NEI 17-06 Initiative for MP#3 Team Vendor Presentation

Acceptance of IEC 61508 SIL Certification for the Acceptance of Third Party Certification Processes for Nuclear Safety Applications

Ron Jarrett PE
Tennessee Valley Authority
Digital Program Manager

NUPIC Conference June 20 2019
https://www.nei.org/home

Commercial Grade Dedication (CGD) of Digital Equipment

- What is Digital?
  - Devices with a microprocessor
  - Devices with software and firmware
  - Devices with digital hardware based devices such as ASICs, FPGAs, Memory, etc
- CGD Method/s?
  - No new methods, digital uses the same 4 CGD methods for acceptance
- What is special about digital dedication?
  - New Critical Characteristic beyond physical and performance CCs – Dependability CCs (EPRI TR-106439 - https://www.nrc.gov/docs/ML1033/ML103360462.pdf)
  - Addressing Common Cause Failures unique to digital
  - Identification – digital component may be embedded and difficult to identify

Difficulties in Digital Dedication

- Acceptance Criteria is subjective and depends on defense design measures and structured processes. EPRI TR-106439 is a methodology and the Dependability CCs can have a large variance and based upon the preponderance of evidence (subjective, not a fixed acceptance criteria) relies heavily on engineering judgement rather than objective criteria.
- Digital and software expertise is not a normal expertise of dedicators
- The digital design of OEMs design is normally **Intellectual property**, requiring working with the OEM under Non disclosure agreements
- Licensees must address Software Common Cause Failure (SWCCF)
  - SWCCF is identical software in redundant divisions where an unidentified systematic flaw, if triggered, could result in failures of multiple divisions, which is a failure with a different result to the plant safety analysis.
  - QA evidence required to support a CCF Qualitative Assessment (NRC RIS 2002-22 Supplement 1 for NEI 01-01 which refers to EPRI TR-106439 as a vehicle for addressing SWCCF)
    - Structured development process
    - Defensive measures (i.e., watchdog that takes device to fail safe state)
    - Must have trigger (i.e., network connection)

What is NEI MP#3 Initiative?

Provide an alternative process that:

1. Simplifies digital CGD for Dependability CCs.
2. Results in crediting higher quality digital devices and systems that are reviewed to higher certified safety standards (i.e., IEC 61508).
3. Increases the number of available commercial products for the nuclear industry.
4. Increases the quality and consistency of technical reviews by crediting IEC 61508 SIL certifications performed by digital design accredited Subject Matter Experts (SMEs).
5. Provides reasonable assurance the SWCCF is low probability and not any greater than other CCF mechanisms (i.e., Harsh environment, Seismic, etc.). EPRI research of SWCCFs shows that the IEC 61508 process does this.
6. Reduces the number of both technical and QA reviews.
7. Has NRC acceptance.

Overview of the NEI MP#3 Initiative

NRC Modernization Plan 3 (MP3) "Acceptance of Digital Equipment" Addressing 3rd Party Certification as a means of verifying dependability Critical Characteristics for Commercial Grade Dedication (CGD) of Digital Equipment

- The Team = NEI, EPRI, Licensees (Mark Coren from Duke also represents NUPIC interests on the team)
- Development of a process (NEI 17-06) and associated NUPIC observation criteria to use and credit IEC 61508 Safety Integrity Level (SIL) certified components not developed under an Appendix B program
- SIL Certification would address digital quality specifically in the area of dependability, (design, reliability and quality processes) which is a type of Critical Characteristic (CC) defined by EPRI TR-106439, CGD of Digital Equipment (endorsed by NRC)
- EPRI is performing an independent assessment of the IEC certification and accreditation processes. EPRI report is in the process of being issued.
- Integrate process with existing Commercial Grade Dedication (CGD) process
- Gain NRC acceptance of the new NEI process

What is the Dependability CC?

- Dependability was initially defined by EPRI TR-106439, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications

  Dependability as used in this document, a broad concept incorporating various characteristics of digital equipment, including reliability, safety, availability, maintainability, and others. [Adapted from NUREG/CR-6294]

- EPRI TR-106439, Table 4-1 provides typical critical characteristics and provides examples of acceptance criteria and verification methods that can be used in verifying them. The matrix covers three categories of critical characteristics: physical, performance, and dependability.
  - CCs,
  - Acceptance Criteria,
  - Methods of Verification, and
  - Application of Methods
- The EPRI CCs are a starting point and must be adapted to the component's defined safety function.

Additional CCs and CGD and Qualification Activities

- IEC-61508 establishes safety characteristics of the devices at the device level as well as the dependability of the devices to execute those safety characteristics. We may want to credit any critical characteristic that was included in the certification. For instance, the standard requires that the device go to a safe state if it experiences certain failures, it requires memory protection for critical functions, etc. If these features are specified as a performance CC, then you should allow them to be included as being certified, as well as that characteristic for dependability.
- 3rd party dedicators and/or licensee would still address:
  - All other aspects of equipment CGD process
  - Dedication process compliance with QA requirements of 10 CFR 50 Appendix B that are subject to NUPIC reviews
  - Performing equipment qualification testing

What is IEC 61508 SIL Certification?

- IEC 61508 is used globally in industries such as transportation, petro chemical, etc. to establish high standards for safety equipment (focus is on saving lives)
- Presently used in a few nuclear non safety applications such as turbine overspeed trip systems
- IEC 61508 is a highly structured standard for software based systems and components
- IEC 61508 is currently the highest and most rigorous global standard
- Addresses product quality from conceptual design through manufacturing
- Product changes require recertification (a weakness in US CGD process concerning identification of commercial changes that affect quality)
- Quantitatively addresses quality and reliability (probability of failure) that is classified by SIL level (SIL 1 thru 4)
- Failure analysis identifies failures and addresses detectability of those failures

Accreditation of IEC 61508 SIL Certifiers

There are presently 3 major SIL Certifiers and 2 Accreditation Bodies (ABs)

Certifiers	Accreditors
• exida • TÜV Rheinland • TÜV SÜD	• ANSI (US) • Deutsche Akkreditierungsstelle or DAkkS (Europe)

IEC 61508 SIL Certification Process

Certifiers

- SIL Certifiers are companies with accreditation by an AB which are signatories to the International Accreditation Forum (IAF)
- Certifiers use Global SMEs to review compliance with IEC standard 61508 requirements
- Certification is performed on a periodic basis or when the product is changed
- Documentation is developed by the vendor to support the certification review

Accreditors (ABs)

- ABs perform periodic audits/reviews of the certifiers to ensure Certifier's performance is in compliance with established standards
- Accreditations are generally valid for a period of five years, but must be monitored by the ABs on a regular basis
- ABs are part of the International Accreditation Forum (IAF) whose primary purpose of IAF is two-fold:
  - To ensure that its accreditation body members only accredit bodies that are competent to do the work they undertake and are not subject to conflicts of interest
  - To establish mutual recognition arrangements, between its accreditation body members which reduces risk to business and its customers by ensuring that an accredited certificate may be relied upon anywhere in the world

Why does the Nuclear Industry need this?

- Facilitate modernization of control systems and application of digital technology
- Take advantage of existing efforts that assess quality of equipment used for the high levels of safety
- Increase the quality and availability of vendor products for Nuclear industry
  - Provides greater consistency in evaluation of EPRI TR 106439 dependability critical characteristics (CCs) for CGD
- Replace NRC reviews with the reviews performed to the highest standard in the world
- Reduce commercial grade surveys for dependability CCs by permitting SIL certification/accreditation to be used in lieu of commercial grade surveys (similar to ILAC accreditation)
- Certifications could provide evidence to support 10CFR50.59 evaluation using Qualitative Assessments for Software Common Cause Failure in digital components (Ref. RIS 2002-22 Supplement 1, NEI 01-01 Digital 50.59s)

Cost savings to US Nuclear Industry

- Pooling of industry resources via NUPIC observations would preclude the need for an alternative process to ensure certifiers work individual licensee reviews on a case by case basis.
  - 2 observations every 3 years versus alternative process for every certification.
- Increased competition between vendors on a global basis.
- Improved project schedule stability by reducing NRC review time frames and associated project uncertainties.

What is the NEI MP#3 Team Doing?

- Working with NRC on the use and acceptance of this approach
- Developing NEI 17-06 that is expected to be endorsed by the NRC
  - Using a similar structure of NEI 14-05 for Calibration Facilities
  - Incorporating the independent research of EPRI on the IEC SIL certification process
  - Establishing the application of SIL Certification to CGD and NUPIC role as observer of ABs (requesting NUPIC acceptance of this role)
- Establishing the NUPIC observation criteria for the SIL ABs
- Obtain NRC endorsement of the final process

What are we asking of NUPIC?

- Accept role as observer of SIL certification process similar to NEI 14-05, Guidelines for the use of Accreditation In Lieu of Commercial Grade Surveys for Procurement of Laboratory Calibration and Test Services
- Provide input into NEI's documentation development of NEI 17-06
- Review and comment on NEI developed criteria for NUPIC observations
- Assuming NRC acceptance of the process and successful NUPIC observations of ABs, Nuclear Power Plant QA organization would accept accreditations and device certifications as QA evidence of digital dependability
- Note that 3rd party dedicators or licensees would still be used to address all other aspects of equipment CGD and comply with QA requirements of 10 CFR 50 Appendix B subject to NUPIC reviews
- Periodically observe ABs (3-year interval) to ensure that they meet the established NEI/NUPIC criteria. Note: There are only two accreditors to be observed ANSI (US) and DAkkS (Europe).

Next Steps

- NEI Schedule
  - Gain the support of NUPIC – June 2019
  - Complete development of NUPIC observation criteria for NUPIC review – June 2019
  - Complete NEI 17-06 for NRC review – September 4th Quarter 2019
    - Integrate EPRI work into NEI 17-06
    - Integrate NUPIC criteria
  - First NUPIC AB Observation – Fall 2019
  - Obtain NRC endorsement of NEI 17-06 – TBD

A Thought to Leave You With

The SIL certification is a positive indicator of commercial products. Even without the NRC giving "credit" for SIL certifications, that is the type of equipment that should be evaluated first for use in the plants. At a minimum, it is a sign that the commercial manufacturer is aware of and interested in meeting the needs of industries that need high systematic integrity and reliability. Getting credit from the NRC for the dependability CCs is just an added bonus!

Questions

Ron Jarrett PE
rajarrett@tva.gov
423 504-8566