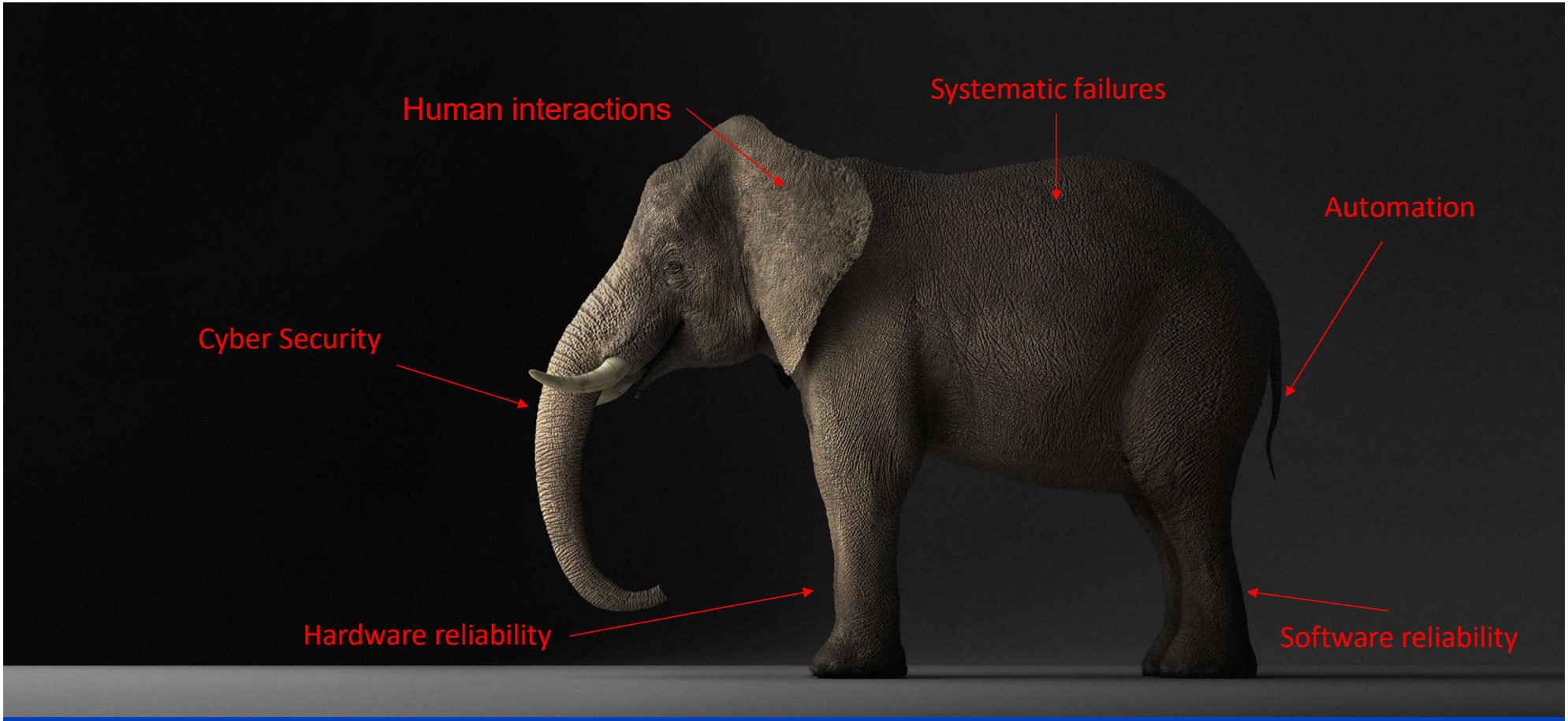
HAZCADS: Hazards and Consequences Analysis for Digital Systems

Mary R. Presley
Technical Executive
EPRI Nuclear Risk & Safety Management

KNS-KAERI STAMP/STPA Workshop
May 17, 2023
Jeju Island, South Korea

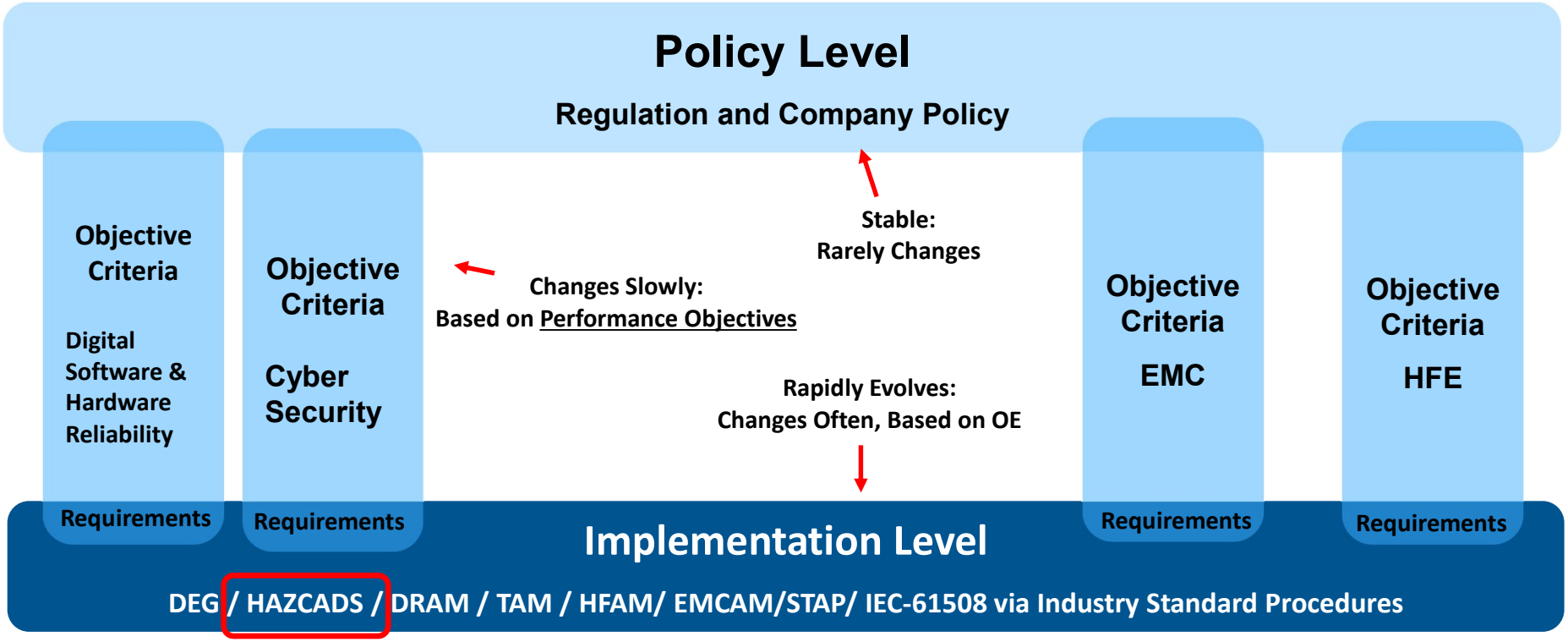
Looking at the Whole Elephant



How to address risks and hazards from various sources in one integrated process

Digital Systems Engineering Framework

Policy Level vs. Implementation Level Activities



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

Performance Objectives provide the Interface between Policy and Implementation. Supports a safety case argument.

EPRI's Digital Framework Elements

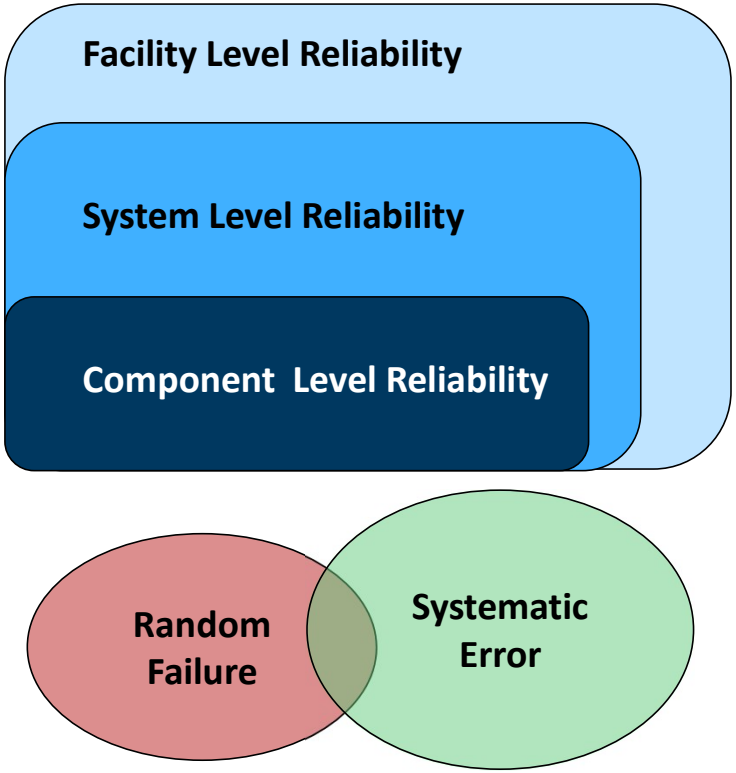
EPRI's ***high-quality engineering process*** uses the same modern methods and international standards used in other safety related industries to reduce implementation cost

Utilize Industry Standards	Use the same proven design and supply chain structures that non-nuclear safety related industries use (IEC-61508/61511/62443). 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 (IEC-15288,IEC-15289, IEC-12207,STPA).
Risk Informed Engineering	Making effective engineering decisions via hazards and risk analysis to integrate all digital engineering topics into a single engineering process. (STPA,FTA)

Capable Workforce

Modern Methods to Support Nuclear Fleet Sustainability and Advanced Reactor Design

Digital Reliability Model



Reliability Axioms

- Common Cause Failures must **first** have a failure or systematic error (including emergent behavior)
- Achieved Systematic and Random Reliability is inversely proportional to the likelihood of a CCF
- Reliability is best achieved via a cost, likelihood, and consequence equilibrium
- Net Functional Reliability is the prime objective (at the system/facility level)
- Focused Models can provide actionable reliability Insights (FTA, STPA, Relationship Sets)

- **Total Reliability is an Equipment Level Challenge**
- **Total Reliability is a Lifecycle Challenge**

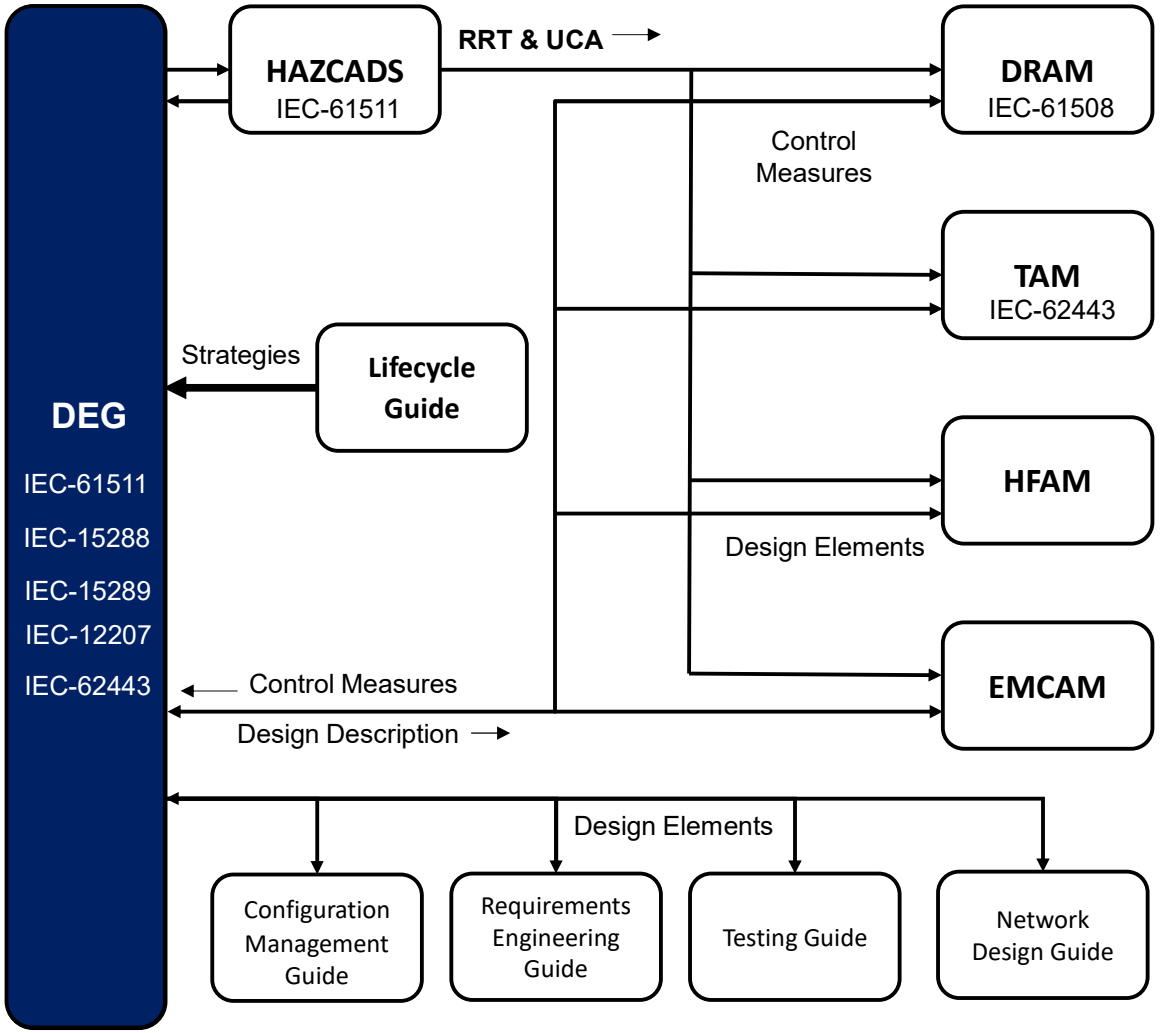
Use of Models for Engineering within the Framework

- The Digital Engineering Framework Currently leverages seven distinct models:

Model	Question to be Answered
Systems Engineering	What are the key systems elements, the functional allocation of those elements, and what is the reliability of those elements?
Fault Trees	What are the Risk Sensitivities within a Dependency Scope
STPA	What are the Systematic Hazards and Pathways? HAZCADS
Relationship sets	What are the system element dependencies and degree of independence across multiple relationships?
HRA	What is the reliability of Human Actions?
Exploit Sequences	What are the exploit objectives, pathways to those objectives, and the method of exploit?
Hardware Reliability Analysis	What are the failure frequencies that impact Probability of failure on demand-PFD

- EPRI continues to leverage or develop additional models as the “questions” become better defined.
- Performance based design requires the design questions to be defined and bounded.

To be useful, model must answer a key question



DEG –Synthesizes the Systems Engineering framework from IEC-15288. Includes all relevant Lifecycle topics. Takes strategic input from the Lifecycle guide

HAZCADS –Uses STPA/FTA to identify hazards and associated UCA . FTA and Risk Matrices develop a Risk Reduction Target (RRT) which informs the downstream processes. Implements a PHA/LOPA from IEC-61511.

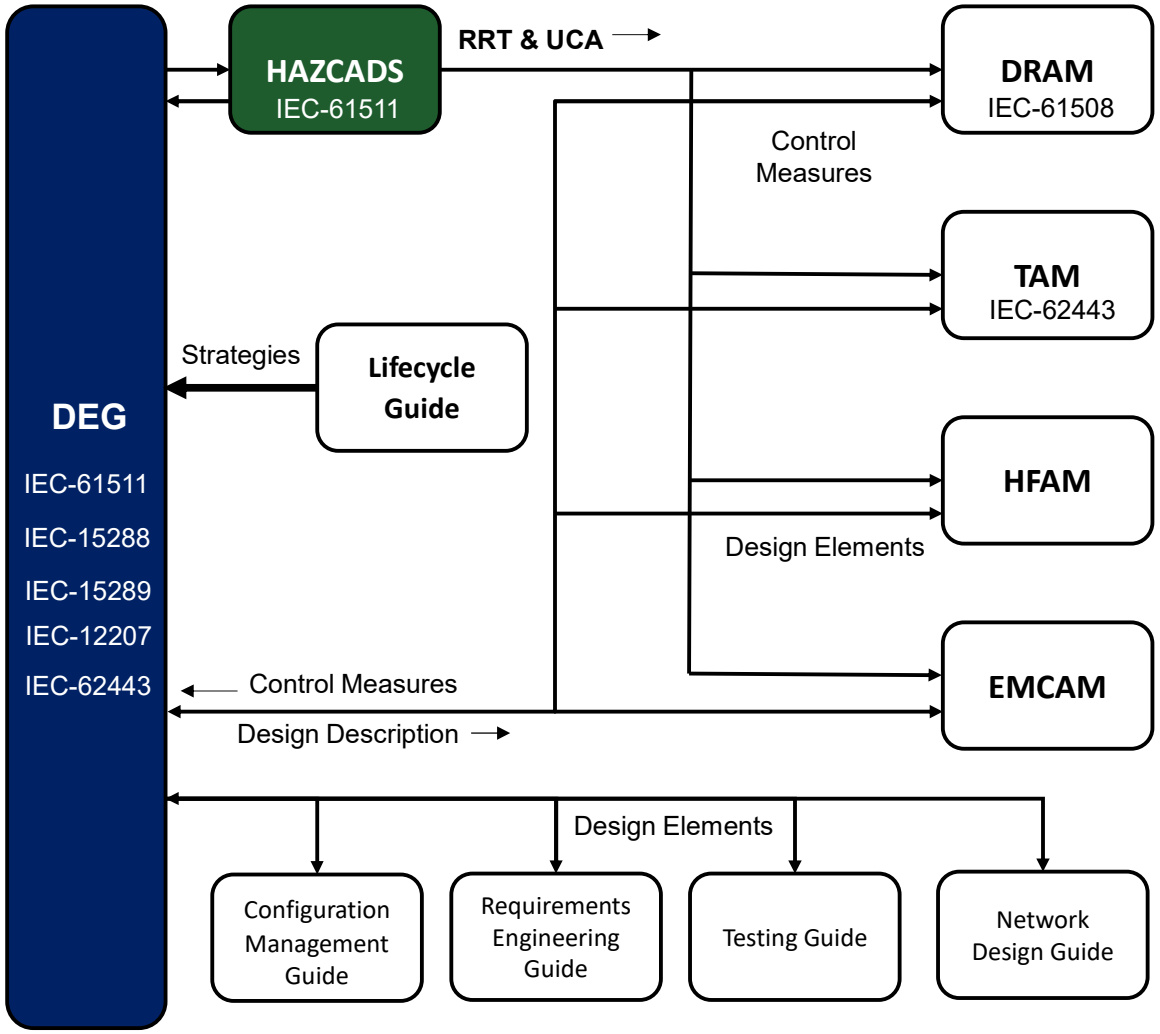
DRAM – Identifies Hardware and Software reliability Vulnerabilities and develops loss scenarios. Develops and Scores protect, detect , and respond/recover control measures using the RRT

TAM –Identifies cyber security vulnerability classes. Develops Exploit Sequences. Develops and Scores protect, detect , and respond/ recover control measures using the RRT

HFAM – Develops human actions and interfaces. Identifies and scores Human Reliability using the RRT

EMCAM – Identifies EMC vulnerability classes. Develops and scores protect, detect , and respond/ recover control measures using the RRT

RRT= Risk Reduction Target STPA=System Theoretic Process Analysis LOPA= Layers of Protection Analysis
UCA= Unsafe Control Action FTA= Fault Tree Analysis EMC= Electromagnetic Compatibility



DEG –Synthesizes the Systems Engineering framework from IEC-15288. Includes all relevant Lifecycle topics. Takes strategic input from the Lifecycle guide

HAZCADS –Uses STPA/FTA to identify hazards and associated UCA . FTA and Risk Matrices develop a Risk Reduction Target (RRT) which informs the downstream processes. Implements a PHA/LOPA from IEC-61511.

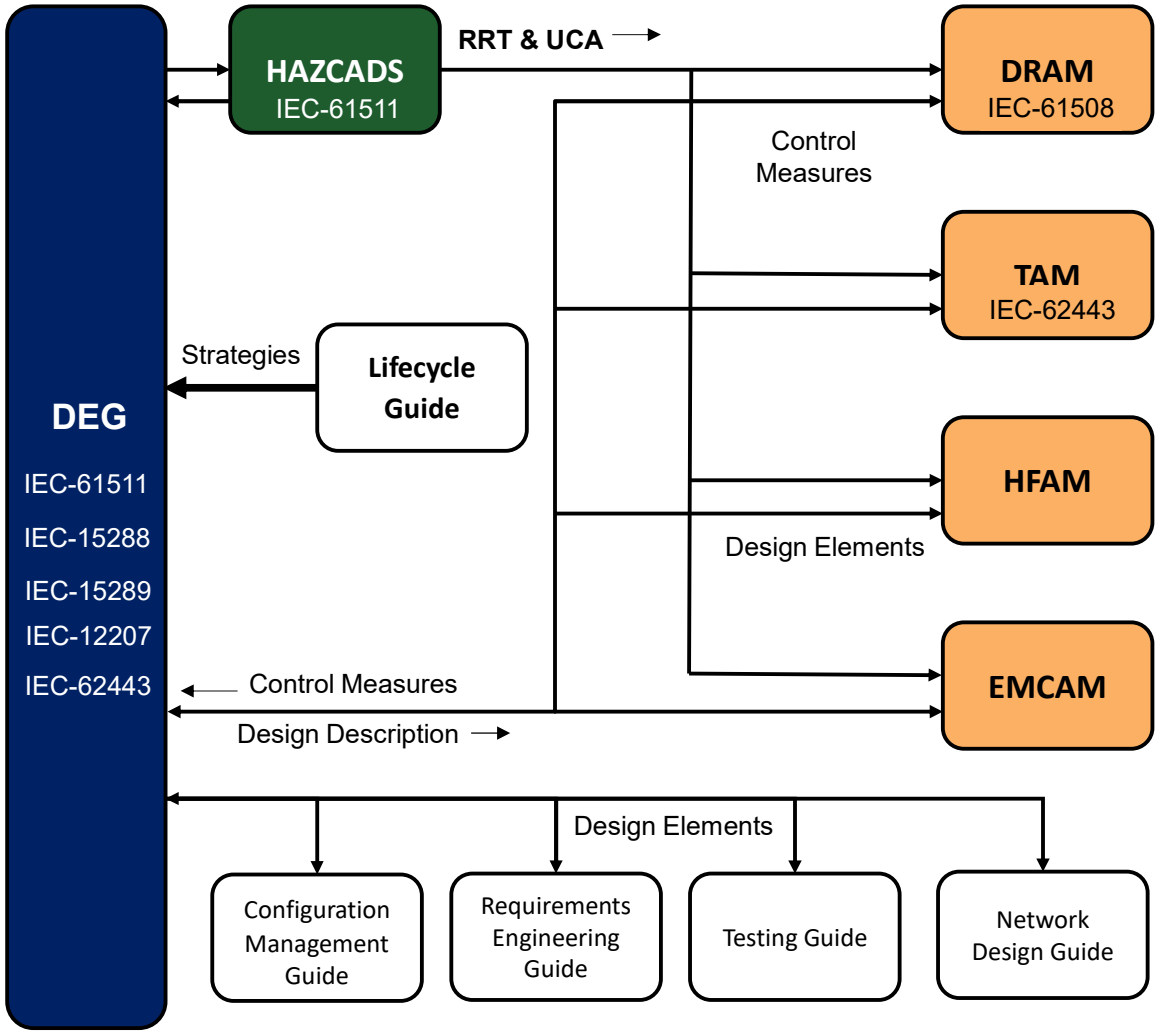
DRAM – Identifies Hardware and Software reliability Vulnerabilities and develops loss scenarios. Develops and Scores protect, detect , and respond/recover control measures using the RRT

TAM –Identifies cyber security vulnerability classes. Develops Exploit Sequences. Develops and Scores protect, detect , and respond/ recover control measures using the RRT

HFAM – Develops human actions and interfaces. Identifies and scores Human Reliability using the RRT

EMCAM – Identifies EMC vulnerability classes. Develops and scores protect, detect , and respond/ recover control measures using the RRT

RRT= Risk Reduction Target
UCA= Unsafe Control Action
STPA=System Theoretic Process Analysis
FTA= Fault Tree Analysis
LOPA= Layers of Protection Analysis
EMC= Electromagnetic Compatibility



DEG –Synthesizes the Systems Engineering framework from IEC-15288. Includes all relevant Lifecycle topics. Takes strategic input from the Lifecycle guide

HAZCADS –Uses STPA/FTA to identify hazards and associated UCA . FTA and Risk Matrices develop a Risk Reduction Target (RRT) which informs the downstream processes. Implements a PHA/LOPA from IEC-61511.

DRAM – Identifies Hardware and Software reliability Vulnerabilities and develops loss scenarios. Develops and Scores protect, detect , and respond/recover control measures using the RRT

TAM –Identifies cyber security vulnerability classes. Develops Exploit Sequences. Develops and Scores protect, detect , and respond/ recover control measures using the RRT

HFAM – Develops human actions and interfaces. Identifies and scores Human Reliability using the RRT

EMCAM – Identifies EMC vulnerability classes. Develops and scores protect, detect , and respond/ recover control measures using the RRT

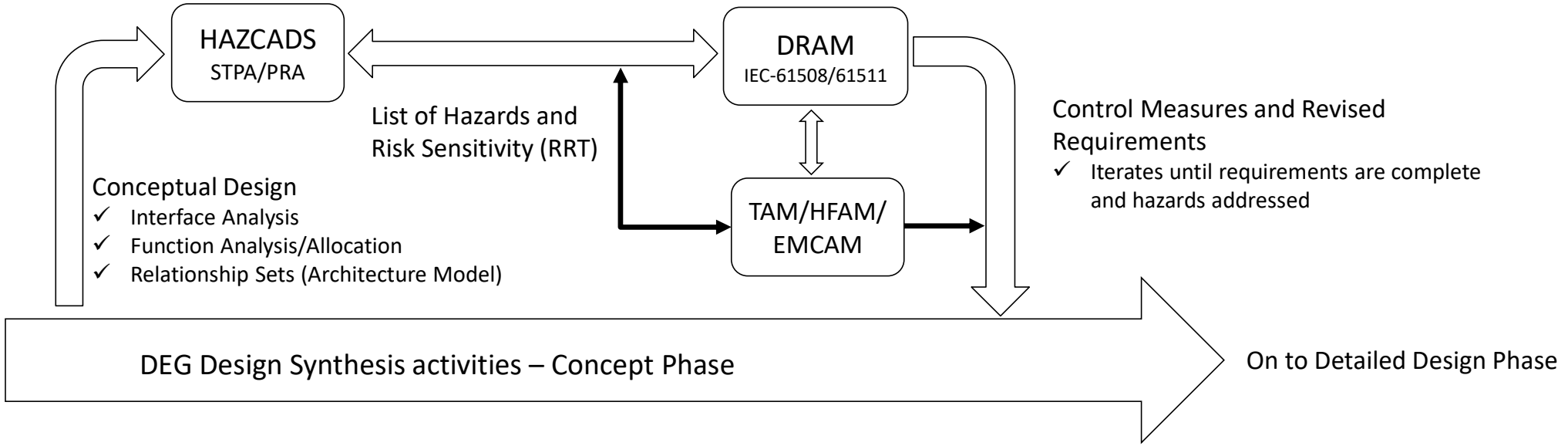
RRT= Risk Reduction Target
UCA= Unsafe Control Action
STPA=System Theoretic Process Analysis
FTA= Fault Tree Analysis
LOPA= Layers of Protection Analysis
EMC= Electromagnetic Compatibility

Workflow- Conceptual Phase

Diagnostic Process to Identify Digital Hazards & Risk Sensitivities and Refine Requirements

Models System and Plant level Hazards and criticality (Risk Sensitivity)

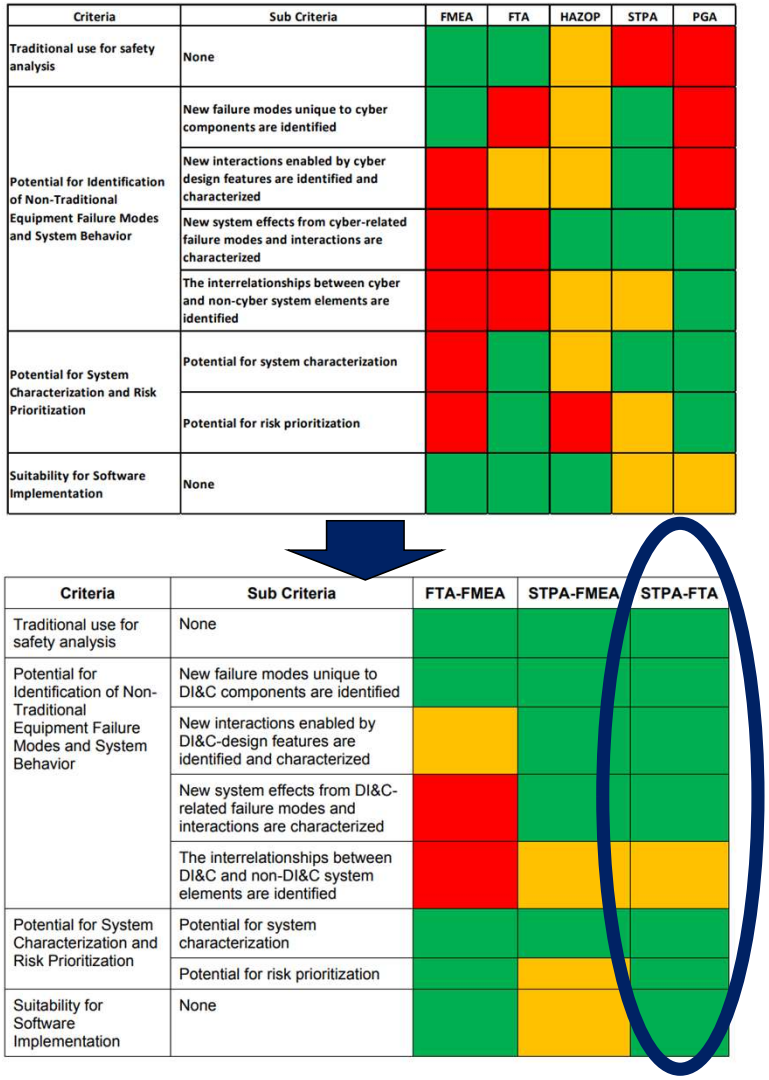
Identifies Hardware, Software, and Human Reliability Vulnerabilities and Mitigations associated with Hazards



Risk-Informed Decision Making for Digital I&C

Choosing a Hazard Analysis Method

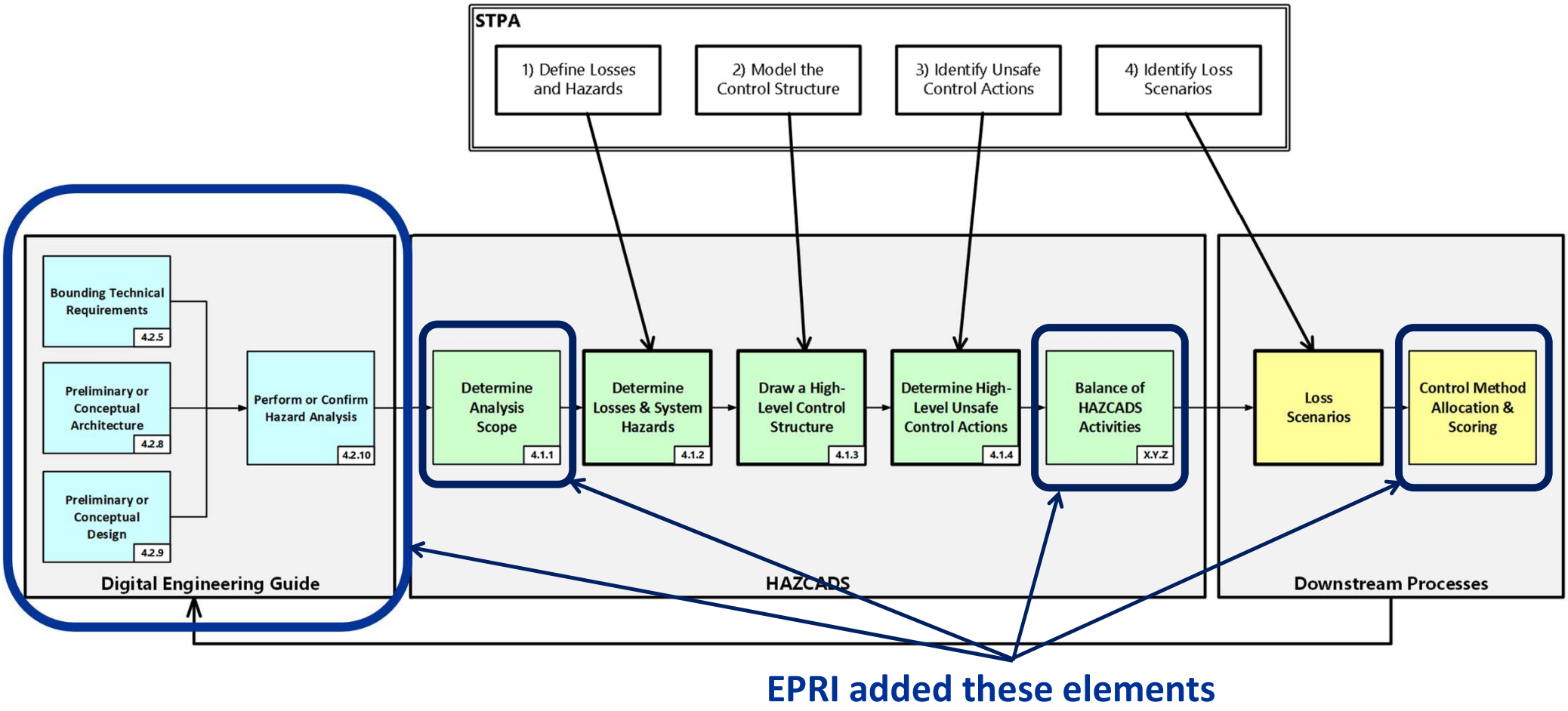
- **HAZCADS evolved from analysis, experimentation, and testing to find an effective methods or combination of methods that would provide usable hazard insights for the design process**
- Comparative analysis and testing concluded:
  - STPA showed the most promise in terms of a holistic approach to diagnosing the systematic errors of a nuclear plant and the related controls.
  - While STPA is strong in many areas it:
    - does not diagnose component level reliability failures
    - does not prioritize or rank the importance of the identified UCA's
    - Is not a design synthesis tool but rather a design diagnostic tool
- EPRI has integrated STPA with a Systems Engineering based design process that achieves design synthesis that can then be analyzed by STPA via HAZCADS.
- HAZCADS combines the results of STPA and FTA to provide risk-informed prioritization of UCA's and the associated loss scenarios.
- Loss scenarios are limited to topical areas of interest which reduces combinatorial growth. This insight is combined with reliability analysis and relationship analysis to fully develop control measures that address each loss scenario.

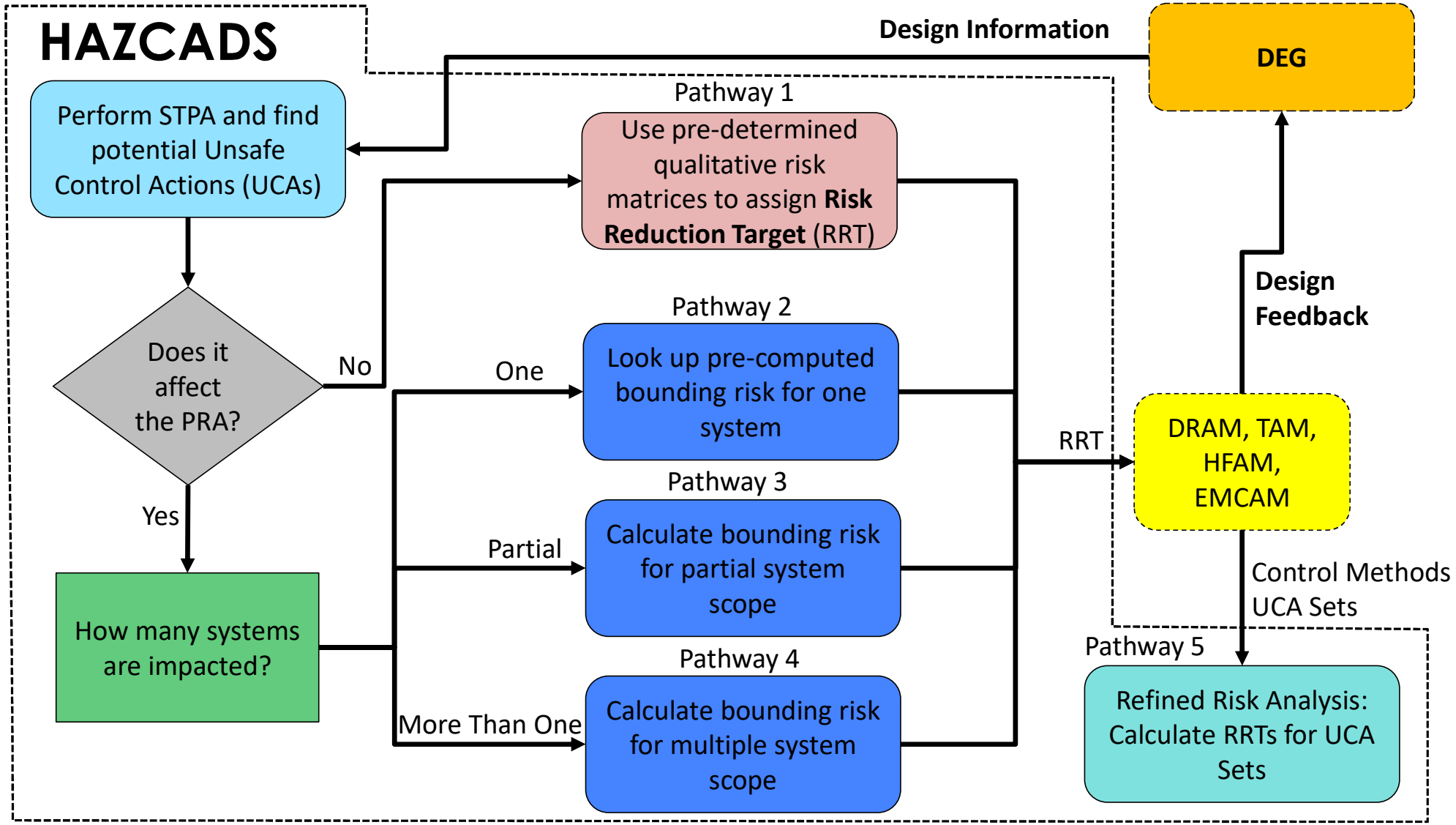


Criteria	Sub Criteria	FMEA	FTA	HAZOP	STPA	PGA
Traditional use for safety analysis	None					
Potential for Identification of Non-Traditional Equipment Failure Modes and System Behavior	New failure modes unique to cyber components are identified					
	New interactions enabled by cyber design features are identified and characterized					
	New system effects from cyber-related failure modes and interactions are characterized					
	The interrelationships between cyber and non-cyber system elements are identified					
Potential for System Characterization and Risk Prioritization	Potential for system characterization					
	Potential for risk prioritization					
Suitability for Software Implementation	None					

Criteria	Sub Criteria	FTA-FMEA	STPA-FMEA	STPA-FTA
Traditional use for safety analysis	None			
Potential for Identification of Non-Traditional Equipment Failure Modes and System Behavior	New failure modes unique to DI&C components are identified			
	New interactions enabled by DI&C-design features are identified and characterized			
	New system effects from DI&C-related failure modes and interactions are characterized			
	The interrelationships between DI&C and non-DI&C system elements are identified			
Potential for System Characterization and Risk Prioritization	Potential for system characterization			
	Potential for risk prioritization			
Suitability for Software Implementation	None			

STPA Implementation in the EPRI Framework





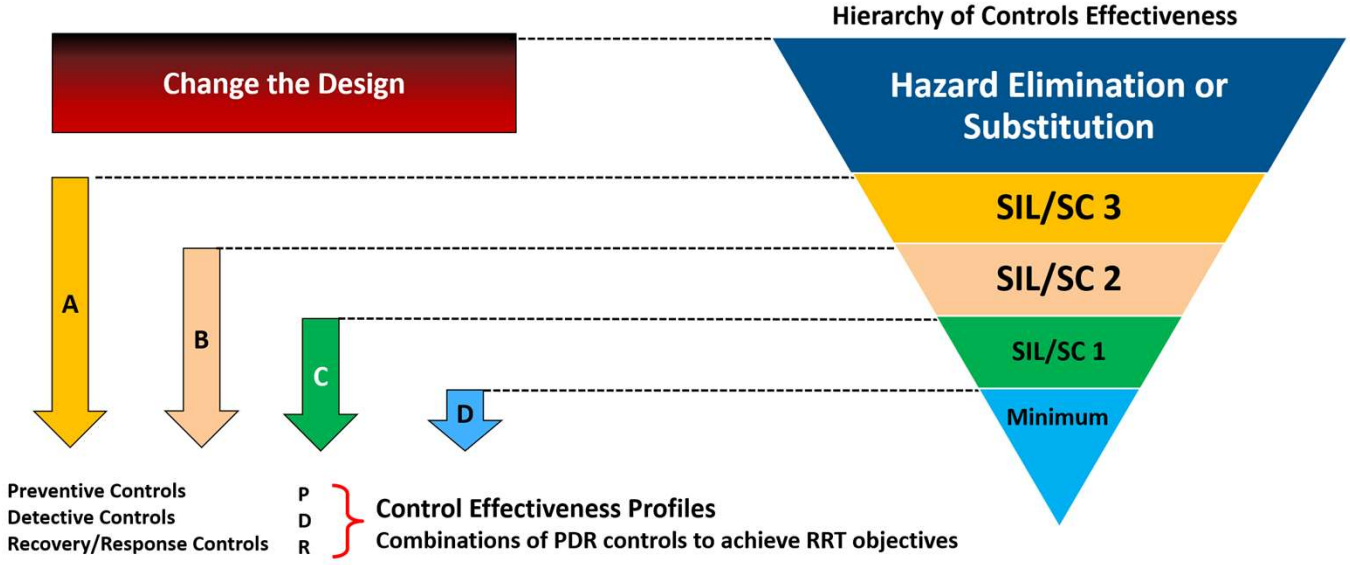
Risk Ranking

- HAZCADS uses a bounding risk assessment process, when the risk is calculated quantitatively through a PRA model
  - This approach evaluates all failures including any common cause (not just software common cause failures)
- The risk sensitivity assessment is based on the change in risk if the UCAs occurred, providing prioritization to the UCA

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

Control Methods

- DRAM, TAM, HFAM, and EMCAM:
  - Determine causal factors for the UCAs
  - Establish control methods that are aimed at addressing those causal factors
  - Score the control methods against the RRT from HAZCADS
- These control methods may impose new design requirements or add implementation requirements on the system



Systems Thinking requires a Cultural Shift

- Systems Thinking is the key skill required to use Systems Engineering and STPA
- It is multidisciplinary and requires teamwork
- Requires ability to see system relationships in a holistic manner
- Ability to communicate across disciplines
- Ability to understand complexity

Matt Gibson
HAZCADS/DEG
I&C Engineering

Stephen Lopez
EMCAM
I&C Engineering

Cristina Corrales
HFAM
I&C Engineering

Matt Gibson
HAZCADS
Risk & Safety Management

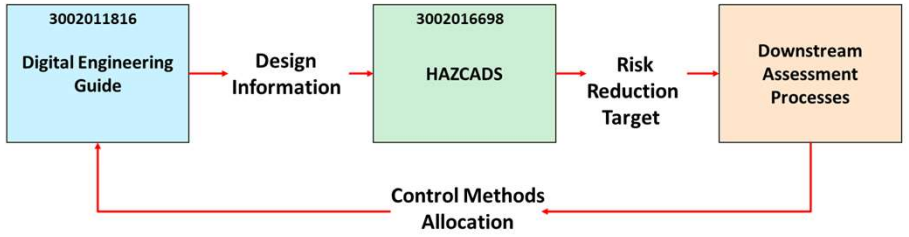
Paul Martyak
TAM
I&C Engineering

Mary Presley
HFAM/Digital PRA & HRA
Risk & Safety Management

Conclusion

- STPA has proven to be an effective systems diagnostic tool in EPRI conducted tests and experiments. This correlates well with feedback outside the nuclear industry
- When integrated into a complete systems engineering process, STPA plays a vital role in ensuring new designs and modifications behave in a safe and desirable way.
- Shifts in organizational work culture and thinking are required for an effective implementation.
- **EPRI continues to improve the Digital Systems Engineering Framework with a new release in the Spring of 2024**.
- Pilot training is being developed to support widespread implementation.

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.
Technical Assessment Methodology (TAM)	3002012752
Digital Reliability Assessment Methodology (DRAM)	3002018387
Electromagnetic Compatibility Assessment Methodology (EMCAM)	3002023743 (Fall 2023)
Human Factors Analysis Methodology (HFAM)	3002018392

EPRI Contacts for further discussion

Matt Gibson: mgibson@epri.com
Mary Presley: mpresley@epri.com
John Weglian: jweglian@epri.com

Status Of HAZCADS in the US

- The following slides from the Nuclear Energy Institute provide the current state of regulatory modernization in this area

Common Cause Failure

- Current policy is outdated (issued 1993) and does not account for risk-informed approaches
- NEI submitted a new approach to addressing digital I&C common cause failure (i.e., NEI 20-07) which proposed HAZCADS/DRAM as a method; however, it did not comply with the existing policy.
- NEI provided industry input to develop a new policy. NRC staff issued a recommendation to expand the existing policy to allow for the use of risk-informed approaches in SECY-22-0076.
- NEI and NRC are aligned on the 3 out of 4 policy points but have differing perspectives on the necessity for additional backup displays and manual controls in the Main Control Room (MCR).
    - NEI continues to advocate for the elimination of prescriptive policy requirements for additional backup displays and manual controls in the MCR without an engineering basis.
- Commission direction is required prior to advancing the review of NEI 20-07. The new SECY is currently in review by the Commission and an SRM is expected soon

Link to SECY-22-0076 https://www.nrc.gov/docs/ML2216/ML22164B003.pdf
Link to SECY-93-087 https://www.nrc.gov/docs/ML0037/ML003708021.pdf

Commercial Grade Dedication

- Regulatory Guide 1.250 released October 2022 endorsing NEI 17-06 Rev. 1
- Process allows for the use of specific product certification to meet digital technology commercial grade dedication requirements
- NEI and NUPIC are establishing a Memorandum of Understanding for ongoing oversight activities on behalf of the industry
- Key Results
  - Expand supply chain for safety-related commercial-off-the-shelf components certified to IEC-61508
  - Reduce burden for digital technology commercial grade dedication

