EPRI Digital Engineering Guide(DEG) and the Standard Digital Design Process NISP-EN-004

Configuration Management Benchmarking Group- 26th Annual Meeting

Matt Gibson- Technical Executive

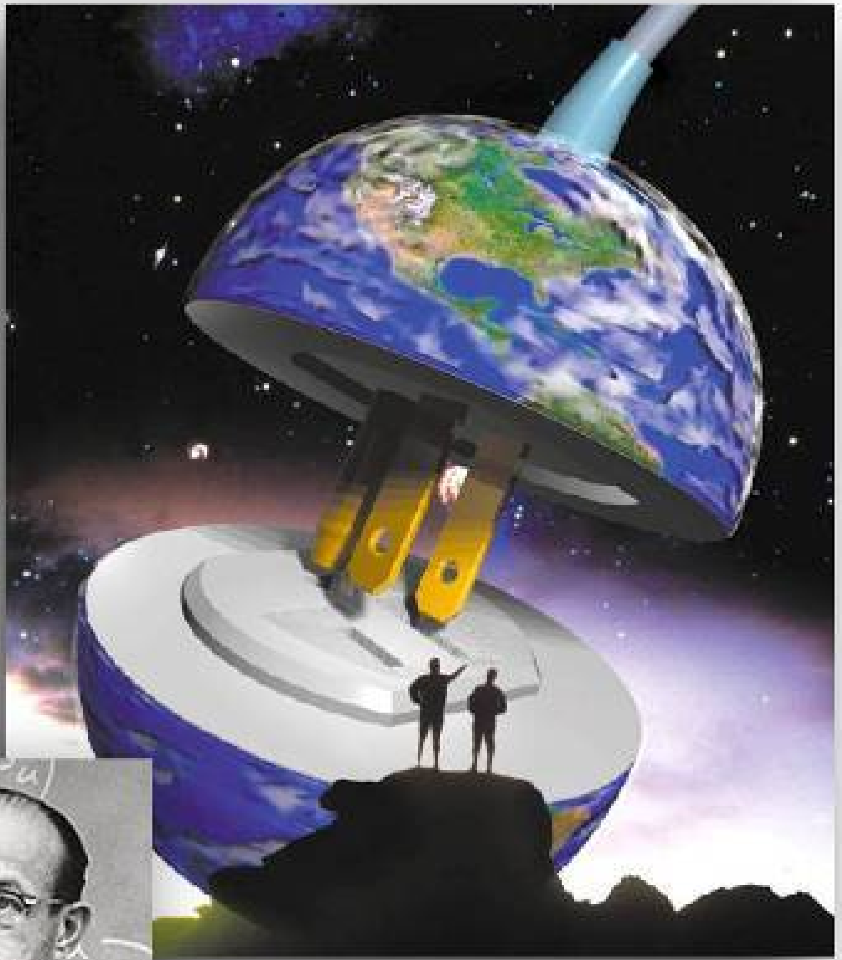
Orlando, FL
July 29th , 2019

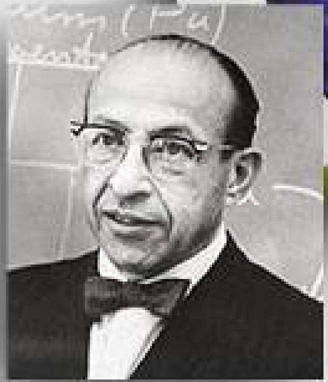
www.epri.com

About us

ELECTRIC POWER RESEARCH INSTITUTE

- **EPRI** is an independent, nonprofit center for public interest energy and environmental research
- Collaborative resource for the electricity sector
- Major offices in Palo Alto, CA; Charlotte, NC; and Knoxville, TN
  - Laboratories in Knoxville, Charlotte, and Lenox, MA





Chauncey Starr
EPRI Founder

www.epri.com

ELECTRIC POWER RESEARCH INSTITUTE

EPRI Members

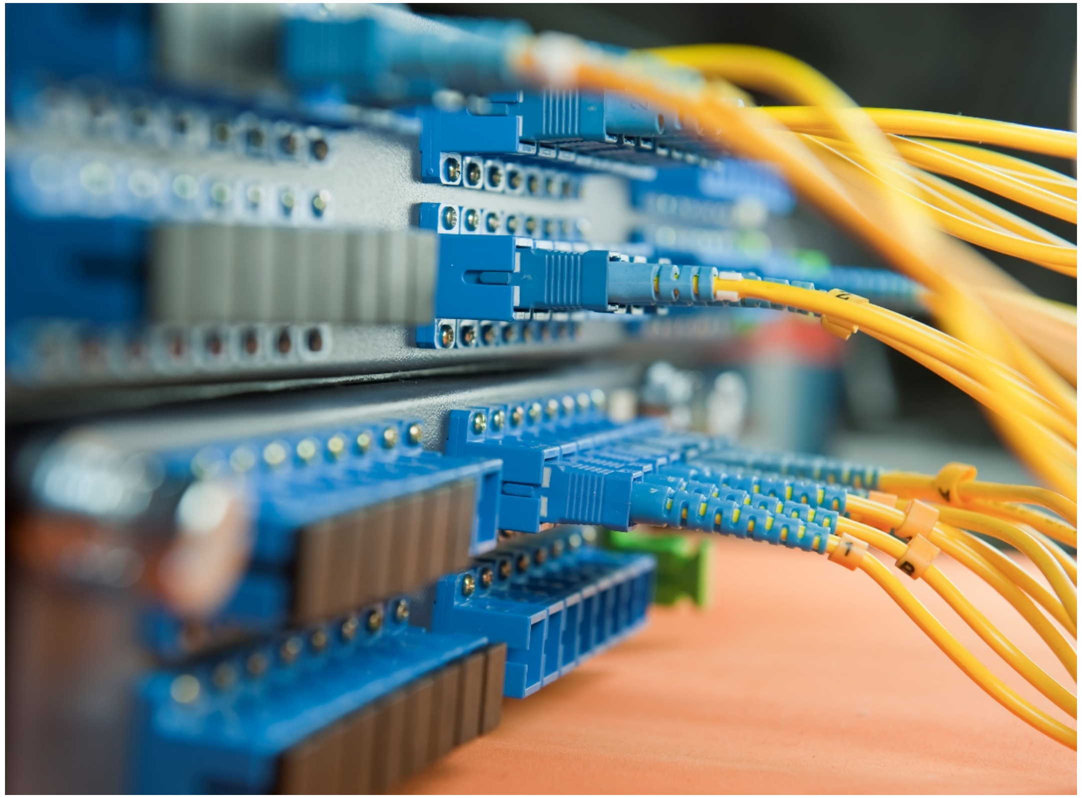
- 450+ participants in more than 30 countries
- EPRI members generate approximately 90% of the electricity in the United States
- International funding – nearly 25% of EPRI’s research, development, and demonstrations

Introduction

Matt Gibson: **Licensed Professional Engineer- (Control Systems), CISSP- (Certified Information Systems Security Professional)**

- EPRI- Technical Executive since Dec. 2013
- Duke/Progress Energy- 1982-2013
  - Fleet Process Systems Architect- 2002- 2013
    - *NUSTART Digital I&C, HFE, and Cyber Security Lead AP1000*
    - *Duke/Progress Legacy Fleet Digital I&C Modernization Architect*
    - *Design and Systems Engineering*
    - *Technology Assessment and Integration*
  - Nuclear IT Manager- Robinson Plant 1994-2002
    - *Business and Digital I&C Systems*
    - *Telecommunications*
    - *Software Quality Assurance(SQA) and Cyber Security*
  - Digital I&C/Computer Technician and Specialist – 1982-1994
    - *System Development and Maintenance*

Digital Convergence



All these instruments

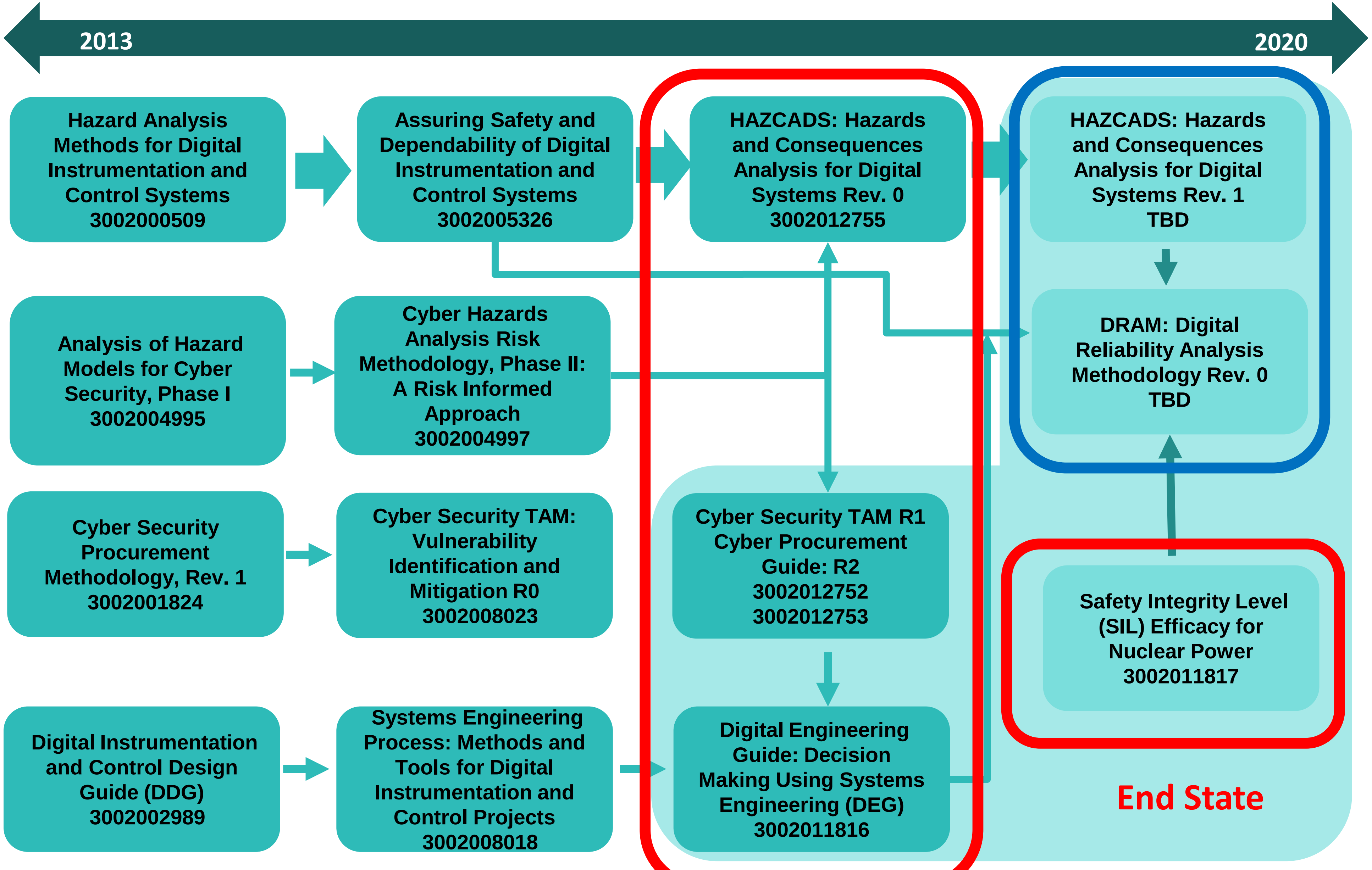
Are now on ONE yellow wire

EPRI's Digital Framework Elements

EPRI has developed a ***high-quality engineering process***, utilizing modern methods and international standards used in other safety related industries.

- **Element 1- Utilize Industry Standards:** Use the same supply chain and structures that non-nuclear safety related industries use (IEC-61508/61511). This leverages the economies-of-scale achieved in other industries.
- **Element 2 - Use of Systems Engineering:** Use of a modern, high performance, single engineering process that leverages systems engineering in the transition to team-based engineering for conception, design, and implementation.
- **Element 3 - Risk Informed Engineering:** Making effective engineering decisions via hazards and risk analysis to integrate all engineering topics (such as cyber security and SCCF) into a single engineering process.

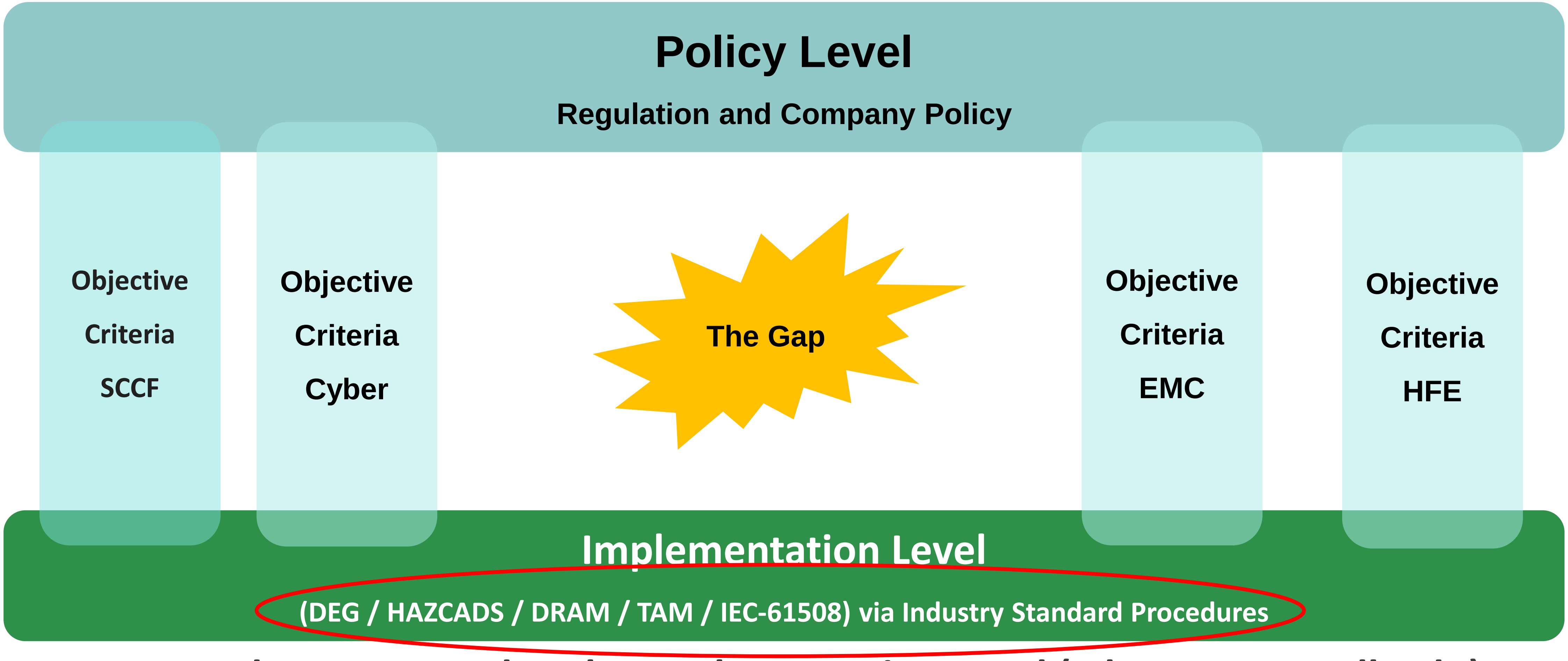
Development History of Integrated Digital Engineering



The Integrated Digital Systems Engineering Framework was developed over a period of approx. 7 years and is nearing completion.

This Framework provides a comprehensive implementation level methodology that supports rapid engineering decision making and the efficient commoditization of I&C

Policy Level vs. Implementation Level Activities



EPRI Products are Used at the Implementation Level (what you actually do)

Objective Criteria provides the Policy to Implementation connector and can be formatted like a safety case argument

Integrated Digital Systems Engineering Framework

- Architecture
- Hazard Analysis (STPA/FTA) – SPV/CCF
- Requirements Engineering
- Procurement
- Human Factors Engineering (HFE)
- Cyber Security
- Data Communications
- Plant Integration
- Testing
- Configuration Management
- Life Cycle Management

EPRI Digital Engineering Guide (DEG)

Systems Engineering Based

Risk Informed

Use of International Industrial Standards

Systems Engineering Based

- ISO/IEEE/IEC - 15288 /12207/15289

Safety reliability and risk framework

- IEC-61508/61511

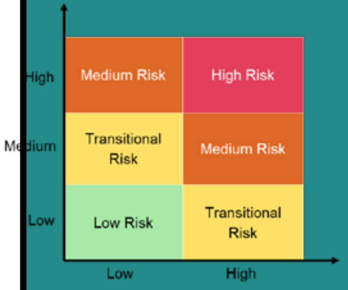
Industry Standard Engineering Process

Optimized Digital Engineering Organization

The EPRI Digital Systems Engineering Framework

DEG

Chapter 1 >3



HAZCADS

Risk-Enabled Digital Hazards Identification and Mitigation

- STPA/FTA integration

DRAM

Digital Reliability Analysis Method

Causal Factors

- Systematic
- Random
- Environmental

TAM

Cyber Security Technical Assessment Methodology

- Design Phase
- In-Situ
- Supply Chain

HFE

Human Factors Engineering

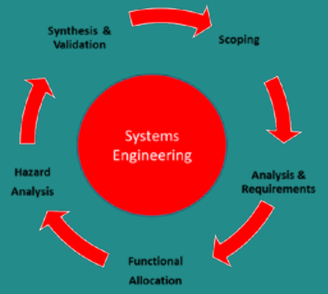
- HFE Guide

EMI/RFI

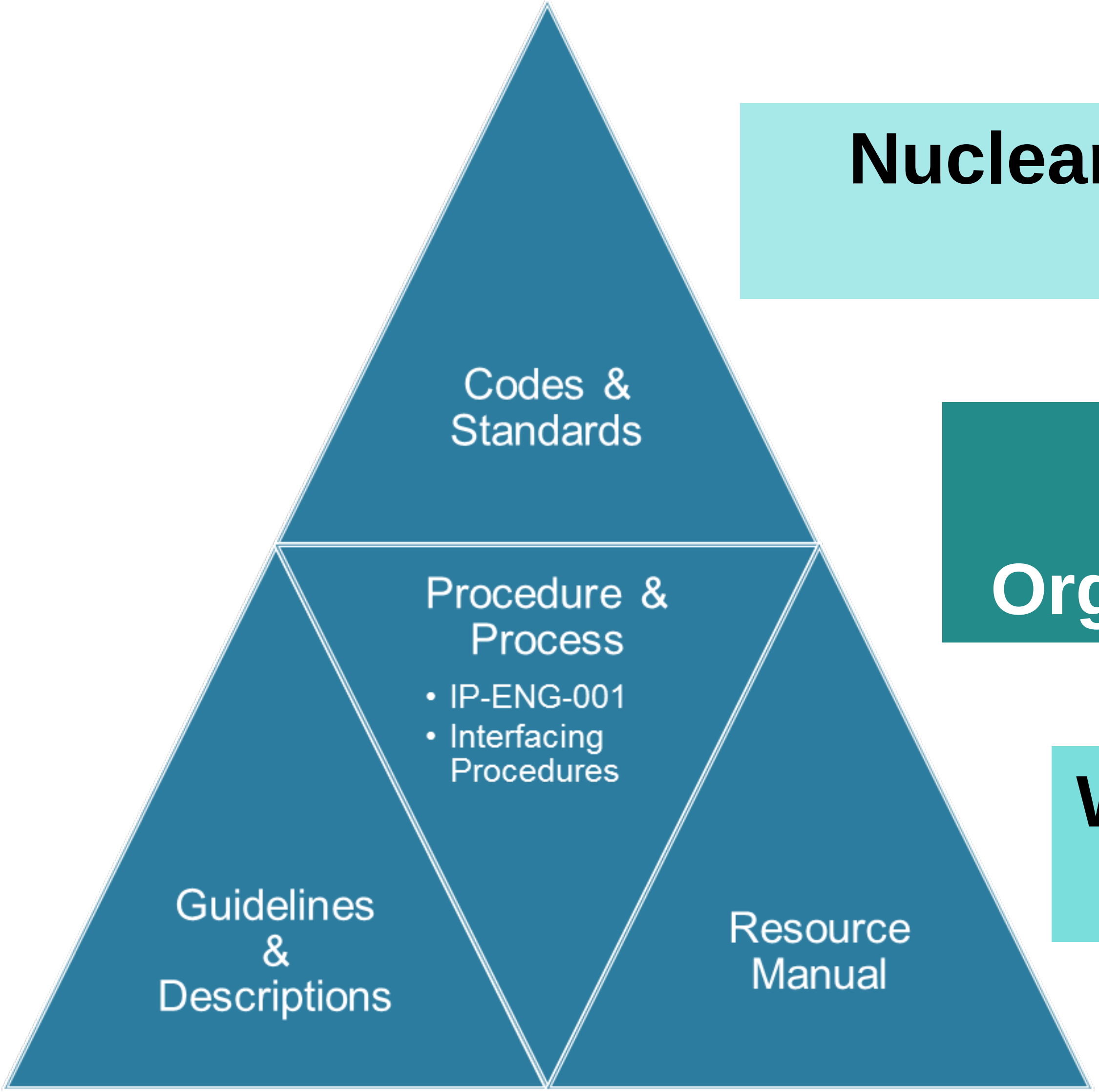
EMI Guides

. . .

Chapter 4- Systems Engineering



Standard Design Process Architecture



Nuclear Leadership wants a return to "Skill Of Craft"

Topical Consolidation (DEG)

Organizational/Technology Alignment

Workforce Developmental and Training Will Take Center Stage

Digital Engineering Efficiency Improvement Goals

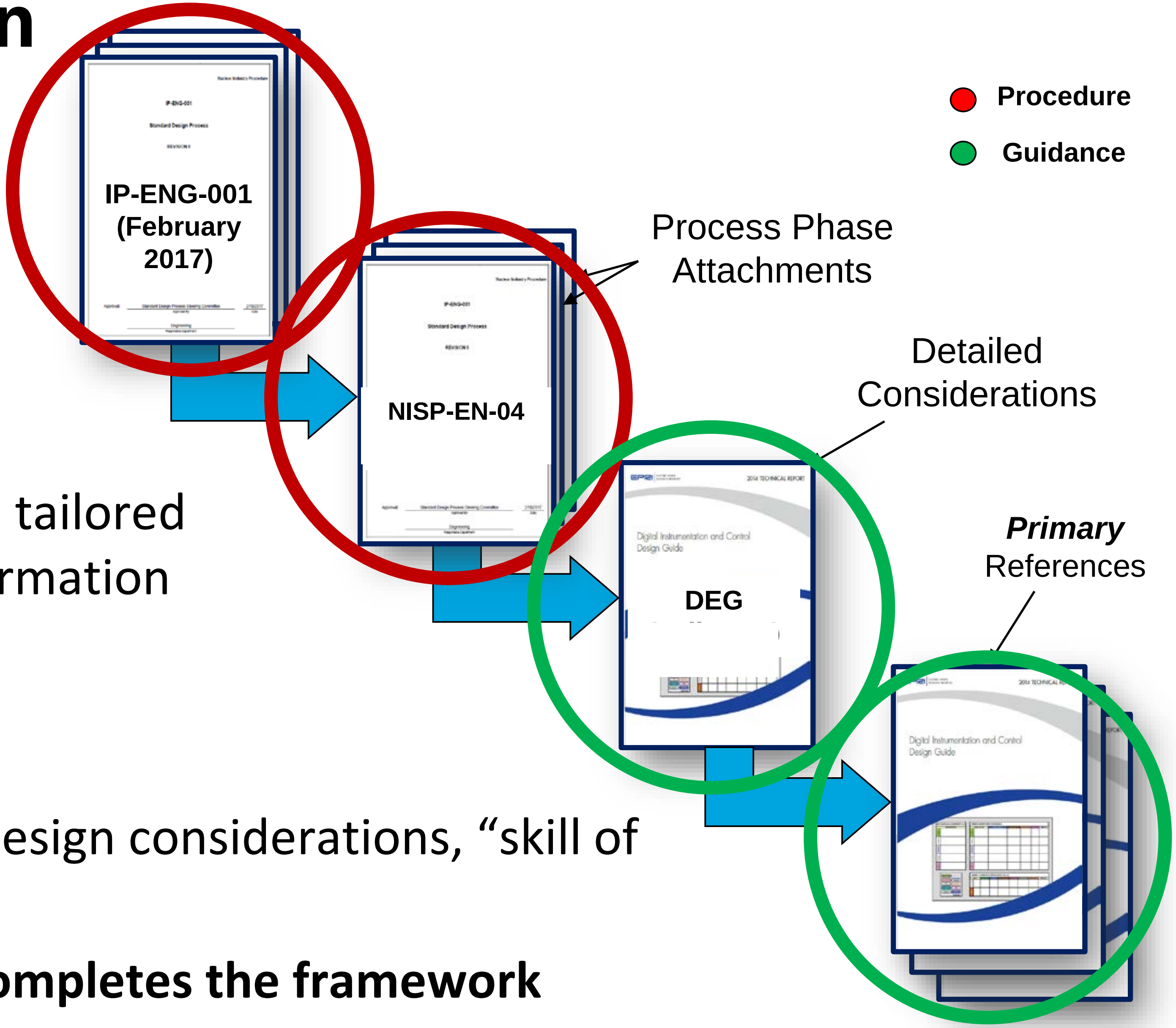
- Efficiency Improvement # 1
  - Use a graded approach to drive elimination of unnecessary work. Do the right suite of activities to achieve design goals and produce the most efficient documentation set. This speeds up the design and implementation process for digital technology and dramatically reduces cost and risk.
- Efficiency Improvement # 2
  - Promote the use of the Systems Engineering process and associated methods and tools to gain efficiencies over traditional system development lifecycle models. One organized process drives rapid and effective results.
  - Integrate hardware and software workflows to eliminate unnecessary multi-process overhead.
- Efficiency Improvement # 3
  - Enable Technical Staff to perform routine "system administrator" activities (e.g., periodic security patches to operating systems, updates of virus definition files) using procedures rather than Modification Changes via pre-bounded plant change activities.
  - Facilitate future replacement of "commodity" digital hardware (e.g., monitors, routers, servers, switches, etc.) as equivalent items using pre-bounded bases.

New Process

- The NISP and DEG provides a robust and efficient process for the design, implementation and lifecycle management of digital systems and components
- Experienced practitioners currently follow much of the process without realizing it
- Even though this is an extension of the Standard Design Process, the NISP/DEG was deliberately constructed around well vetted process that have been used in other industries for decades
  - Systems Engineering – An efficient and iterative process to develop and refine modifications for high performance and reliability
  - Risk informed selection of deliverables based on configurability, risk and consequence – moving industry away from checklists and artifact production to true engineering
  - **Integration of cyber security** with standardized assessment process
  - Fully integrated “cradle-to-grave approach”

Industry Implementation

- IP-ENG-001 (SDP)- Main Procedure
- NISP-EN-04 is the Digital Specific Addendum to the SDP under the same mandatory Efficiency Bulletin (EB)



- Same process phases as IP-ENG-001, tailored with DEG-specific supplemental information
- Provides the user with “what to do”

- DEG provides detailed guidance on design considerations, “skill of the craft,” and primary references
- **Digital Training and Tech Transfer completes the framework**
- **Implementation by 2021**

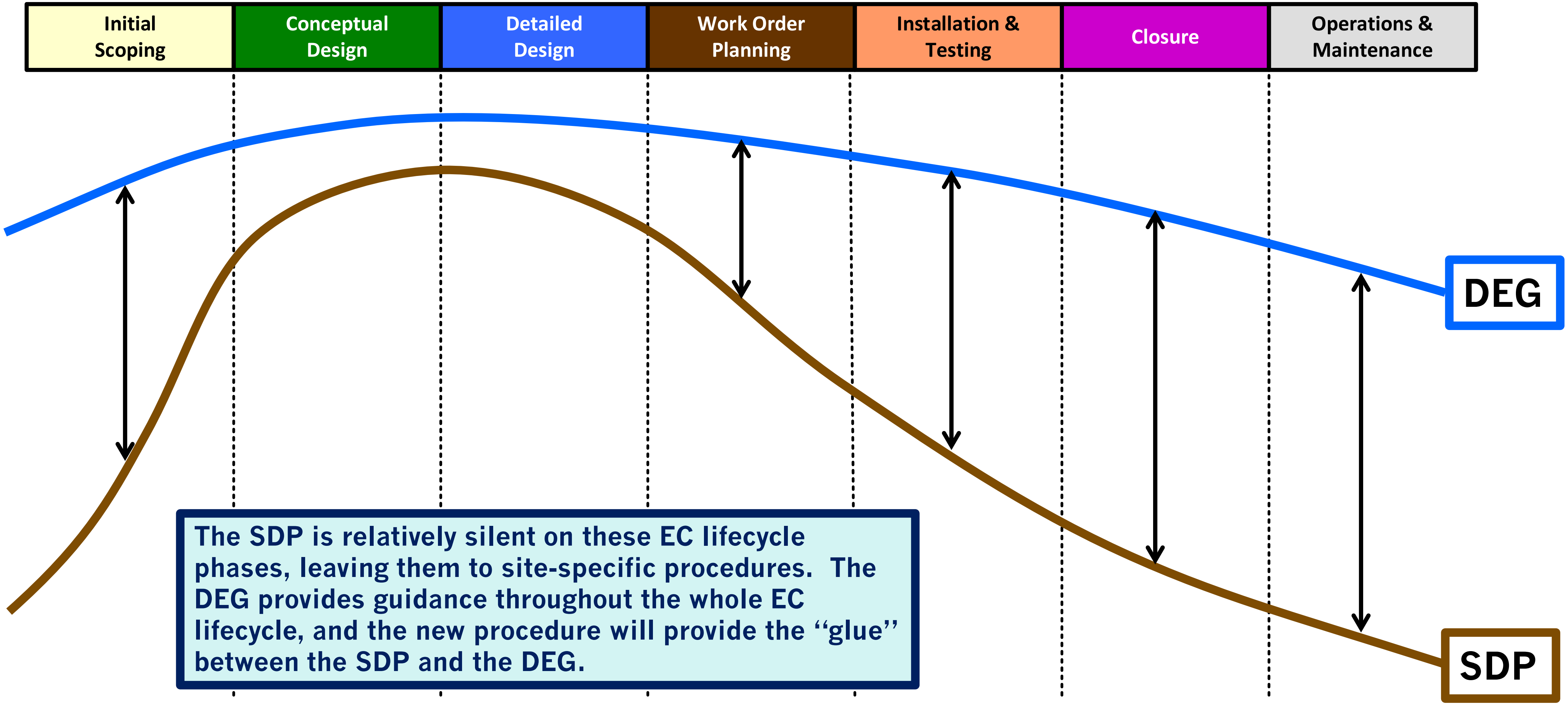
Application

- The NISP/DEG is to be used on all digital modifications – from the simple replacement of a control room chart recorder to a complete replacement of the Reactor Protection System
- The NISP/DEG provides a graded approach based on component/system configurability and consequences of failure
- Examples of typical digital changes where the NISP/DEG will be used:
  – Simple indicator / transmitter /chart recorder replacement
  – Turbine / Feedwater controls upgrades
  – Reactor Protection/Engineered Safety Features
  – Protective relaying – safety and non-safety
  – Distributed control system platform installations
  – Process Computer Replacement

Digital Engineering Guide(DEG) and NISP-EN-04

- NISP-EN-04 describes what to do as part of the SDP > Maps to DEG
- Digital Engineering Guide – Activity based
  - Describes how to do as a Desktop Guide – Maps to additional guidance
- Systems Engineering (Chapter 4) drives architecture determination and design tradeoffs.
- Topical Areas drive technically effective practices (Chapter 5 thru 12)
- Optimized by:
  - Configurability
  - Consequence
  - Technical Scope (DEG Topics)
  - Documentation Value

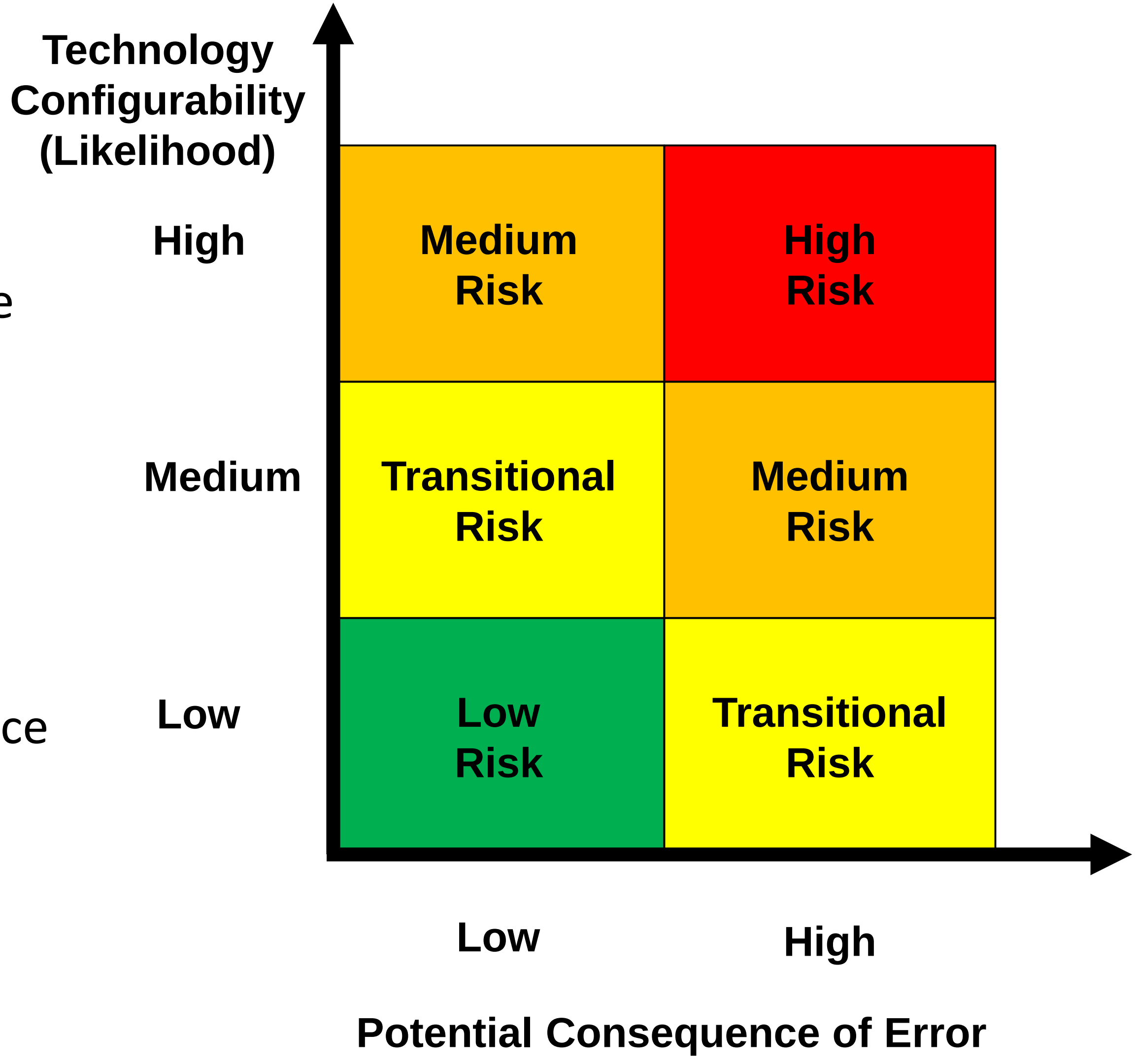
Relative Depths of SDP and DEG Guidance



The SDP is relatively silent on these EC lifecycle phases, leaving them to site-specific procedures. The DEG provides guidance throughout the whole EC lifecycle, and the new procedure will provide the "glue" between the SDP and the DEG.

DEG Graded Approach
Section 1 > 3

- **The DEG is Activity Based**
- Activities are applicable as a function of technology configurability (first) and the potential consequence of error (second, for some activities)
- If Applicable then…
  - Risks Drives level of Activity Rigor and Documentation
  - Rigor is defined as assurance methods that reduce the likelihood of error
  - Some activities may be completed <u>without documentation</u>



Graded Approach

- **Step 1: Configurability Screen**
  - **Low** (A Few Settings)
  - **Medium** (Wide Range of Settable Parameters)
  - **High** (Custom Application Software)

For plant modifications involving digital equipment, the likelihood of error correlates to the degree to which the equipment can be configured by, or on behalf of, the plant owner/operator. In general, the degree of configurability determines which digital engineering activities are performed (i.e., the greater the configurability, the more activities are required).
Equipment configurability is categorized as "low", "medium", or "high" in accordance with the criteria in NISP-EN-04 Attachment 7.

DELIVERING THE NUCLEAR PROMISE / nuclear matters	Nuclear Industry Standard Process - Engineering	NISP-EN-04
	Standard Digital Engineering Process	Revision 0
		Page 52 of 112

ATTACHMENT 7
Page 1 of 2

Configurability Grading Criteria

[Note: When applying these criteria, focus on capabilities the technology has at the application level, not the product development level. For example, most digital equipment is high configurability from the product developer's perspective, but it may only be medium (or even low) configurability from the end user's perspective, depending on its capabilities at the application level.]

Digital equipment shall be classified as "high configurability" if one or more of the following criteria are satisfied:

- Digital equipment applications are developed by or for the end user via a Full Variability Language (FVL) and/or a Limited Variability Language (LVL). (See EPRI DEG Section 3.2 for discussion of FVL and LVL.)
- The digital equipment is a collection of module types that can be interconnected in a physical architecture that is synthesized from system design criteria and an application-specific functional architecture.
- Using engineering tool software, application-specific modules are developed such that the modules can be interconnected in a physical architecture that is synthesized from system design criteria and an application-specific functional architecture.
- Application-specific operator, maintenance, or engineering workstation displays are user configurable via engineering tool software that provides a library of display objects and/or a method for developing display objects, and a method for developing workstation displays.
- Application-specific control functions are user configurable via engineering tool software that provides a function block library and a method for developing control logic. The engineering tool software may also provide a method for developing or programming custom function blocks.

Digital equipment shall be classified as "medium configurability" if none of the "high configurability" criteria are satisfied and one or more of the following criteria are satisfied:

- Digital equipment applications are developed by or for the end user via a Fixed Program Language (FPL). (See EPRI DEG Section 3.4 for discussion of FPL.)
- The digital equipment is user configurable by setting one or more parameter values within a range defined by the product vendor. Parameter values are set using the product faceplate and/or a data communications port connected to a mobile device provided with configuration tool software supplied by the product vendor or a third party.
- The digital equipment is user configurable by removing an internal device, assembly, or circuit board and replacing it with a different version.
- The digital equipment is user configurable by loading a different version of firmware via a data communications port connected to a mobile device provided with configuration tool software supplied by a vendor or a third party.

Graded Approach

- **Step 1: Configurability Screen**
  - **Low** (A Few Settings)
  - **Medium** (Wide Range of Settable Parameters)
  - **High** (Custom Application Software)
- **Step 2: Consequence Screen**
  - **High**: Meets Risk and Impact thresholds for High Consequences
  - **Low**: Does not meet High Consequence Criteria

For example, greater intensity may include a greater scope of analysis across all normal and abnormal system operating conditions, and greater rigor may include more formal techniques and documentation. The potential consequences of error are categorized as "low" or "high" in accordance with the criteria in NISP-EN-04 Attachment 8.

DELIVERING THE NUCLEAR PROMISE. nuclear matters:	Nuclear Industry Standard Process - Engineering NISP-EN-04	
	Standard Digital Engineering Process	Revision 0
		Page 54 of 112

ATTACHMENT 8
Page 1 of 1

Consequence Grading Criteria

Digital equipment shall be classified as "high consequence" if it has the potential, via equipment failure, design error related malfunction, or human performance error, to directly (i.e., immediately and without any other concurrent events) result in any of the following unacceptable consequences:

- Reactor scram/trip
- Significant reactor and/or plant electrical power transient of > 20 percent rated power
- Mitigating System Performance Index (MSPI) monitored component failure
- Complete loss of any of the following critical safety functions:
  - Core, reactor coolant system, or spent fuel pool heat removal
  - Containment isolation, temperature, or pressure
  - Reactivity control
  - Vital AC electrical power
- Loss of a Maintenance Rule high-safety-significant or risk-significant function

[Note: The above criteria are adapted from INPO AP-913, Equipment Reliability Process Description, and their meanings in this procedure are intended to match those used in equipment reliability processes. One important difference, however, is that their application in this procedure goes beyond single random hardware failures to also include, for example, malfunctions attributable to software errors (which could potentially occur in multiple instances of similar software) and human performance errors potentially prompted by poor human factors engineering.]

[Note: An MSPI monitored component failure is essentially a component failure in a front-line system needed for maintaining reactor coolant inventory following a loss of coolant accident, for decay heat removal following a reactor trip or loss of main feedwater, for providing emergency AC power following a loss of plant off-site power, or for the cooling functions provided by service water and component cooling water or their direct cooling water equivalents (for the front-line systems).]

Digital equipment shall be classified as "low consequence" if it does not satisfy any of the "high conse

Use these measures to drive the *depth* and *rigor* applied to the activities identified in Step 2

Graded Approach

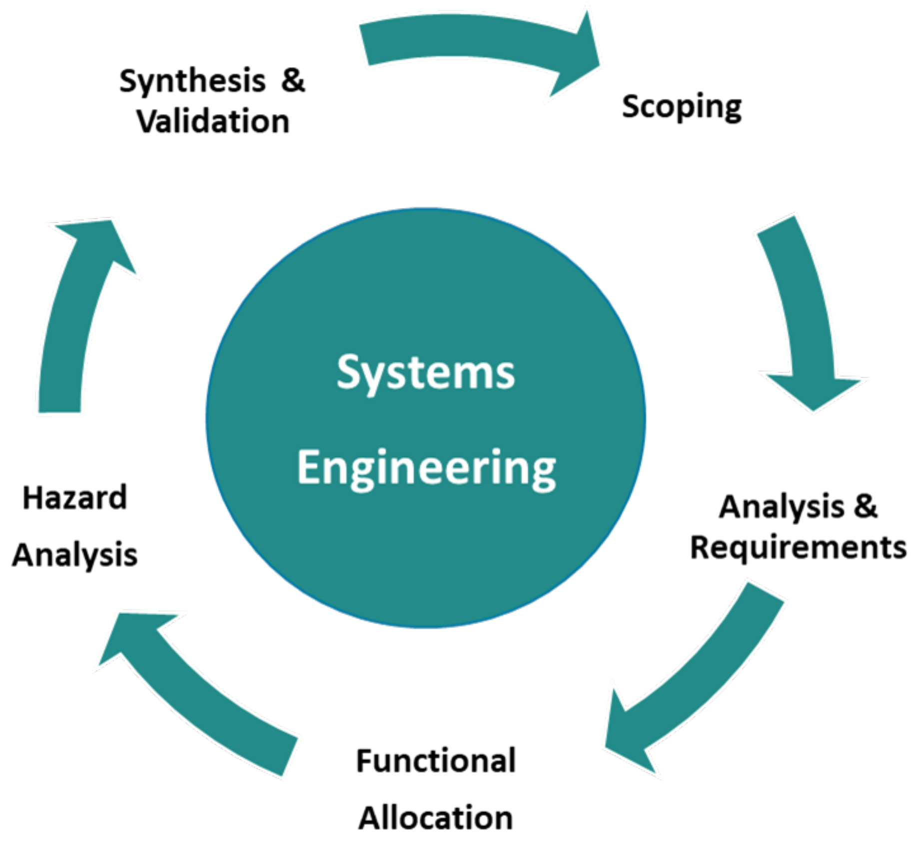
- **Step 1: Configurability Screen**
  - **Low** (A Few Settings)
  - **Medium** (Wide Range of Settable Parameters)
  - **High** (Custom Application Software)
- **Step 2: Consequence Screen**
  - **Low**: Does not meet High Consequence Criteria
  - **High**: Meets Risk and Impact thresholds for High Consequences
- **Step 3: DEG Activity Applicability**
  - Activity Not Applicable – Technology/Function does not exist
  - Activity Conditional – See each DEG Section Guidance
  - Activity Required

For each activity in the DEG, this form provides suggested applicability by configurability category. However, RE/RS have the final decision.

Project Title Here

Digital Engineering Guide Activities	Configurability			Division of Responsibility			Notes
	Low	Med	High	Internal	External	Shared	
3 Overview							
3.4 Graded Approach							
3.4.1 Determine the Configurability of the Applied Technology		R					
3.4.2 Determine Applicability of DEG Activities		R					
3.4.3 Determine the Potential Consequences of Error		R					
3.5 I&C Program Management							
3.5.1 Develop, Apply and Maintain an I&C Strategy		C					
3.5.2 Develop, Apply and Maintain a Knowledge Management Plan		R					
4 Systems Engineering							
4.1 Initial Scoping Phase							
4.1.1 Identify System(s) or Component(s) of Interest		R					
4.1.2 Plan for Discovery, Iterations and Refinements	N	C	R				
4.2 Conceptual/Common Design Phase							
4.2.1 Develop a Division of Responsibility		C					
4.2.2 Develop or Confirm Conceptual/Common Interface Analysis	N	C	R				
4.2.3 Develop Insights from Existing Analyses		C					
4.2.4 Perform Operating Experience Revoew		R					
4.2.5 Identify Bounding Technical Requirements		R					
4.2.6 Elicit Input & Confirmation of Bounding Technical Requirements		R					
4.2.7 Perform or Confirm Requirements Analysis	N	C	R				
4.2.8 Perform or Confirm Functional Analysis and Allocation	N	C	R				
4.2.9 Synthesize or Confirm the Synthesized Conceptual/Common Design		R					
4.2.10 Develop or Confirm Hazard Analysis of Conceptual/Common Design	C	C					
4.2.11 Assess or Confirm Assesment of CCF Susceptibility in the Conceptual/Common Design		C					
4.2.12 Perform or Confirm CCF Coping Analysis (if needed)		C					
4.2.13 Perform or Confirm Conceptual/Common Design Implementation		C					
4.2.13 V&V or Confirm V&V of Concept/Common Requirements, Architecture, Design & Impl.		R					
4.3 Detailed Design Phase							
4.3.1 Develop or Confirm Interface Analysis	N	C	R				
4.3.2 Provide Input, Develop or Confirm Detailed I&C Requirements	N	C	R				
4.3.3 Perform or Confirm Requirements Analysis	N	C	R				
4.3.4 Perform or Confirm Detailed Functional Analysis and Allocation	N	C	R				
4.3.5 Synthesize or Confirm the Synthesized Detailed Design		R					
4.3.6 Develop or Confirm Hazard Analysis of the Detailed Design		C					
4.3.7 Perform or Confirm Detailed Design Implementation		R					
4.3.8 V&V or Confirm V&V of Detailed Requirements, Architecture, Design & Implementation		R					
4.4 Installation Planning Phase							
4.4.1 Perform or Confirm System or Component Integration	C	R					
4.4.2 V&V or Confirm V&V of the Integrated System or Component	C	R					
4.4.3 Support Installation Planning		R					
4.5 Installation/Testing Phase							
4.5.1 Perform, Confirm and/or Support Installation & Commissioning		R					
4.5.2 V&V or Confirm V&V of Installed System or Component		R					
4.6 Closeout Phase							
4.6.1 Perform or Confirm Closeout of the Facility Change		R					
4.7 Operations and Maintenance Phase							
4.7.1 Support System or Component Operations and Maintenance Activities		R					
4.7.2 Perform or Confirm Corrective Actions		R					
4.7.3 Initiate Engineering Changes as Needed		C					
4.7.4 Control Bounded Configuration Changes via Administrative Procedure		C					
4.7.5 Perform or Confirm Disposal of I&C System or Component Elements		R					
5 Procurement							
5.1 Initial Scoping Phase							
5.1.1 Develop or Apply Procurement Strategy		R					
5.2 Conceptual/Common Design Phase							
5.2.1 Determine the Suitability of the Item(s) to be Procured		C					
5.2.2 Specify Vendor Activities and Requirements		C					
5.2.3 Perform Vendor Oversight		C					
5.3 Detailed Design Phase							
5.3.1 Perform Vendor Oversight		C					
5.4 Installation Planning Phase							
5.4.1 Perform Vendor Oversight		C					
5.4.2 Determine the Acceptability of the Procured Items		R					
5.5 Installation/Testing Phase							
5.5.1 Perform Vendor Oversight		C					
5.6 Closeout Phase							
5.7 Operations and Maintenance Phase							
5.7.1 Initiate Vendor Support		C					
5.7.2 Track Vendor Problem Reports		R					
5.7.3 Perform or Confirm Configuration Control		R					

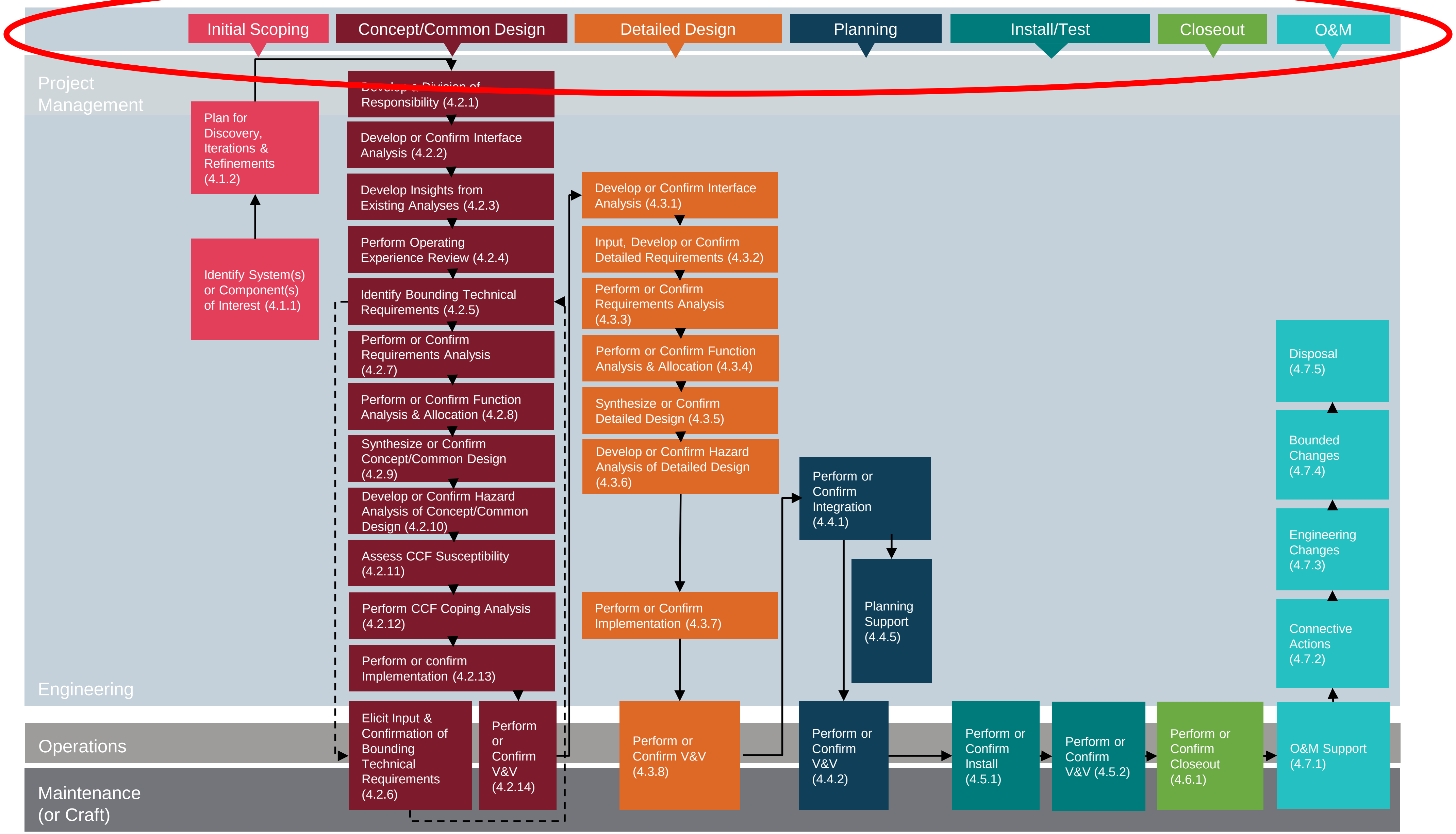
Section 4 – Systems Engineering



- **Phase Based using Perform/Confirm method**
- **Iterates through the SE process for each phase in a non-linear fashion**
- **Includes links to the topical chapters**
- **Iteratively converges on the final synthesized design**
- **Addresses:**
  - Division of Responsibility (DOR)
  - Requirements Development
  - Hazard Analysis (including CCF) and Mitigations
  - Architecture Development
  - Functional Allocation (including Human/System Allocation)
  - Verification and Validation
  - Testing
  - Transition to the O&M Phase

DEG Section 4 > System Engineering Activities

Roles

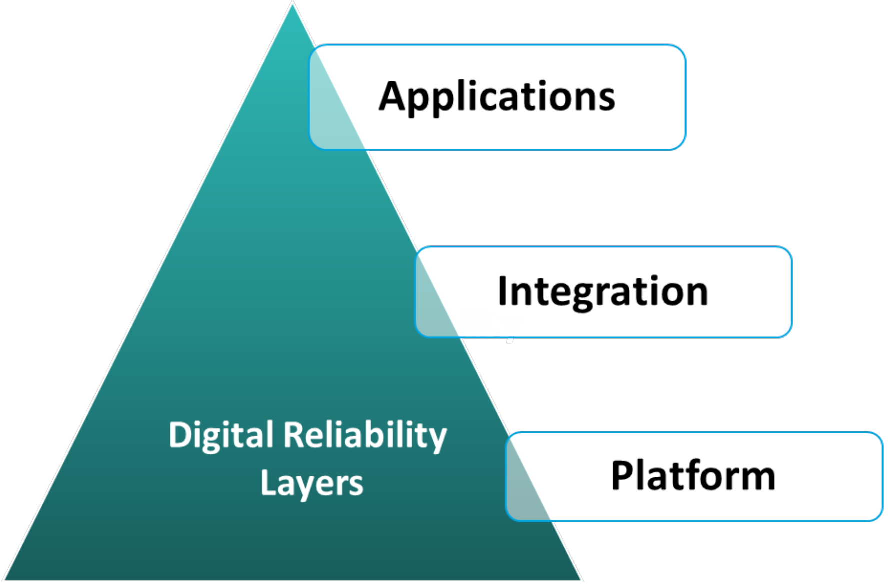


EPRI ELECTRIC POWER RESEARCH INSTITUTE

EPRI Perspective On Digital Reliability

- Recent research using field failure data revealed no platform level Software Common Cause Failures(SCCF) over approx. 2 billion hours of operation for IEC-61508 SIL certified PLC's
- Efficacy of using existing SIL certifications, ***at the platform level***, as surrogates for some existing design and review processes has proven to be effective.

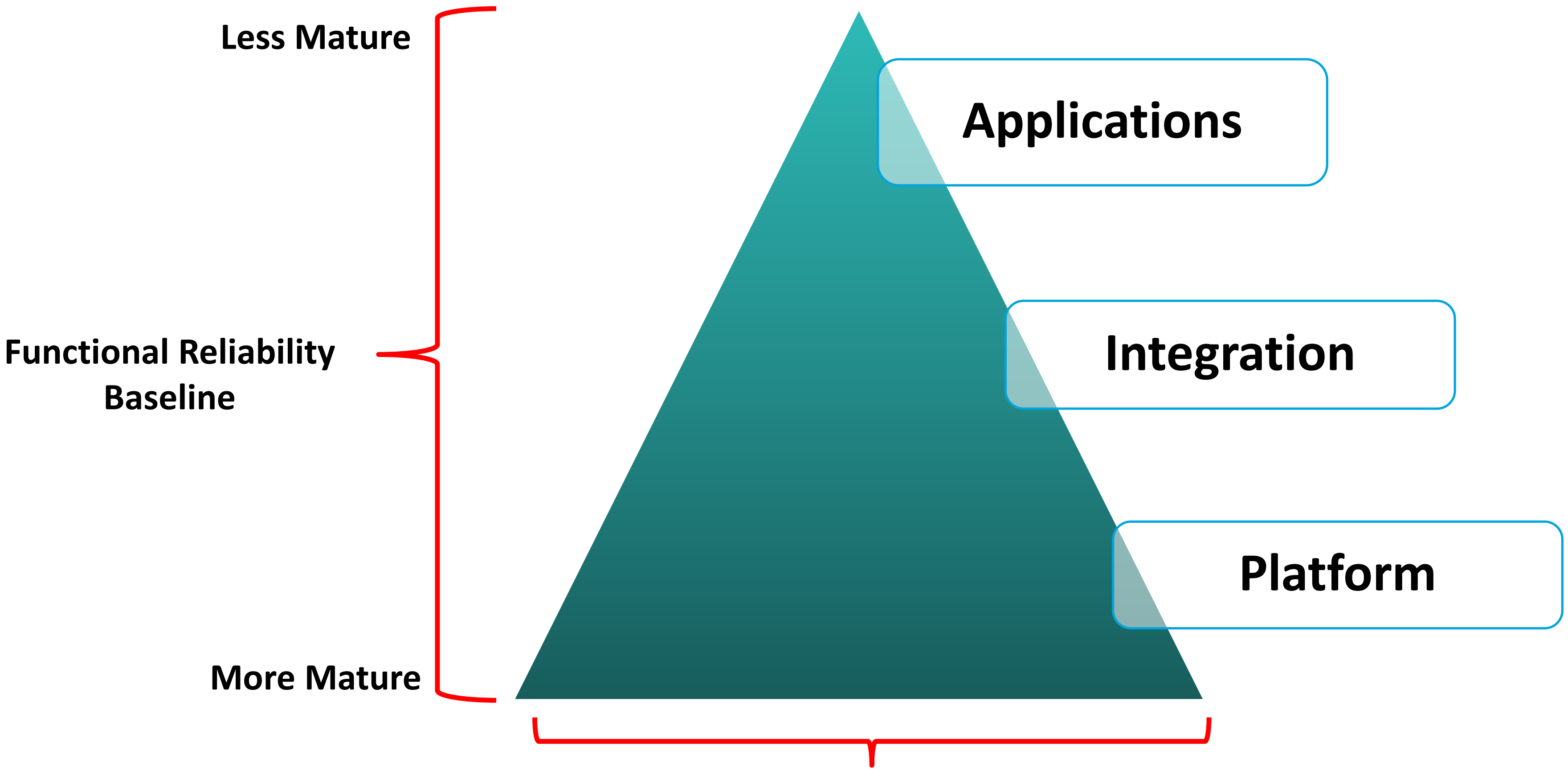
- Additionally, cumulative OE from across the world (Korea, France, China, etc.) indicate that:
  - Safety Related Software is no more problematic than other SCCF contributors.
  - There have been no events where diverse platforms would have been effective in protecting against SCCF.
  - Several events confirmed effectiveness of signal and functional diversity in protecting against SCCF



ELECTRIC POWER RESEARCH INSTITUTE

Reliability Layers

Reliability, especially software reliability, including CCF, should be segmented by *platform, integration, and application*. Then Considered Separately



Production Data and OE Quantity and Quality Dive Maturity and Reliability using IEC-61508/SIL

Three Step Digital Reliability Assessment Methodology (DRAM) Revision 0

Risk-Informed Digital Failure/Error Mode Identification and Mitigation

DRAM Step 1
Characterize the System and Component Interfaces and Identify Control and Data Flow

Identify Failure/Error Type
Identify Failure/Error Mechanisms
DRAS Part 1

This step bounds the problem of reliability assessment by limiting its scoping to the actual system characteristics and the failure/error mechanisms and types at the selected level of composition and decomposition. Addresses random and systematic modes and the identified types

DRAM Step 2
Identify, Score & Allocate Engineered Reliability Control Methods to address **Failure/Error Mechanisms**

DRAS Part 2

This step identifies the reliability control methods available on or via the system under assessment that can mitigate the failure/error modes. Provides a risk-informed approach by scoring the control effectiveness of identified engineered control methods and setting a target level score based on the potential consequences of an failure/error(HAZCADS). It supports allocation of control methods that meet or exceed the effectiveness target level.

Residual Failures/Errors

DRAM Step 3
Mitigate Failure/Error Modes

Administrator/Operator Actions- Shared Controls Relationship Sets
DRAS Part 3

A residual failure/error can occur when engineered controls methods do not meet the effectiveness target level. They are mitigated by scoring and allocating shared reliability control methods until the effectiveness target level is met or exceeded for each failure/error.

Optional
Regulatory Requirements and Compliance Map
RRCM

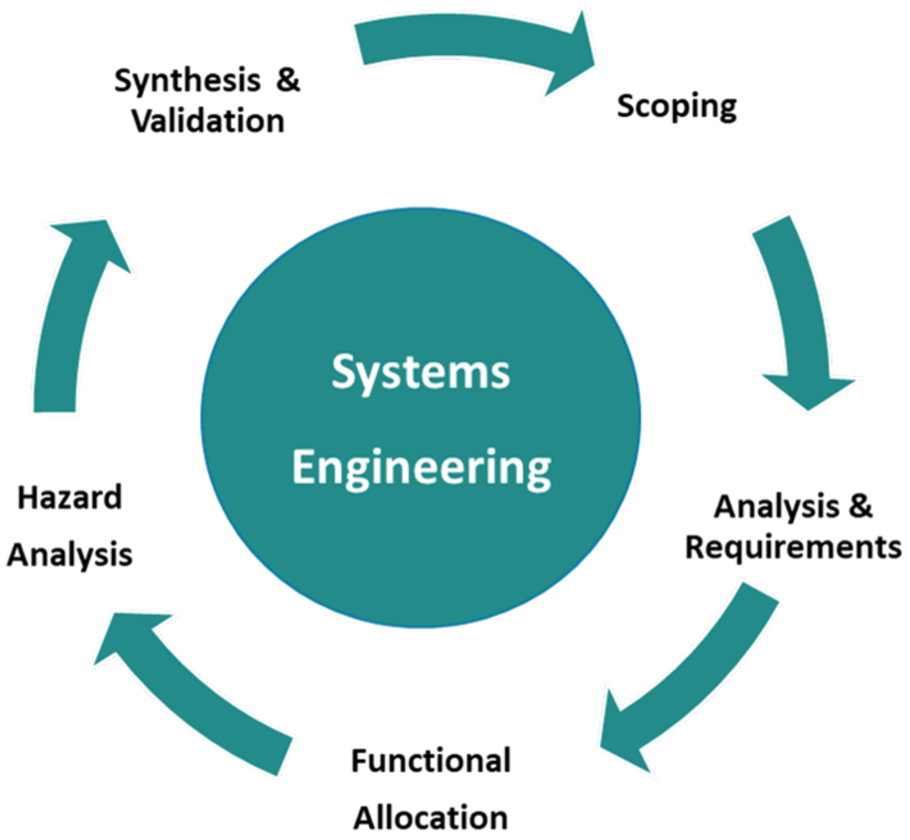
This step can be used to demonstrate compliance to a regional rule or regulation by mapping the reliability control methods allocated via steps 2 and 3 to any applicable regulatory requirements.

The DRAM can be applied to systems and components in a relationship set and gain efficiencies by
1) allowing a higher level system or components to mitigate residual failure/error mechanisms in lower level assets in the same set, or
2) support inheritance of shared control methods for all systems/components in the same set.

Relationship Sets

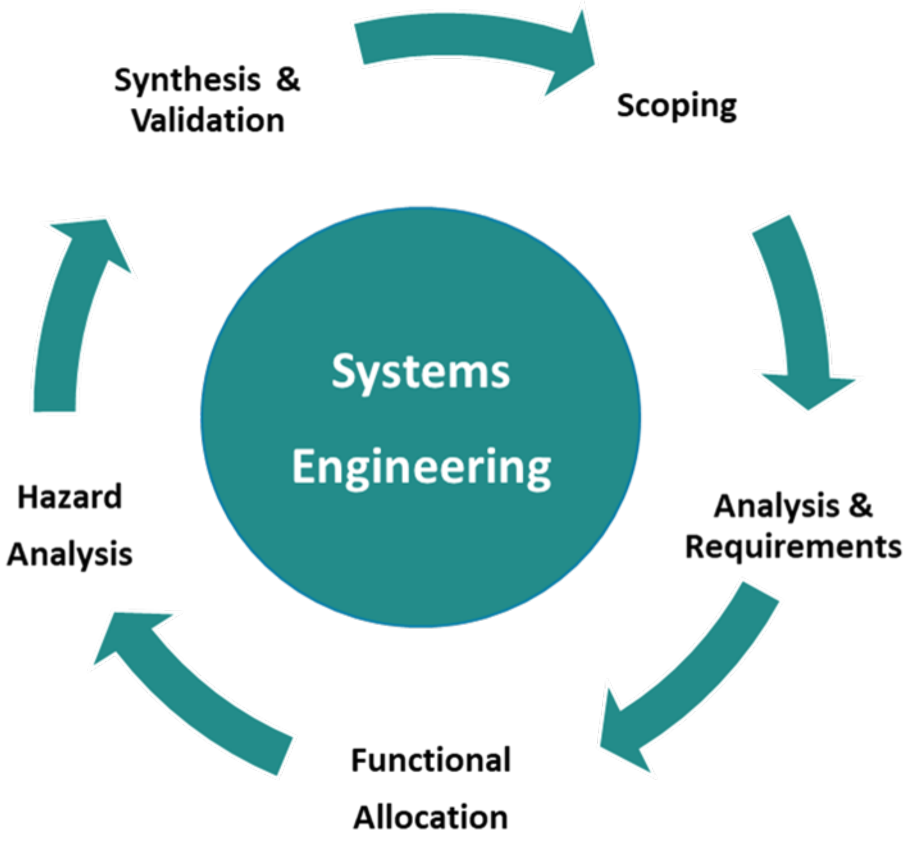
System 1	System 2	System 3
DRAS Part 1	DRAS Part 1	DRAS Part 1
DRAS Part 2	DRAS Part 2	DRAS Part 2
DRAS Part 3		

Section 5- Procurement



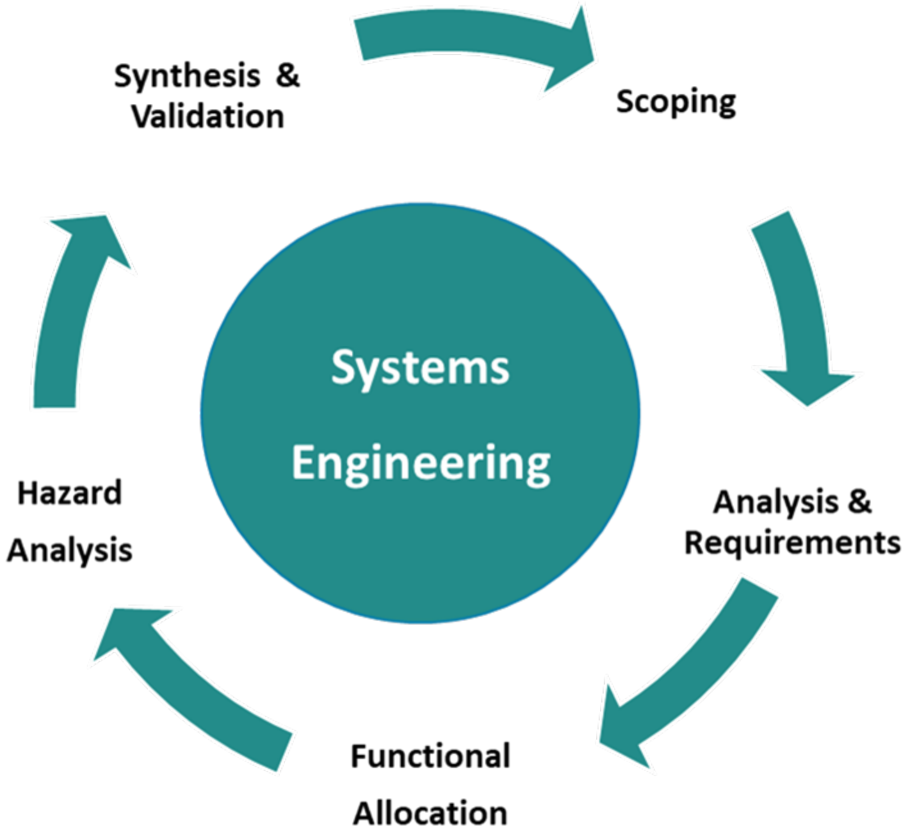
- **Phase Based using Perform/Confirm method**
- **Develops a Procurement Strategy**
- **Synthesizes EPRI Guidance**
- **Addresses:**
  - Procurement Requirements
  - Vendor Oversight
  - Acceptance Criteria
  - Configuration control

Section 6- Human Factors



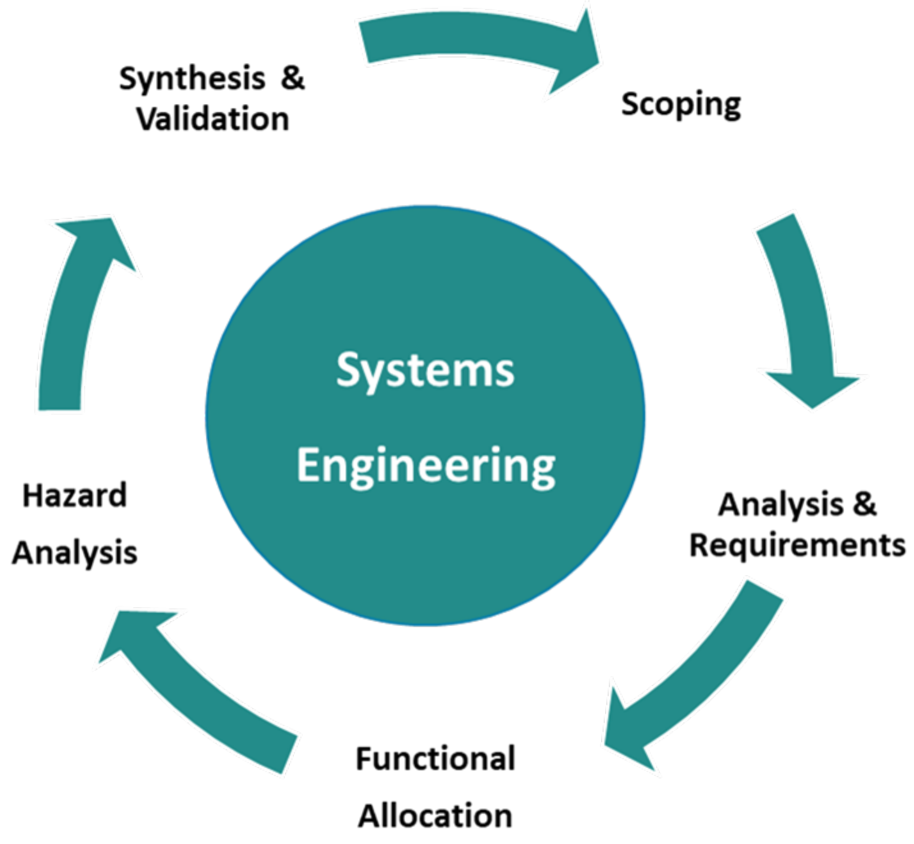
- **Phase Based using Perform/Confirm method**
- **Establishes HFE Methods and Tools/Stakeholder interface**
- **Addresses:**
  - HFE Requirements
  - Task Analysis
  - Functional Allocation (including Human/System Allocation)
  - HSI design
  - Human Action/Error Analysis
  - HFE V&V
  - Monitoring of In-Service Human Performance

Section 7 – Data Communications



- **Phase Based using Perform/Confirm method**
- **Establishes the Data Communications architecture**
- **Addresses:**
  - Data and Control Flow
  - Interface and Protocol Inventory
  - Defensive Measures against Errors
  - Capacity and Performance
  - Allocation and Segmentation
  - Monitoring and Managing Data Communications

Section 8 – Cyber Security

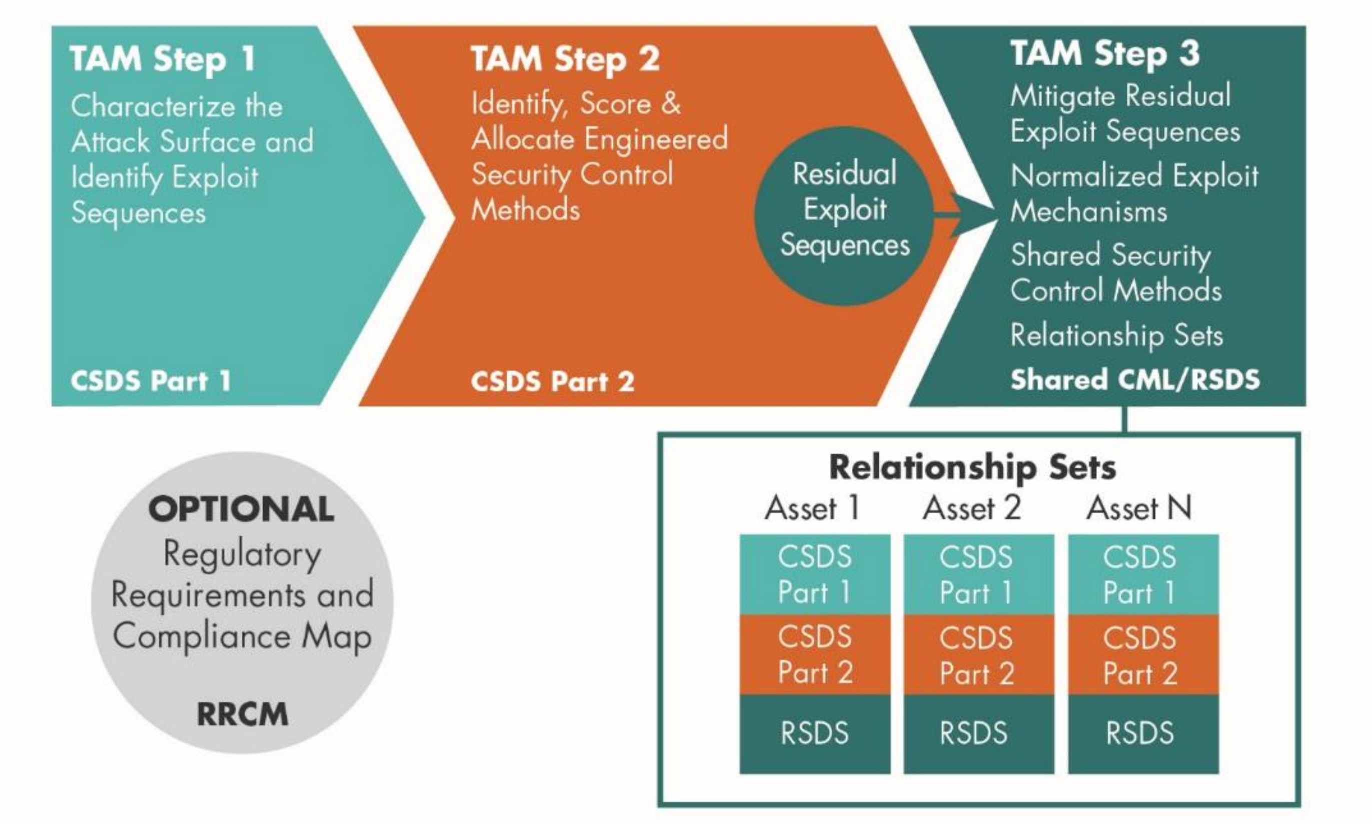


- **Phase Based using Perform/Confirm method**
- **Identifies Affected Digital Components and Systems**
- **Uses EPRI Cyber Security Technical Assessment Methodology (TAM)**
- **Engineering/Cyber integration**
- **Addresses:**
  - Defensive Strategy Considerations
  - Attack Surface Analysis
  - Exploit Sequence Identification
  - Efficient and Balanced Control Method Allocation
    - Protect
    - Detect
    - Respond/Recover

EPRI Cyber Security Technical Assessment Method (TAM)

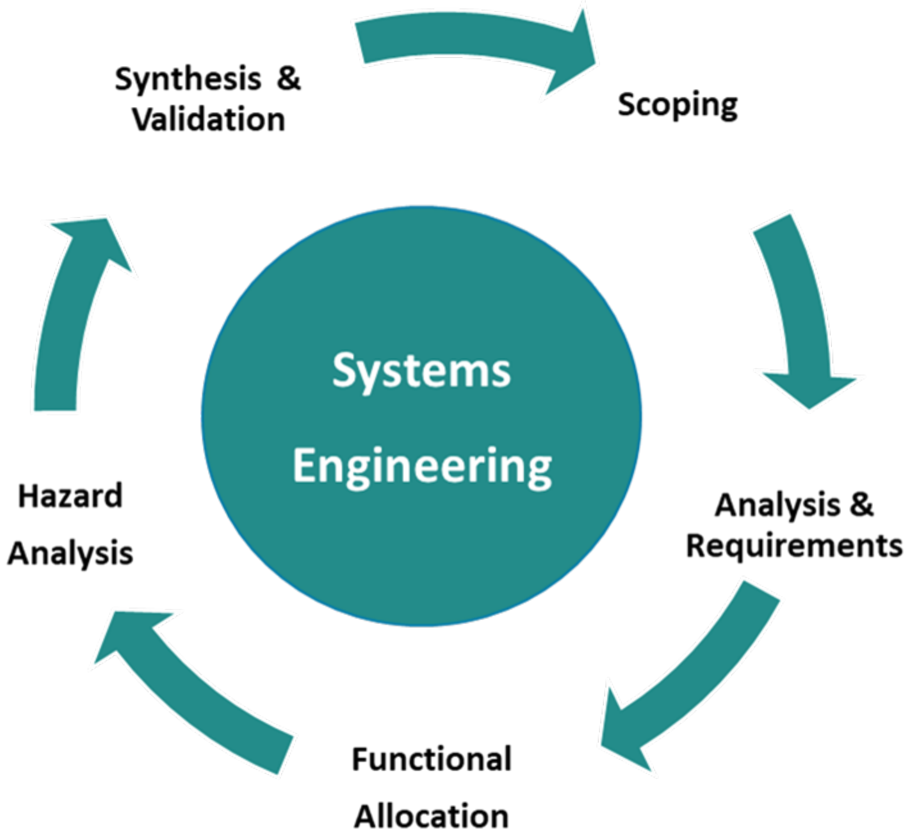
- TAM Early Adopters

Vogtle 3&4 > Barakah (UAE) > NuScale> Exelon >OSISoft



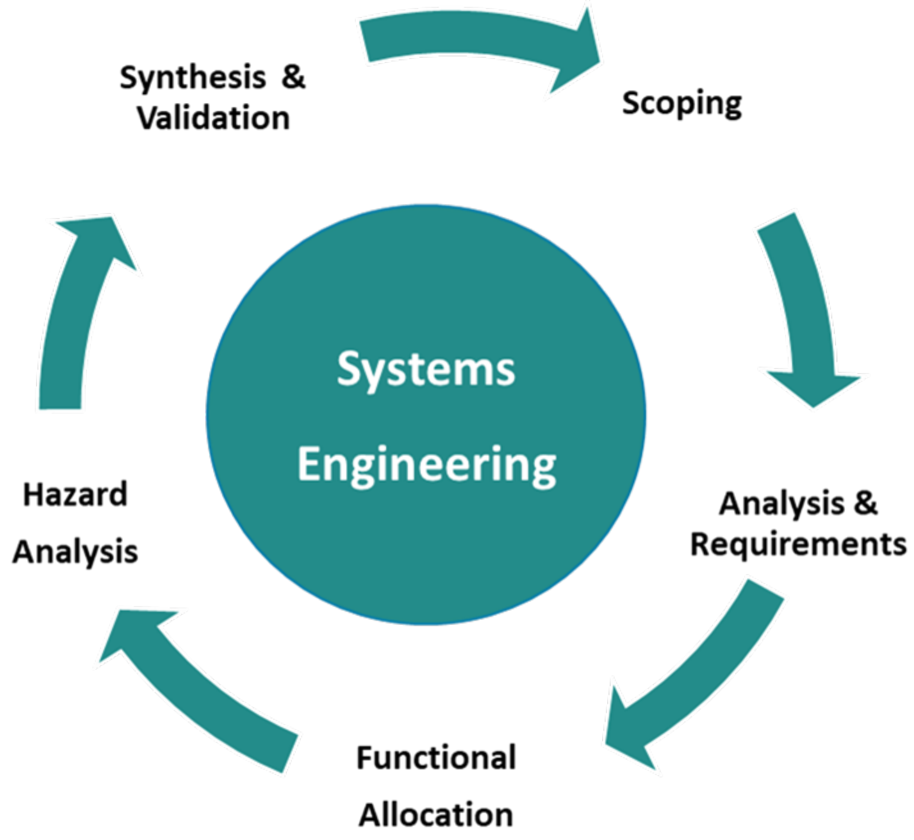
- Revision 1 published Nov 2018
  - Compatible with most existing standards and regulation including IEC 62443
  - Integrated with Supply Chain
  - Designed to integrate into the overall engineering and design processes, including the DEG.
  - Leads the transition to sustainable engineering-based cyber assessment and mitigation methodologies.
  - Standardizes the assessment methodology and documentation

Section 9 – Plant Integration



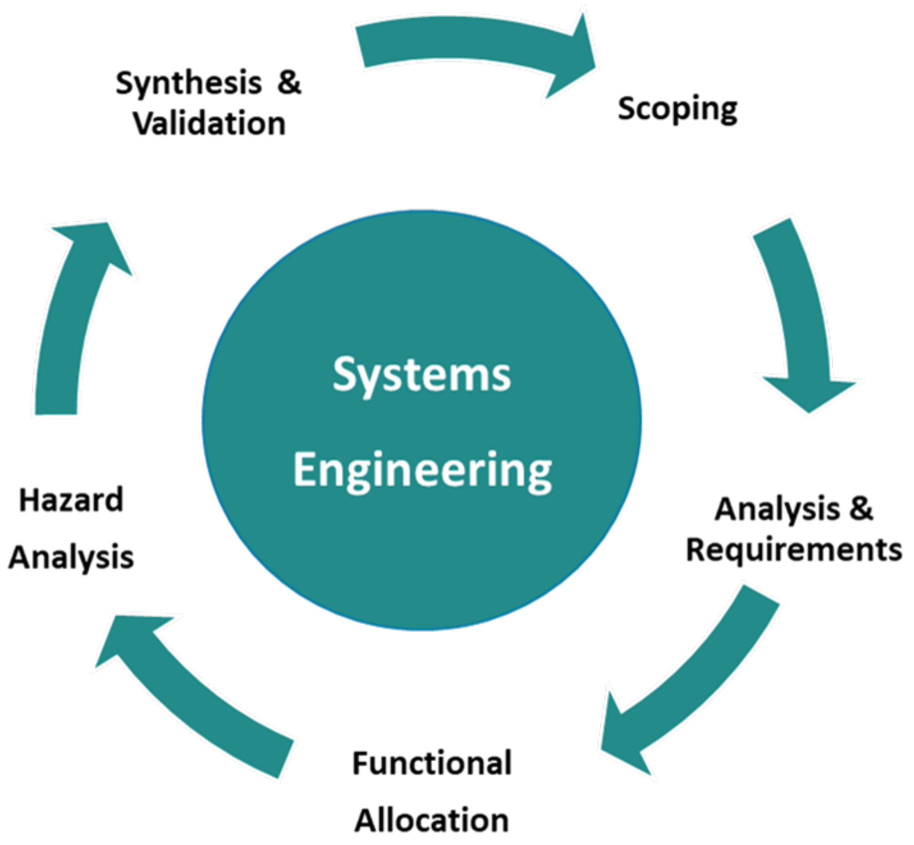
- **Phase Based using Perform/Confirm method**
- **Establishes the Modification Boundary**
- **Addresses:**
  - Overall Plant Interface
  - Electrical Independence
  - Electrical Power Design
  - EMC and Grounding
  - Environmental Compatibility (HVAC, EQ, etc.)
  - Seismic Considerations
  - Uncertainties and Set points
  - Operability and Maintainability
  - Installation and Commissioning

Section 10 – Testing



- **Phase Based using Perform/Confirm method**
- **Identifies Testing Impacts**
- **Develops a Test Strategy**
- **Addresses:**
  - Identification of Test Methods
  - Regression Analysis
  - Component and Integration Testing
  - Post-modification/Commissioning Testing
  - Virtual Commissioning
  - Use of Simulators

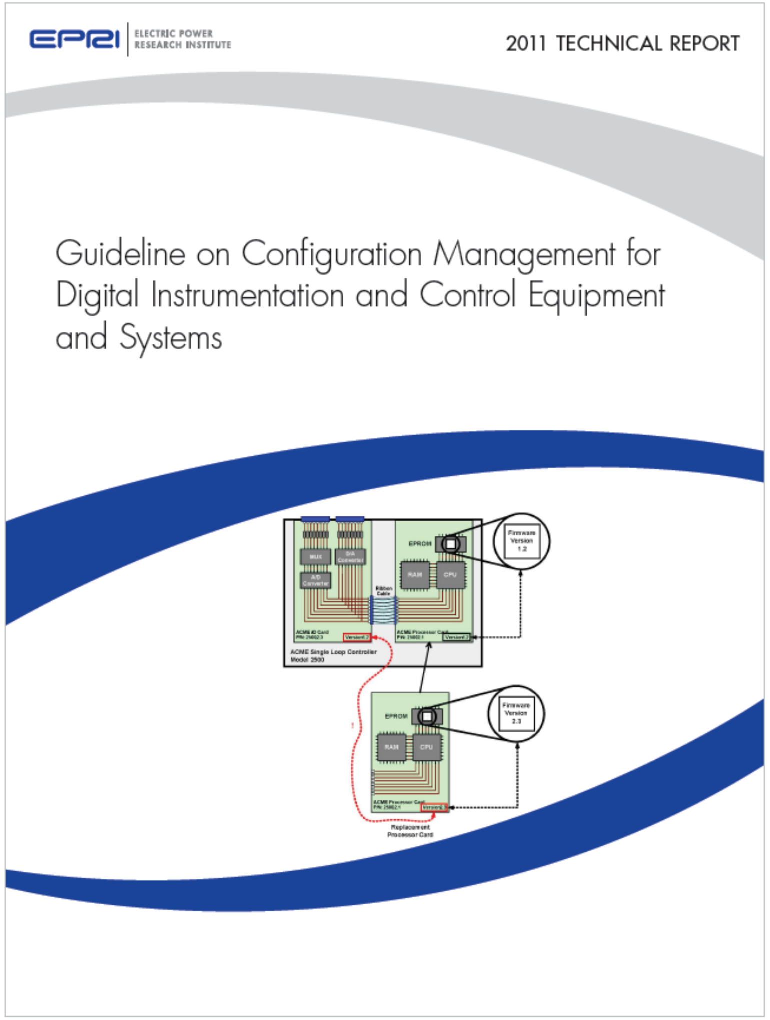
Section 11 – Configuration Management



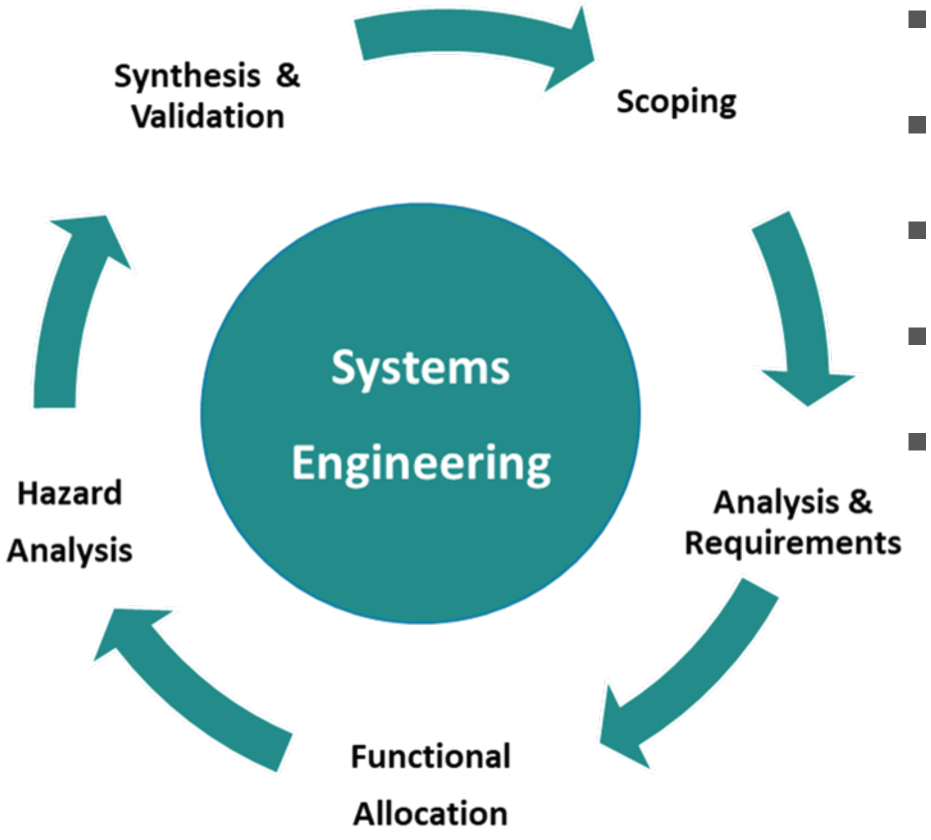
- **Phase Based using Perform/Confirm method**
- **Identifies Affected Configuration Items**
- **Identifies Affected Facility Configuration Information**
- **Identifies and Assess Configuration Management Interfaces**
- **Addresses:**
  - Digital Specific CM items
  - Configuration Control Methods
  - Configuration Status Accounting
  - Configuration Audits
  - Disaster Recovery

Configuration Management (CM)

- *Digital Engineering Guide* – Section 11
- 102299-*Guideline on Configuration Management for Digital Instrumentation and Control Equipment and Systems* (2011)
  - Defines critical CM elements for digital
  - Details CM processes for digital systems
  - Described CM documentation approaches
  - Explains change control methods for digital
- Will be updated and integrated with the DEG and align with international standards.

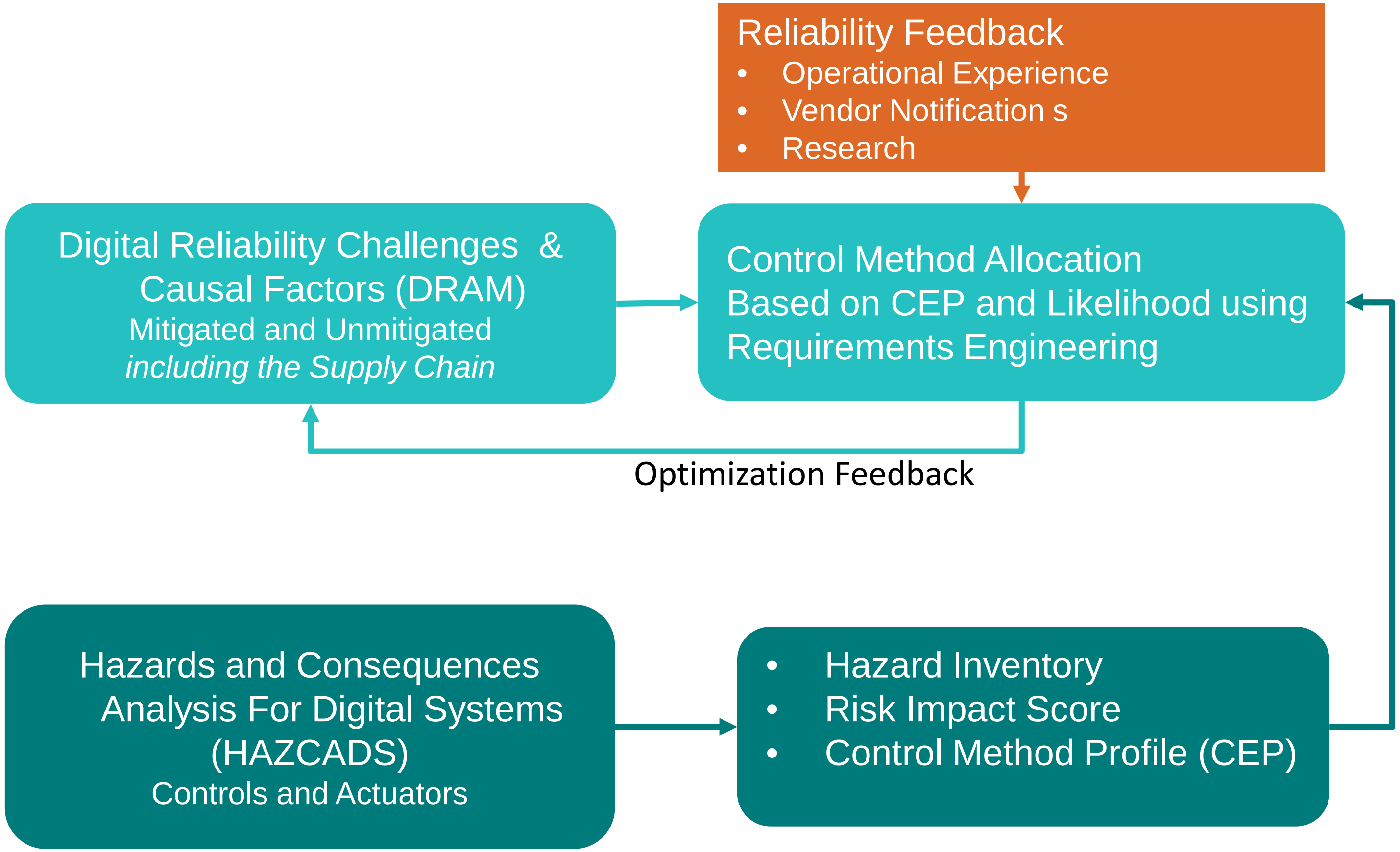


Section 12 – Digital Obsolescence Management



- **Phase Based using Perform/Confirm method**
- **Identifies System Lifecycle Planning Impacts**
- **Identifies Digital System or Component Lifecycle**
- **Assesse Risks Due to Obsolescence**
- **Addresses:**
  – Obsolescence Management Strategies
  – Periodic Lifecycle Management Effectiveness Reviews
  – Refinement of Existing or Ongoing Strategies

EPRI Risk-Informed Digital Reliability Process Model



Hazard Inventory & CEP

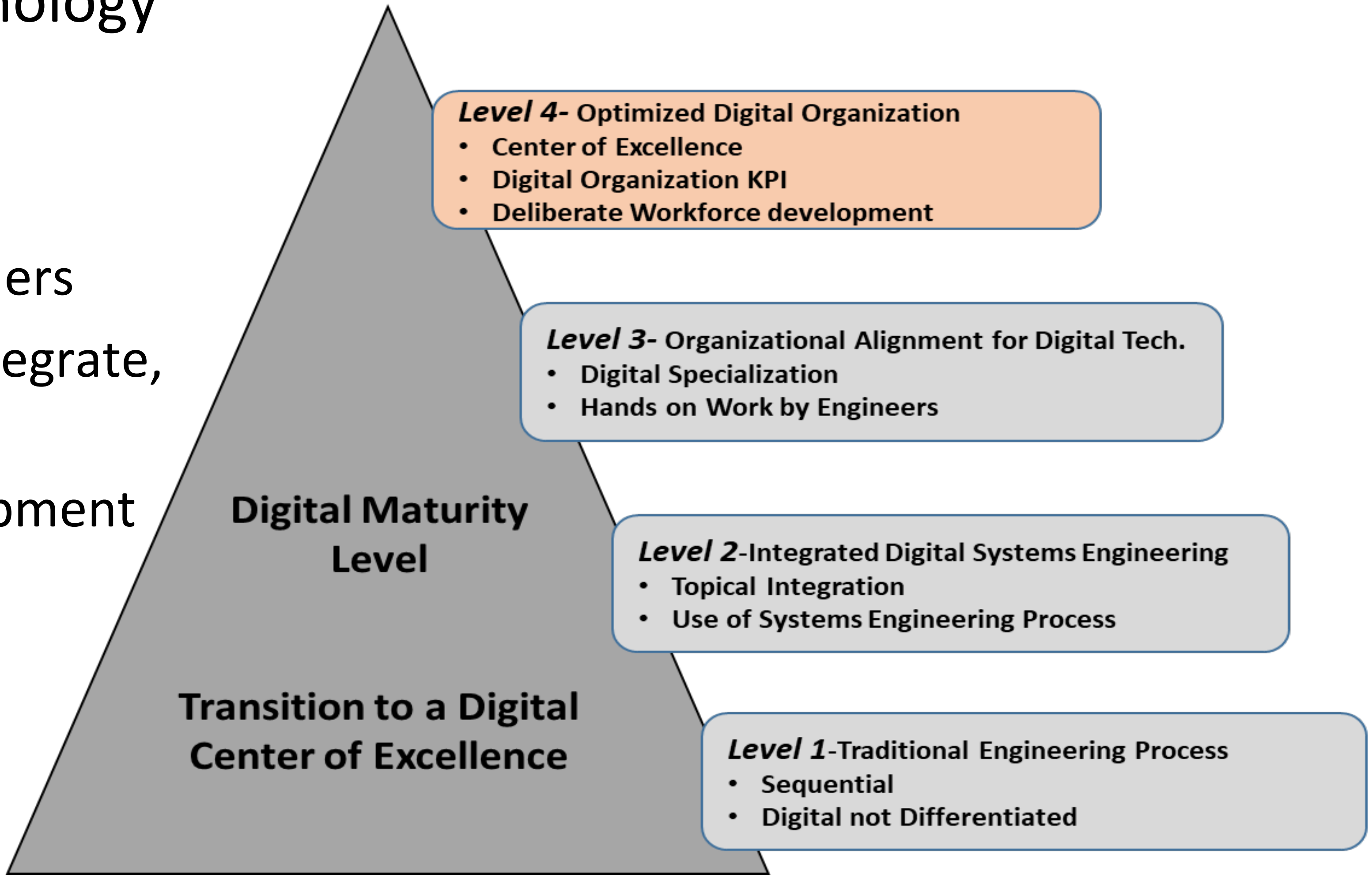
Target Reliability based on analyzed hazards, informed by Feedback sources, can dramatically **REDUCE THE SENSITIVITY** of a nuclear facility to the introduction of digital technologies.

Organizational Maturity

- Transition of I&C to Operational Technology (OT) Model
- Specialization in Digital Technology

  - Integration Centered
  - Transition to Technology Leaders
  - Conceive, Procure, Design, Integrate, Maintain, and Support
  - Deliberate Workforce Development
  - Simulator Integration

Detailed in Attachment B to DEG



Together…Shaping the Future of Electricity