2026 EPRI Update

NEI Cyber Security Workshop

Matt Gibson – Senior Technical Executive
Plant Reliability and Resilience
March 24th 2026

PRR: Instrumentation & Control

MISSION

To provide industry leading tools, technologies, methods, and knowledge transfer, that support the implementation of modern information and operational technologies in both new and existing facilities.

Our goal is to advance system reliability and performance through direct engagement and research developed with a strong technical basis and demonstrated efficacy.

EXECUTION

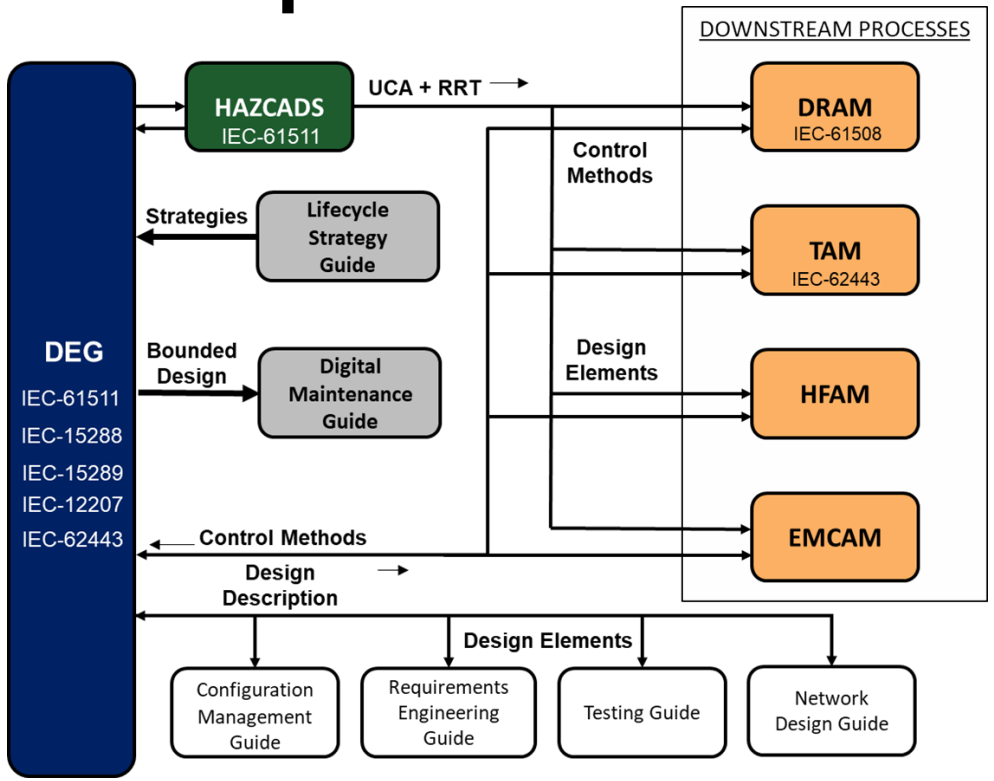
This mission achieved through…

- Use of modern international, industry standards
- Demonstration of new technologies and risk-informed methods and processes
- Advances in knowledge transfer and training to support rapidly and continuously changing technology

Together…Shaping the Future of Energy®

Digital Systems Engineering Framework Update

- Latest revisions to the Framework Guides released in November 2025
  - The guides ensure structured thinking and are not procedures.
- Industry feedback incorporated to improve usability
- Updated to the latest insights from standards and processes



- **The framework is now free and public to facilitate wide usage and availability.**
  - TAM R2 structured into Pathways and Activities similar to other Framework guides.
  - Leverages DEG activities for baseline and data flows.

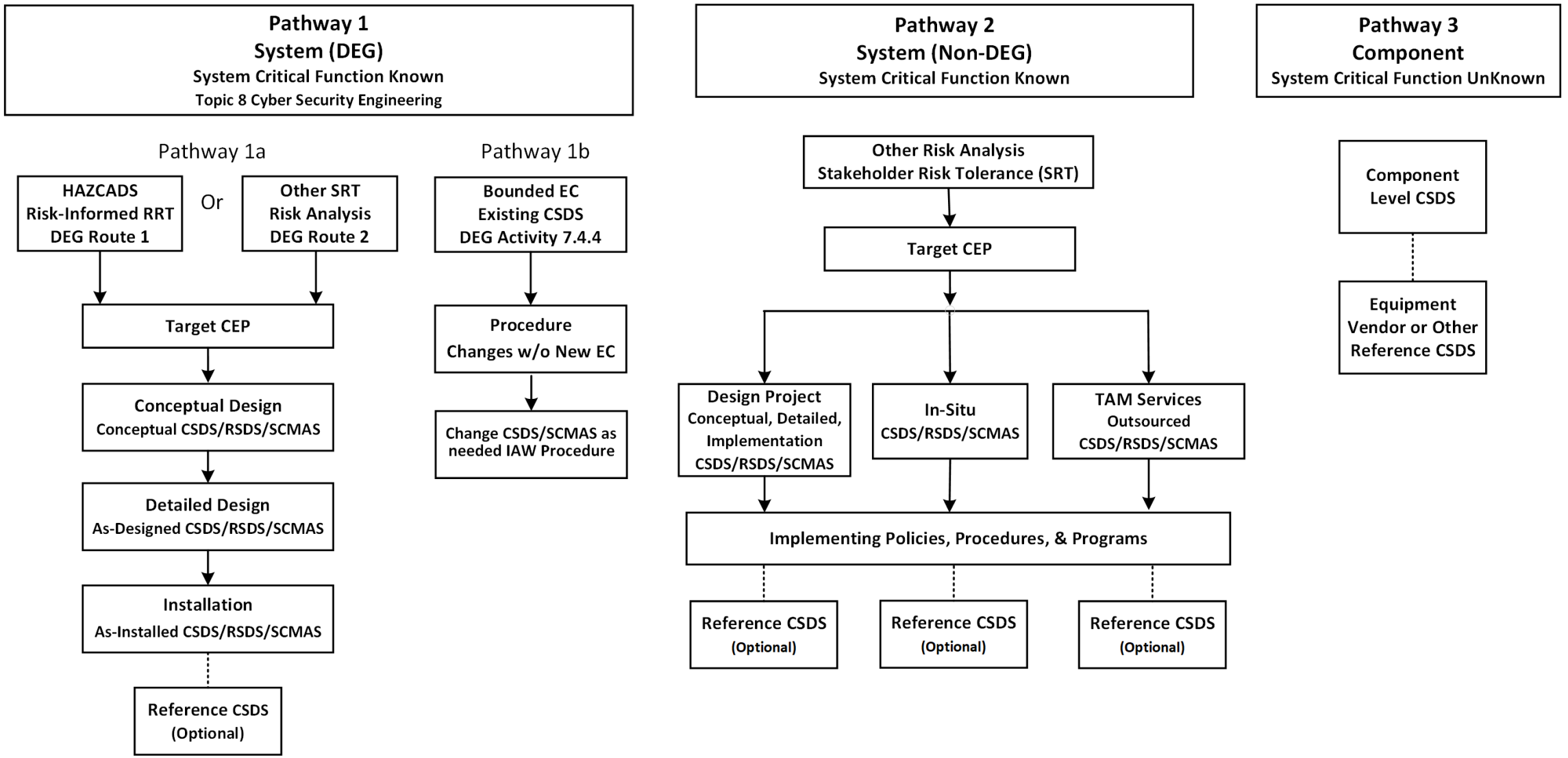
DEG and TAM implement Cyber Informed Engineering

The Digital Systems Engineering Framework Guides

Year	Product ID	Title	Item Type	Completion Date	Deliverable Status
2025	**3002031207**	**Cyber Security Technical Assessment Methodology (TAM)-Risk Informed Exploit Sequence Identification and Mitigation: Revision 2**	**Guide**	**11/1/2025**	**Published**
2025	3002031208	Network Design Guide (NDG)- Use Case Based Approach for Operational Technology (OT) Networks: Rev 1	Guide	11/1/2025	Published
2025	3002031209	Digital Maintenance and Management Guide (DMG): Revision 0	Guide	11/1/2025	Published
2025	3002031210	Digital Systems Configuration Management Guide (DCMG): Revision 1	Guide	11/1/2025	Published
2025	3002031211	Digital Systems Requirements Engineering Guide (DREG): Revision 1	Guide	11/1/2025	Published
2025	3002031212	Digital Systems Testing Strategies and Methods (DTS): Revision 1	Guide	11/1/2025	Published
2025	3002031213	Digital IC Lifecycle Strategy Guide (DLSG): Revision 2	Guide	11/1/2025	Published
2025	3002031215	Human Factors Analysis Methodology (HFAM) for Digital Systems- A Risk-Informed Approach to Human Factors Engineering: Revision 1	Guide	11/1/2025	Published
2025	3002031216	Digital Reliability Analysis Methodology (DRAM): Revision 1	Guide	11/1/2025	Published
2025	3002031217	Hazards and Consequence Analysis for Digital Systems (HAZCADS): Revision2	Guide	11/1/2025	Published
2025	3002031218	Digital Engineering Guide (DEG) - Decision Making Using Systems Engineering: Revision 1	Guide	7/30/2025	Published

11 Harmonized and Updated Guides Publicly Available - EMCAM R1 will be added in 2026

TAM R2 Pathways for Systems and Components



TAM Revision 2 Activities

TAM Initial Implementation
1: Incorporate the TAM into the Cyber Security Program
2: Assign and train resources
3: Determine Risk Analysis Methods
4: Develop and Score Shared Control Method Library
5: Determine Normalized Exploit Mechanisms (NEM)

	Pathway Activities			
	System (DEG)		System (Non-DEG)	Component
	Path 1a	Path 1b++	Path 2	Path 3
Activity 1: Screen for TAM Pathway				
1.1: Screen for TAM Pathway				
Activity 2: Bound Scope and Identify Asset Characteristics				
2.1: Bound Assessment Scope				
2.1.1: Determine Asset Composition	From DEG		x	x
2.1.2: Identify Hardened Baseline Configuration (Optional)	From DEG		x	x
2.1.3: Determine Asset Decomposition and TIA Level	From DEG		x	x
2.1.4: Identify Relationship Sets	From DEG		x	
2.1.5: Identify the Data Flow	From DEG		x	*
2.1.6: Identify Critical Data At-Rest & In-Transit	From DEG		x	*
2.2: Identify Detailed Configuration				
2.2.1: Identify Firmware Version, Update Method, & Update Control Measures	From DEG		x	x
2.2.2: Identify OS Version, Update Method, & Update Control Measures	From DEG		x	x
2.2.3: Identify App Software Version, Update Method, & Update Control Measures	From DEG		x	x
2.2.4: Identify Physical Communication Ports and Terminals	From DEG		x	*
2.2.5: Identify Removable Media and/or Portable Devices Used in Asset O&M	From DEG		x	*
2.2.6: Identify HMI Capabilities	From DEG		x	*
2.2.7: Identify Data Communication Protocols	From DEG		x	*
2.2.8: Identify Logical Ports & Services	From DEG		x	*
2.2.9: Identify Data Files and Software Objects	From DEG		x	*
2.2.10: Determine if Third Party Software can be Installed	From DEG		x	x
2.2.11: Identify Asset Site Characteristics (Tailored CSDS)	From DEG		x	Optional
2.2.12: Search Vulnerability Databases for Published Vulnerabilities	From DEG		x	x
2.2.13: Verify and Establish Configuration Control	From DEG		x	x
2.3: Identify Potential Control Measures				
2.3.1: Identify Unused Features and Functions that can be Disabled or Blocked	From DEG		x	x
2.3.2: Identify Access Control and Authentication Capabilities	From DEG		x	x
2.3.3: Identify Event/Alert/Audit Log Capabilities	From DEG		x	x
2.3.4: Identify Backup & Restore Capabilities	From DEG		x	x
2.3.5: Identify Vendor Security Advisory & Patch Program	From DEG		x	x
2.3.6: Identify Vendor Supply Chain Cyber Security Program	From DEG		x	x
2.3.7: Identify Vendor Product/Company Security Certifications	From DEG		x	x
2.3.8: Identify Other Asset Capabilities that are Potential Control Measures	From DEG		x	x
Activity 3: Characterize the Attack Surface				
3.1: Identify Attack Pathways	x		x	*
3.2: Identify Exploit Sequences	x		x	*
Activity 4: Identify, Score, and Allocate Engineered Control Methods				
4.1: Identify and Score Engineered Control Methods	x		x	*
4.2: Determine Target CEP from Risk Analysis Input	x		x	*
4.3: Allocate Engineered Control Methods	x		x	Optional
Activity 5: Mitigate Residual Exploit Sequences				
5.1: Allocate Shared Control Methods to Residual Exploit Sequences (Achieved CEP)	x		x	
5.2: Feedback to Program and Procedure Implementation	From DEG		x	*

"From DEG" indicates that engineering analysis is performed in the DEG with results passed to the TAM.

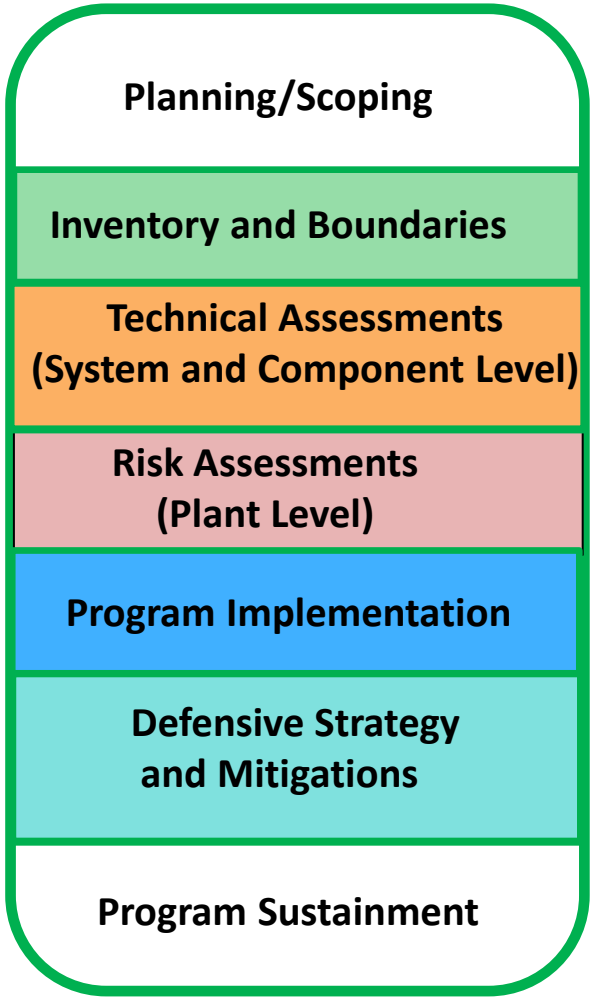
* May be Postulated

++ Performed by Procedure

TAM Revision 2 Activities

DEG provides the information needed for all of Activity 2 and Activity 5.2 in Pathway 1a.

Cyber Security Program Development Guide



- **Risk Informed** - Guideline to develop cost-effective cybersecurity programs using risk-informed, performance-based approaches
- **Regulator Agnostic** - and internationally applicable
- **International Standards** - Leverage international standards
- **Engineering Integration**- Integrate cybersecurity activities within an engineering framework that leverages the EPRI Digital Engineering Guide (DEG)
- **Reactor Agnostic-** Supports New Build reactors with non-traditional use cases and current Legacy Reactors doing major digital upgrades.
- **NEI 08-09/RG 5.71 Replacement** - Supports current Generation III major digital upgrades, fully or partially replaces existing programs.

Global Industry Workshops in Planning for Late Q2, publish Q1 2027

Available Framework Training and Pilot Offerings

Key Workforce Development Tools

HAZCADS/DRAM

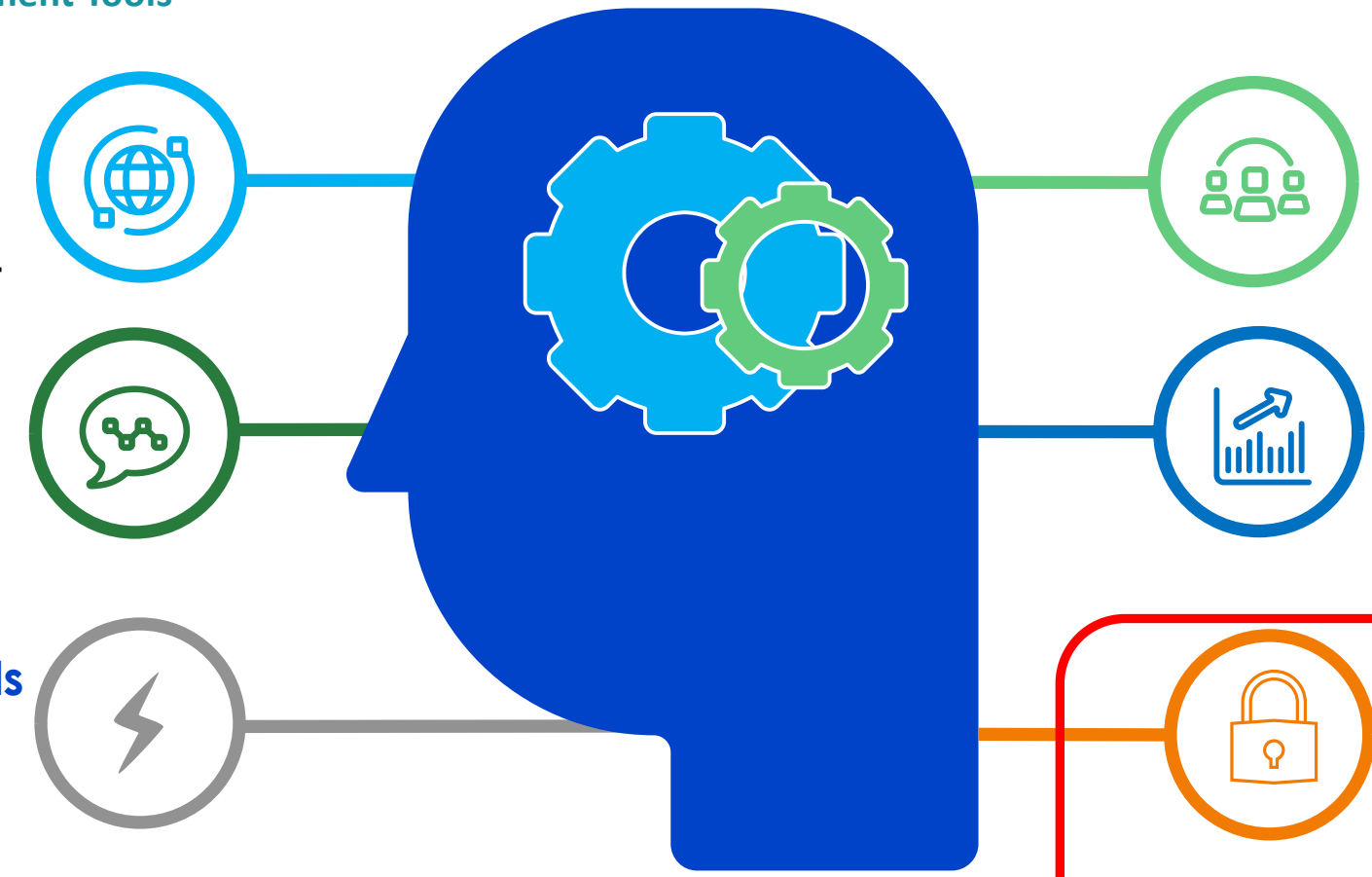
Training Bundle includes STPA and e-learnings
Developed and ready for delivery

HFAM R1*

Integrates HRA and HFE fundamentals into the DEG/HAZCADS process
Pilot in Q2 2026

EMC Fundamentals

Review foundational principles including coupling, grounding, filtering, shielding, etc.



DEG R1 for Practitioners

Developed with 8 sessions delivered in 2025.

DEG R1 for Managers & Auditors

Brings the DEG into focus for managers and auditors. Strong industry need.

TAM Rev 2 Pilot

Adds pathways and integrates cyber security more with the EPRI Digital Framework. Pilot completed in Q1 2026. Production in Q2

EPRI's training is now mixed mode to achieve better results at less cost

***Participants needed for HFAM pilot offering in Q2**

TOGETHER…SHAPING THE FUTURE OF ENERGY®

www.epri.com