Presentation to the Nuclear Regulatory Commission for Application & Lessons Learned from RIS 2002-22, Supplement 1

Wesley Frewin
Corporate Manager-ERT Digital
February 27, 2019

Disclaimer

For the purpose of ensuring on-going compliance with 10 CFR 810 requirements and staying within the constraints of NextEra Energy's non-disclosure agreements with applicable equipment suppliers, this presentation will NOT discuss technical details, including hardware/ software design and configuration. The level of detail will be sufficient to support feedback on the first-time use of RIS 2002-22, Supplement 1 for a complex digital modification and noteworthy Lessons Learned.

- **Focus is on:**
  - Application of RIS 2002-22, Supplement 1 for a complex digital upgrade in progress
  - Lessons Learned

FPL

Scope of the Change

- **St. Lucie Units 1 & 2, the activity replaces the Control Element Assembly (CEA) Control System with Westinghouse Advanced Rod Control Hybrid (ARCH) digital control system with Ovation-based logic, including:**
  - Step count position indication logic
  - Rod Control and Rod Position Indication Human-Machine Interface equipment
  - Upgrade to existing Turbine Control Ovation system, such that network equipment will be common to both Turbine Control and Rod Control

Threshold for Application of RIS 2002-22, Supplement 1

- **Thresholds for applying RIS 2002-22, Supplement 1**
  - "This guidance applies to modifications of safety-related systems or components but may also be applied to modifications of non-safety related systems or components at the discretion of the licensee."
  - "The activities listed below are examples of digital I&C modifications that licensees can likely implement without prior NRC approval using properly documented qualitative assessments… digital upgrades to non-safety related control systems
  - "The evaluation of these proposed modifications is expected to be straightforward if they have no interconnectivity across channels, systems, and divisions; and they do not reduce the redundancy, diversity, separation, or independence of their UFSAR-described design functions. However, digital modifications that involve networking, combining design functions from different systems; interconnectivity across channels, systems, and divisions; or shared resources merit careful review to ensure that such modifications incorporate appropriate design attributes so that reductions in the redundancy, diversity, separation, or independence of UFSAR-described design functions are not introduced.

FPL

UFSAR-Described System Functions

- The Rod Control System and Main Turbine Control System are both non-safety-related and were originally designed as separate systems (i.e., no sharing of component resources or communication for the purpose of control).
- Each system has many Design Functions stated in the UFSAR
- Both systems have a system-related description in UFSAR Chapter 15: CEA Drop Accident and Loss of Load Event
- Other functions not described in the UFSAR include RG 1.97, Type B, Category 3, Post Accident Monitoring display for CEA "Full In" and "Full Out"

FPL

Qualitative Assessments

- **Based on the complexity of this change, St. Lucie chose a segmented approach to performing Qualitative Assessment per RIS 2002-22, Supplement 1**
  1. Replacement of the Core Mimic Display with Ovation Logic and a Touch Screen Display
  2. Replacement of the Pulse Count Foxboro Rod Position Indication with Ovation Logic
  3. Replacement of Reed Switch Position Transmitters (RSPT) Control Element Assemblies Position Display System (CEAPDS) Rod Position Indication with National Instruments PLC logic
  4. Replacement of Control Element Drive System (CEDS)/Coil Power Programmers (CPP) rod control with Westinghouse ARCH and Ovation Logic
  5. Hardware/Software Update of Turbine Control Logic with revised Westinghouse Design

FPL

Common Outline for each Qualitative Assessment

- **Failure Mode Comparison (Existing versus Replacement)**
  - Failure due to mal-operation of an active component in the circuit logic
  - Failure due to loss of power
  - Failure resulting from environmental factors
- **Failure Results**
- **Qualitative Assessment Factors**
  - Design Attributes
    - -- Defense-in-depth, Diversity, Independence & Redundancy
    - -- Inherent Design Features for Integrated Software and Hardware or Architectural /Network
    - -- Mitigation of design weaknesses and low-reliability components in the current design
    - -- Non-Concurrent Triggers
    - -- Extensively Tested
    - -- Diverse Indication of Failure
- **Quality of Design Process**
- **Operating Experience**

FPL

Qualitative Assessment – Discussion Areas

- **Design Attributes to increase reliability and decrease failures**
  - Software version upgraded to ensuring full compatibility of communication between systems and hardware.
  - Revised architecture reflects the latest Emerson/Westinghouse standard design for Ovation DCS
  - Network design is a fully integrated cyber security solution
  - Battery-backed, redundant, and independent power supplies
  - Diverse (i.e., active and passive sensors) and triple redundant process level sensing
  - Redundant HMI screen-control stations with redundant traffic switches
  - More robust environmental testing, RG 1.180, Rev. 1 for EMC.
  - Organizational measures established for software development to minimize the probability of common cause failure
    - -- Turbine Control design team in one location
    - -- Rod Control design team on different location
  - Basis software functionality (widespread use in multiple industries)

FPL

Qualitative Assessment – Discussion Areas (cont'd)

- **Design Attributes to increase reliability and decrease in failures (cont'd)**
  - Network Design is single fault tolerant (two levels of redundant switches and multiple servers). No single failure results in loss of functionality
  - Application software logic executes at the controller level
  - Redundant controller pairs – duel attached to redundant switches providing 4-communication paths between a controller pair and the top level network; automatic failover
  - Critical software applications at the top-level network are hosted on multiple servers.
  - System segregation between controller pairs
  - Human Factors to avoid undesired commands (e.g., 2-action approach)
  - Self-Diagnostic Features
    - -- Capable of identifying credible failures
    - -- Graphics that pin-point source of postulated failure, accessible from any work station.
    - -- Watchdog timers for all critical components/processes

FPL

Qualitative Assessment

- **Failure mode comparison by examining "existing system" to "replacement system"**
- **Postulated Failure Scenario Approach**
  - Failure due to mal-operation of an active component in the logic circuit
  - Failure due to loss of power
  - Failure resulting from environmental factors
- **Examine each postulated failure and determine impact on design functions**
- **Examine environmental factors to ensure specifications support operation within the environment with margin**
- **Examine HU-related factors in design**
- **Examine common components to both Rod Control and Turbine Control and determine if a common cause failure exists**
- **Examine Testability**
- **Diverse indication of failure**

FPL

Qualitative Assessment (Cont'd)

- **Quality of Design Process – Confirmed compliance to appropriate sections of over 30 current industry and regulatory standards stated in:**
  - Westinghouse Ovation Distributed Control System (DCS) Design Specification; and,
  - Westinghouse System Quality Assurance Plan

  Including, Reg. Guides, ANSI, EPRI, IEC, IEEE, NEI, and several Westinghouse product quality documents

- **Operating Experience – Many foreign and domestic applications:**
  - AP-1000 & APR-1400 plants
  - Combined system applications at domestic plants (with differences) at Byron and Braidwood plants
  - Turbine Control System Retrofit OE at several foreign and domestic plants

FPL

Qualitative Assessment Conclusion Guidance

- **RIS 2002-22, Supplement 1 states the following:**
  - "A qualitative assessment can be used to support a conclusion that a proposed digital I&C modification will not result in more than a minimal increase in the frequency of occurrence of accidents or in the likelihood of occurrence of malfunctions (10 CFR 50.59(c)(2)(i) and (ii)). A qualitative assessment can also be used to support a conclusion that the proposed modification does not create the possibility of an accident of a different type or malfunction with a different result than previously evaluated in the updated final safety analysis report (10 CFR 50.59(c)(2)(v) and (vi)). These conclusions can be satisfied if a proposed digital I&C modification has a sufficiently low likelihood of failure."
  - "For digital I&C modifications, an adequate basis for a determination that a proposed change involves a sufficiently low likelihood of failure may be derived from a qualitative assessment of factors such as design attributes, the quality of the design processes used, and an evaluation of relevant operating experience of the integrated software and hardware used (i.e., product maturity and in-service experience). The licensee may use a qualitative assessment to document the factors and rationale for concluding that an adequate basis exists for determining that a digital I&C modification will exhibit a sufficiently low likelihood of failure."

FPL

Qualitative Assessment Conclusions

- **Based on the guidance stated above and the detailed guidance in the RIS attachment, St. Lucie prepared five Qualitative Assessments that, in aggregate, envelope the proposed change to both the Turbine Control System and Rod Control System.**
- **Assessing the change, considering both standalone and shared resources described by the change, St. Lucie has concluded the following:**
  - The proposed digital I&C modification will not result in more than a minimal increase in the frequency of occurrence of accidents or in the likelihood of occurrence of malfunctions (10 CFR 50.59(c)(2)(i) and (ii))
  - The proposed modification does not create the possibility of an accident of a different type or malfunction with a different result than previously evaluated in the updated final safety analysis report (10 CFR 50.59(c)(2)(v) and (vi))
- **To arrive at this conclusion, the qualitative assessments considered factors such as design attributes, quality of the design processes used, the ability to be extensively tested along with consideration of worldwide relevant operating experience of the integrated software and hardware used (i.e., product maturity and in-service experience).**

FPL

Lessons Learned

- **Use of OE**: Use of OE in a qualitative assessment is essential and important for the following reasons:
  - To derive “a sufficiently low likelihood of failure” conclusion
  - To determine likelihood of failure in order to provide additional assurance for a digital device or system that may not be “highly testable”
  - To compensate for weaknesses in qualitative assessment “design attributes” and “quality of design” factors
  - To help “evaluate and demonstrate” “adequate dependability”

  However, ensuring that we are properly citing OE becomes a challenge when attempting to comply with the following RIS guidance for OE:
  - “product maturity and in-service experience” (understandable)
  - “substantially similar” (difficult to understand)
    - -- “differences may exist” (application and integration of hardware and software)
    - -- “architecture”, “design conditions” (e.g., ambient environment, continuous duty), “mode of operation”, and “design features that serve to prevent or limit possible CCFs”.
    - -- Table 1 has additional factors

  Additional clarity would be beneficial

Lessons Learned (cont'd)

- **Preparation Time:** On average, each Qualitative Assessment was ~32 pages in length, involving, on average, 3 days for each assessment to prepare. This does not include subsequent review during review of the 10 CFR 50.59 Review process
- **Format:** Format recommended by the RIS has some repetitive discussion areas that should be eliminated to improve efficiency
- **PLUS:** RIS specifies an approach that is clear cut and understandable. NRC expectations are thoroughly presented and adaptable. Success path is well laid out
- **PLUS:** Evaluation process inherently assists the preparer for reviewing original equipment manufacturer-supplied Failure Modes & Effects Analyses
- **PLUS:** Although Appendix D recommends the Qualitative Assessments be part of the modification package, they are also well suited as Attachments to 10 CFR 50.59 Evaluations
- **PLUS:** One benefit is the significant reduction in the level of detail when responding to the 10 CFR 50.59 Evaluation questions

FPL

Questions