Risk-Informed Design

A Modern Approach to Digital I&C

Matt Gibson
Technical Executive
EPRI Nuclear I&C Program

Energiforsk Software Certification in Nuclear I&C Components

February 21st, 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.*

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

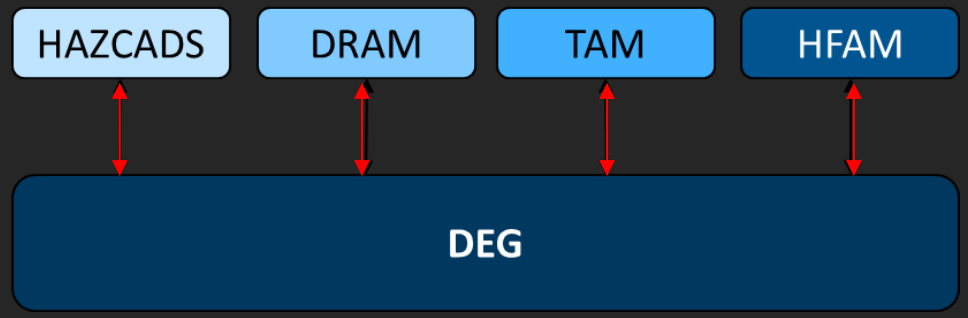
Utilize Industry Standards	Use the same proven design and supply chain structures that non-nuclear safety related industries use (IEC-61508/61511/62443). This leverages the economies-of-scale achieved in other industries.
Use of Systems Engineering	Use of a modern, high performance, single engineering 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.

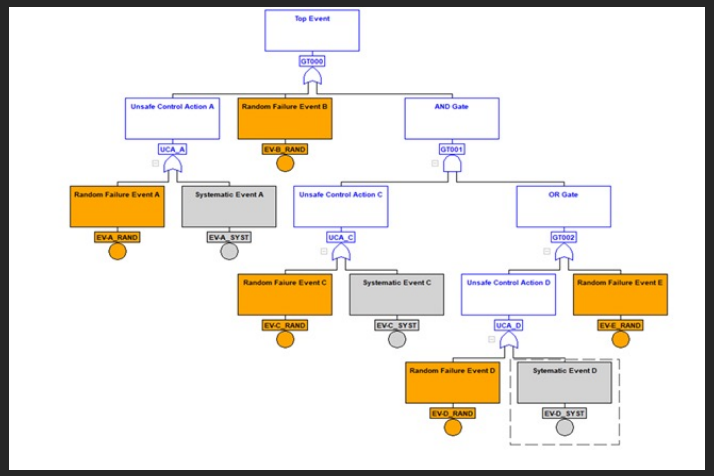
Capable Workforce

Modern Methods to Support Nuclear Fleet Sustainability and Advanced Reactor Design

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

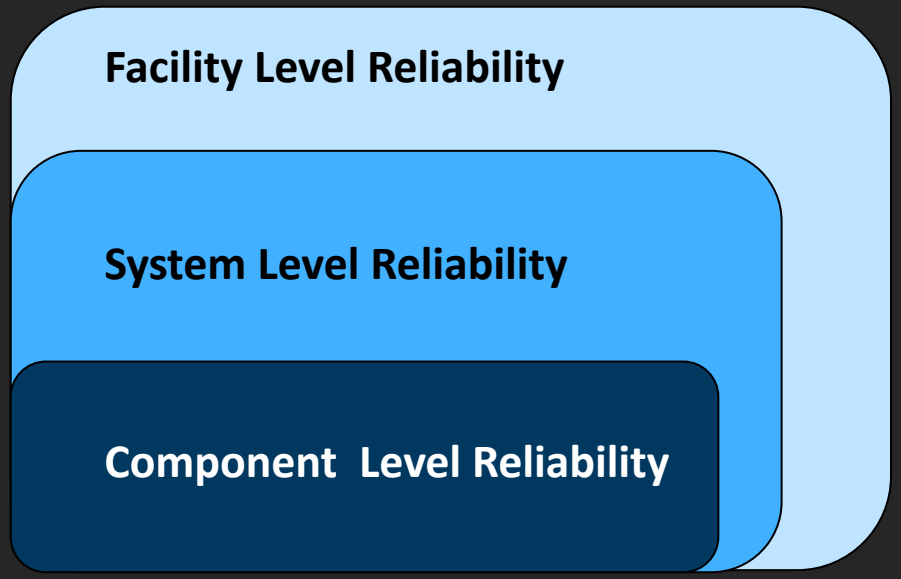


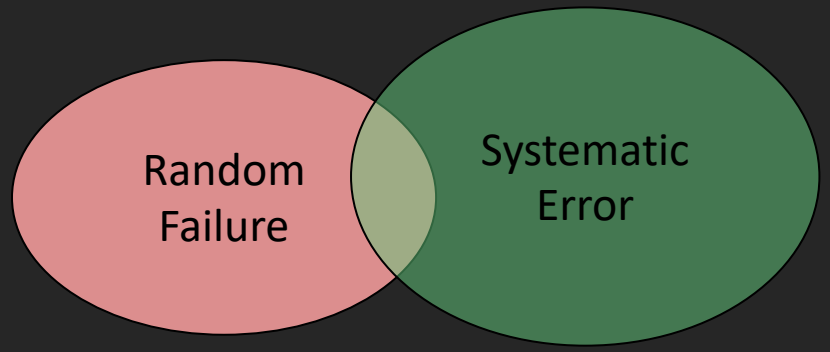


- **HAZCADS, DRAM, & HFAM delivered in 2021- Integrated with DEG**
  - ✓ Constellation Pilot Ongoing
  - ✓ Integrated Proof Test Completed (DEG, HAZCADS, DRAM, TAM)
    - Simulated plant Design Change over 3-month period with diverse participants
- HFE and HRA integrated into HFAM
  - ✓ Risk-Informs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

Digital Reliability Model





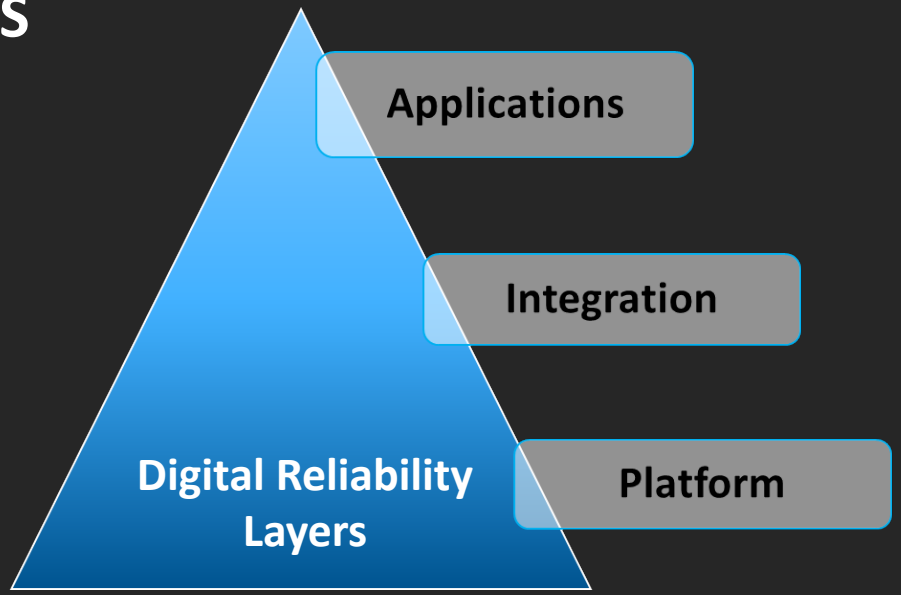
Reliability Axioms

- 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.
- Cumulative Functional Reliability is the prime objective (at the system/facility level).

Safety Integrity Level (SIL) Efficacy for Nuclear Power

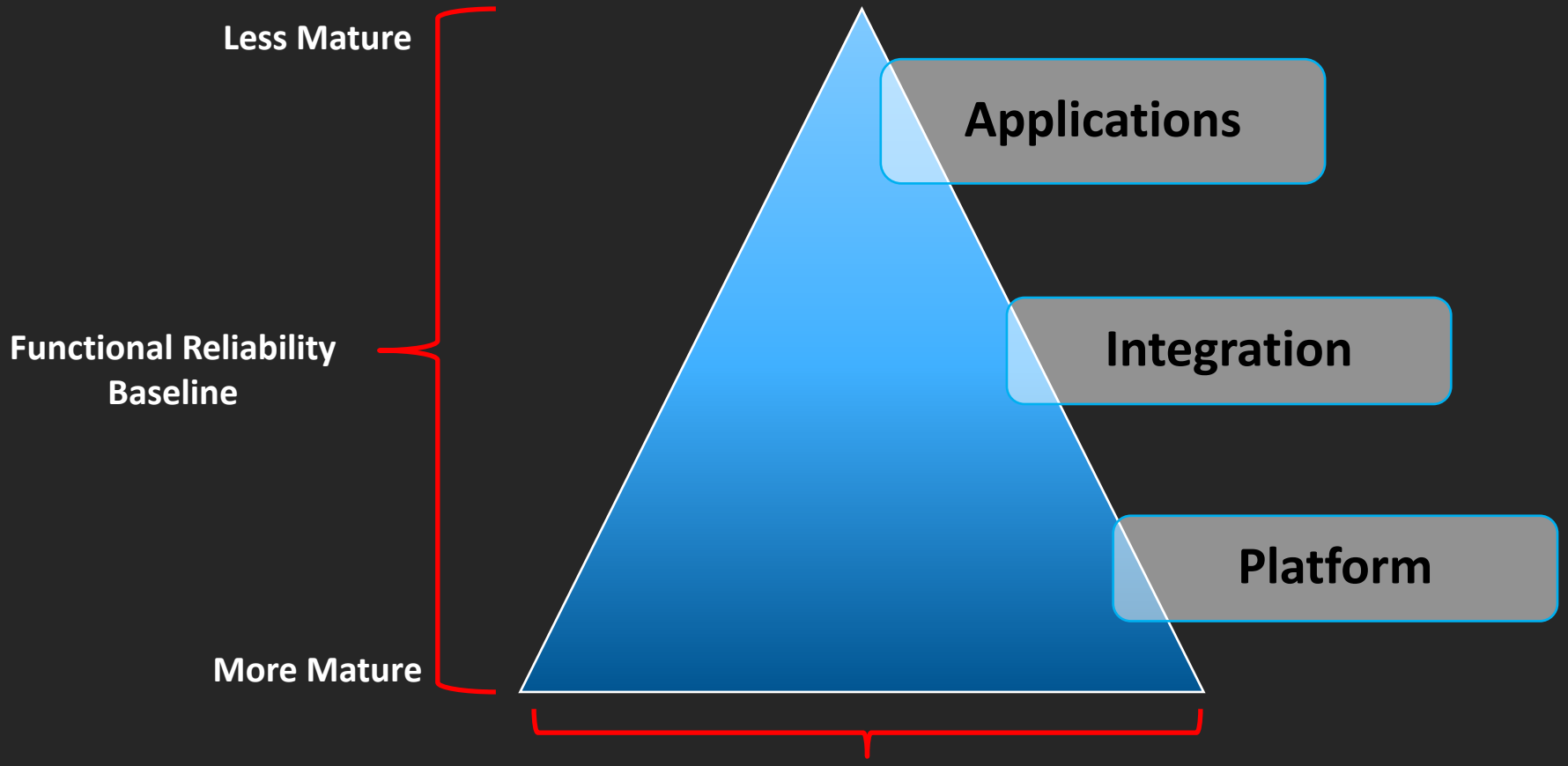
- EPRI research on field failure data from SIL certified logic solvers revealed no ***platform level*** Software Common Cause Failures (SCCF) after over 2 billion combined hours of operation for IEC-61508 SIL certified PLC's (3002011817)
- Indicates that using existing SIL certifications, at the ***platform level***, has a high efficacy for use as surrogates for some existing design and review processes.
- **Being Leveraged in for NEI 17-06 and NEI 20-07 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



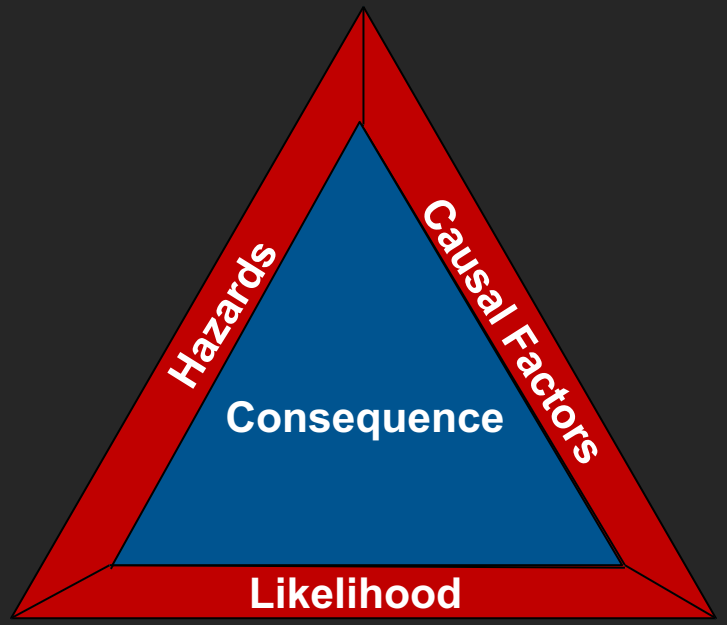
Reliability Layers

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

Practical Risk Model



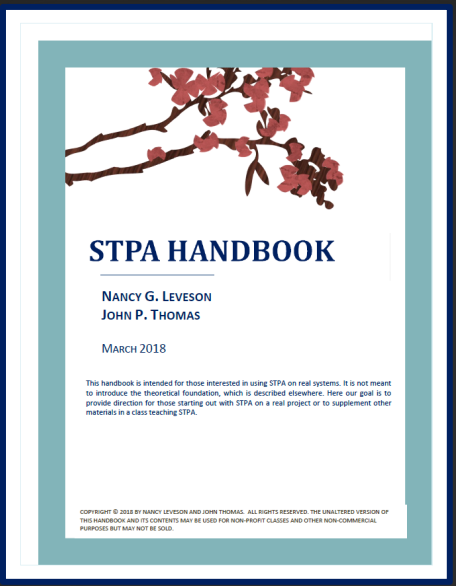
Risk Triangle

- Consequences (Losses) = The Impact
- Hazards =The Undesired Condition that results in a Consequence
- Causal Factors = Realize a Hazard
- Likelihood = Systematic/Random characteristics that impact reliability

Risk can be Reduced or Eliminated by Reducing Any Part of the Risk Triangle

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.



STPA Step One
Identify
Stakeholder Losses

→

STPA Step Two
Identify
System Hazards

→

STPA Step Three
Identify
Unsafe Control Actions

→

STPA Step Four
Identify
Loss Scenarios

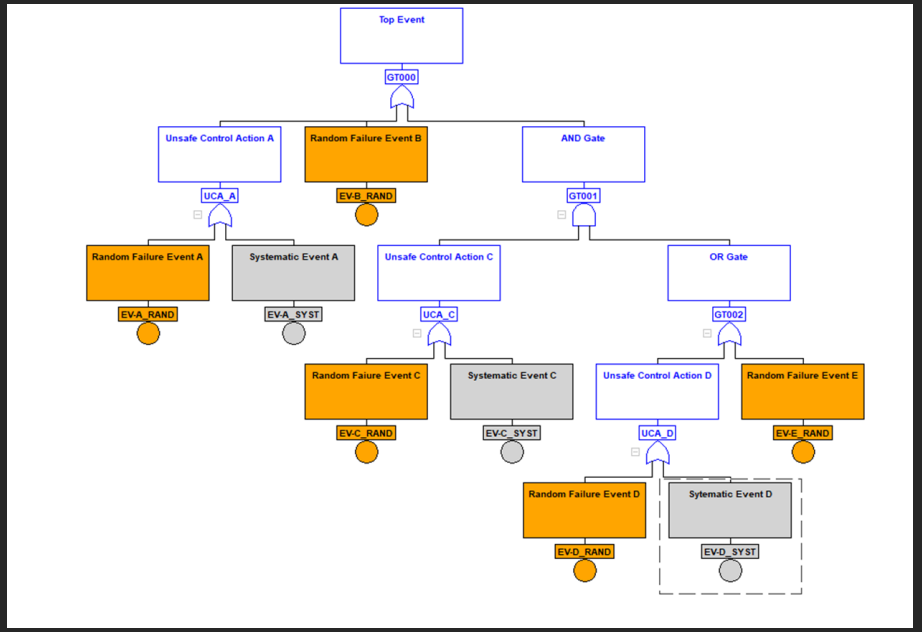
These steps are in HAZCADS

This step completed in Downstream Processes

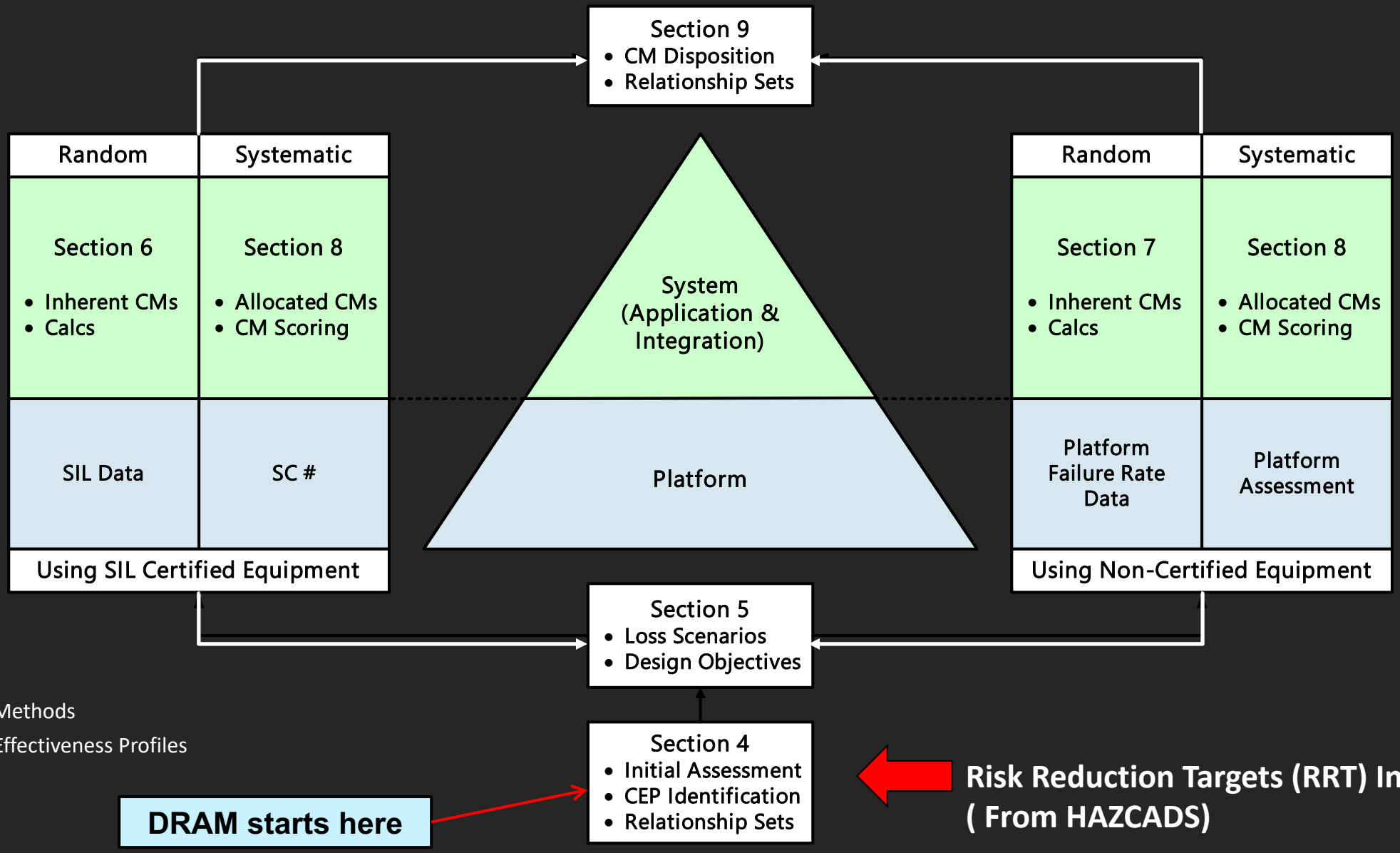
HAZCADS: Hazards and Consequences Analysis for Digital Systems-3002016698

- ✓ 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*.**
- **Provides Risk Reduction Targets(RRT) to shape downstream loss scenario identification and analysis methods for a complete reliability assessment and resolution methodology.**



Digital Reliability Assessment Methodology (DRAM) Revision 0

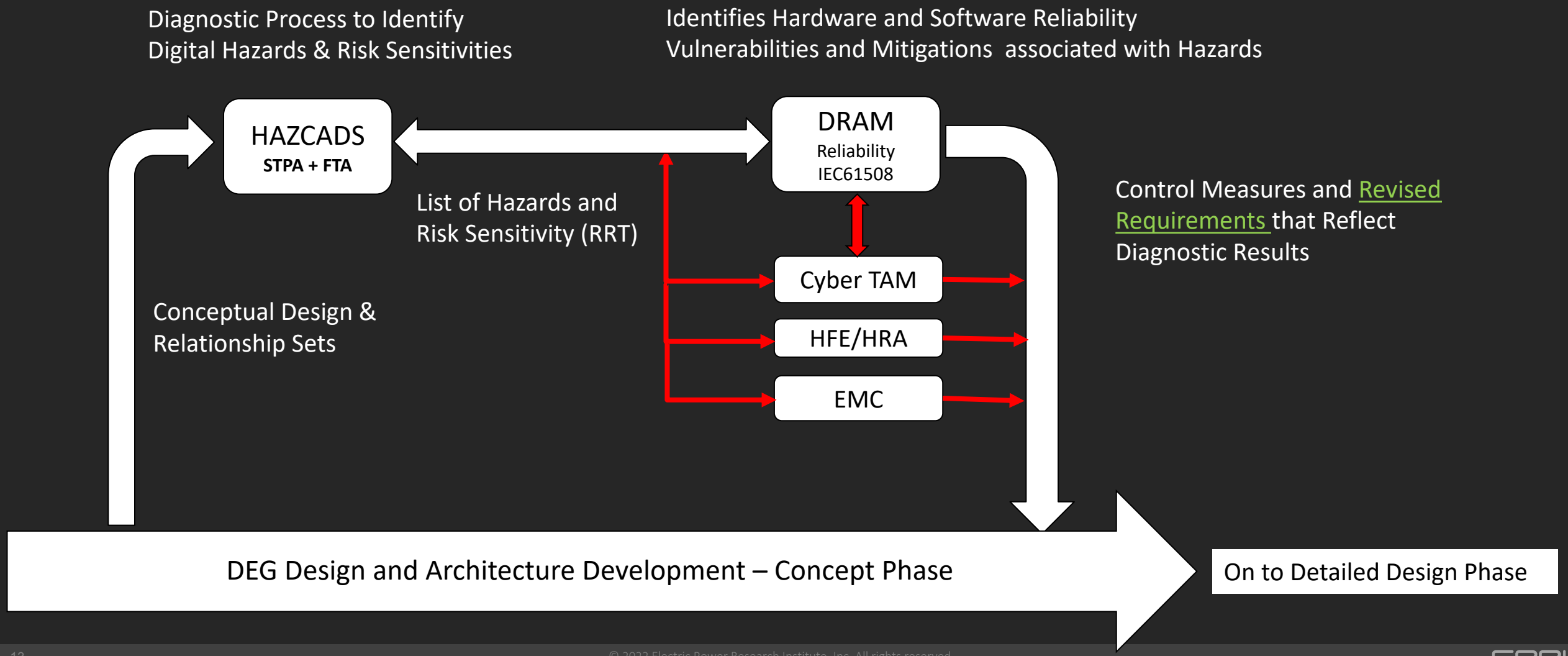


CM= Control Methods

CEP= Control Effectiveness Profiles

Workflow- Conceptual Phase

Establishes the Safety of the Intended Function (SOTIF)



Questions?

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