



Risk-Informed and Performance Based I&C Design

A Modern and Integrated Approach

Matt Gibson
Technical Executive
EPRI Nuclear I&C Program

Risk Informed and Performance Based Community Of Practice

June 24th , 2022

About US



Nonprofit

Chartered in 1972 to serve the public benefit, with guidance from an independent advisory council. 450 member in 45 countries



Thought Leadership

Systematically and imaginatively looking ahead to identify issues, technology gaps, and broader needs that can be addressed by the electricity sector. \$420M in Annual R&D



Independent

Objective, scientific research leading to progress in reliability, efficiency, affordability, health, safety, and the environment.



Scientific and Industry Expertise

Provide expertise in technical disciplines that bring answers and solutions to electricity generation, transmission, distribution, and end use.



Collaborative Value

Bring together our members and diverse scientific and technical sectors to shape and drive research and development in the electricity sector.

Speaker Introduction

Matt Gibson:

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

- EPRI- Since December 2013
- Duke/Progress Energy(US Utility)- 1982-2013
 - Fleet Digital 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 Lead*
 - *Technology Assessment and Integration Lead*
 - Nuclear IT/OT Manager- Robinson Nuclear 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*
- US Navy – Electronic Warfare Specialist 1975 -1982
 - *Operated and maintained digital EW equipment in a complex tactical environment.*





Introduction to the EPRI Digital Systems Engineering Framework

Digital Convergence



All these instruments



Are now on ONE yellow wire

EPRI's Digital Framework Elements

EPRI's **structured ,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-61508/61511/62443). 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.

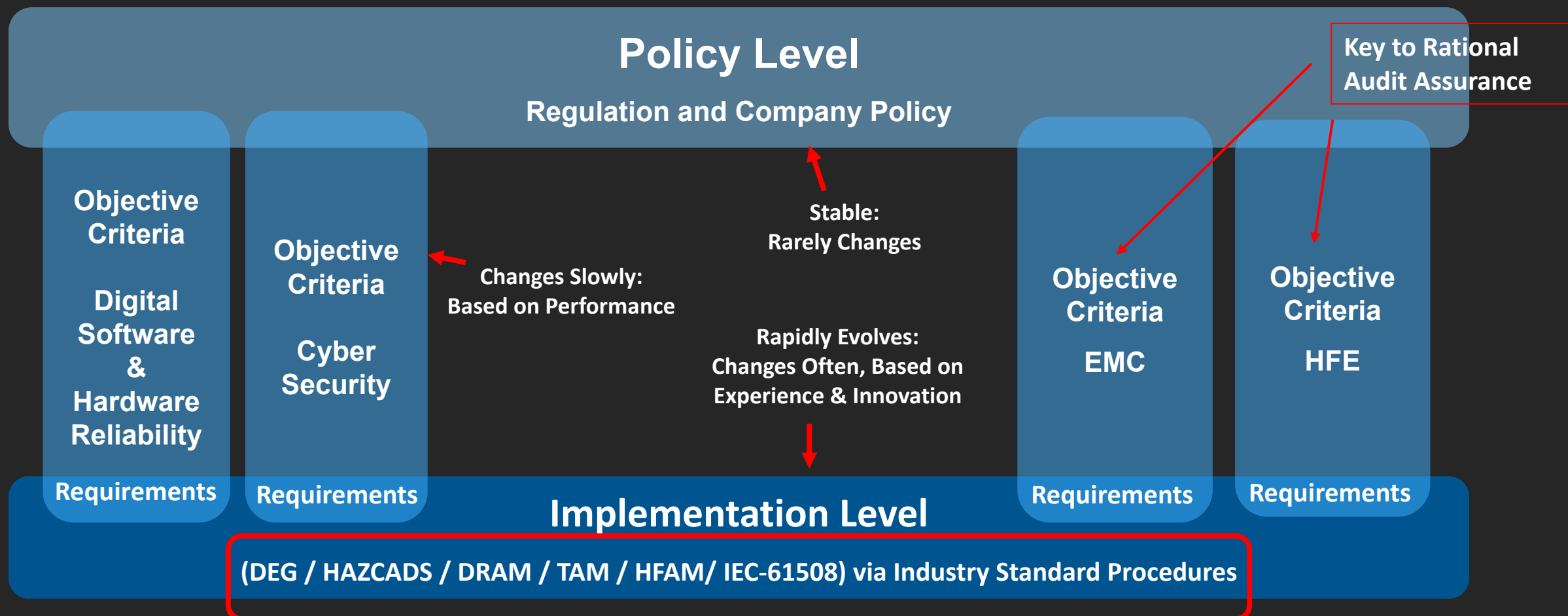
Risk Informed Engineering

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

Risk Informed, Technology Neutral Framework



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

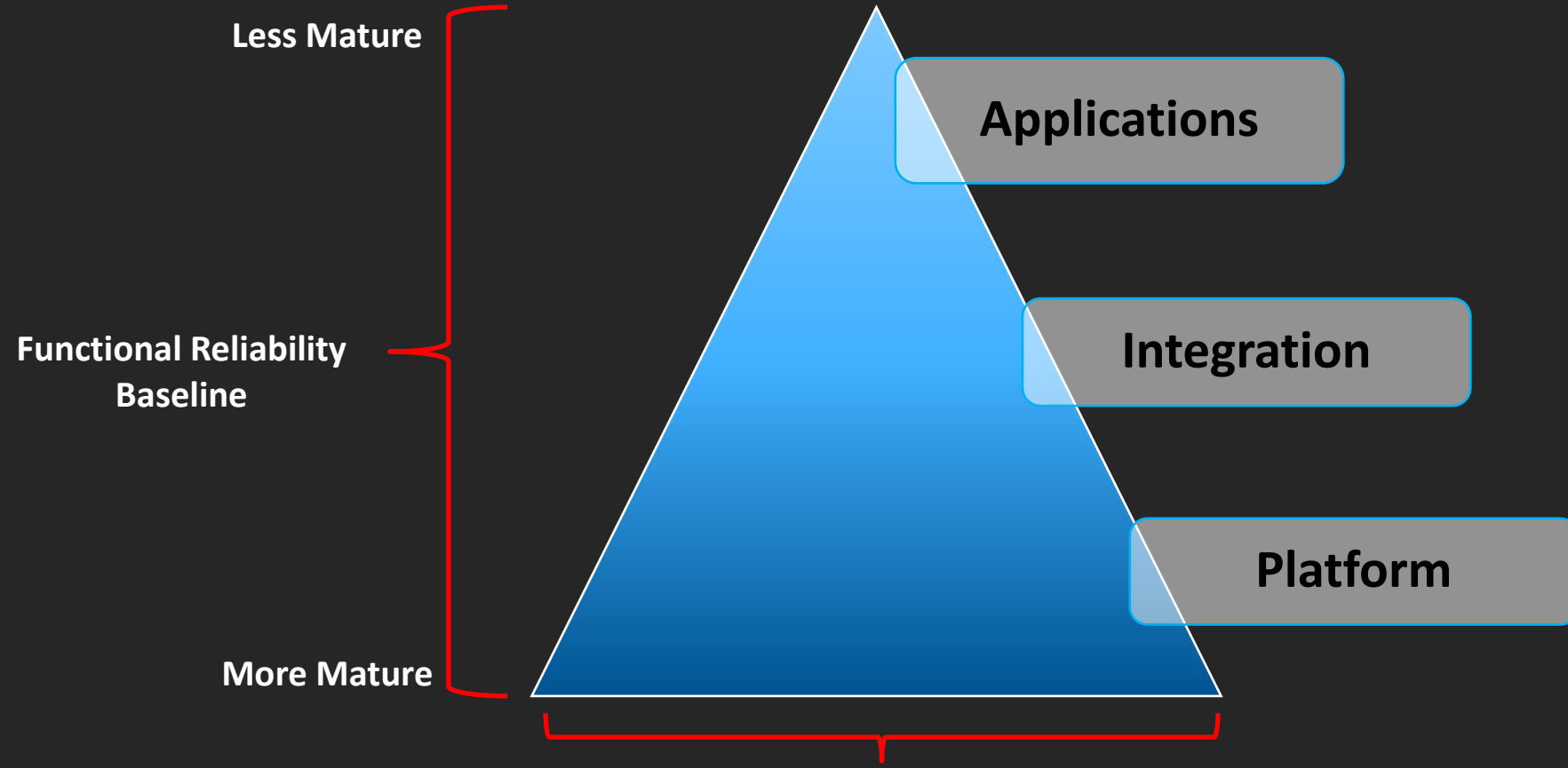
Objective Criteria provides the Interface between Policy and Implementation. Supports a structured safety case argument.



Risk Informed Digital Systems Engineering An Integrated Processes

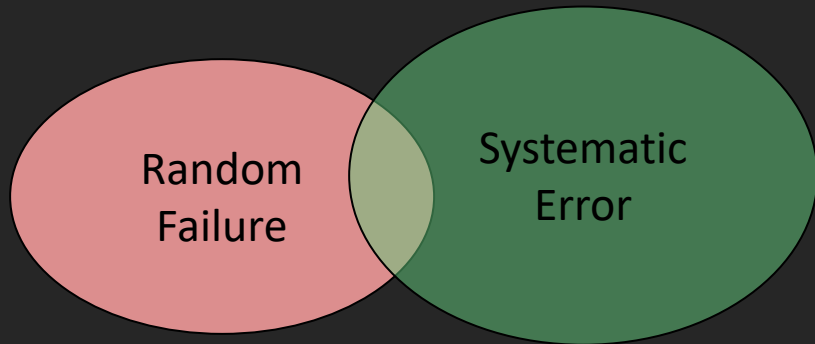
Reliability Layers

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

Digital Reliability Model



Reliability Axioms

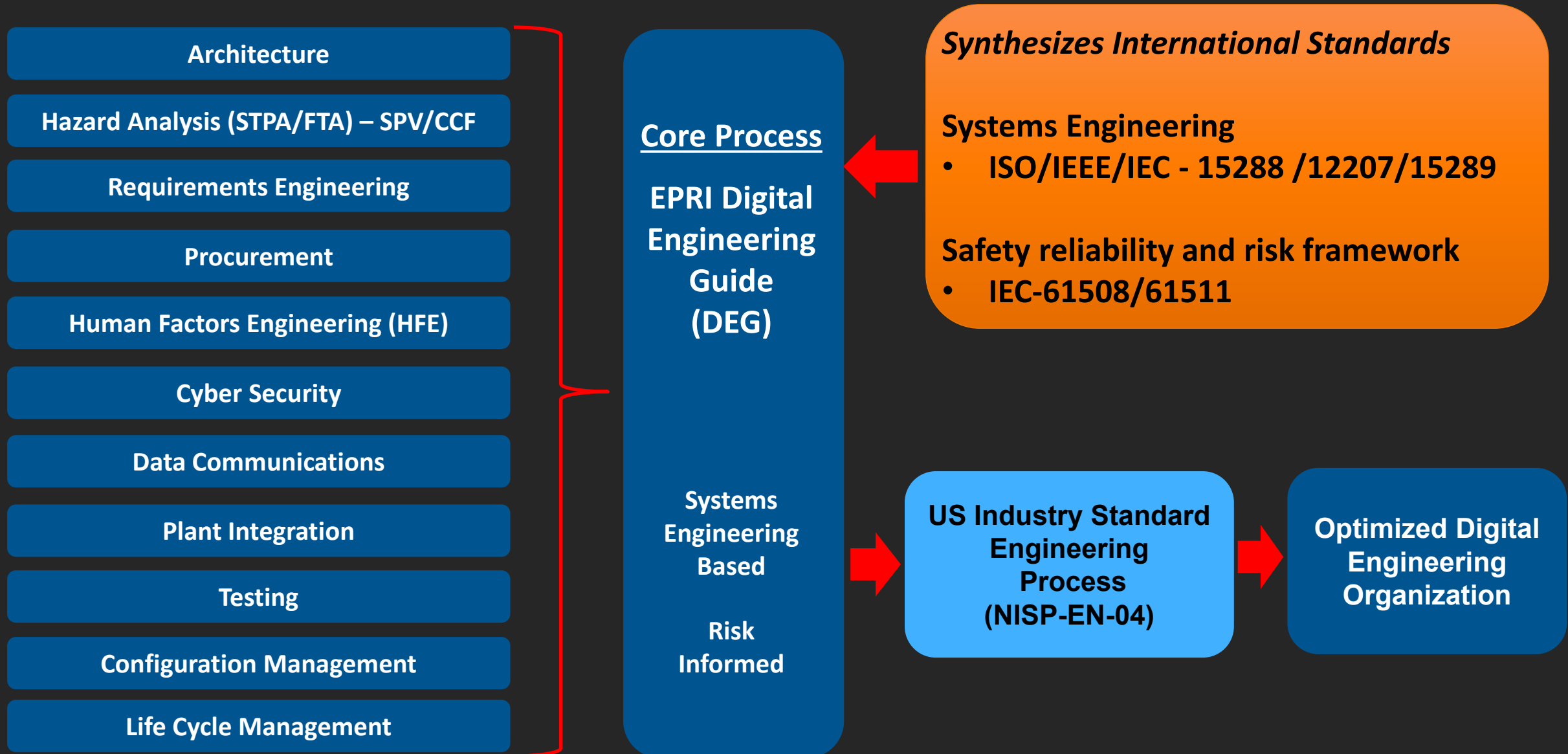
- Equipment Design and Random Failure, Cyber Vulnerabilities, and Human Reliability are the same thing from an Engineering Perspective.
- Achieved Systematic and Random Reliability is inversely proportional to the likelihood of any event, CCF or otherwise.
- Common Cause Failures must **first** have a failure or systematic error (including emergent behavior).
- Reliability is best achieved via a cost, likelihood, and consequence equilibrium.
- Net Functional Reliability is the prime objective (at the system/facility level).

Digital Framework Value Features

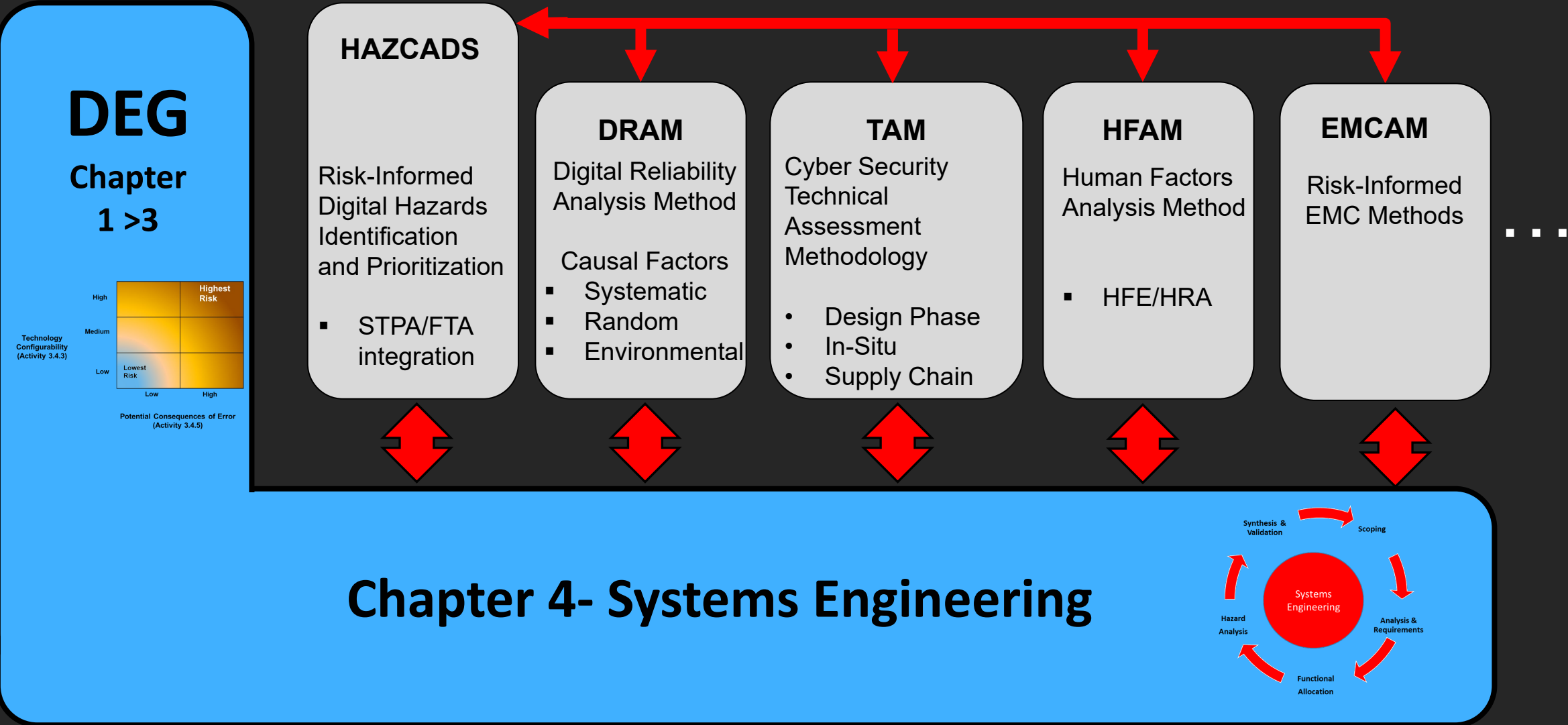
- Provides a modern systems engineering methodology which has proven to be very efficient in other industries- better results in less time. Covers all digital design considerations.
 - ✓ Regulatory and Reactor Technology Neutral
 - ✓ A single process for all digital topics allows rapid integration and tradeoff analysis, Including Cyber and Human Factors
 - ✓ A risk-Informed and performance based graded approach focuses on the right work with the most impact and eliminates low value processes.
- A systems approach aligns with modern standards and eliminates separate processes such as SQA.
- Structured results allow for higher assurance and faster **(PB)** reviews

Refinement Ongoing via User Group Feedback

Integrated Digital Systems Engineering Framework

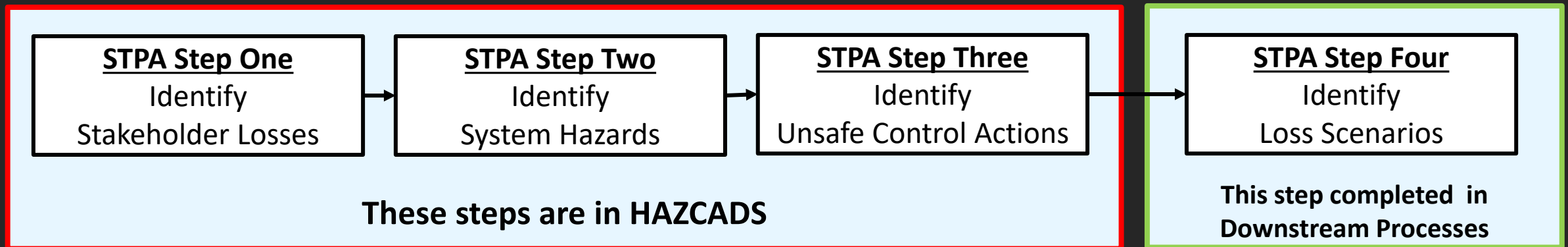
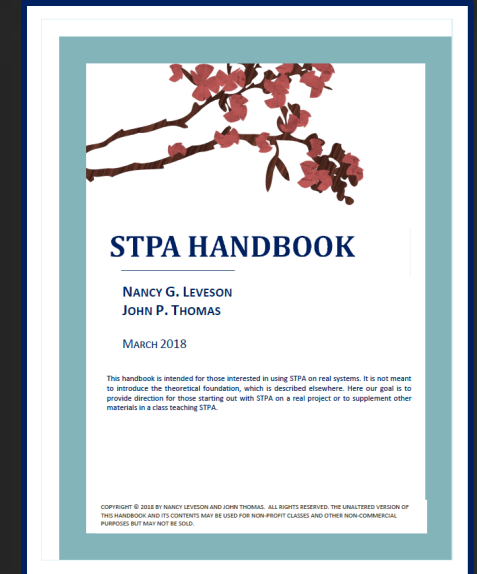


Modular Subprocess Framework



Hazard and Reliability Analysis for Risk Informed Decisions

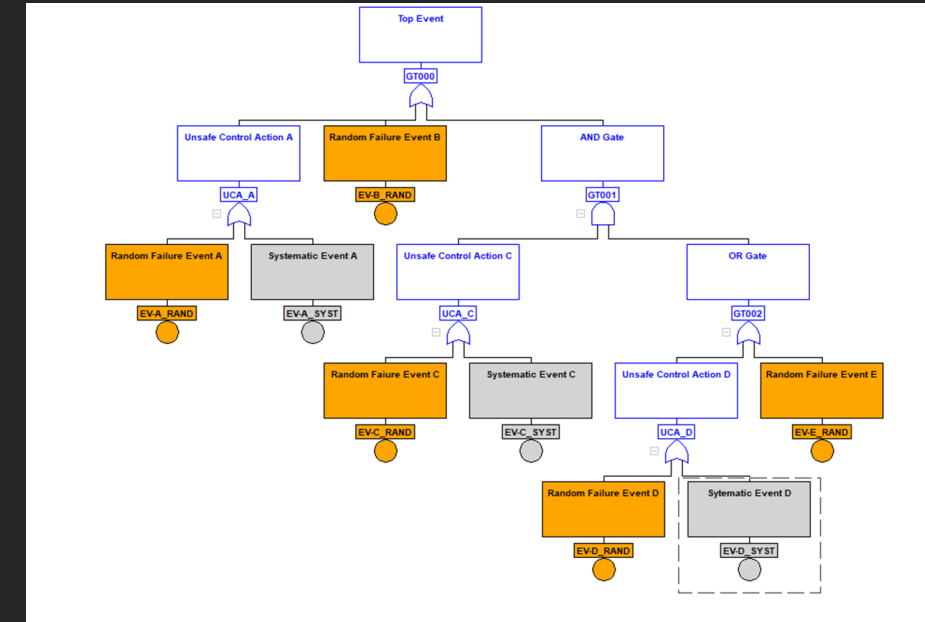
- IEC 61508-1 requires a determination of hazards of the Equipment Under Control(EUC) and the EUC control system, and “consideration shall be given to the elimination or reduction of the hazards.”
- For the determination of hazards and their causes, HAZCADS and DRAM/TAM/etc. apply the four-part Systems Theoretic Process Analysis (STPA) developed by MIT. STPA is an efficient and proven method, successfully applied other safety critical domains, and evaluated in multiple EPRI workshops and experiments.



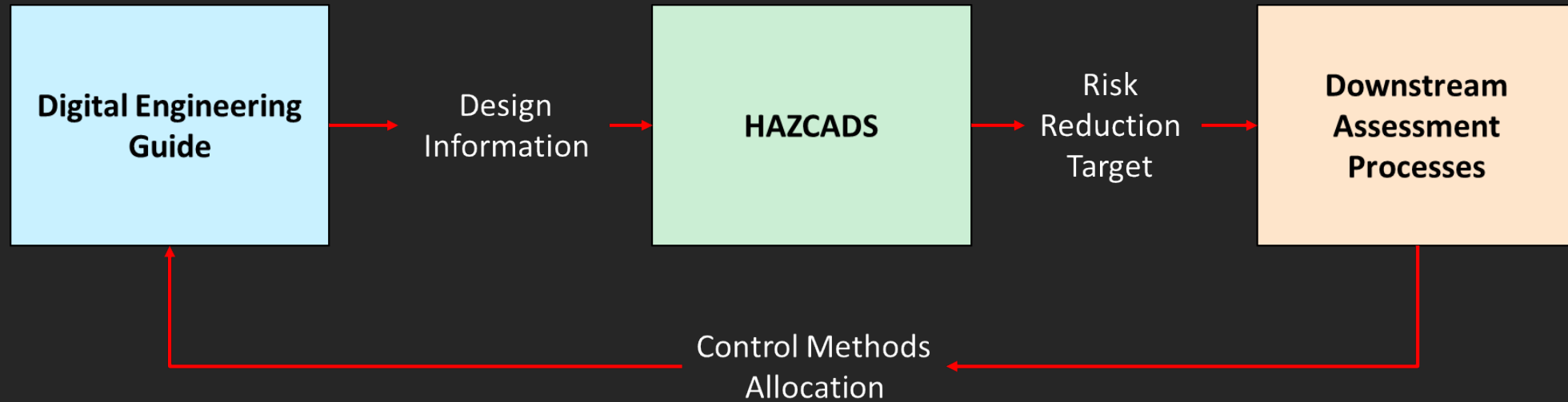
HAZCADS: Hazards and Consequences Analysis for Digital Systems-3002016698

- ✓ Advances the use of hazards and risk analysis to implement risk informed digital and cyber security designs , targeting the economic implementation of digital technology.
- ✓ Supports the industry and regulatory initiative to risk inform digital I&C.
- ✓ Integrates System Theoretic Process Analysis(STPA) and FTA into a modern analysis process by blending qualitative hazards with quantitative FTA based sensitivity analysis.

- Dramatically improves hazard detection, resolution, and overall system reliability. Can be used with any consequence(lost generation, reputational loss, etc.)
- Achieves a credible risk informed I&C infrastructure compatible with existing processes.
- Validated through blind studies and usability workshops.
- Used with downstream loss scenario identification and 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**
- **The Downstream assessment processes guides users in the development of control methods and design attributes 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 Analysis Methodology (HFAM)	3002018392

Workflow- Conceptual Phase

Diagnostic Process to Identify
Digital Hazards & Risk Sensitivities

Identifies Hardware, Software, and Human Reliability
Loss scenarios associated with Hazards

HAZCADS
STPA + FTA

DRAM
Reliability
IEC61508

List of Hazards and
Risk Sensitivity (RRT)

Loss Scenarios, Scored Control Measures
and Revised Requirements that Reflect
Diagnostic Results

Conceptual Design &
Relationship Sets

Cyber TAM

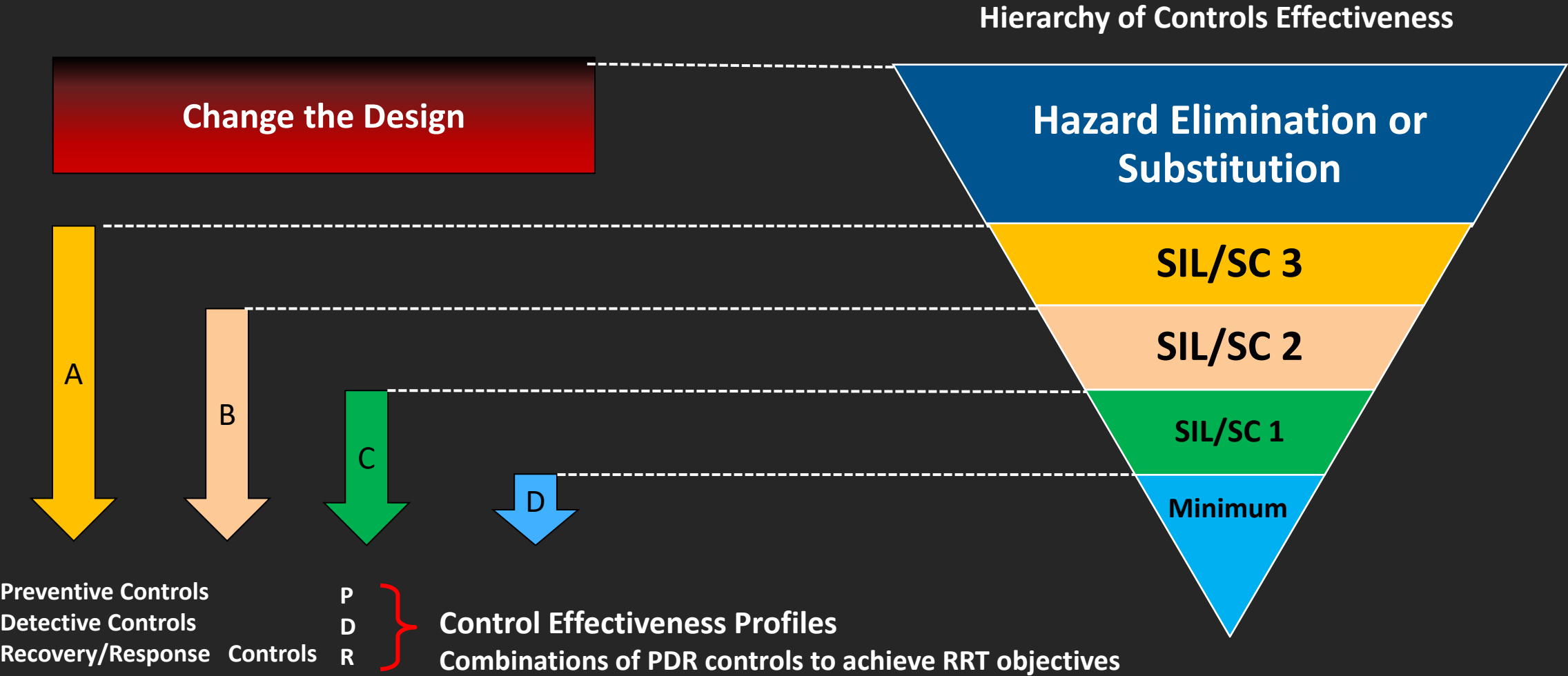
HFAM

EMCAM

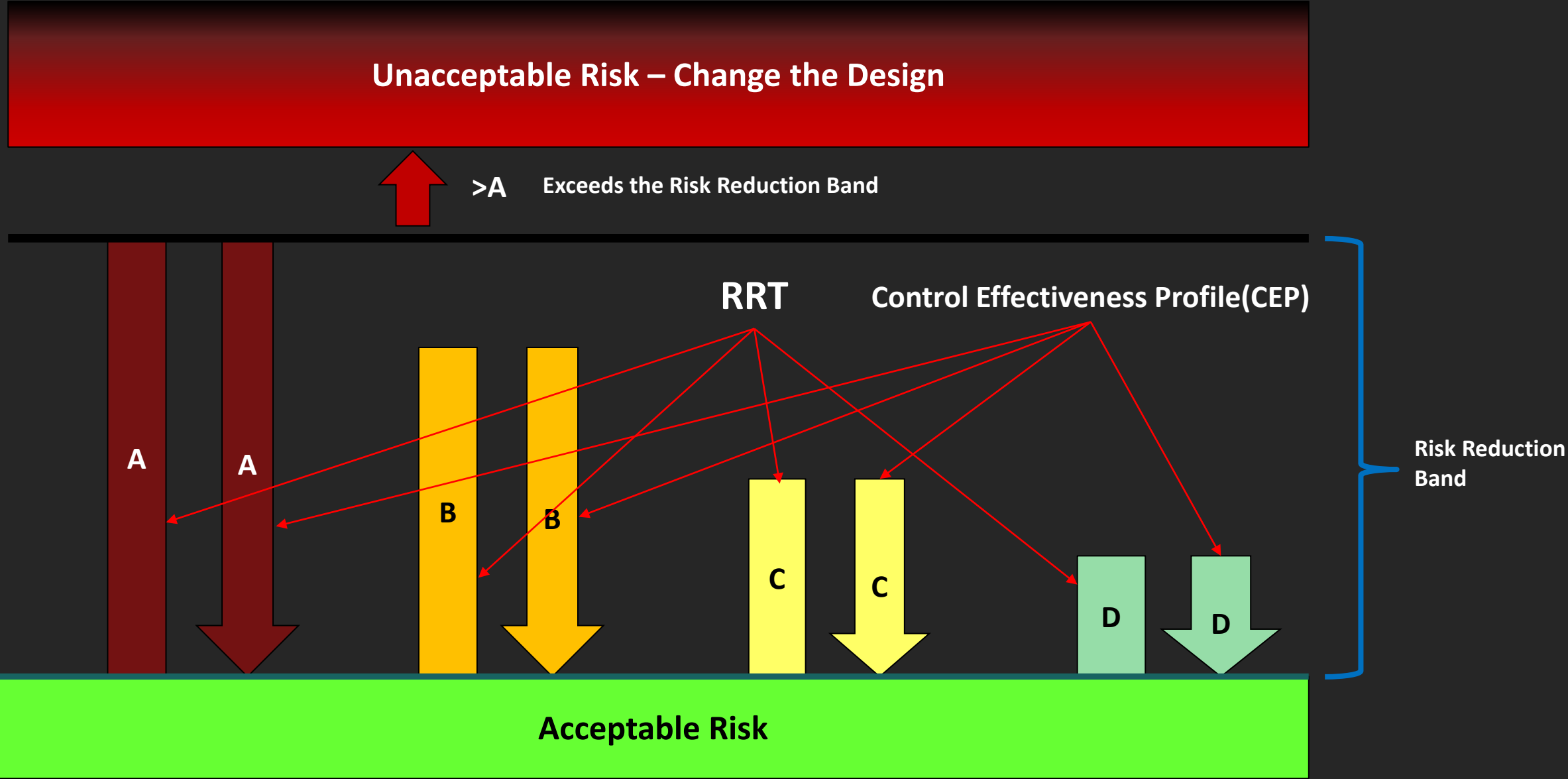
DEG Design and Architecture Development – Concept Phase

On to Detailed Design Phase

Risk Reduction via Control Effectiveness (DRAM Example)

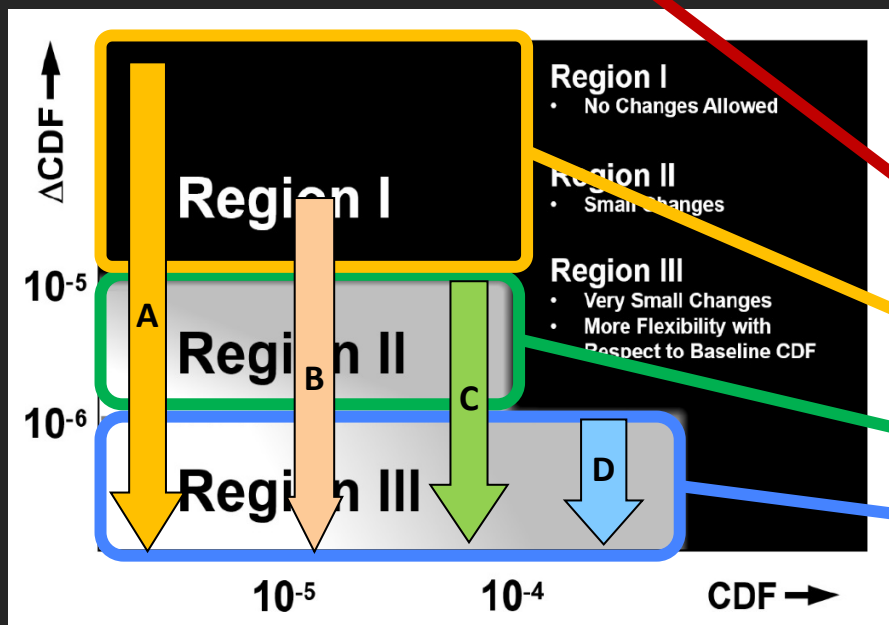


Relationship Between HAZCADS RRT and DRAM CEP



RRT Acceptance Criteria

Change the Design



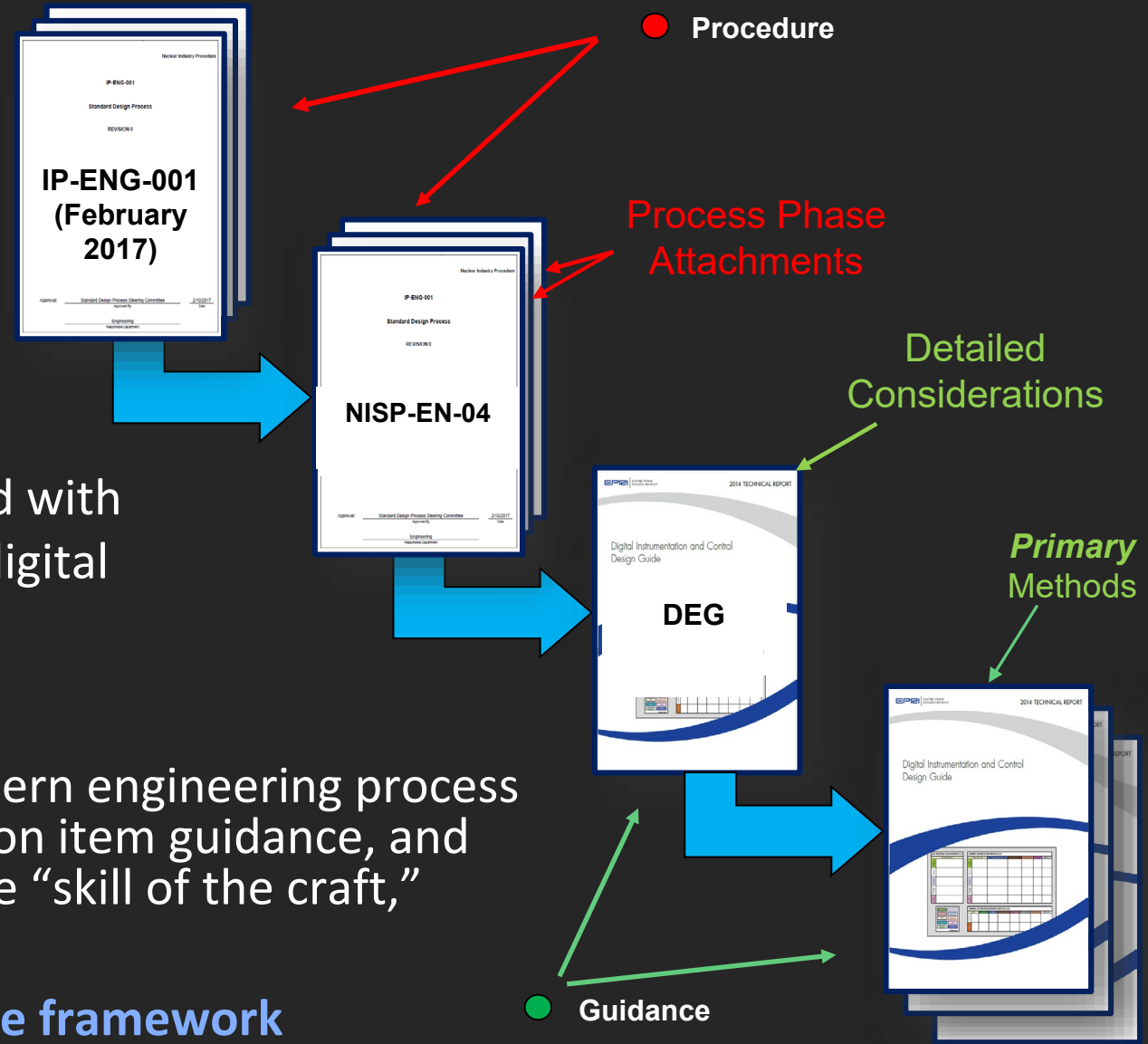
RG 1.174 Example

RRT	Change in Core Damage Frequency – CDF (per year)	Change in Large Early Release Frequency – LERF (per year)
Change the Design	$\Delta CDF > 1E-3$	$\Delta LERF > 1E-4$
A	$1E-4 < \Delta CDF \leq 1E-3$	$1E-5 < \Delta LERF \leq 1E-4$
B	$1E-5 < \Delta CDF \leq 1E-4$	$1E-6 < \Delta LERF \leq 1E-5$
C	$1E-6 < \Delta CDF \leq 1E-5$	$1E-7 < \Delta LERF \leq 1E-6$
D	$\Delta CDF \leq 1E-6$	$\Delta LERF \leq 1E-7$

HAZCADS

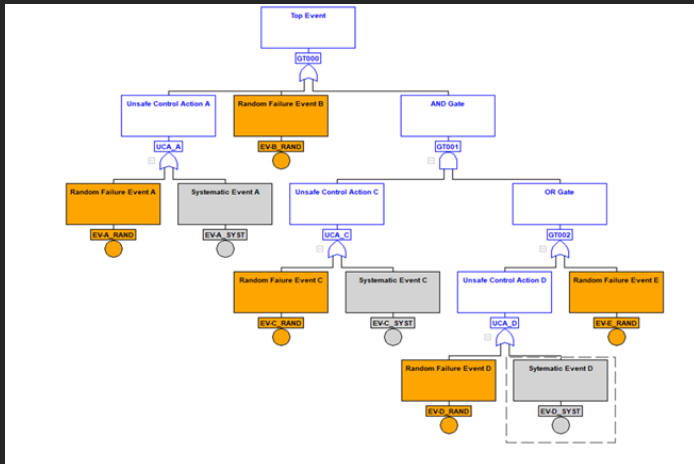
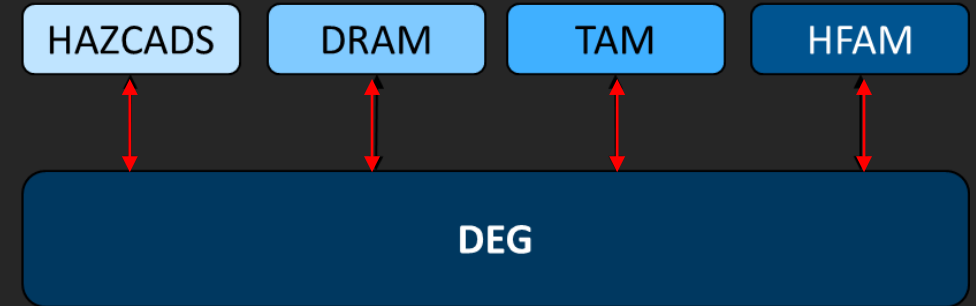
U.S. DEG Implementation

- 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**
- **500+ Practitioners Trained to Date.**



EPRI Risk Informed Digital and Cyber Security Framework

- Risk-Informed Digital and Cyber Security positioned to accelerate the industry use of technology to achieve their business objectives.
- EPRI Risk Informed Digital/Cyber Framework in Production
 - ✓ US Regulatory initiative in progress via NEI 20-07 & 17-06
 - ✓ US Pilots Being Identified (NEI Collaboration)
 - ✓ Workforce Development Resources available in 2022
 - ✓ Implementation Resources Available 2022



- **HAZCADS, DRAM, & HFAM delivered in 2021- Integrated with DEG**
 - ✓ Constellation Pilot Ongoing
 - ✓ Integrated Proof Test Completed (DEG, HAZCADS, DRAM, TAM)
 - Simulated plant Design Change over 3-month period with diverse participants
- HFE and HRA integrated into HFAM
 - ✓ Risk-Informs HFE
- Multi-Disciplinary process includes Engineering and Risk Professionals

DEG= Digital Engineering Guide
HAZCADS= Hazards and Consequence Analysis for Digital Systems
DRAM = Digital Reliability Analysis Methodology
TAM= Cyber Security Technical Assessment Methodology
HFAM=Human Factors Analysis Methodology

RIPB Challenges

- Implementation Challenges stem from:
 - Work Culture Bias.
 - RIPB represents a radical departure from check list QA and quality concepts based on “procedure adherence”
 - Changes how engineers interact with management/auditors/regulators
 - Challenges oversight groups – “we don’t know how to audit RIPB outcomes”
 - Elevates the responsibility of engineers and risk professionals. Now performance driven not procedure driven. Agreement on what good performance (outcomes) looks like.
 - Requires active, team-based/participation-based engineering.
 - Industry Workforce Knowledge, Skills , and Abilities are misaligned with RIPB
 - Engineers/Management/Regulators will need to transition to a RIPB skill set
 - Nuclear practitioners will need better systems and technology skills (better performance tools)
 - Enhanced Systems Thinking needed

Senior Leadership and Workforce Development Are Needed



Digital I&C Research For Assessment PRA

What are we trying to accomplish?

- We have a great tool for the design/evaluation phase – HAZCADS (and related processes)
- We need something equally useful for “day-to-day” use once the digital I&C mods are installed
 - Digital I&C operating experience and reliability/failure data for PRA purposes is scarce and will remain so for some time:
 - Software/systemic/cyber
 - Human Actions
 - Thus, we need something that is simple to build, simple to understand, and “roughly right” – that can be implemented and used now and refined over time

Digital I&C “Assessment” PRA

Our starting point

- Hypothesis: HAZCADs, Unsafe Control Actions (UCAs), PRA model insights/updates to perform risk sensitivities of UCA sets (UCAs that can fail together) give us the structure of the 'digital I&C' PRA model
- Hypothesis: We don't need to complicate things...we can "black box" much of digital input to the PRA model
- Hypothesis: The "evaluation" model can be re-baselined relatively easily to reflect the improvements to safety (from a risk metric perspective)
 - Improvement in system reliabilities
 - Decrease in "digital-caused" initiating event frequency
 - Human error probabilities (separate project, underway)

Start with PRA model Informed/updated for HAZCADs

Some things we're thinking about

- Considerations:

- “CDF” and “LERF” may not be the (only) metrics of importance
 - “End of plant operation” may be appropriate, e.g., system operation saves the core, but renders plant inoperable from that point forward (think of boron injection in BWR)
 - Advanced reactors may have different metrics.
- From a radiological risk perspective, digital I&C may have limited benefits depending on overall design features
 - But other factors, e.g., reduced maintenance, reduced spare parts inventory, etc., may be significant
- Configuration control must be considered – maintenance, software updates/upgrades, etc., may affect failure likelihoods
 - High degree of coupling between Engineering/Maintenance and Risk Analysts

Revise/modify/enhance model

Some things we're thinking about (continued)

- Considerations:
 - Ensure model captures “cause-effect” relationship
 - Such major (high impact) relationships should already be identified and designed out in the evaluation/design phase
 - There is operational experience with digital failures, e.g., consequential loss of offsite power due to digital failure in a non-power system
 - Look at how to model, or if to model, “burn in” failures (first cycle)

Revise/modify/enhance model

What are our current activities?

- Creating “white paper” to capture/expand upon thoughts regarding digital in assessment PRA
- Reviewing and incorporating best practices, recommendations, findings, insights of other projects, such as:
 - Digital operating experience in Korea
 - DI&C operating experience reviews
 - Incorporating DI&C into PRAs
 - Common cause failure (CCF) considerations in decision making
- Defining/developing “use cases,” including cyber security (cases will be used to test hypotheses)

Revise/modify/enhance model

Future...

- Respond to thoughtful challenges to hypotheses
- Test (use cases)
- Reflect operating experience as it becomes available
- Iterate as HAZCADS and related processes are refined

Continuous improvement



Questions?

**Contact Matt Gibson for Further Information
(mgibson@epri.com)
+1 (919) 218-1323**

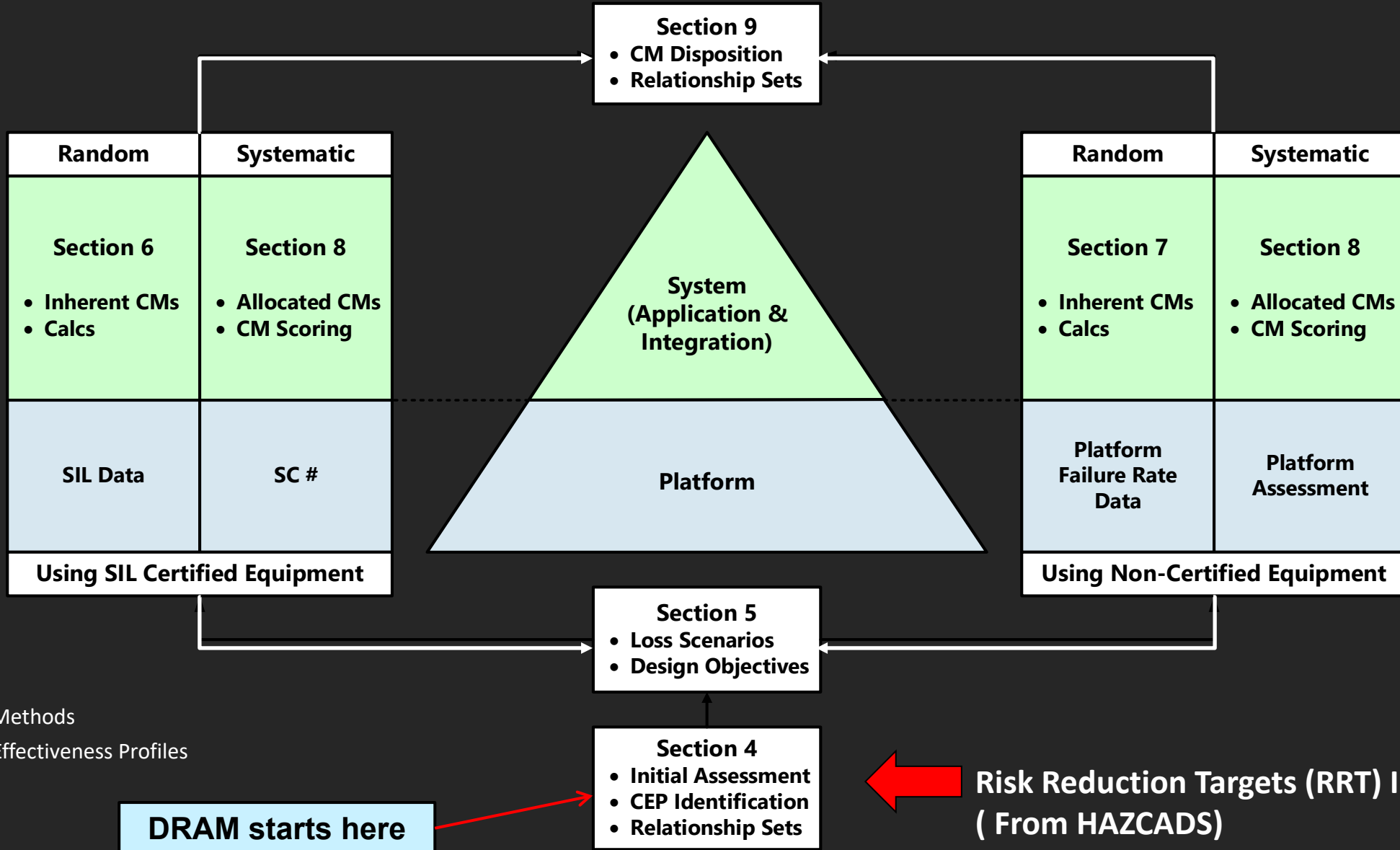
A grayscale photograph of four people, two men and two women, standing in a row. They are all wearing white lab coats with the EPRI logo on the left chest. The woman in the center is also wearing a white hard hat. They are all smiling and looking towards the camera. The background is a plain, light-colored wall.

Together...Shaping the Future of Energy™



Reference Slides

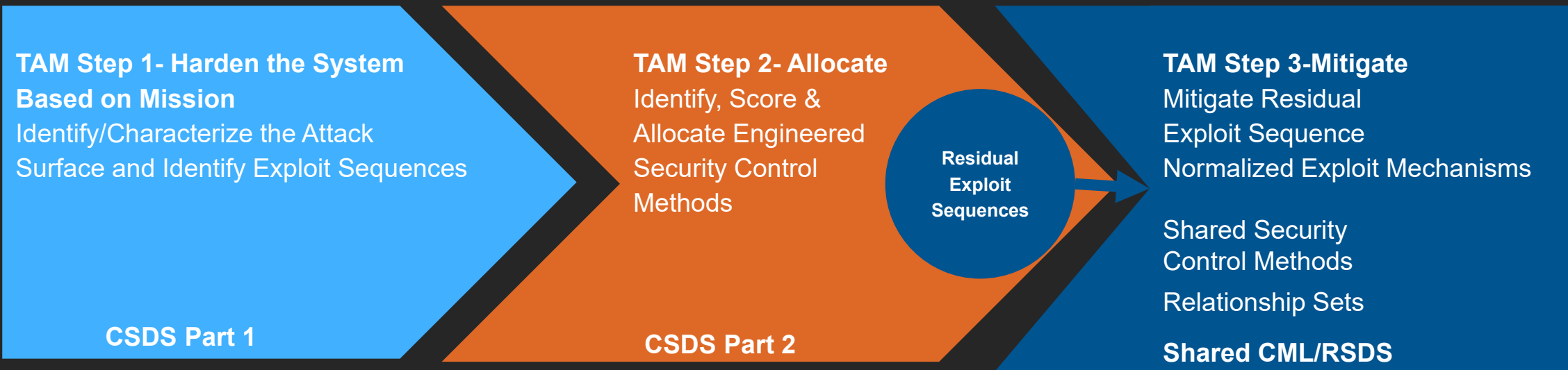
Digital Reliability Assessment Methodology (DRAM) Revision 0



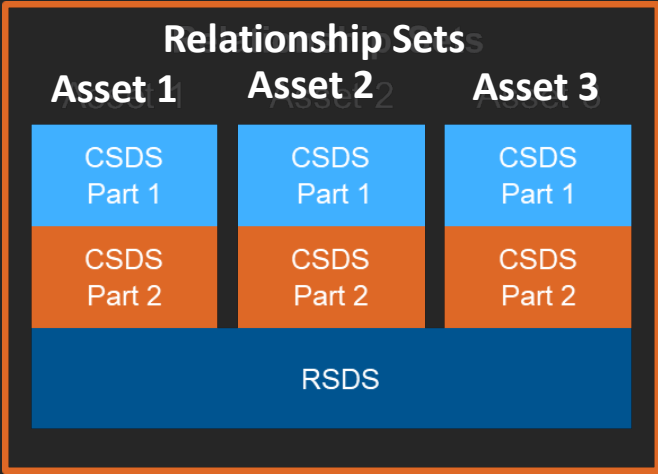
CM= Control Methods

CEP= Control Effectiveness Profiles

EPRI Cyber Security Technical Assessment Method Rev 1(TAM)

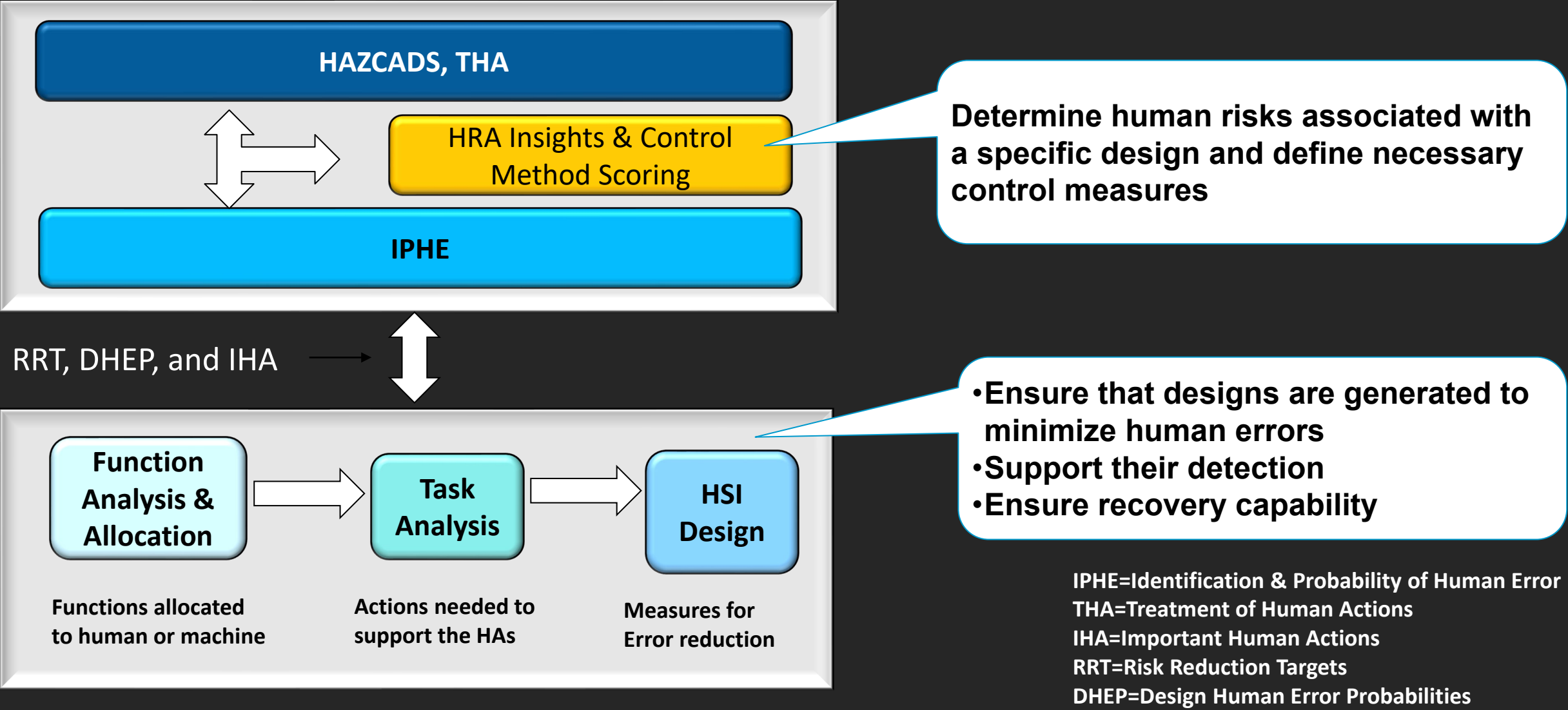


- **Compatible with existing standards and regulations including IEC 62443**
- **Integrated with Supply Chain**
- **Designed to integrate into the overall engineering and design processes, including the DEG.**
- **Leads the transition to sustainable engineering-based cyber assessment/mitigation.**
- **Standardizes the assessment methodology and documentation**



Implementations Underway in US & UAE

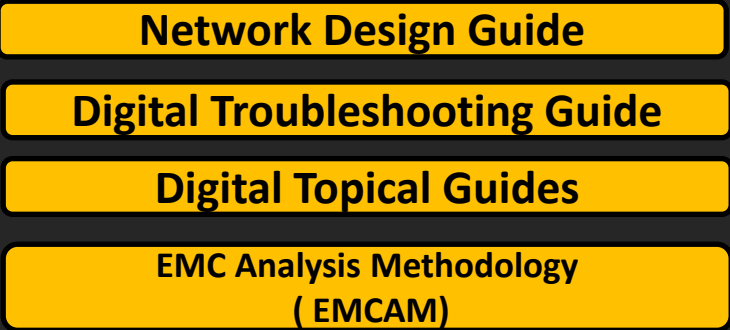
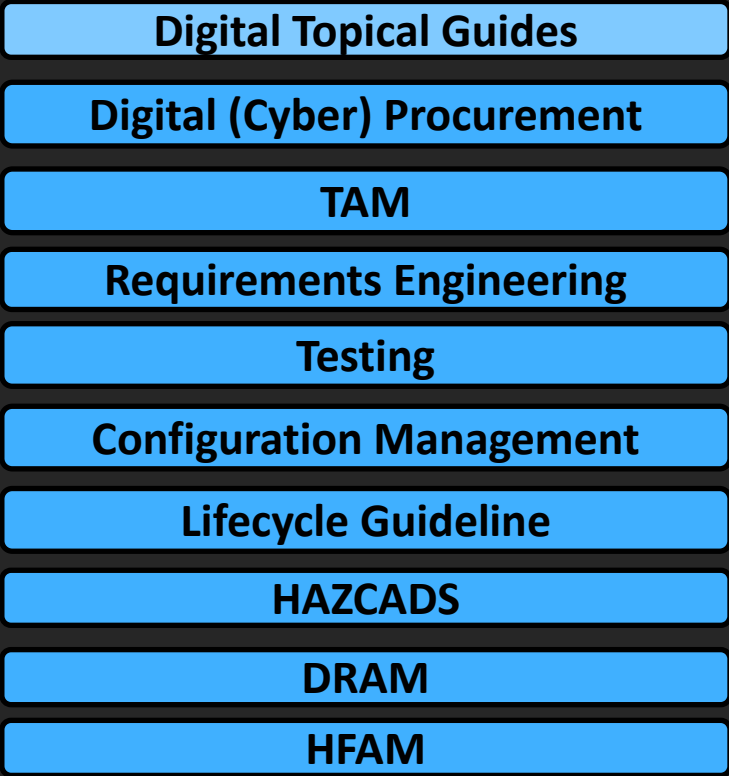
Human Factors Analysis Method (HFAM) Architecture



Integrated Digital Framework Status

In Production

Planned/In Production 2022/2023



- Topical Guides are succinct extensions to the main guides and methods.
- Key topics in the DEG have or will have extended methods/tools
- Uses an integrated risk-informed/performance-based approach that can be used now and expanded in the future

The Integrated Framework is Nearing Full Production

EPRI Workforce Development Strategy for Digital Skills

Nuclear Workforce is Evolving due to Retirements and Economic Re-alignment due to Covid

- Enable the full value of EPRI products and related technology to address the rapidly changing business and regulatory environment.
- **Develop the nuclear workforce worldwide through highly effective training and skills assessments based on EPRI products.**
 - Develop remote delivery methods that provide a compelling “virtual” classroom with as close to the same or possibly better effectiveness as a live classroom.
 - Address the high overhead of student and instructor travel and hosting for both EPRI and Utilities to meet the business needs of members and stakeholders.
 - Conduct digital skills assessments based on published “**Bodies of Knowledge**”(BoK)
- Distance Learning (DL) development was accelerated/validated by COVID-19 travel restrictions.

Expansion and Refinement Ongoing

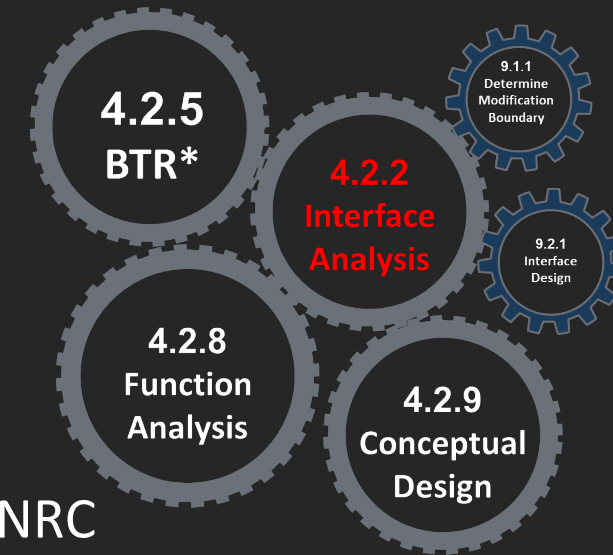
Technology Transfer- Training Product Timeline

2021		2022		2023
DEG 4-day	In Delivery	HAZCADS/DRAM 3-day *RSM collaboration	Available Summer 2022	Digital Reliability Maintenance
Requirements Engineering 2-day	In Delivery	Probabilistic Thinking/IEC-61508 1-day	Available Summer 2022	Network Design
TAM (Cyber) 4-day	In Delivery	Systems Thinking 1-day	Available Summer 2022	Digital Technology for Engineers
Cyber Procurement 1 1/2-day	Ready Now	HFAM 3-day	Available Summer 2022	Digital Testing Strategies and Methods

Expansion and Refinement Ongoing

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/year with max of 24 student/session
 - 500+ students trained in 2020 & 2021 from 13 utilities, 3 EOC's, INPO & NRC
 - Open Enrolment Courses planned for 2022, Custom Sessions are available
 - Contact EPRI/U for course delivery options in 2022



*Bounding Technical Requirements

Part of an Integrated Digital Training Portfolio Supporting Workforce Development

Supplemental Funded: Digital Systems Engineering User Group - 3002022140

A forum for information sharing of digital specific material

- ✓ Operational Experience
- ✓ Lessons Learned
- ✓ Interactive community
- ✓ Common Design Packages
- ✓ Cyber Security Evaluations
- ✓ Member Feedback

ADDITIONAL VALUE

- ✓ Ongoing product maintenance
- ✓ Feedback- driven evolution of the Digital Framework Products (DEG, TAM, HAZCADS, et.al.)
- ✓ Other UG identified digital materials

Spring Meeting Feb 28th –March 1st
(complete)

Fall Meeting August 22nd – 23rd

Current Members to Date

Framatome
Constellation Energy
Dominion Energy South Carolina, Inc.
Dominion Energy, Inc.
Duke Energy Corp.
Entergy Services, Inc.
Evergy Services (Wolf Creek)
Callaway (Ameren)
Palo Verde
Sargent & Lundy Engineers
Southern Company
Tennessee Valley Authority (TVA)
Vistra Corp. (Comanche Peak)
Westinghouse Electric Company, LLC
Xcel Energy

