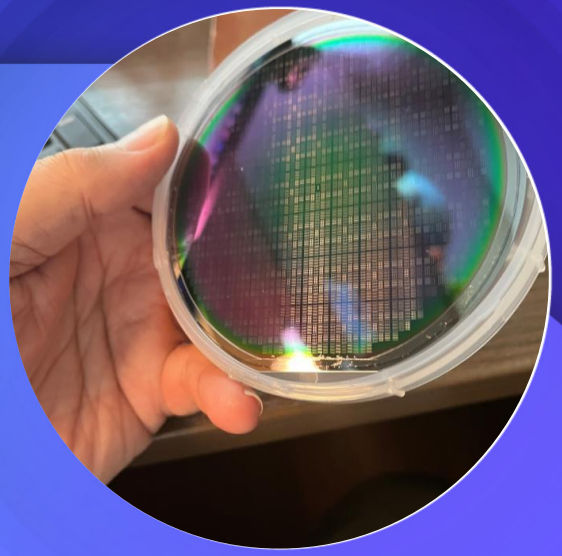
Digital Obsolescence Management

EPRI OT Products and Processes



Jason Castro, Principal Technical Leader
Marc H. Tannenbaum, Principal Technical Executive

Poland Ministry of Industry – Clean Energy Center Workshop on Nuclear Procurement
December 2-4, 2025

Obsolescence for Digital Systems/Components

Obsolescence of equipment has been a significant concern due to the extended life spans of nuclear generation facilities. This is further complicated by the lifecycles of digital components as compared to other analog devices.

Mitigating actions to address the shorter lifecycles of digital components must be taken into account, especially when considering the long system design and implementation processes associated with nuclear plant systems.

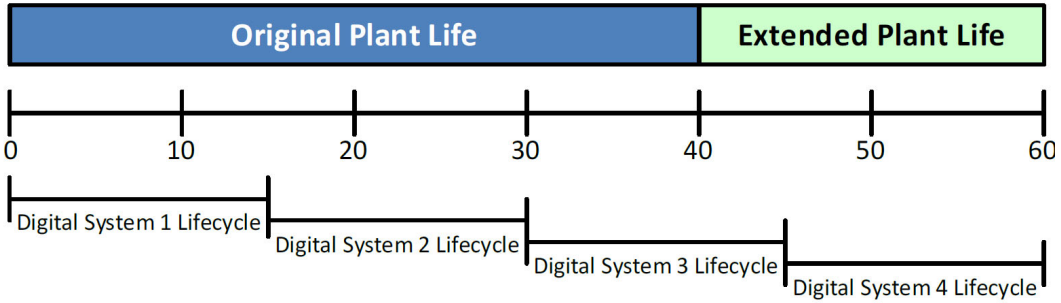
Typical Lifecycle Durations

	Typical Product Lifecycle Duration		
Component Type	**< 5 years**	**5 to 10 years**	**> 10 years**
Commodity Hardware*	**X**		
Controllers	X	**X**	
Platform Software	X	X	
Application Software	X	X	**X**
Physical I/O	X	X	**X**

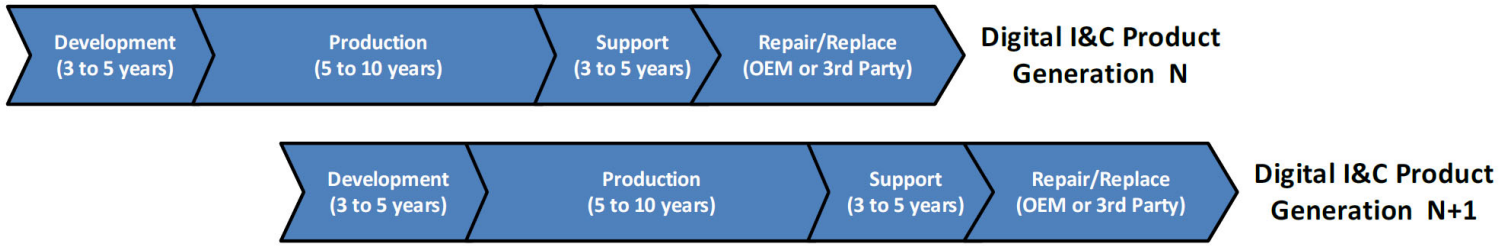
*Such as workstations and servers

Typical Lifecycle Durations

New Plant Lifecycle vs. I&C System Lifecycles

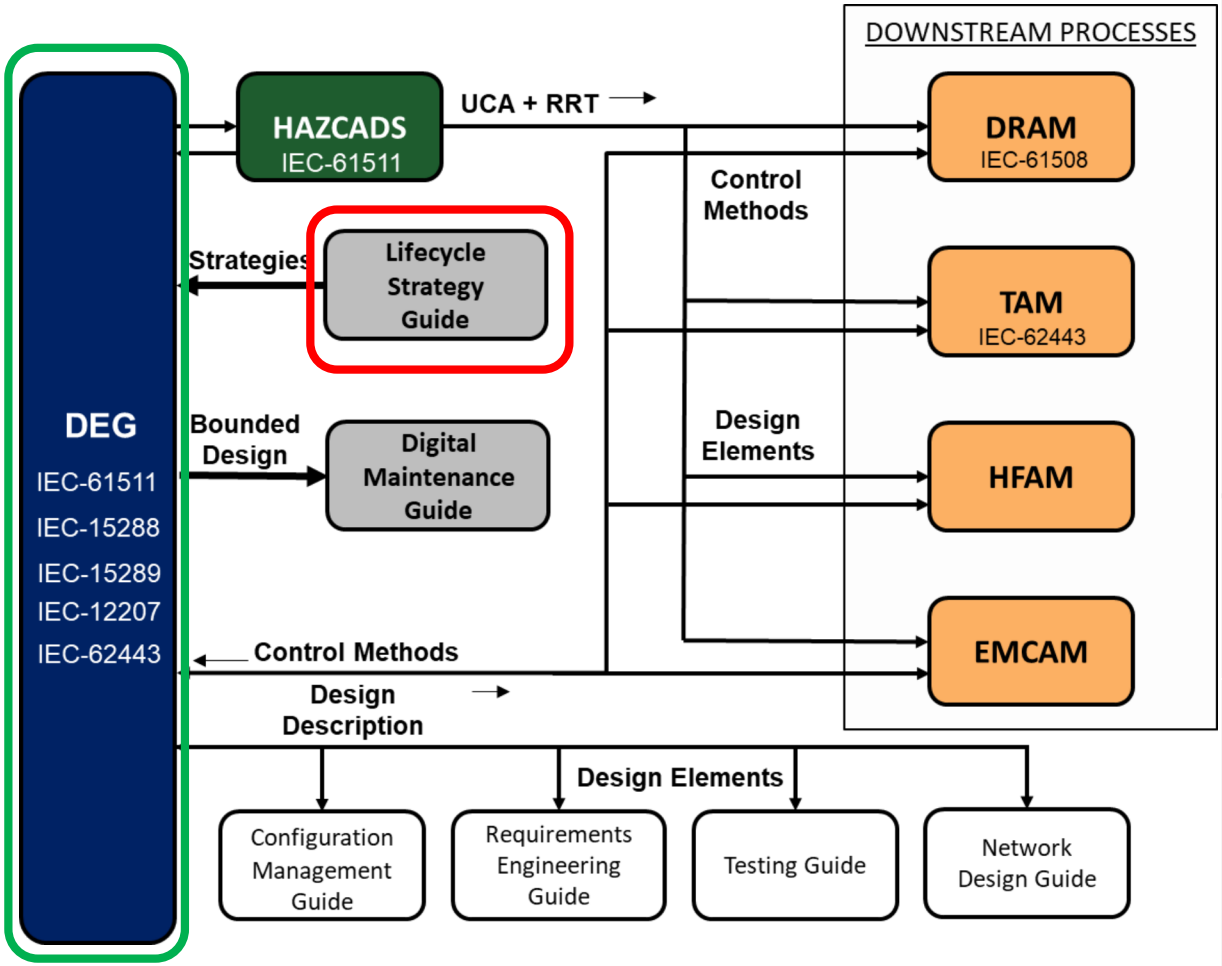


Overlapping Digital I&C Product Generations



EPRI Guidance on Digital Obsolescence Management

- The Digital Engineering Guide (DEG, EPRI 3002031218) provides a single, activity-based process for all activities related to digital systems engineering, including Digital Lifecycle Management (previously Digital Obsolescence Management)
  - The DEG leverages EPRI 3002002852, Advanced Nuclear Technology: Guidance and Methodologies for Managing Digital Instrumentation and Control Obsolescence
- The Digital I&C Lifecycle Strategy Guide (DLSG, 3002031213) provides methods to create effective lifecycle strategies for digital systems and components in a nuclear plant setting, including key aspects such as Digital Obsolescence Management Requirements.



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

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.

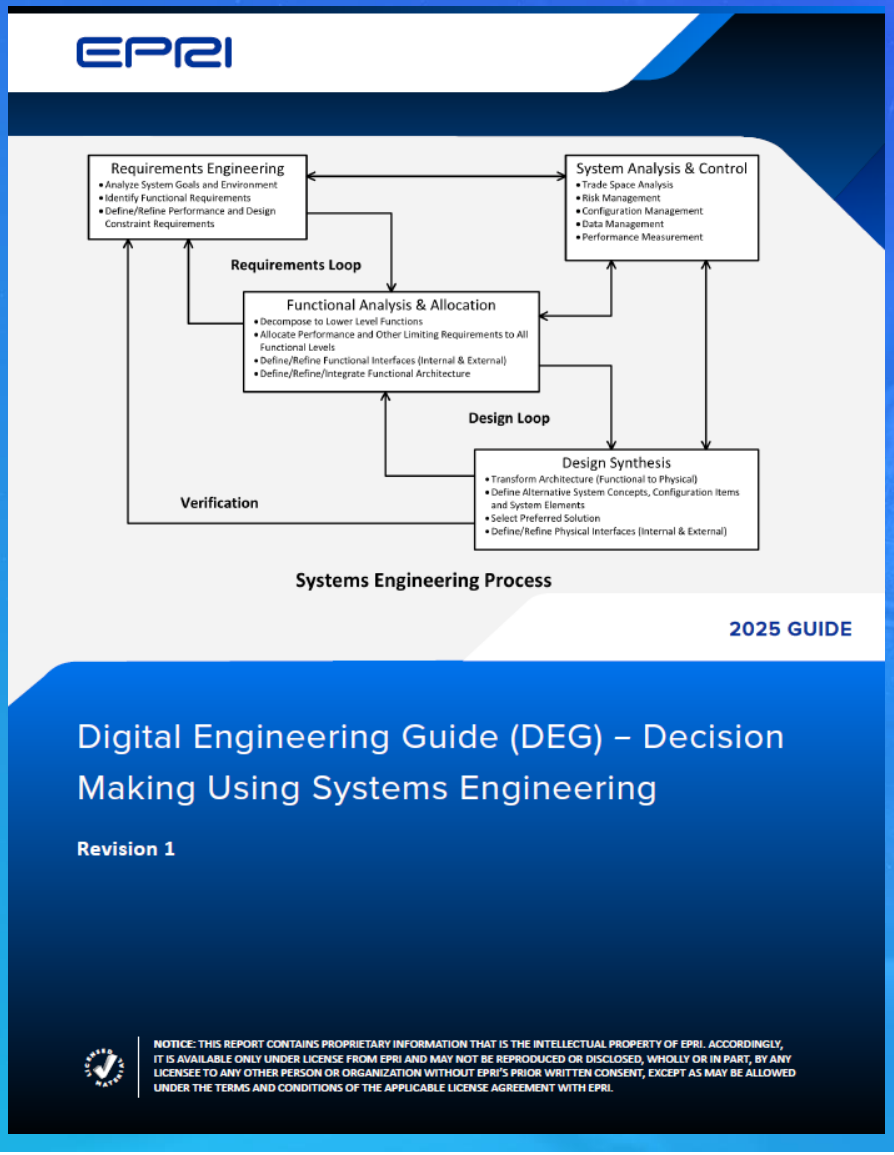
DRAM – Identifies Hardware and Software reliability vulnerabilities and develops Loss Scenarios. Formulates and scores Control Methods to protect, detect , and respond/recover from UCA to meet the RRT.

TAM – Identifies cyber security vulnerability classes and develops Exploit Sequences. Develops and scores control methods to protect, detect and respond/ recover from UCA to meet the RRT.

HFAM – Identifies important human actions and develops Loss Scenarios. Identifies and scores control methods to "design out" Human Error until meeting the RRT.

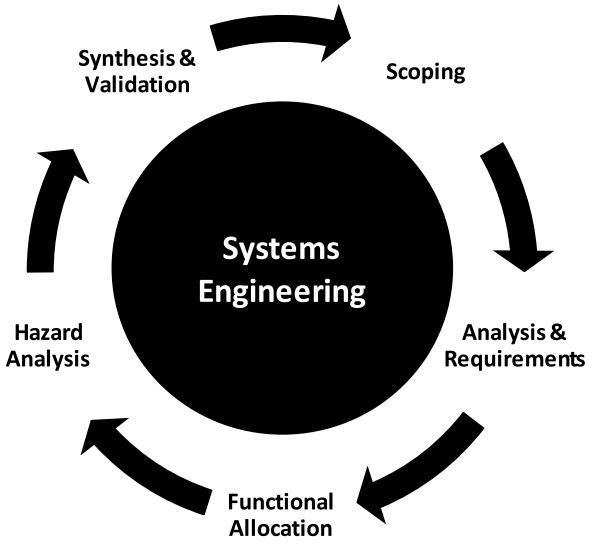
EMCAM – Identifies EMC vulnerability classes. Develops and scores protect, detect , and respond/ recover control methods using the RRT

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



Digital Engineering Guide(DEG)- Decision Making Using Systems Engineering Revision 1 3002031218

Digital Engineering Guide (DEG) – Systems Engineering

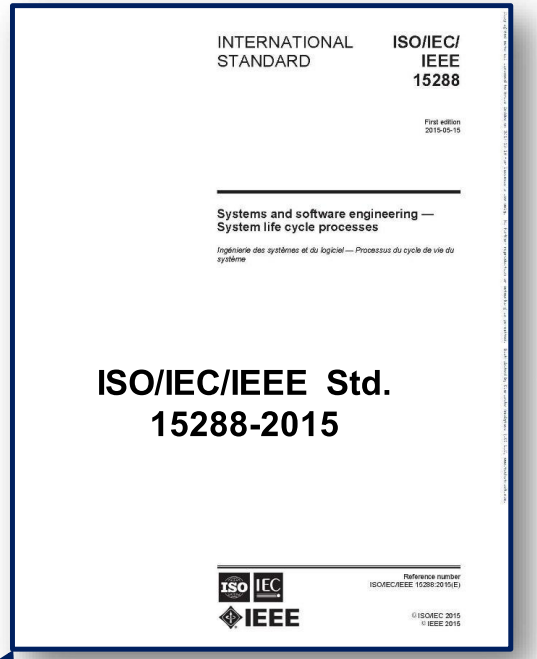


- **Synthesized from the ISO/IEC/IEEE-15288/15289/12207 Framework**
- **Life Cycle Phase, Activity, and Level of Interest Based**
- **Iterates through the SE process for each phase in a non-linear fashion**
- **Includes topical guidance for each phase**
- **Iteratively converges on the final synthesized design**

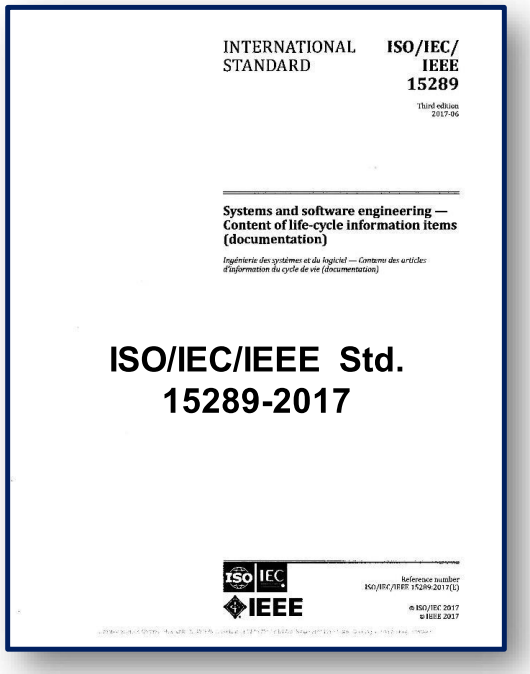
The DEG Addresses The Following Areas

- Division of Responsibility (DOR)
- Interface Analysis
- Topical Elements (Cyber, HFE, Procurement, EMC,CM, Data Comm)
- Requirements Development
- Architecture Development including Relationship Sets
- Functional Allocation (including Human/System Allocation)
- Hazard Analysis , Reliability Analysis (including CCF) and Mitigations (2.4.10. 2.4.11. 2.4.12)
- Verification and Validation (V&V)
- Testing & Discovery
- Transition to the O&M Phase

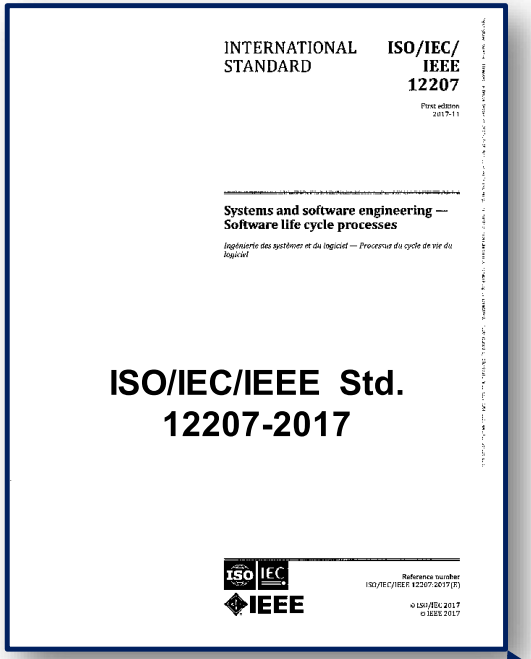
“This document ***specifies the purpose and content*** of all identified systems and software life-cycle ***information items***…”



ISO/IEC/IEEE Std. 15288-2015



ISO/IEC/IEEE Std. 15289-2017



ISO/IEC/IEEE Std. 12207-2017

“This International Standard ***does not detail information items* in terms of name, format, explicit content and recording media. ISO/IEC/IEEE 15289 addresses the content for life cycle process information item (documentation).”**

“This document ***does not detail information items* in terms, of name, format, explicit content and recording media. ISO/IEC/IEEE 15289 addresses the content for life cycle process information items (documentation).”**

Standards are Synthesized into Actionable Guidance

DEG R1 Activity Phases

- The DEG is organized by Phases. This phases match most lifecycle models that implement new or modified designs for systems or facilities. Activity numbers are formatted by [Phase.Topic.Sequence]. The Phases are:
- Phase 1- Initial Scoping (1.X.X)
- Phase 2- Conceptual Design (2.X.X)
- Phase 3- Detailed Design (3.X.X)
- Phase 4- Installation Planning Phase (4.X.X)
- Phase 5- Installation and Test Phase (5.X.X)
- Phase 6- Closeout Phase (6.X.X)
- Phase 7- Operations and Maintenance Phase (7.X.X)

DEG Activity Groups

"Activity groups" are clusters of related activities that promote engineering efficiency in digital projects by:

- Focusing on key technical decisions
- Promoting distillation of technical information into key information items
- Helping you make decisions that are informed by various topics, instead of thinking about each topic in isolation

This is an example "activity"

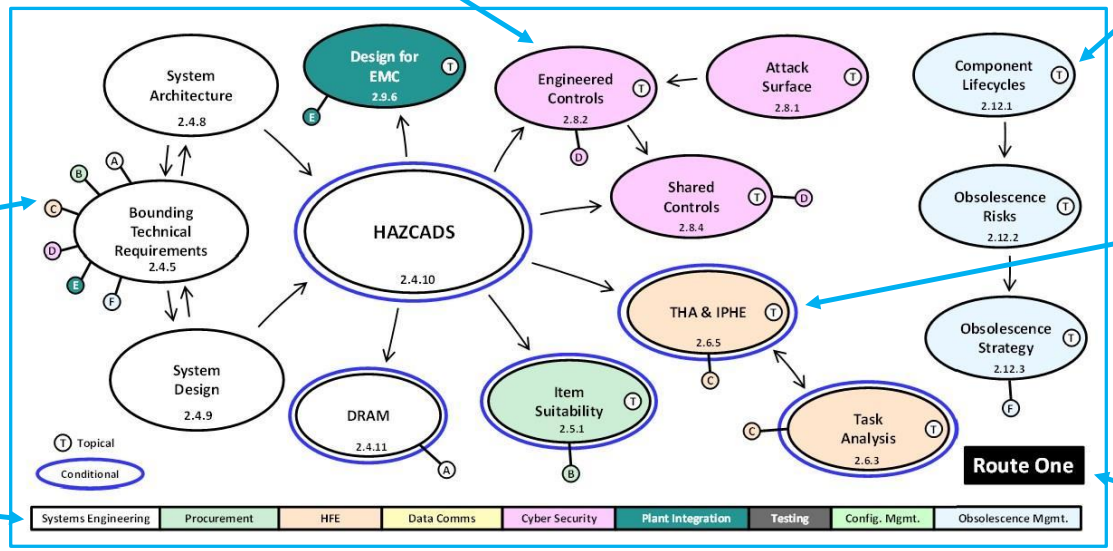
The "T"s indicate "topical screens"

The letters "A-F" refer to connections to other activities, which in turn are labeled with these letters

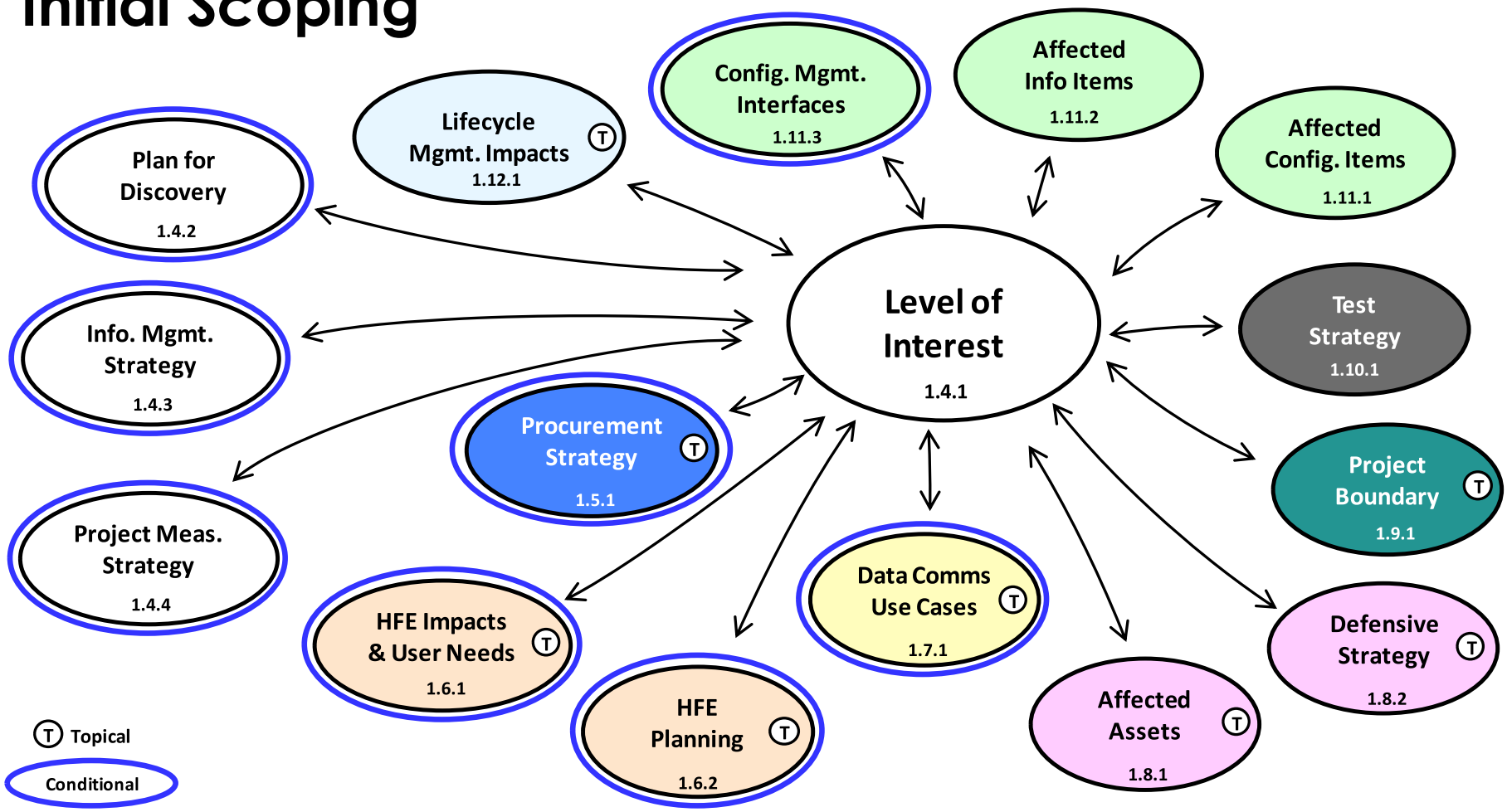
The blue outer circles indicate "conditional screens"

These are the nine "topics," which are color-coded in the activity bubbles

This activity group covers route one (risk informed analysis) of the two routes



Initial Scoping



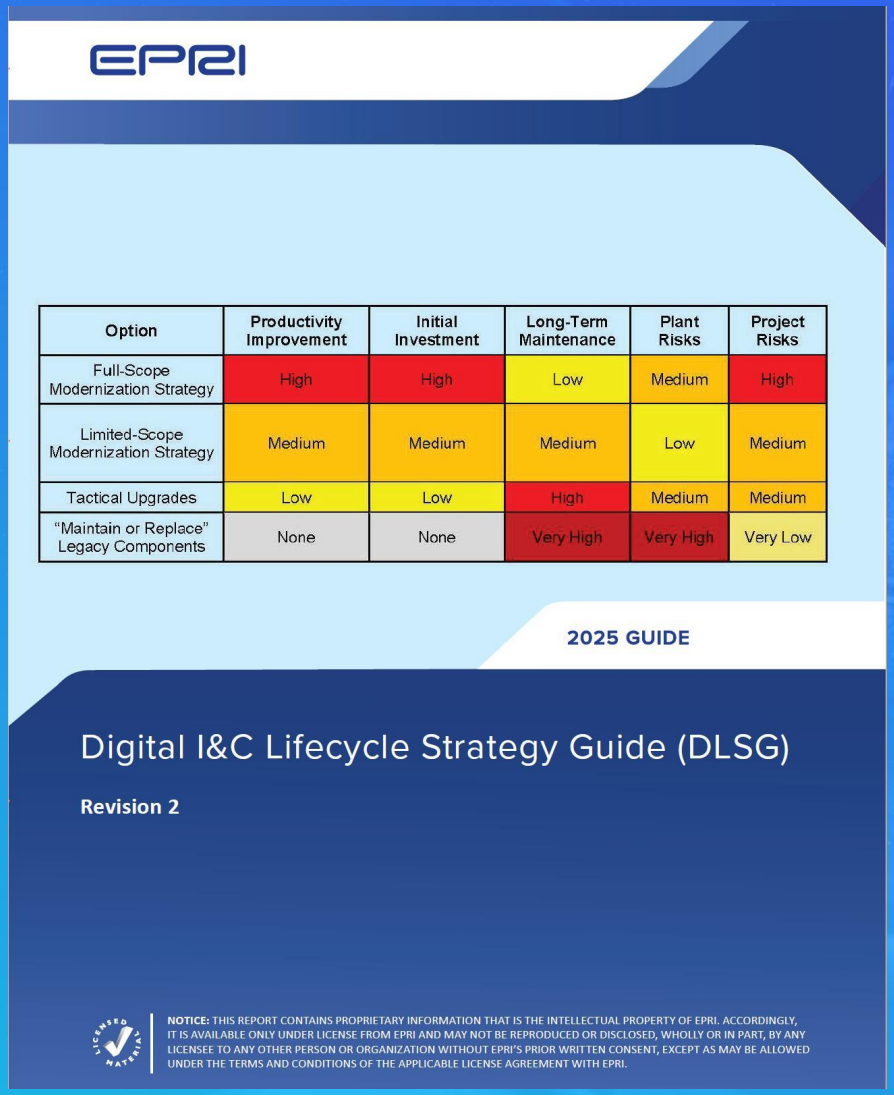
Systems Engineering	Procurement	HFE	Data Comms	Cyber Security	Plant Integration	Testing	Config. Mgmt.	Lifecycle Mgmt.

DEG R1 Activity Topics

- Topic 4 – Systems Engineering (X.4.X)
- Topic 5 – Procurement (X.5.X)
- Topic 6 – Human Factors Engineering (X.6.X)
- Topic 7 – Data Communications Engineering (X.7.X)
- Topic 8 – Cyber Security Engineering (X.8.X)
- Topic 9 – Plant Integration Engineering (X.9.X)
- Topic 10 – Testing (X.10.X)
- Topic 11 – Configuration Management (X.11.X)
- Topic 12 – Digital Lifecycle Management (X.12.X)

Topic 12 – Digital Lifecycle Management Activities X.12.X

- Consideration for long-range plant life and identify potential for multiple lifecycles of proposed or affected digital systems or components. (Conceptual, 2.12.X)
- Iterate, extend, and refine previous digital lifecycle management activities (Detailed Design, 3.12.X)
- Implement and integrate digital lifecycle management strategy elements (Installation Planning, 4.12.X)
- Perform or support installation, commissioning, and testing of digital system lifecycle management elements (Installation and Test, 5.12.X)
- Perform periodic lifecycle management effectiveness reviews (O&M, 7.12.X)



Digital I&C Lifecycle Strategy Guide Revision 2 3002031213

DSLG Overview

The Digital I&C Lifecycle Strategy Guide (DSLG): Revision 2 was developed to address Digital I&C Lifecycle Planning Implementation as part of the EPRI Digital Systems Engineering Framework.

- The central resource in identifying I&C lifecycle strategies within Topic 12 (Digital Lifecycle Management) within the core process described in the DEG.
- Developed through industry feedback and synthesization of multiple prior EPRI guidance documents:
  - EPRI 3002023428, Digital Systems Engineering – Digital I&C Lifecycle Strategy Guide, Revision 1
  - EPRI 3002015797, Digital Systems Engineering – Modernization Guide for Practitioners
  - EPRI 3002002852, Advanced Nuclear Technology: Guidance and Methodologies for Managing Digital Instrumentation and Control Obsolescence

Lifecycle Strategies

- Full-Scope Modernization
  - Seeks to maximize potential long-term O&M benefits by investing in pervasive changes to technologies, processes, and organizations.
- Limited-Scope Modernization
  - Emphasizes the management of equipment aging and obsolescence within the limitations of investment capital and the ability of the organization to absorb change.
- Tactical Upgrades
  - Strategy focusing on upgrades system-by-system as obsolescence or plant availability risks become unacceptably high.
- Maintenance of Legacy Components
  - Targeted replacement strategy emphasizing like-for-like replacements.

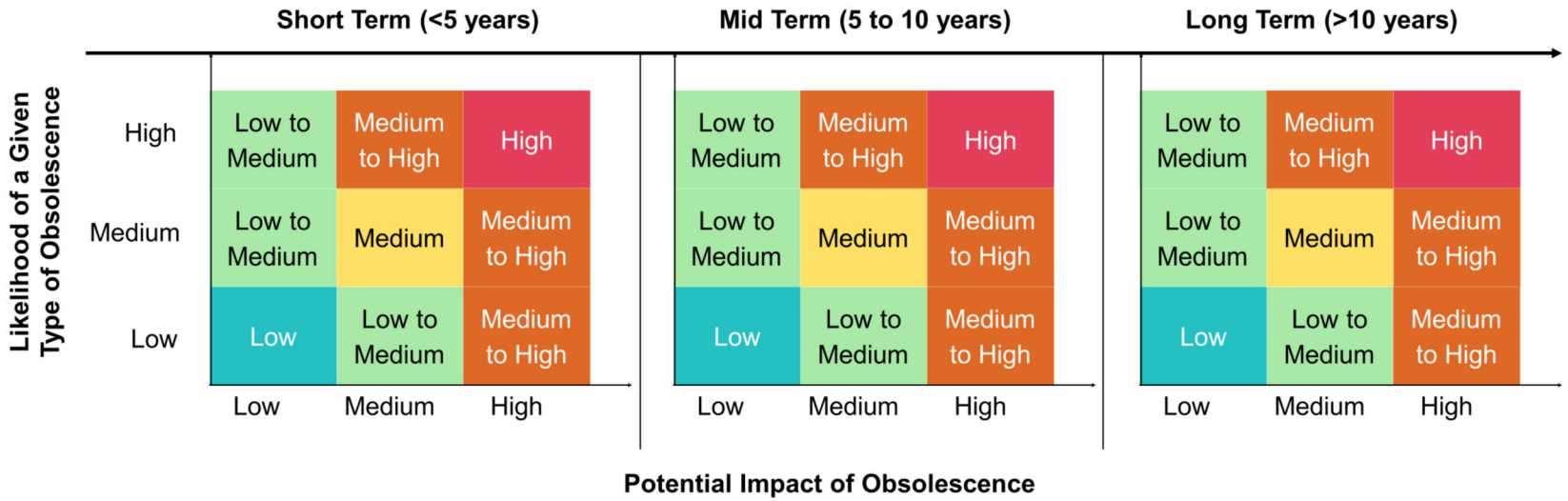
Option	Productivity Improvement	Initial Investment	Long-Term Maintenance	Plant Risks	Project Risks
Full-Scope Modernization Strategy	High	High	Low	Medium	High
Limited-Scope Modernization Strategy	Medium	Medium	Medium	Low	Medium
Tactical Upgrades	Low	Low	High	Medium	Medium
"Maintain or Replace" Legacy Components	None	None	Very High	Very High	Very Low

2.1.4 Obsolescence Management Requirements

Focuses on addressing successive obsolescence through the development of a lifecycle management plan (LCMP) or long-term asset management (LTAM) plan for each digital system.

Successive obsolescence refers to the reality in which commercial digital products have a much shorter lifespan than the analog I&C hardware, power switching components, or mechanical components they replace.

Obsolescence Risk



Types of Obsolescence
Technical
Functional
Supply Chain
Planned
Knowledge Base

Obsolescence Impacts
Depleted Spares
Loss of Support
Reduced or Lost Capacity Margin
Reduced Availability
Operations & Maintenance Burden

Obsolescence Management Strategies

Virtualization	Equivalent Items	Repair/Refurbish	Defensive	Full/Incremental Replacement
The simulation of software and/or hardware upon which other software operates	Used when it is acceptable to use, and it is possible to find equivalent parts	Continue to repair and/or refurbish existing equipment	Long-term freeze with the idea to manage obsolescence by replacing failed components with exact replacements	Replacing technologies with newer or upgraded technology either incrementally or all at once

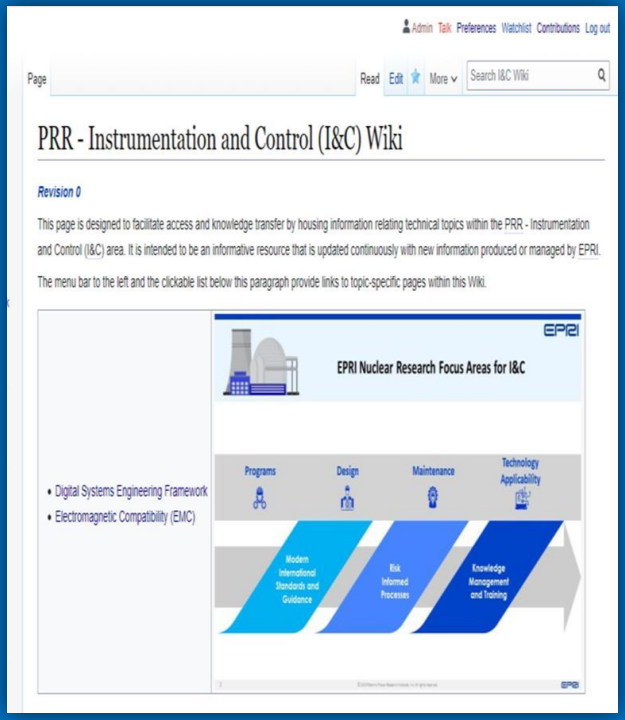
Blended

Utilizes more than one strategy at a time or utilizes different strategies at various times over the lifespan of a digital component or system.

Connecting with EPRI

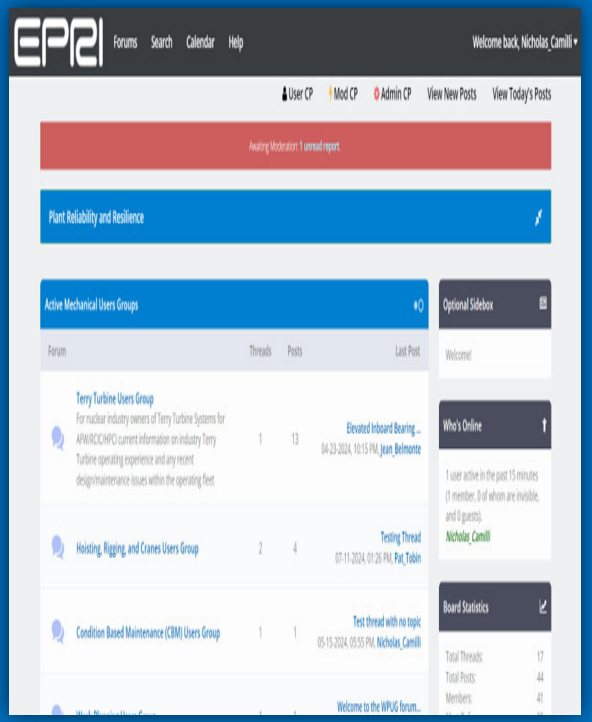
PRR WebApp

https://NuclearPRR.epri.com



I&C Wiki

https://icwiki.epri.com



PRR Forum

https://NuclearPRRforum.epri.com

www.epri.com