ELECTRIC POWER RESEARCH INSTITUTE

EPRI Integrated Digital Systems Engineering

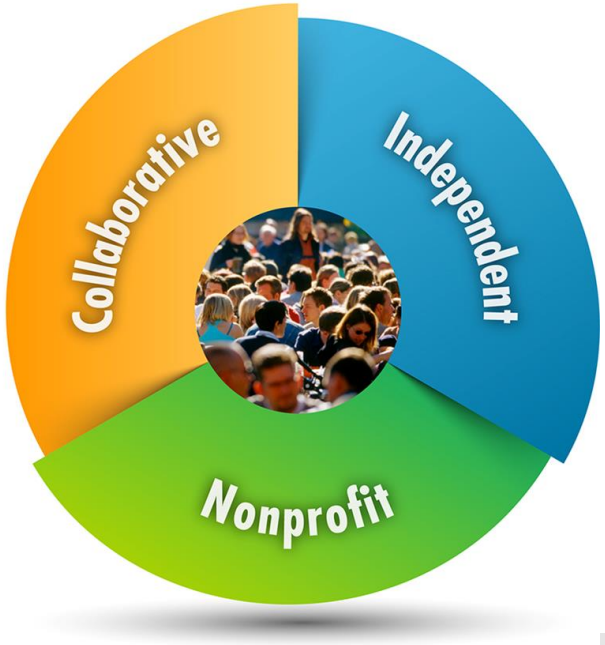
US-NRC Commission Briefing on Digital Instrumentation and Control

Neil Wilmshurst
Chief Nuclear Officer-EPRI

May 14th , 2019

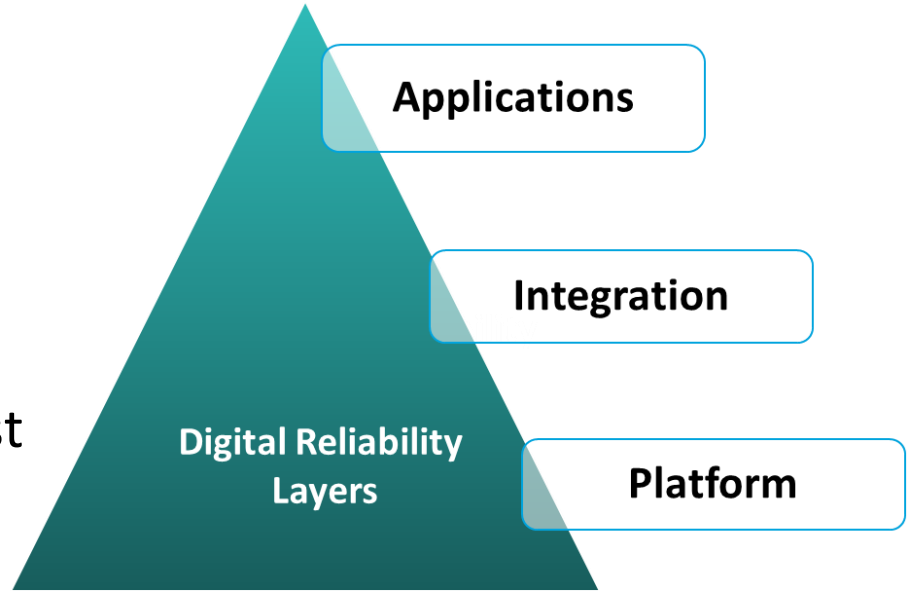
EPRI

- 450+ participants in more than 30 countries
- EPRI members generate approximately 90% of the electricity in the United States
- International funding – nearly 25% of EPRI's research, development, and demonstrations



EPRI Perspective On Digital Reliability

- Recent research using field failure data revealed no platform level Software Common Cause Failures (SCCF) over approx. 2 billion hours of operation for IEC-61508 SIL certified PLC's
- Application of existing SIL certifications, ***at the platform level***, in place of existing design and review processes has proven to be effective.
- Additionally, cumulative nuclear OE from across the world (Korea, France, China, etc.) indicate that:
  - SCCF failures are no more problematic than other CCF contributors
  - There have been no identified events where diverse platforms would have been effective in protecting against SCCF
  - Several events confirmed effectiveness of signal and functional diversity in protecting against SCCF



Integrated Digital Systems Engineering Framework

- Architecture
- Hazard Analysis (STPA/FTA) – SPV/CCF
- Requirements Engineering
- Procurement
- Human Factors Engineering (HFE)
- Cyber Security
- Data Communications
- Plant Integration
- Testing
- Configuration Management
- Life Cycle Management

EPRI Digital Engineering Guide (DEG)

Systems Engineering Based

Risk Informed

Use of International Industrial Standards

Systems Engineering Based

- ISO/IEEE/IEC - 15288 /12207/15289

Safety reliability and risk framework

- IEC-61508/61511

Industry Standard Engineering Process

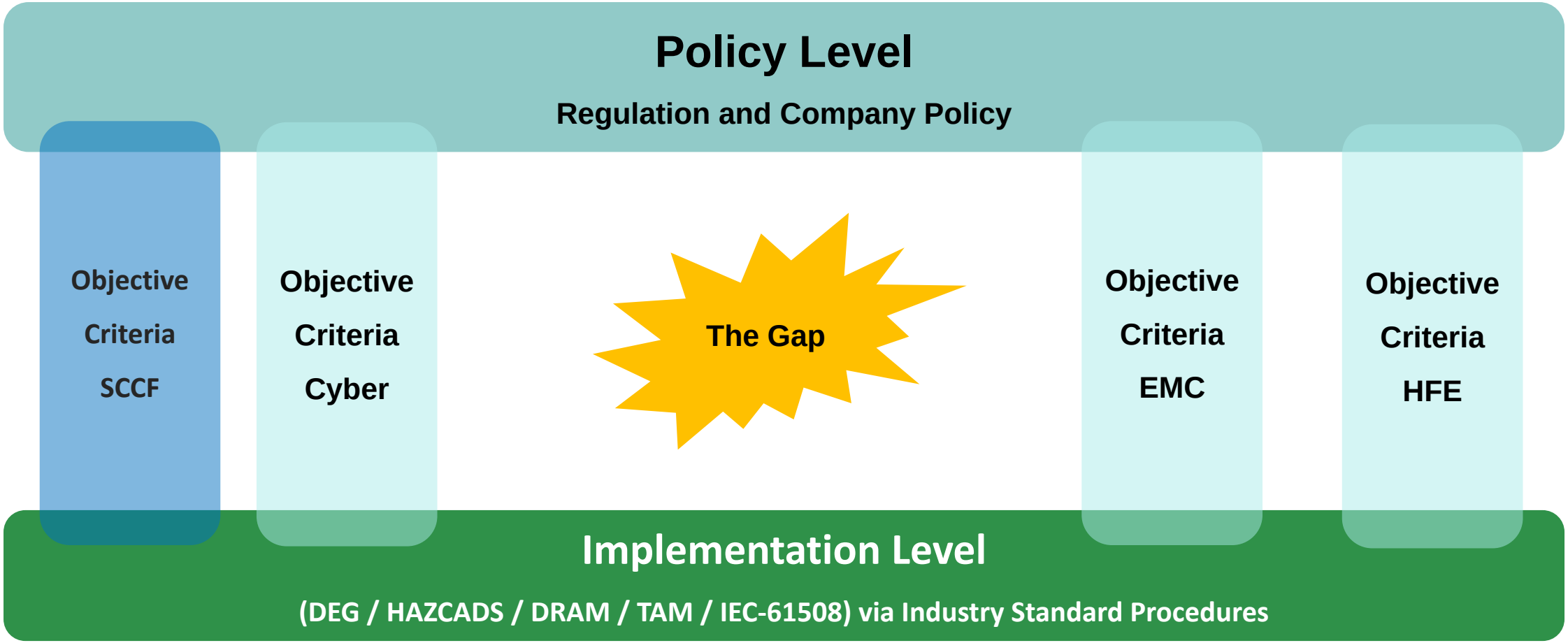
Optimized Digital Engineering Organization

EPRI's Digital Framework Elements

EPRI has developed a ***comprehensive engineering process***, utilizing modern methods and international standards used in other safety related industries.

- **Element 1- Use of Industrial Standards:** Use the same supply chain and structures that non-nuclear safety related industries use (IEC-61508/61511) to harvest the economies-of-scale of other safety industries.
- **Element 2 - 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.
- **Element 3 - Risk Informed Engineering:** Effective engineering decision-making via hazards and risk analysis to integrate all engineering topics (such as cyber security and SCCF) into a single engineering process.

Policy Level vs. Implementation Level Activities



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

Objective Criteria provides the Policy to Implementation connector and can be formatted like a safety case argument

Acronyms

- CCF – Common Cause Failure
- DEG – Digital Engineering Guide (EPRI 3002011816, Oct 2018)
- DRAM – Digital Reliability Analysis Methodology (EPRI product in development, sch. Q1 2020)
- EMC – Electromagnetic Compatibility
- EPRI – Electric Power Research Institute
- FTA – Fault Tree Analysis
- IEC – International Electrotechnical Commission
- IEEE - Institute of Electrical and Electronics Engineers Standards Association
- HAZCADS – HAZCADS: Hazards and Consequences Analysis for Digital Systems (EPRI 3002012755 Dec. 2018)
- HFE – Human Factors Engineering
- ISO – International Organization for Standardization
- OE – Operating Experience
- PLC – Programable Logic Controller
- SCCF – Software Common Cause Failure
- SIL – Safety Integrity Level (based on IEC-61508)
- SPV – Single Point Vulnerability
- STPA – Systems Theoretic Process Analysis
- TAM – Cyber Security Technical Assessment Methodology (EPRI 3002012752, Nov. 2018)

Together...Shaping the Future of Electricity