Evidence that the Operational and Maintenance Requirements and Constraints are Identified Correctly and Satisfied

U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Presented by: Norbert Carte NRC/NRR/DE/EICB

Software Certification Consortium - Meeting #10
January 7 - 8, 2013

Disclaimer

This presentation represents the personal opinions and viewpoints of the presenter. Although the presenter is an employee of the NRC, the NRC expresses no opinion whatsoever either in support of, or in opposition to, the contents of this presentation. The NRC supports the efforts of the presenter in the preparation of this presentation in the interest of fostering discussion and of the broad promulgation of ideas, but does not endorse the ideas themselves. Reference to this presentation is not a sufficient basis for establishing the acceptability of any proposed system, and will not be accepted as an adequate justification or technical explanation in any licensing application. The contents of this presentation have not been reviewed or approved by the NRC. Applicants and licensees who wish to adopt any of the ideas presented herein will need to provide their own justifications and demonstrations of suitability.

Agenda

- Regulated Domain
- Evidence
- Evidence For Who?
- Safety vs. NonSafety
- Protection vs. Control
- Traditional Regulatory Evidence
  - Acceptable Plans
  - Faithful Implementation
  - Acceptable Results
- Design Bases
- Plans as a basis for evidence

Regulated Domain

- Nuclear Power Plant (NPP)
  - Initial Licensing
    - Construction Permit and Operating License vs.
    - Design Certification and Combined License
  - Digital Upgrade
  - Existing, Small Modular, Passive, non-Light Water, …
- Non-Power Reactors
  - Research & Test Reactors; Isotope production facilities
- Fuel Cycle Facilities
  - Mining, Enrichment, Disposal, & Reprocessing
- Medical

Regulated Domain Existing NPP Digital Upgrade

- Digital upgrade of a Single Safety System
  - Mostly Logic, some Displays and Controls
    - Not sensors, Not actuators
  - Context of System is defined
    - Operating Procedures
    - Maintenance Procedures
    - Other Systems & Functions
  - QA Program (10CFR50 Appendix B)
    - Programmatic Approval
    - Continued Oversight of Implementation

Evidence

- Demonstrates that requirements are complete, consistent, and correct (i.e., necessary and sufficient).
  - Functionality, Timing, Accuracy, Reliability …
  - Robustness, Safety, Security, …
- Demonstrates that the system faithfully implements the requirements, and nothing else.
- Types of Evidence
  - Signatures & Certificate
  - Summary Reports, Analysis Reports …
- Acceptance Criteria
  - Existence & Competence
  - Standards, Techniques …
- Who Produces Evidence (e.g., Independent, Third Party, …)

Evidence For Who?

- The Public
  - Safety Evaluation & Publically available material
  - Processes Followed & Regulations Met
  - That the health and safety of the public is protected
- The Regulator
  - Docketed Material, Audits & Inspections of all material
  - That Licensee did its job to design and implement a safe system
- The Nuclear Power Plant (Licensee)
  - For: (1) itself, (2) Regulator, …
- The Vendor
  - For: (1) itself, (2) Licensee, …

Safety vs. NonSafety

- Safety-Related
  - Credited in Accident Analysis
  - Protection System
  - Certain Controls and Indications
- NonSafety
  - Not Credited to function in Accident analysis
    - UNLESS functioning is more adverse
- Important-to-Safety
  - E.g., Reactivity Control System

Protection vs. Control

- Protection Systems
  - Manual (Indications & Controls) or Automatic Means
  - Receive most regulatory scrutiny
  - Limited functionality
- Control Systems
  - Safety-Related
    - E.g., Pressurizer Pressure
  - Important-to-safety
    - E.g., Reactivity Control Systems
  - NonSafety-Related
    - E.g., Balance of Plant

Layers of Design - Iteration

- Nuclear Power Plant
  - Diversity and Defense-in-Depth (i.e., Multiple systems)
  - Natural Occurrences
- Systems – equipment for accomplishing a safety function
  - E.g., Reactor Trip System, Engineered Safety Features, …
  - Single Failure, Independence, Redundancy, …
- Safety Group - minimal set of that can accomplish a safety function
- Divisions - set of components that is independent from other redundant sets of components.
- Functions / Channel - generate a single protective action signal
- Components / Modules – field replaceable items

Traditional Regulatory Evidence

- The staff's acceptance of software for safety system functions is based upon:
  - (1) confirmation that acceptable <u>plans</u> were prepared to control software development activities,
    - E.g., Software Operations Plan
    - E.g., Software Maintenance Plan
  - (2) evidence that the plans were <u>followed</u> in an acceptable software life cycle, and
  - (3) evidence that the process produced <u>acceptable design outputs</u>.

Design Basis

- Design Basis for Safety System Documentation Must Include
  - Modes of Operation, for each mode:
    - events
    - initial conditions and allowable limits
    - safety functions and corresponding protective actions
  - variables that are to be monitored to control each protective action; the limit associated with each variable,
  - ranges and the rates of change of the variables to be accommodated until completion of the protective action
  - Environmental conditions
  - Performance requirements
- No comparable regulatory requirement to document the design basis of control systems

Digital Upgrade to a Safety System

- Ensure Equipment Specifics are addressed
  - E.g., cycle power every refueling outage

- Ensure that any Design Bases changes are addressed
  - E.g., new requirements because new technology is used
    - Software Common Cause Failure
    - EMI / RFI Suseptability
    - Type Testing or not
    - Cyber Security

Initial Licensing Operations Plan

- Describe general operation functions
  - Design Bases
    - Functions
    - Operating Bypass
  - Constraints
    - Safety
    - Security

Initial Licensing Maintenance Plan

- Describe general maintenance functions
    - Preventive Maintenance
        - Operability Determinations
            - Operable/inoperable/degraded
        - Repair, Test, and Calibrate
        - Maintenance Bypass
    - Corrective Maintenance
        - Fault location (e.g., diagnostic indications)
        - Repair procedures
    - Adaptive Maintenance
        - Design Change
            - Design Bases Documentation Change

Questions?

End of Presentation