Dedication of Digital COT Components for Use in U.S. Nuclear Industry

Steven A. Arndt

U.S. Nuclear Regulatory Commission

Seminar on Industry Standard Components in Nuclear I&C Applications

22 October, 2019

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Outline

- Dedication of Commercial Grade Items in the US
- Key considerations for digital system dedication
- Challenges to digital system dedication in the U.S.
- Potential new process in the U.S.
- Summary

Definition

- “Commercial-grade dedication(CGD) is a process by which a commercial-grade item (CGI) is designated for use as a basic component. This acceptance process is undertaken to provide reasonable assurance that a CGI to be used as a basic component will perform its intended safety function and, in this respect, is deemed equivalent to an item designed and manufactured under a 10 CFR Part 50, Appendix B, quality assurance program. This assurance is achieved by identifying the critical characteristics of the item and verifying their acceptability by inspections, tests, or analyses by the purchaser or third-party dedicating entity”

Aspects of CGD in the US

- Although CGD process focuses on the quality assurance aspects of developing a safety grade basic component, it is also about assurance that the basic component will perform its intended safety function
- Can be used for any level of components
  - This includes sub-component, component, sub-system, system, etc.
  - The choice of using CGD impacts, but is not tied to the use of the 50.59 process

System and Component Safety

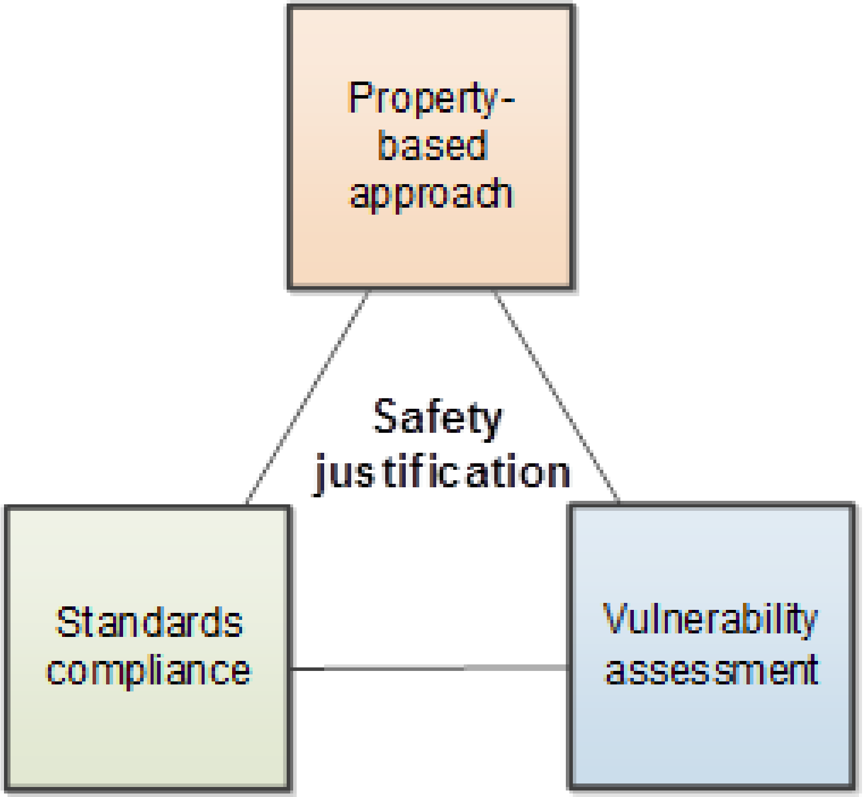
- Software Common Cause Failure
  - Diversity and defense-in-depth (D3)
- Independence
- Separation
- Redundancy
- Single failure criteria
- Deterministic performance
- EMI/RFI
- Environmental qualification

Dedication Process

- Commercial-grade dedication is an **acceptance** process by which a CGI is designated for use as a **basic component**
- An acceptable dedication program involves:
  - Review for suitability of application per Criterion III, "Design Control," of Appendix B
    - (i.e., Technical Evaluation)
  - Acceptance controls per Criterion VII, "Control of Purchased Material, Equipment, and Services," of Appendix B
    - (i.e., Four Acceptance Methods)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Dedication Process



Property-based approach

Safety justification

Standards compliance

Vulnerability assessment

The strategy triangle of justification

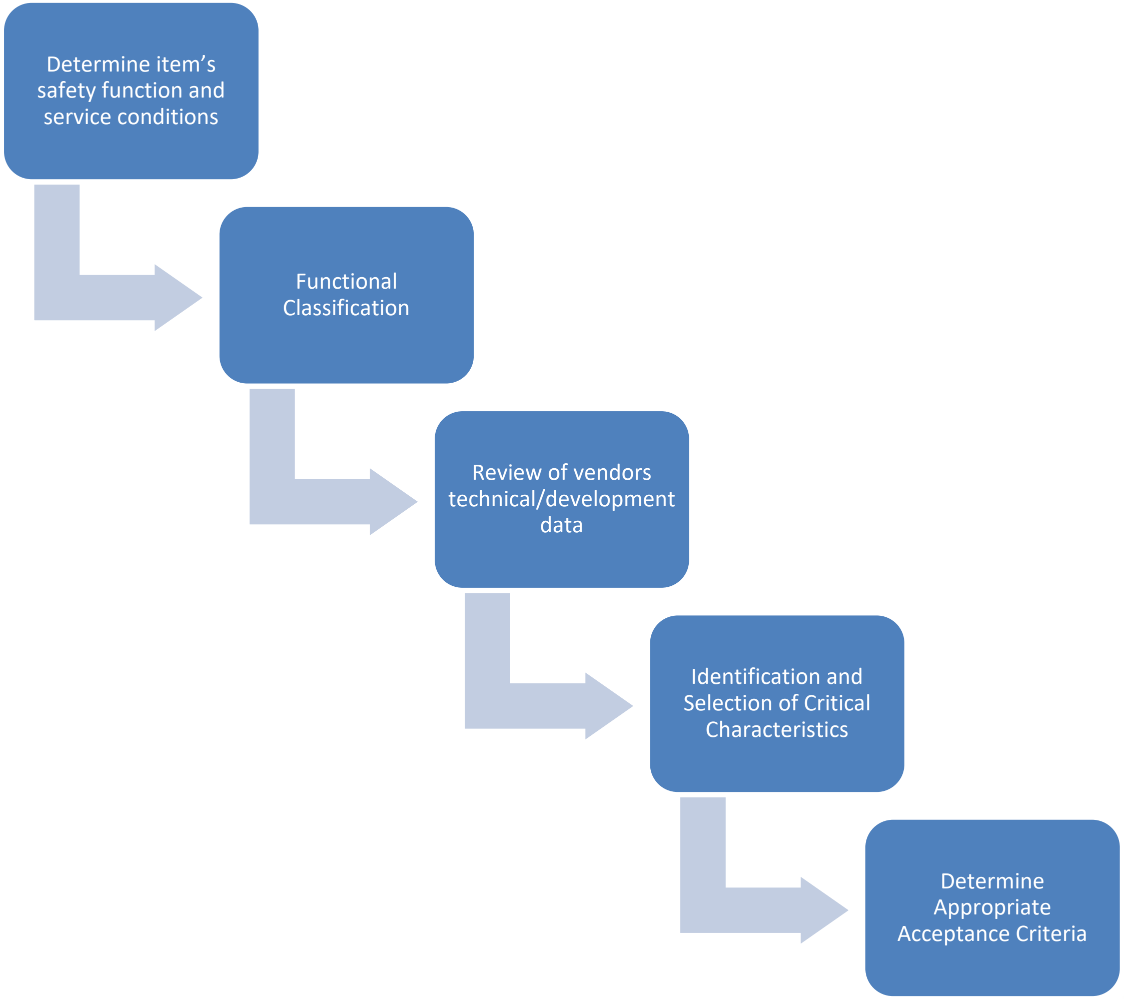
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Dedication Process

- **Technical Evaluations**
  - Determine item’s safety function and service conditions
  - Functional classification of items and components
  - Review of vendor’s technical/development data
  - Identification and selection of item’s critical characteristics
  - Determine appropriate acceptance criteria

- **Acceptance Process**
  - Method 1: Special tests and inspections
  - Method 2: Commercial-grade survey of supplier
  - Method 3: Source verifications
  - Method 4: Acceptable supplier/item performance record

Technical Evaluation



Determine item’s safety function and service conditions

Functional Classification

Review of vendors technical/development data

Identification and Selection of Critical Characteristics

Determine Appropriate Acceptance Criteria

Dedication of Digital I&C Equipment

- NRC conditionally accepted the following EPRI Guidance Documents for Dedication of Digital I&C including Programmable Logic Controllers (PLC):
  - EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," October 1996
  - EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," December 1996

Dedication of Digital I&C Equipment

- Digital I&C equipment introduces additional challenges
  - Access to detailed information/documentation (design, development, testing, verification/validation, configuration control)
  - Proper identification and verification of critical characteristics
    - Hardware + software (operating/application)
    - Extent and thoroughness of Critical Design Review (CDR)

Dedication of Digital I&C Equipment

- Digital I&C equipment introduces additional challenges
  - Complexity of the device – including its internal architecture, external interfaces, communication links, etc.
  - Use of software tools
  - Cybersecurity
  - Crediting relevant operating history
  - Environmental qualification
- Not all commercial digital I&C equipment can be successfully dedicated

Critical Design Reviews

- Often, the critical design review (CDR) is considered synonymous with the use of commercial grade survey (CGS), and this can cause confusion
- While the CDR and CGS both involve seemingly similar vendor assessment activities, the goals of these two activities are very different
- A CDR is a very technically focused activity that includes some quality assurance (QA) oriented reviews, which results in a determination of the suitability of the design for the application

Critical Design Reviews

- A CGS is a very QA focused activity that includes some technical reviews resulting in a determination of whether items are being manufactured in compliance with the already accepted design
- Although it is not endorsed by the US NRC, EPRI 1011710 is often used as guidance for performing the CDR

Critical Design Reviews

- Critical characteristics are those important design, material, and performance characteristics that, once verified, will provide reasonable assurance that the item will perform its intended safety function

Critical Design Reviews

- Translation of design requirements into critical characteristics is a key element in the dedication process
  - A complete definition of requirements, including hardware, software, human-machine interface, quality and reliability requirements, is an important prerequisite for dedication of a commercial grade item
  - For mechanical and electrical equipment most of the critical characteristics fall into the category of physical or performance characteristics
  - A third type of critical characteristic, referred to as dependability, becomes significantly more important when dedicating digital equipment including software

Critical Characteristics

- Types of Characteristics
  - Physical Characteristics
  - Performance Characteristics
  - Dependability Characteristics
- Failure analysis supports dedication as well as design and licensing (10 CFR 50.59) — in fact, the failure analysis may identify some of the critical characteristics, and it provides information that assists in evaluating and verifying critical characteristics

Critical Characteristics

- Dependability Characteristics
  - The dependability attributes, such as reliability and built-in quality, are influenced by the process and personnel used in the design, development, V&V, configuration management, etc.
  - The dependability of a digital device also can be influenced by robustness of the hardware and software architectures, self-checking features such as watchdog timers, and failure management schemes
  - Evaluation of these attributes requires that the dedicator focus on more than just the development and QA processes

Dedication Activities

- Third party dedicators will need to:
  - Review design and documentation
  - Review the design process
  - Failure analysis
  - QA and configuration control
  - Verification and Validation
  - Vendor testing
  - Performance analysis
  - Operations experience and its use in the design process
  - Problem reporting by 10 CFR 21
  - Supplemental activities

Dedication Activities

- IEEE 7-4.3.2 and software tools
  - IEEE 7-4.3.2-2010 added CGI dedication (Clause 5.17) as an alternative to establish suitability of software tools for use in safety related systems
  - Although the scope of EPRI guidance does not directly address software tools used to support the development of operating and/or application software the guidance provided may be considered

Developments Impacting Software Dedication

- Embedded digital devices (EDDs)
  - EDD, RIS 2016-05, issued April 29, 2016
  - Commercial-grade products containing EDDs that include software, software-developed firmware, or software-developed logic that have not been developed in accordance with guidance and acceptable industry standards
  - Requirements to identify the use of EDDs and sufficiently document the quality of the EDDs to support commercial-grade item dedication

Challenges

- Common cause failure (CCF) mitigation
- Effective grading of licensing reviews
- No policy on configurable versus programmable devices
- Configuration management
- Cyber Security

New process

- A new process has been proposed to make greater use of previously completed third party reviews of commercial products
- This approach takes advantage of the internationally recognized SIL certification process when accepting commercial grade digital equipment
- Purchasers that procure commercial grade equipment would be able to rely on the third party SIL certification process in lieu of conducting a commercial grade survey

New Process

- Process will focus on the dependability characteristics that are usually evaluated using commercial grade survey
- The specific processes and procedures used are driven by a particular SIL level (usually SIL 2 or SIL 3)
- The process uses Part 3 of IEC 61508 that focuses on the software development aspects
- IEC 61508 process includes
  - Visiting and auditing the manufacturer’s design and manufacturing facilities
  - Reviewing design documentation, and verifying calculations and technical evaluations
  - Evaluate data

New Process

- The SIL certification process requires the component vendor to identify (and correct) problems as part of the certification process
- The supplier shall have a contractual relationship in place to ensure notification of errors is obtained
- There would need to be some process to observe accreditation bodies that accredit to IEC 61508
- Dedication maintenance would also have to be tied in some way to the maintenance of the SIL certification

Clarifying Commercial Grade Dedication Expectations

- Industry guidance has been for evaluating and accepting CGIs for use in safety-related applications
- NRC endorsed (RG 1.164) industry guidance
- Critical characteristics must be defined and verified
- Use of third party certification (IEC 61508) to verify certain critical characteristics, such as "dependability" has been proposed

Questions ?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment