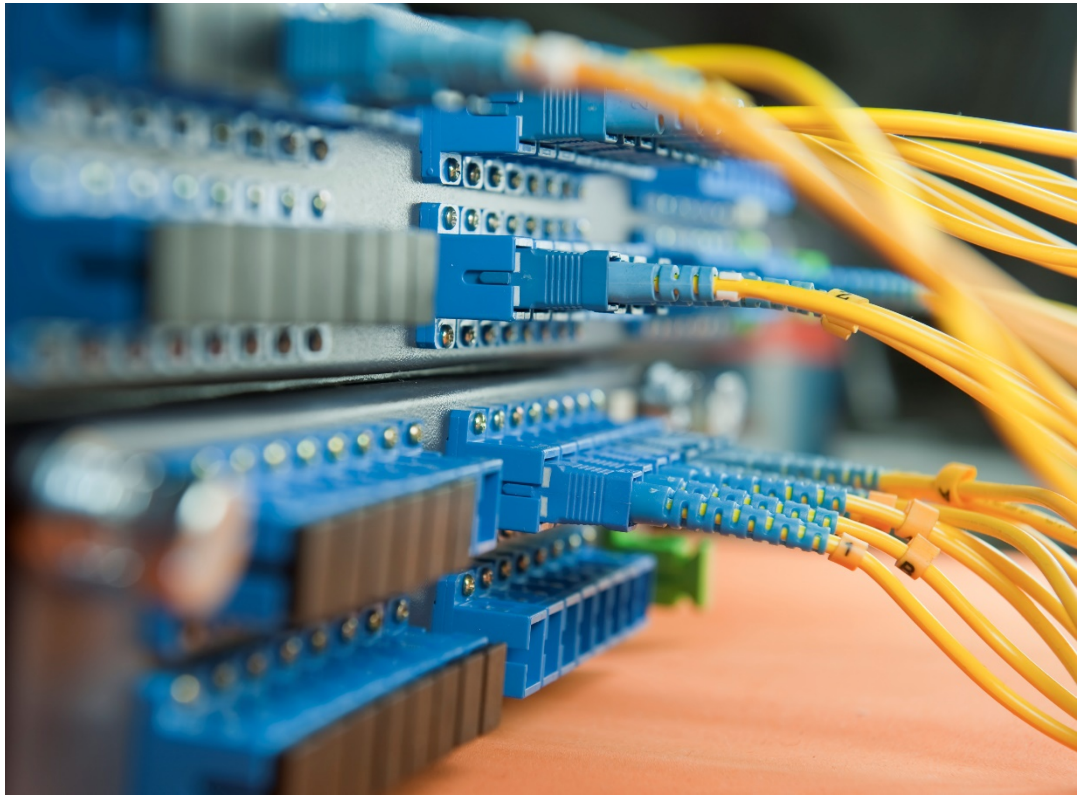
EPRI Integrated Digital Systems Engineering Framework

Overview of the Modular Elements, Architecture, and Workforce Development

Matt Gibson
Technical Executive
Nuclear I&C Program

NRC Public Meeting on NEI 20-07 April 7th, 2021

Digital Convergence



All these instruments ▶ ▶ ▶ Are now on ONE yellow wire

EPRI's Digital Framework Elements

EPRI's ***high-quality engineering process*** uses the same modern methods and international standards used in other safety related industries to reduce implementation cost

Utilize Industry Standards

Use the same proven design and supply chain structures that non-nuclear safety related industries use (IEC-61508/61511). This leverages the economies-of-scale achieved in other industries.

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.

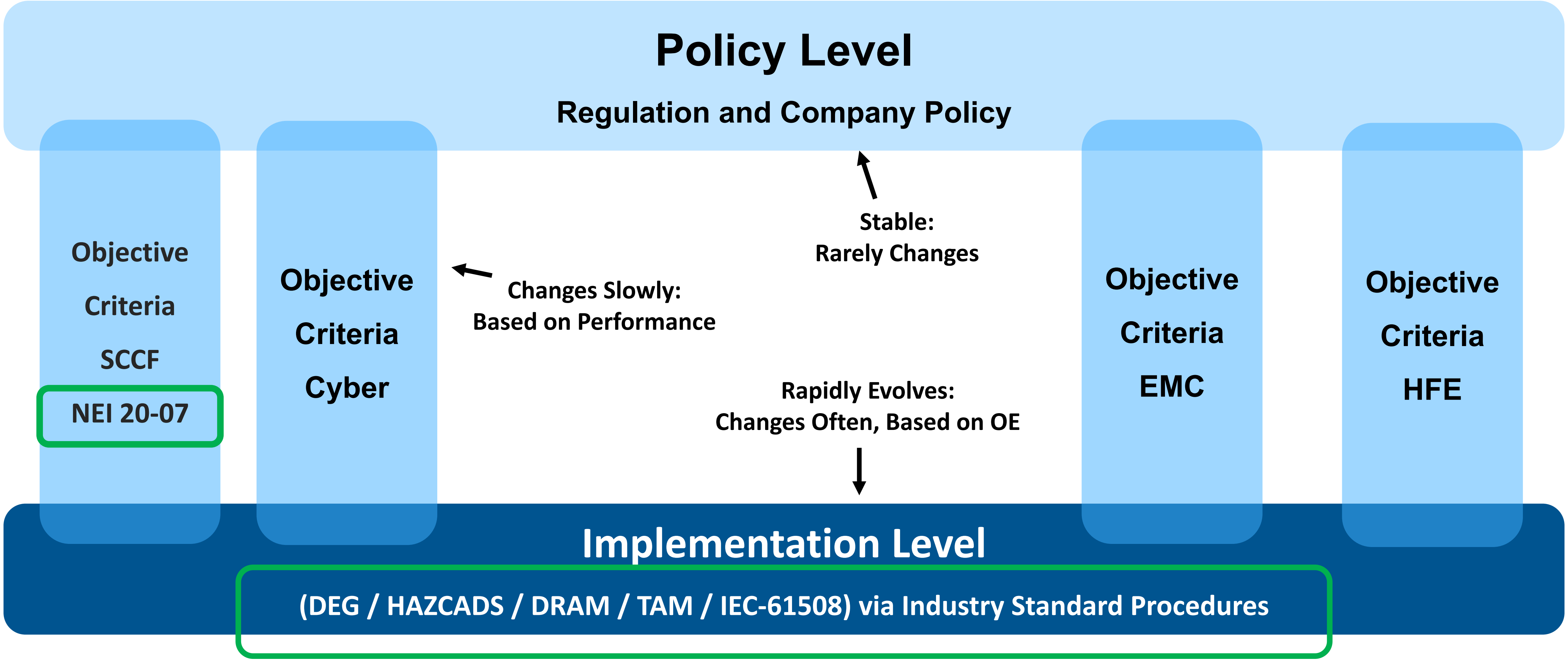
Risk Informed Engineering

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.

Capable Workforce

Modern Methods to Support Nuclear Fleet Sustainability and Advanced Reactor Design

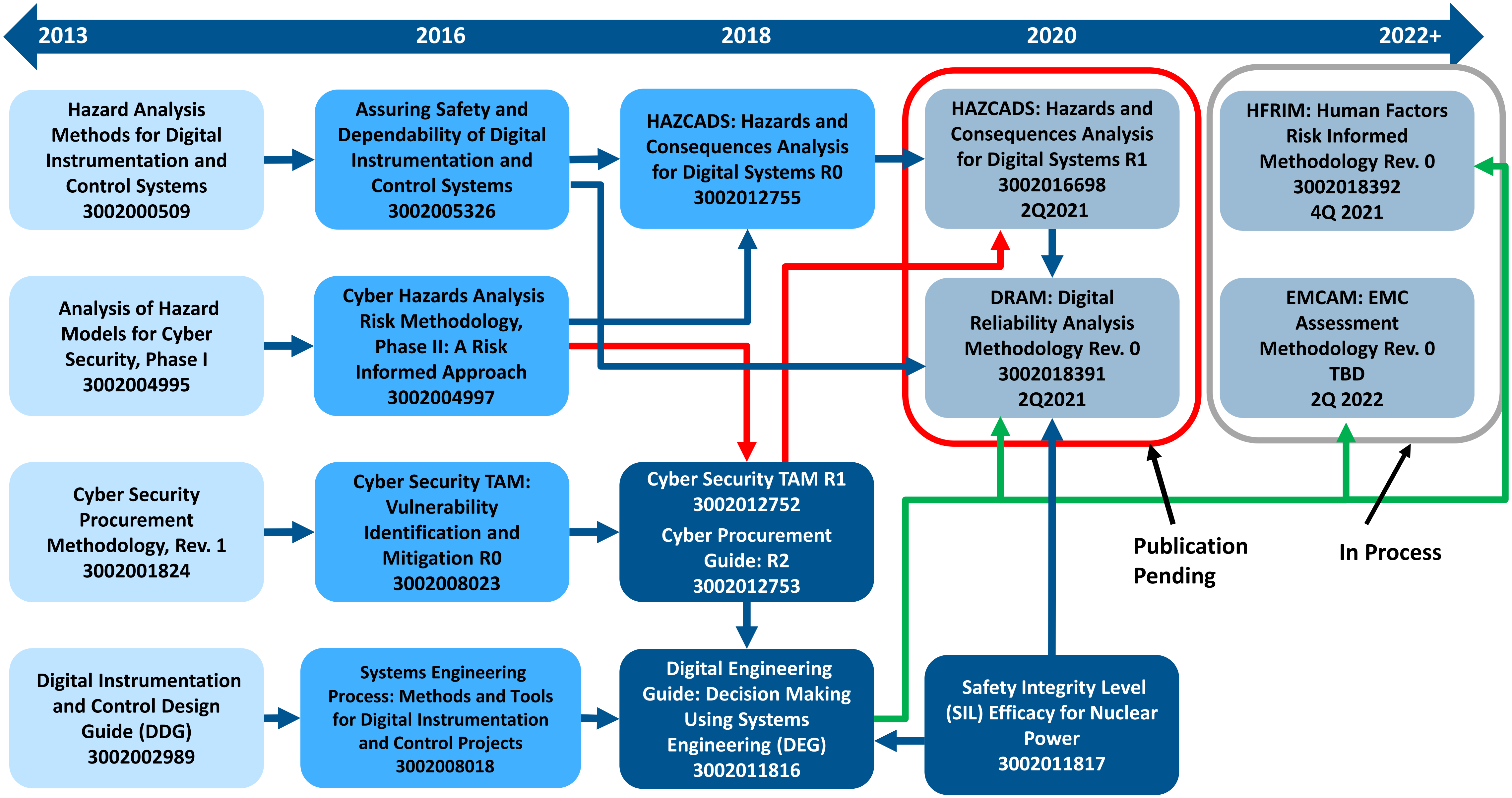
Policy Level vs. Implementation Level Activities



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

Objective Criteria provides the Interface between Policy and Implementation. Supports a safety case argument.

EPRI's Integrated Digital Engineering Development History



ELECTRIC POWER RESEARCH INSTITUTE

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

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

Safety reliability and risk framework

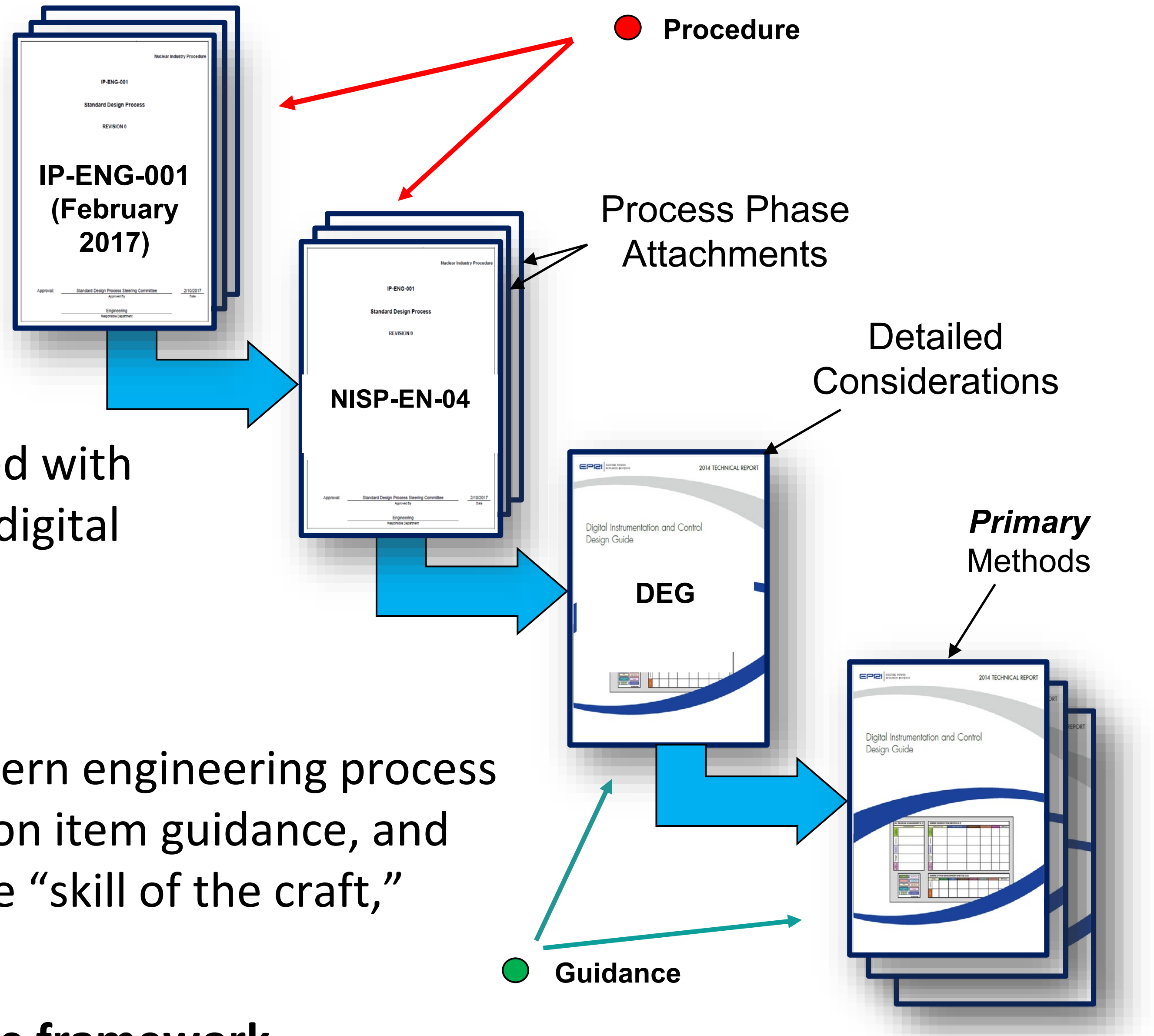
- IEC-61508/61511

US Industry Standard Engineering Process (NISP-EN-04)

Optimized Digital Engineering Organization

US DEG Implementation

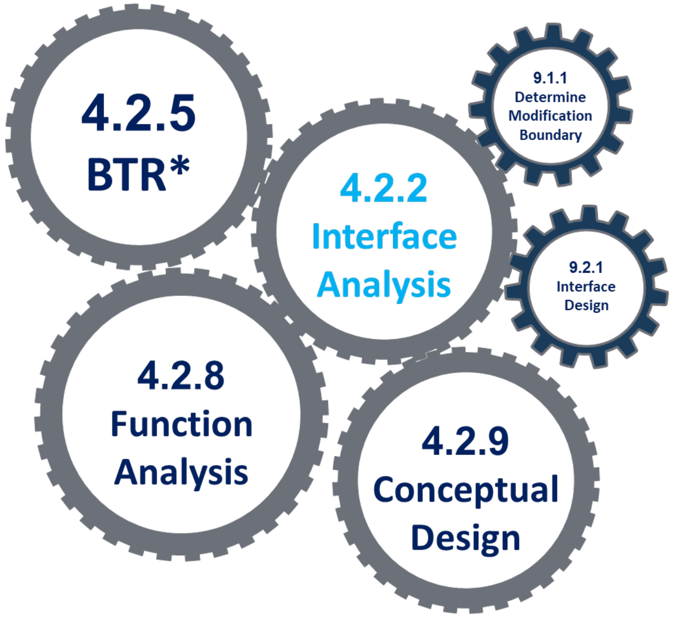
- IP-ENG-001 (Standard Design Process)- Main Procedure
- NISP-EN-04 is the Digital Specific Addendum to the SDP under the same mandatory Efficiency Bulletin (EB 17-06)
- Same process phases as IP-ENG-001, tailored with DEG-specific supplemental information for digital implementations. **Including Cyber Security**.
- Provides the user with **"what to do"**
- DEG provides detailed guidance using a modern engineering process with digital design considerations, information item guidance, and division of responsibility methods to improve "skill of the craft,"
- Provides the user with **"How to Do"**
- **Digital Training/Tech Transfer completes the framework**



Digital Engineering Guide(DEG) Training For Practitioners

- **Product ID: 3002015792**
- 4-day course available on EPRI/U for Classroom and Distance Learning (DL) Delivery
- Developed to support Technology Transfer of *Digital Engineering Guide: Decision Making using Systems Engineering,* 3002011816

- Supports Industry initiative to implement the DEG in US in 2021:
  - The DEG is a new and transformative engineering method
  - Training requires both SME and effective instructor skills
  - DL supports low cost/high volume delivery
  - Immersive, classroom-like DL environment achieved
  - Delivery capped at 12 sessions this year, all DL
  - 300+ students trained in 2020 from 11 utilities, 3 EOC's, INPO
  - Four Open Enrolment Courses available in 2021, plus Custom Sessions
  - **Max Class Size is 24**: Contact EPRI-U for course pricing and delivery option

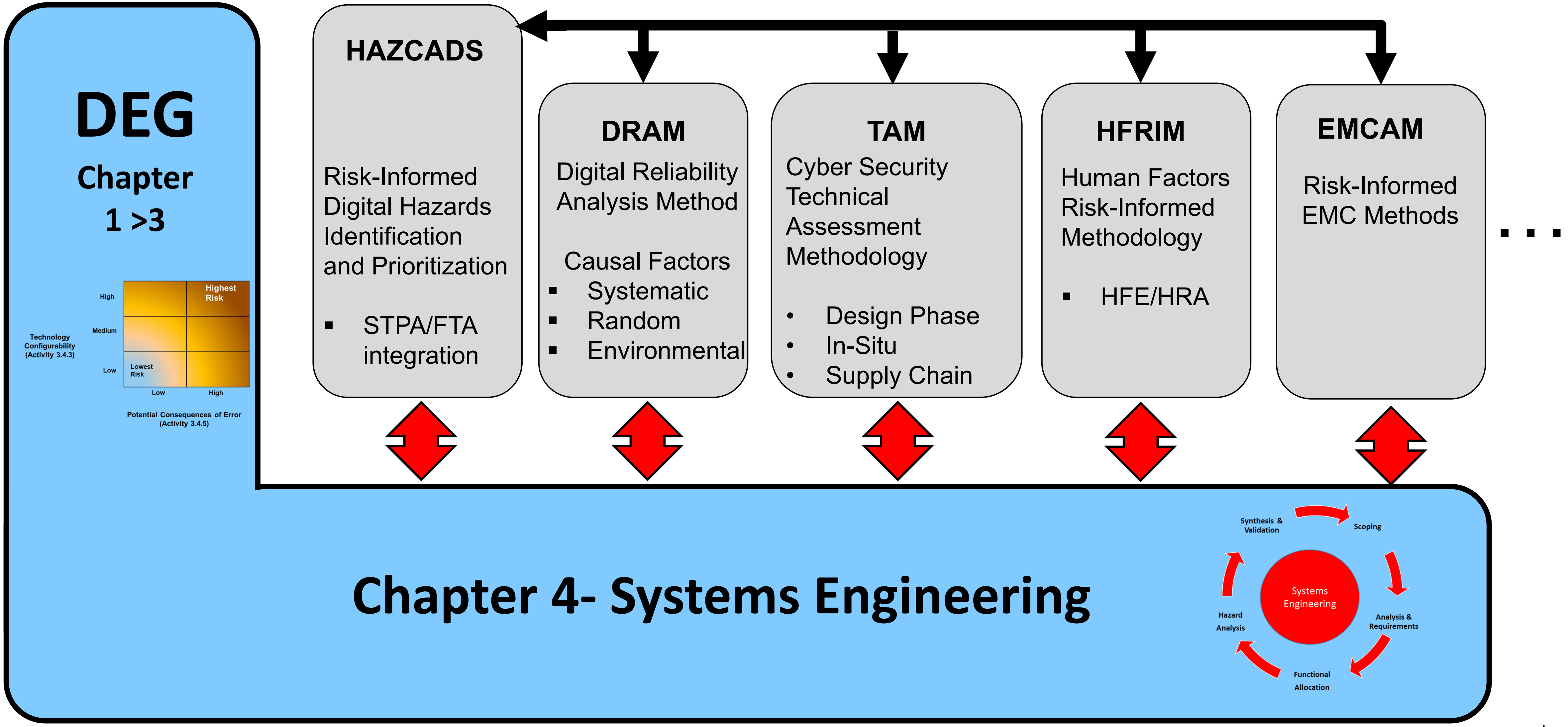


*Bounding Technical Requirements

Part of an Integrated Digital Training Portfolio Supporting Workforce Development

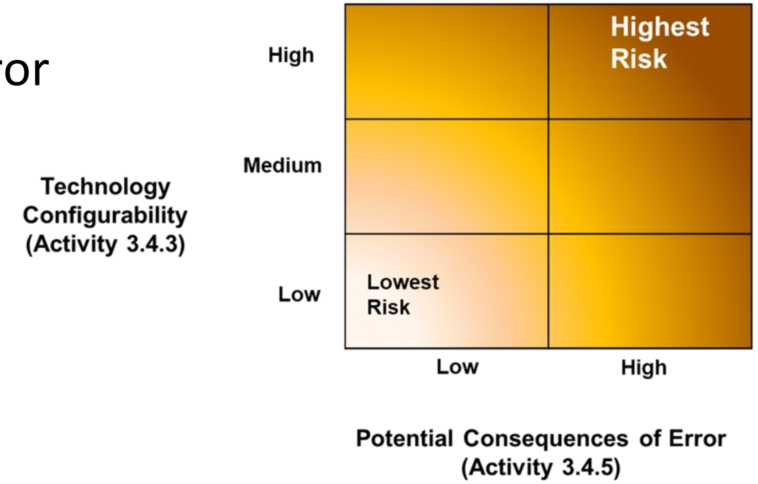
Risk Informed Digital Systems Engineering Integrated Processes

The EPRI Digital Systems Engineering Framework



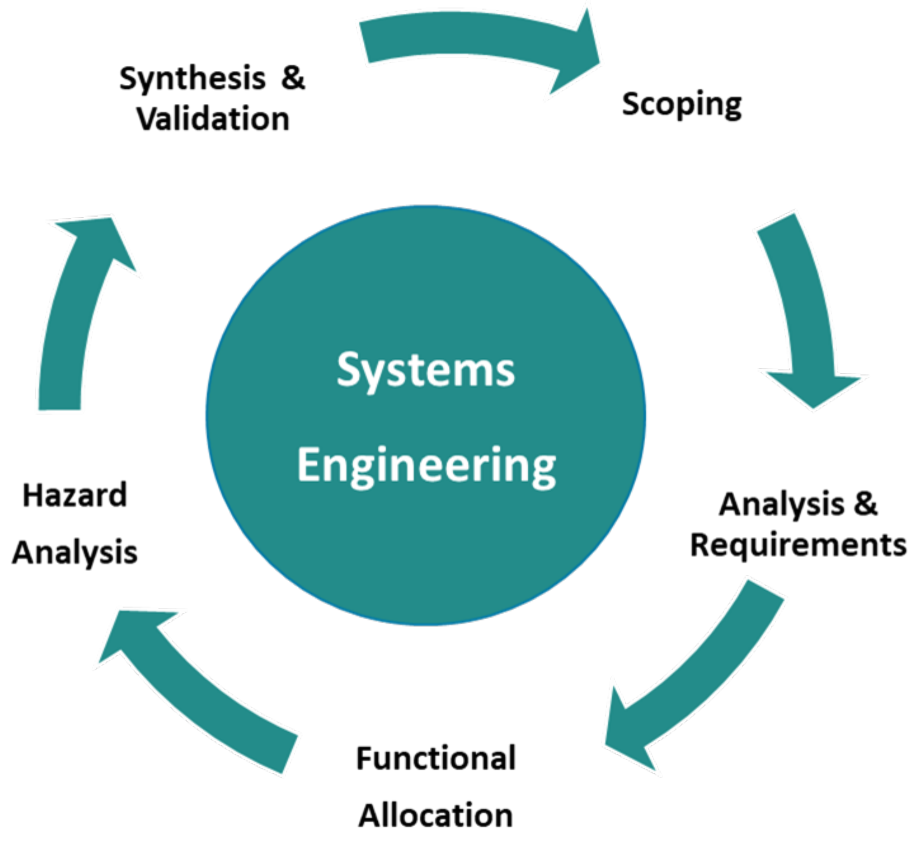
DEG Graded Approach Section 1 thru 3

- **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>



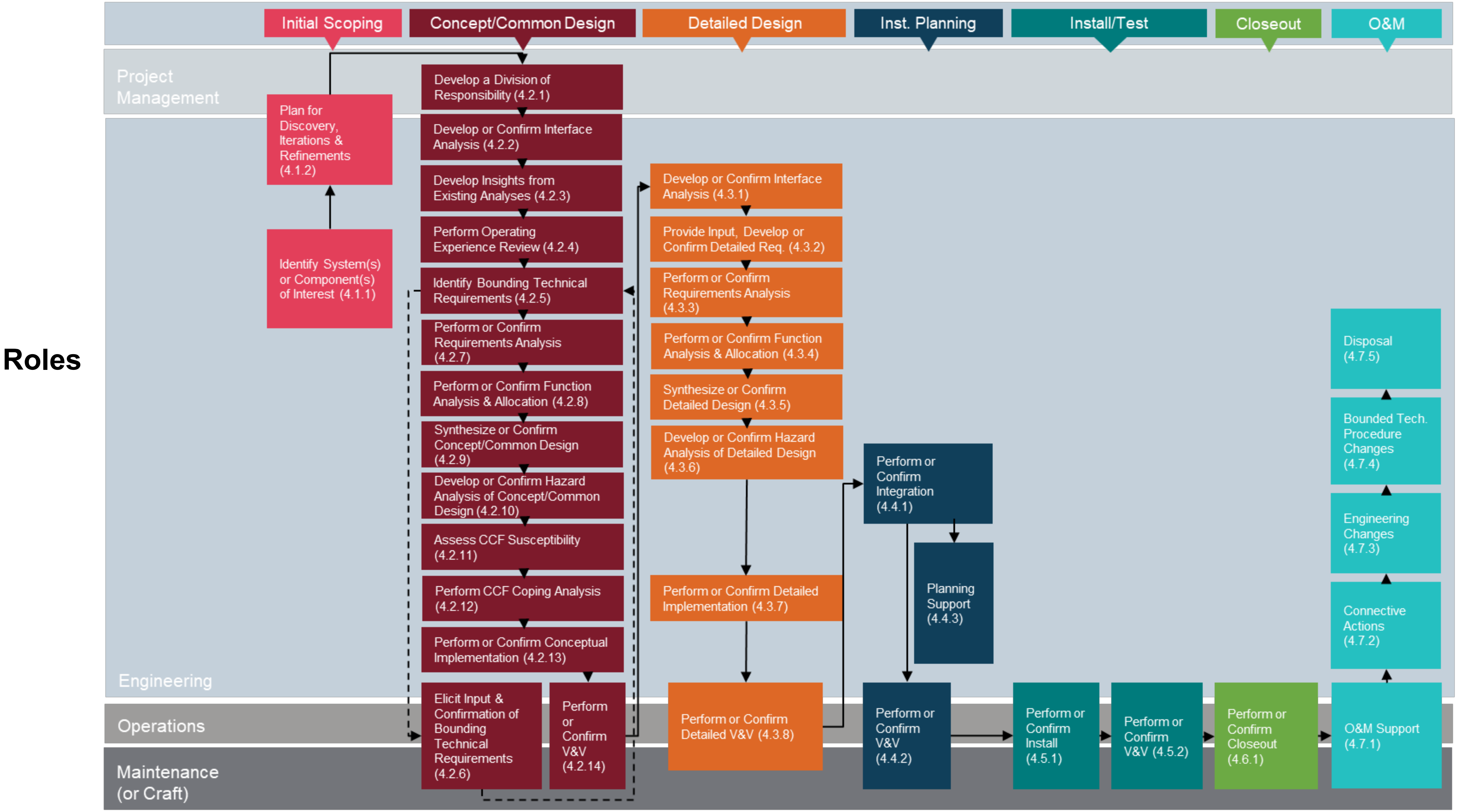
- **Step 1: Configurability Screen**
  - **Low** (A Few Settings)
  - **Medium** (Wide Range of Settable Parameters)
  - **High** (Custom Application Software)
- **Step 2: Consequence Screen**
  - **Low**: Does not meet High Consequence Criteria
  - **High**: Meets Risk and Impact thresholds for High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

Systems Engineering Based



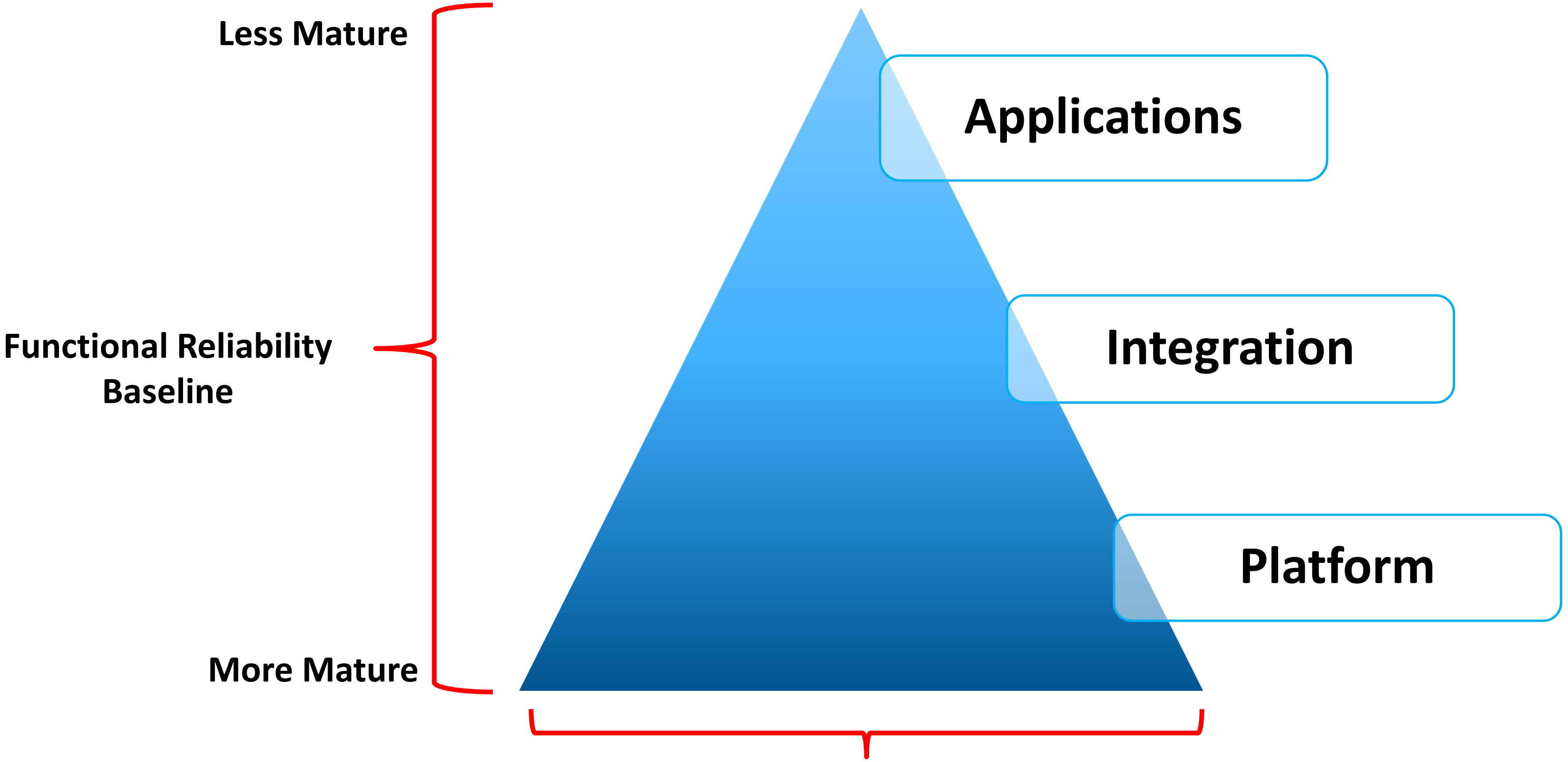
- **Phase Based using Perform/Confirm method**
- **Iterates through the SE process for each phase in a <u>non-linear fashion</u>**
- **Includes links to the topical chapters and sub-processes**
- **Iteratively converges on the final synthesized design**
- **Addresses:**
  - Division of Responsibility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

DEG Section 4 - Systems Engineering Activities



Reliability Layers

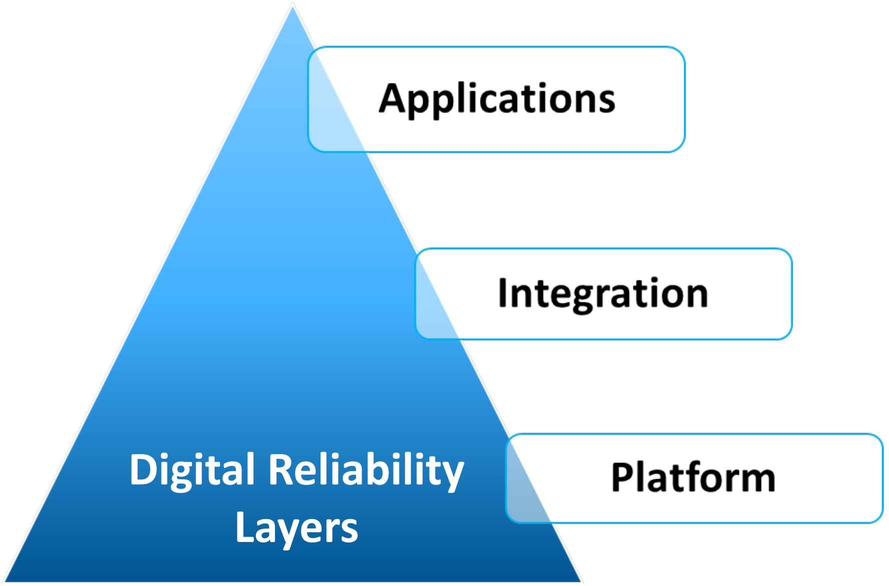
Reliability, especially software reliability, including CCF, should be segmented by *platform, integration, and application*. Then Considered Separately



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

Safety Integrity Level (SIL) efficacy for Nuclear Power

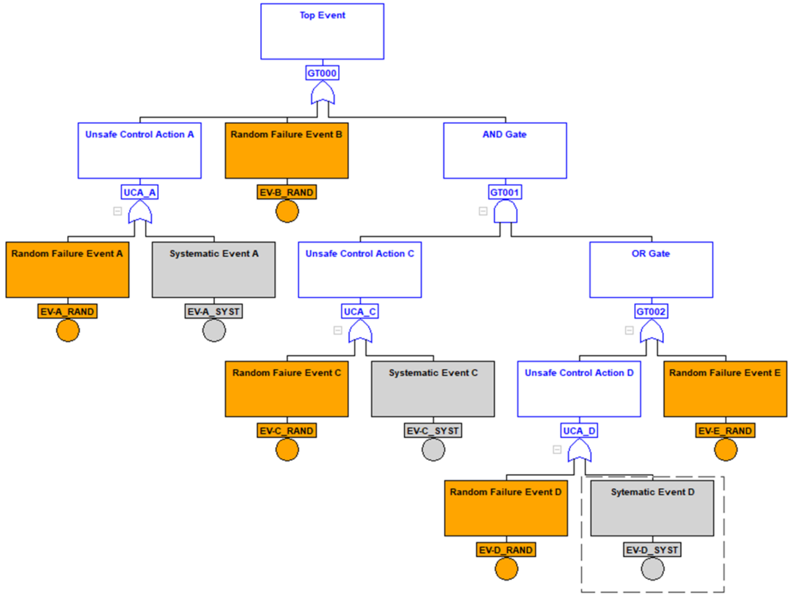
- EPRI research on field failure data from SIL certified logic solvers revealed no ***platform level*** Software Common Cause Failures (SCCF) after over 2 billion combined hours of operation for IEC-61508 SIL certified PLC's (3002011817)
- Indicates that using existing SIL certifications, at the ***platform level***, has a high efficacy for use as surrogates for some existing design and review processes.
- **Being Leveraged in MP#3 for NEI 17-06 in US**



- Correlates well with EPRI review of global OE (Korea, France, China, etc.) that indicates:
  - Safety related software is no more problematic than other SCCF contributors when subjected to deliberate safety processes.
  - There have been no events where diverse platforms would have been effective in protecting against SCCF

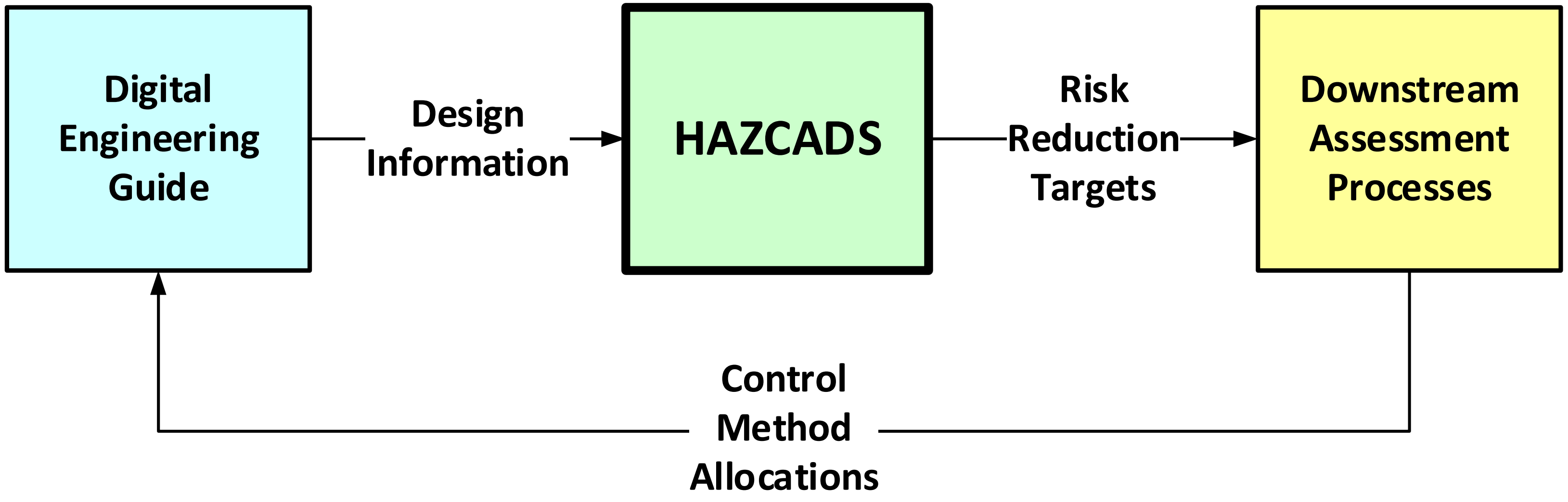
HAZCADS: Hazards and Consequences Analysis for Digital Systems R1-3002016698

- Advances the use of hazards analysis to identify system and plant level <u>digital</u> I&C design and implementation issues, including cyber, CCF and SPV.
- Executed throughout the design and implementation lifecycle.
- Uses System Theoretic Process Analysis(STPA) and FTA.
- Integrates qualitative hazards and random failures with Fault Tree Analysis based sensitivity analysis.



- **Achieves a credible risk informed I&C infrastructure compatible with existing processes.**
- **Dramatically improves hazard detection, resolution, and overall system reliability.**
- **Validated through blind studies and usability workshops.**
- **Used with causal factor analysis methods for a complete reliability assessment and resolution methodology.**

DEG/HAZCADS/Downstream Process Workflow

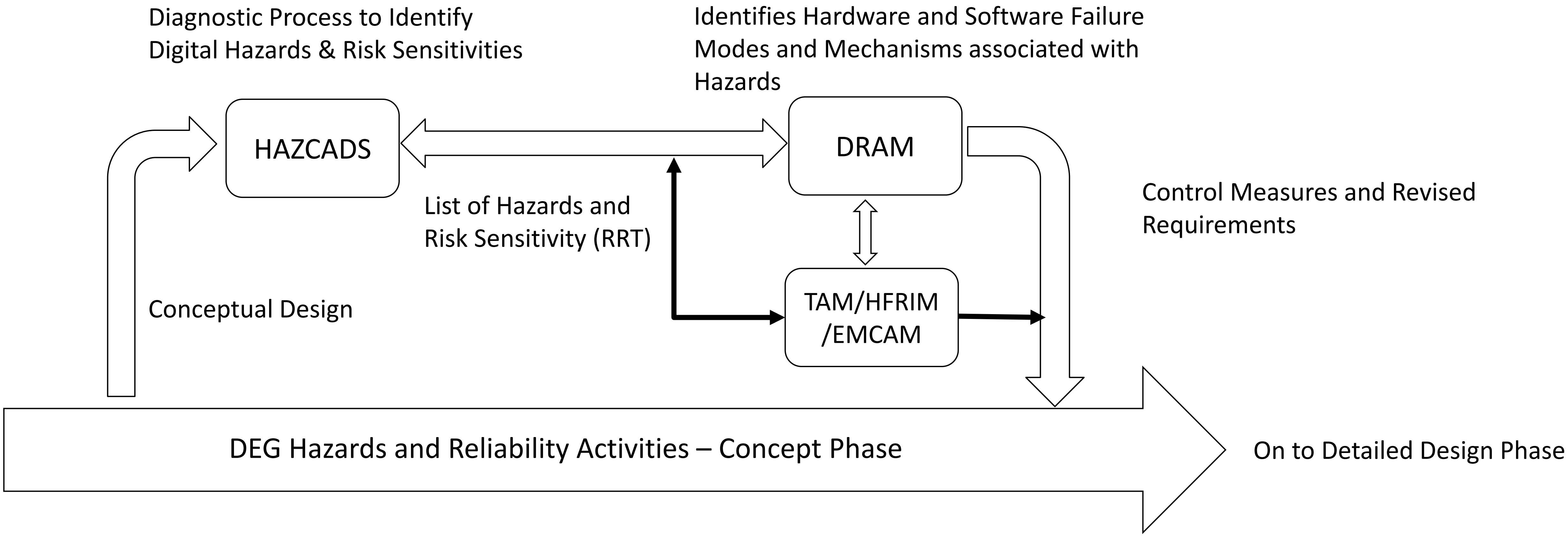


- HAZCADS diagnoses hazards in the I&C design-in-progress for inherent risks and determines Risk Reduction Targets (RRT) to be achieved via technical and/or administrative control methods

- Downstream assessment processes guide users in the allocation of control methods sufficient for achieving the RRT

Downstream Assessment Process	Report No.
Cyber Security Technical Assessment Methodology (TAM)	3002012752
Digital Reliability Assessment Methodology (DRAM)	3002018387
Electromagnetic Compatibility Assessment Methodology (EMCAM)	TBD (2022)
Human Factors Risk Informed Methodology (HFRIM)	3002018392

Workflow- Conceptual Phase



Digital Reliability Assessment Methodology (DRAM) Revision 0

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

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

DRAS Part 2

Residual Failures/Errors

DRAM Step 3
Mitigate Failure/Error Modes

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

DRAS Part 3

- **Identifies Causal Factors for identified Hazards- Synthesized from IEC-61508**
- **Identifies the most effective Control Measures to Prevent, Detect, and Respond to the Identified Hazards**
- **Results in specific requirements.**
- **DRAM will replace EPRI 3002005326* in 2021**
- **Being leveraged for NEI-20-07 for SCCF**

Relationship Sets

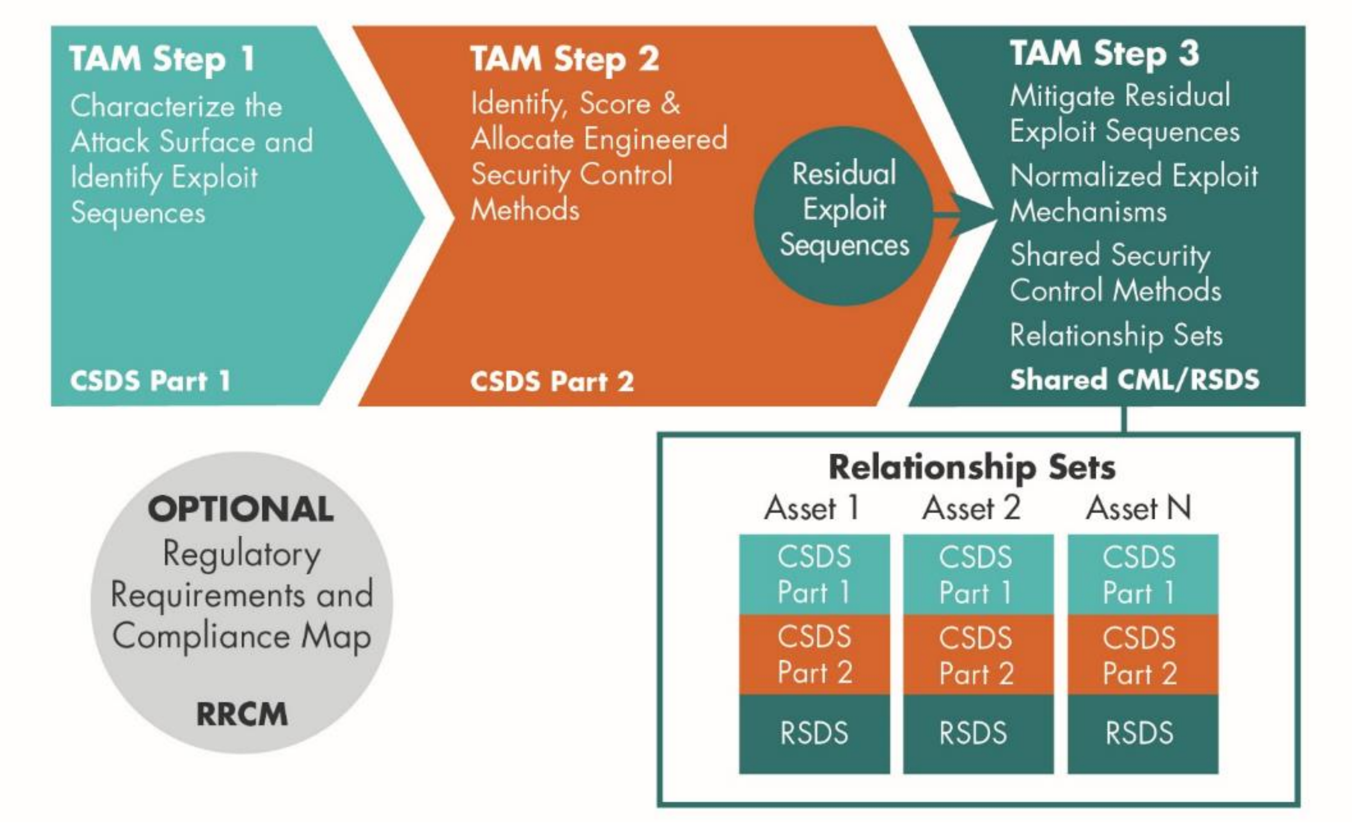
System 1	System 2	System 3
DRAS Part 1	DRAS Part 1	DRAS Part 1
DRAS Part 2	DRAS Part 2	DRAS Part 2
DRAS Part 3		

Optional
Regulatory Requirements and Compliance Map
RRCM

Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems, June 2016

EPRI Cyber Security Technical Assessment Method (TAM)

- TAM Early Adopters
- Vogtle 3&4 > Barakah (UAE) > NuScale> Exelon > OSISoft > Fisher Valves (Emerson)>SEL
- Significant Generation Sector Penetration



- Revision 1 published Nov 2018
  - Compatible with most existing standards and regulations 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

ELECTRIC POWER RESEARCH INSTITUTE

EMC Assessment Methodology-EMCAM

EMCAM Step 1- Identify
- Identify EMC Failure Error Type
- Identify EMC Failure Error Mechanisms

EMCAM Step 2- Assess
- Assess and Analyze
- Identify EMC Hardening
- Identify Control Methods

Residual EMC Vulnerabilities

EMCAM Step 3- Mitigate
Mitigate EMC Failure Modes
- Operator Manual Actions
- Shared Controls
- Relationship Sets

- **Identifies EMC Causal Factors for identified Hazards**
- **Identifies the most effective Control Measures to Prevent, Detect, and Response(CEP) to the Identified Hazards and Risk Reduction Target(RRT) (Results in specific requirements.**
- **EMCAM will implement a graded and risk informed approach to EMC Engineering**
- **Graded approach via adjusted susceptibility and radiated emissions limits plus proportional engineering controls**

Risk Reduction Target(RRT)	Susceptibility	Radiated	Engineering
A	x-db	x-db	Profile A
B	y-db	y-db	Profile B
C	z-db	z-db	Profile C
D	N/A	N/A	Profile D

Relationship Sets

System 1	System 2	System 3
EMCAM Step 1	EMCAM Step 1	EMCAM Step 1
EMCAM Step 2	EMCAM Step 2	EMCAM Step 2
EMCAM Step 3		

Integrated Use Cases (Common to DRAM, TAM, HFRIM, EMCAM)

Downstream Processes have been designed to be flexible and utilized in multiple use cases:

1

- Integrated into the overall digital engineering modification process.
  - As digital systems, assets, and services are being considered and designed to be utilized in a critical infrastructure facility, provides detailed analytical information needed to assist the engineer with making well informed decisions for mitigating cyber hazards.

2

- Use throughout the supply chain.
  - The modularity of the Framework and its documentation artifacts, allow it to be easily integrated throughout the supply chain, clarifying the division of responsibilities between the buyer and supplier and reducing a variety of digital hazards, including cyber.

3

- In-Situ Diagnostic or Baseline assessments for assets, systems, and services already installed. Can be used for root cause evaluations and other diagnostic purposes.

All three use cases take advantage of the Framework's modularity and efficiency.

Questions ?

Together...Shaping the Future of Electricity