module Cards

a, b, d



Card Top

a, b, d





PLATFORM CONFIGURATION ITEM DEVELOPMENT GLM – CIRCUIT DESIGN

Power Management Scheme

a, b, d





I/O Module Input Options^{a, b, d}



I/O Module Output Options a, b, d



a, b, d

CLEARED FOR PUBLIC RELEASE











a, b, d

CLEARED FOR PUBLIC RELEASE



a, b, d

CLEARED FOR PUBLIC RELEASE





a, b, d

CLEARED FOR PUBLIC RELEASE









a, b, d

CLEARED FOR PUBLIC RELEASE



a, b, d

CLEARED FOR PUBLIC RELEASE









PLATFORM CONFIGURATION ITEM DEVELOPMENT GLM – PROGRAMMABLE LOGIC







a, b, d

CLEARED FOR PUBLIC RELEASE





a, b, d

CLEARED FOR PUBLIC RELEASE



a, b, d

CLEARED FOR PUBLIC RELEASE



a, b, d

CLEARED FOR PUBLIC RELEASE



a, b, d

CLEARED FOR PUBLIC RELEASE







a, b, d

CLEARED FOR PUBLIC RELEASE



a, b, d

CLEARED FOR PUBLIC RELEASE



a, b, d

CLEARED FOR PUBLIC RELEASE



a, b, d

CLEARED FOR PUBLIC RELEASE









a, b, d

CLEARED FOR PUBLIC RELEASE



a, b, d

CLEARED FOR PUBLIC RELEASE



a, b, d

CLEARED FOR PUBLIC RELEASE





PLATFORM CONFIGURATION ITEM DEVELOPMENT CHASSIS

a, b, d

CLEARED FOR PUBLIC RELEASE





a, b, d

CLEARED FOR PUBLIC RELEASE



a, b, d

CLEARED FOR PUBLIC RELEASE





a, b, d

CLEARED FOR PUBLIC RELEASE





a, b, d

CLEARED FOR PUBLIC RELEASE





a, b, d

CLEARED FOR PUBLIC RELEASE





a, b, d

CLEARED FOR PUBLIC RELEASE



a, b, d

CLEARED FOR PUBLIC RELEASE



a, b, d

CLEARED FOR PUBLIC RELEASE





a, b, d

CLEARED FOR PUBLIC RELEASE





a, b, d

CLEARED FOR PUBLIC RELEASE



a, b, d

CLEARED FOR PUBLIC RELEASE





PLATFORM INTEGRATION, VERIFICATION & VALIDATION

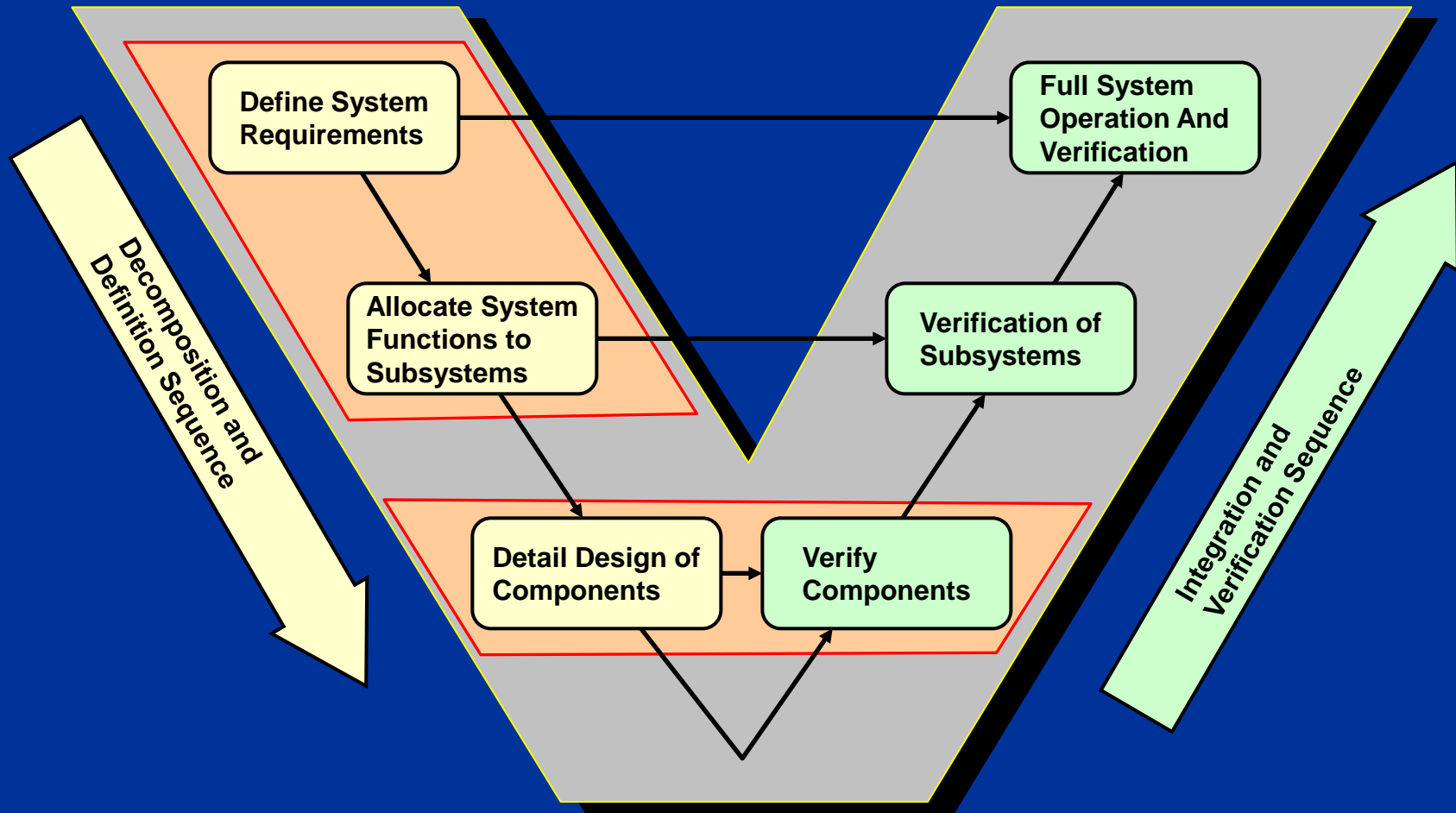
Integration, Verification & Validation



a, b, d



“Vee” Process Model



The “Vee” Process Model

a, b, d

CLEARED FOR PUBLIC RELEASE





Requirements Allocation

a, b, d







PLATFORM INTEGRATION, VERIFICATION & VALIDATION TEST SPECIMEN CONFIGURATION

















PLATFORM INTEGRATION, VERIFICATION & VALIDATION PROGRAMMABLE LOGIC INDEPENDENT V&V



What is PLD I-V&V*?

- **Verification and Validation (V&V)**
 - The process of checking whether the PLD design meets its requirements (verification) and its intended use (validation)
- **Independent Verification and Validation (I-V&V)**
 - V&V performed by a person or group that is financially, technically, and organizationally independent from the design team
 - Independence ensures design team has no influence over how V&V is performed

* I-V&V is used for Independent V&V and IV&V is used for Integration, Verification and Validation



Why PLD I-V&V?

- **The safety-critical nature of the DS³ requires assurances that the programmable logic will perform its intended function in a reliable manner**
- **To ensure that computer-based tools used to design do not introduce errors**
- **To meet Nuclear Regulatory Commission's (NRC) expectations**













a, b, d

CLEARED FOR PUBLIC RELEASE





PLATFORM INTEGRATION, VERIFICATION & VALIDATION QUALIFICATION TEST PROGRAM





Qualification Test Program

a, b, d



Qualification Test Program

a, b, d

Qualification Test Program



a, b, d





PLATFORM SPECIALTY ENGINEERING INTEGRATION

System Safety



a, b, d



Reliability



a, b, d





PLATFORM QUALITY ASSURANCE



Quality Assurance

- **Quality Assurance through:**

- **Appendix B of 10 CFR Part 50**

- [Redacted] a, b, d

- **Commercial Grade Item Dedication**

- [Redacted] a, b, d

- **Define critical characteristics**
 - **Acceptance Plan - Ensure critical characteristics are met through special tests, surveillance inspections and analysis**

- [Redacted] a, b, d



TOPICAL REPORTS



Topical Reports

- **Overview**
- **Need, Purpose and Scope of TRs**
- **Acceptability**
- **Proposed Methodology**
- **Proposed Schedule**
- **Supporting Material**
- **Protocols**



Overview

- **NS&S will submit two topical reports in July for review**
 - **Process Topical Report**
 - **Platform Topical Report**
- **NS&S will request December 2011 approvals**
- **NS&S does not plan to request fee exemptions for the reviews**

Concurrent Review and Two SERs



Need and Purpose

- Fully address the need for pre-approved platforms that don't require diverse backups
- Reduce the amount of review effort needed to approve license amendment requests and other applications
- Increase design and process standardization
- Contribute to improved plant safety through proper reuse of previously-evaluated designs

Multiple Benefits to Nuclear Safety Systems



Process TR Overview

- **Scope**
 - NS&S general development process for safety-related designs
- **Purpose**
 - U.S. NRC evaluation and approval of the NS&S development process
 - For reference in future applications

Process Applies to Any Safety-related Design



Platform TR Overview

- **Scope**
 - **NS&S platform for safety-related designs**
 - **design, design process, and qualification**
- **Purpose**
 - **U.S. NRC evaluation and generic approval of the NS&S platform**
 - **Use of platform in future replacements and new system designs**

Specific to the DS³ Digital Platform Design



Acceptance Criteria

- Address specific safety-related subjects that require safety assessments by the NRC staff
- Can be evaluated independent of a specific license application
- Will be referenced in a number of license amendment requests, license applications or design certification requests
- Contain complete and detailed information on the specific subject presented
- Approval of the reports will increase the efficiency of the review process for applications that reference the reports

The NS&S Topical Reports Meet the Acceptance Criteria



TR Features

- Information presented in an order that will facilitate the staff's review
 - DI&C-ISG-06 used as a guide
- Supporting documents referenced
- Supporting documents are not required to understand content
 - For confirmation and added detail only

Features Based on Regulator Feedback To Industry



Development Approach

- Use of latest NRC DI&C-ISG-06
- Use of latest NRC LIC-500
- LM participation in NRC/industry working groups
- Use of personnel experienced in preparing topical report submittals
- Involvement of subject matter experts
 - Development process
 - Generic platform design

The Latest Guidance, Used by a Multi-discipline Team



Process TR Outline

Major Headings

1. Introduction
2. Process Environment
3. Product Development Process
4. Nuclear Requirements
5. Glossary, References, etc

*Describes the NS&S Development Process for
Safety-related Products*

Process TR Level of Detail (1)



a, b, d



Process TR Level of Detail (2)



a, b, d





Platform TR Outline

Major Headings

1. Scope
2. Regulatory Compliance
3. Organization and Process Interfaces
4. System Description
5. Physical Architecture
6. Life Cycle Processes for Programmable Devices
7. EQ Testing
8. Supporting Analyses
9. Conclusions
10. Etc.

Patterned After the Sample Safety Evaluation in ISG-06



TR Schedule

a, b, d

- Submittal less qualification results in July
 - Non-proprietary versions prepared and submitted after NRC proprietary review
- All qualification results submitted in 2010

Requesting Approval by the End of 2011



Key Dates

- **March 17, 2009 – 1st Phase 0 Meeting**
- **May 26, 2010 – 2nd Phase 0 Meeting**
- **TBD – 3rd Phase 0 Meeting (if required)**
- **July 16, 2010 – Topical report submittal**
- **3Q 2010 – Acceptance review meeting**
- **3Q 2010 – TR accepted/Safety Evaluation started**
- **TBD 2011 – RAI and on-site inspections**
- **TBD 2011 – Safety Evaluation Report issued**



Documentation Plan

- Developed by matching program documents with information listed in DI&C-ISG-06 Enclosure B
- Two sets of documents
 - Set due at submittal (July)
 - Set due 12 mo prior to requested approval date (December)
- FPL life-cycle documents similar to those for software life cycles

Documentation Plan That Meets Regulator's Expectations



Documents Due at Submittal

- Management Plans
- Development Plans
- Quality Assurance Plans
- Configuration Mgmt Plans
- V&V Plans
 - Includes Integration
 - Includes Testing
- Equipment Qualification Plans
- Design Procedures
- Design Review Procedures
- System Specifications
- Requirements Specifications
- Hardware Specifications
- Design Specifications
- FPL Specifications
- Design Analysis Reports
- Design Descriptions
 - System
 - Hardware
 - Programmable Logic
- Commercial Grade Dedication Plans

Includes Programmable Logic Life Cycle Documentation

Documents Due During Review



- **V&V Reports**
 - Reviews
 - Integration
 - Testing
- **Commercial Grade Dedication Reports**
- **Qualification Results**
 - Defines Qualification Envelope



Standard Topics

- **TR acceptability**
- **Expected level of detail**
- **Review hour estimate**
- **Review schedule estimate**
- **TR merits and problem areas**
- **Potential relationships to ongoing or proposed activities**

Possible NRC Feedback per LIC-500



Other Topics

- **TR scope and content**
- **Level of TR detail**
- **Supporting document approach**
- **Objective evidence for audit/inspection**
- **Feasibility of TR submittal schedule**

Correction of Issues As Early As Possible



TR Priority

Draft TR Prioritization Scheme Matrix*			
* NRR will evaluate the shaded areas. Industry input on these areas is not requested.			
Factors	Select the Criteria That the TR satisfies	Points Assigned For Each Criteria	Total Points (if points are cumulative, total them for each factor in this column)
TR Classification (Points are cumulative)	Generic Safety Issue	6	
	Emergent Technical Issue	3	
	Standard TR	1	
Applicability (Points are not cumulative)	Industry-wide Implementation	3	
	Applicable to entire groups of licensees (BWROG, PWROG, BWRVIP, etc.)	2	
	Applicable only to partial groups of licensees	1	
Specialized Resource Availability (Points are cumulative)	NRC staff expertise is readily available <i>(The NRC staff will evaluate this criteria)</i>	1.5	
	Technical data is available/readily accessible <i>(The NRC staff will evaluate this criteria)</i>	1	
	A SE is requested by a certain date (less than two years) to support a licensing activity. Provide justification.	0.5	
Total Points (Add the total points from each factor and total here): (NRC staff will total the points)			

Priority of At Least 4.5 Expected



Summary

- **NS&S will submit two topical reports in July 2010 for review**
 - **Process TR**
 - **Platform TR**
- **NS&S will request December 2011 approvals**
- **NS&S does not plan to request fee exemptions for the reviews**

Concurrent Review and Two SERs



CONCLUSION



Meeting Review

- **Introduction**
- **Product Development Process**
- **Quality Assurance**
- **Platform Design and Process**
- **Topical Reports**
- **Conclusion**



Questions



Staff Comments





In Closing

- **Our processes and our platform will benefit nuclear safety and the safety evaluation process**
- **Thank you for your time and attention**

