Duke Energy

Oconee Digital LAR Licensing Plan - Update

❖ Introduction

❖ Digital LAR Finding

❖ Digital LAR Regulatory Requirements

❖ Digital LAR Regulatory Guidance

❖ Digital LAR Format and Content

❖ Cyber Security Licensing

❖ Document Availability

❖ Document Review Options

❖ Acceptance Review Checklist

❖ Proposed Digital LAR Review Plan

❖ Key Dates

❖ Licensing Actions

- ❖ The purpose of the Digital LAR Licensing Plan Update is to establish a regulatory framework that reduces the risk and uncertainty of licensing a digital LAR

- ❖ We are now approximately 5 months prior to planned submittal date – need to freeze all guidance documents and requirements

- ❖ Changes in guidance documents that occur after this date will be considered to extent practical (we can't hit a moving target)

- ❖ We'd like the staff to document its position with respect to this licensing plan

❖ *The facility and equipment, the operating procedures, the processes to be performed, and other technical requirements provide reasonable assurance that the licensee will comply with the regulations of 10 CFR Chapter I, and that public health and safety will be protected*

(RG 1.206, C.I.7, page C.I.7-1)

- ❖ **10 CFR 50.36 – "Technical Specifications"**

- ❖ **10 CFR 50.55a (h) – "Codes and Standards"**

- ❖ **10 CFR 50.62 – "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants"**

- ❖ **10 CFR 50, Appendix A – "General Design Criteria for Nuclear Power Plants"**

- ❖ **10 CFR 50, Appendix B – "Quality Assurance Criteria"**

- EPRI Topical Report (TR)-102348, Revision 1 - "Guideline on Licensing Digital Upgrades" as endorsed by RIS 2002-22

- SECY 93-087 - "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs"

- Branch Technical Position HICB-19 - "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems"

- Regulatory Guide (RG) 1.47 – "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," Revision 0, May 1973

- RG 1.53 – "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," Revision 2, November 2003

- RG 1.62 – "Manual Initiation of Protective Actions," Revision 0, October 1973

- RG 1.75 – "Physical Independence of Electric Systems," Revision 3, February 2005

- RG 1.118 – "Periodic Testing of Electric Power and Protection Systems," Revision 3, April 1995

- RG 1.152 - "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"

- RG 1.153 - "Criteria for Safety Systems" and IEEE 603-1991 - "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"

- ❖ RG 1.168 – "Verification, Validation, reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 1, February 2004

- ❖ RG 1.169 – "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, September 1997

- ❖ RG 1.170 – "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, September 1997

- ❖ RG 1.171 – "Software Unit Testing for Digital Computer Software in Safety Systems of Nuclear Power Plants," Revision 0, September 1997

- ❖ RG 1.172 – "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, September 1997

- ❖ RG 1.173 – "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, September 1997

- ❖ RG 1.180 – "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety Related Instrumentation and Control Systems," Revision 1, October 2003

- ❖ RG 1.206– Combined Licenses for Nuclear Power Plants (LWR edition)," June 2007; specifically, C.1.7, "Instrumentation and Controls."

- ❖ RG 1.209 – "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," March 2007

❖ Note – in many instances the existing regulatory guidance documents endorsed IEEE Standards that have been recently revised

❖ The policy of Oconee will be to state explicitly within the LAR the IEEE Standard to which the Digital RPS/ES Systems has been designed

- ❖ NEI 06-02 provides guidance for the basic format and content

- ❖ RG 1.206 provides guidance for the technical portion of the LAR

  - ↗ BTP 7-14 will be used to address Software QA

- ❖ Comparison of RG to SRP identified differences

  - ↗ RG does not require auxiliary features or multi-unit stations to be addressed/SRP does

    - ☞ Concerns in IEEE standard and Regulatory Guidance do not apply to the Oconee RPS/ES modification
    - ☞ Human factors considerations are to be addressed in Chapter 18 – Oconee will address in LAR itself using the existing Oconee human factors process

9

- ❖ May 1, 2007, meeting discussed cyber security

- ❖ Duke plans to submit two letters (AREVA & Duke) addressing cyber security requirements (labeled withhold from public disclosure pursuant to 2.390)

- ❖ Submittal will be prior to RPS/ES LAR submittal and incorporated by reference as permitted by 10 CFR 50.32

- ❖ Duke may request a separate SE that would permit use on not only the Oconee RPS/ES LAR submittals but also future Duke digital LAR submittals

Duke Energy

- ❖ Existing regulatory guidance assumes that all design documents will be available at time of LAR submittal

- ❖ All documents listed in NRC letter dated January 11, 2006 will be available at time of submittal with a few exceptions

Post-Submittal Document Availability

❖ Factory Acceptance Test Procedures   January 2008

❖ Site Acceptance Test Plan   1st quarter 2008

❖ Factory Acceptance Test Results   December 2008
Requirements Traceability Matrix (post FAT version)
SAT Procedures

❖ SAT Results   June 2009

❖ Power-Imbalance Safety Limits and Setpoints   July 2009

❖ Removal and Restoration Procedures   October 2009
Training documents
Operating documents
Maintenance documents

Duke Energy — Document Review Options

- ❖ Option 1 – Onsite Reviews at Oconee (1 or more)
  - ↗ Availability of Duke/AREVA personnel to answer questions
  - ↗ Unit 1 equipment available for observations
  - ↗ Document in trip report
  - ↗ Staff travel may be a concern
- ❖ Option 2 – Reading Room at AREVA Offices in Bethesda
  - ↗ Reading room open for a set period of time
  - ↗ Duke/AREVA personnel could meet with staff periodically to answer questions
  - ↗ Document review in trip reports
  - ↗ Minimizes staff travel impact
- ❖ Option 3 – Meetings in NRC Offices (Open or Closed)
  - ↗ Pre-send documents for staff review
  - ↗ Meetings to answer questions
  - ↗ Document in meeting summaries

Duke Energy

❖ See draft proposed Acceptance Review Checklist

❖ LAR Submittal

❖ + 1 Month – Acceptance Review Complete

❖ + 4 months – All RAIs sent by NRC to Duke

❖ + 6 months – All RAI responses submitted by Duke

❖ + 8 months – Staff conducts on-site audit

❖ + 9 months – Management Meeting to identify any areas of concern not resolved

❖ +11 months – Technical Review complete

❖ +12 months – NRC issues Safety Evaluation

❖ Estimated date of submittal by 11/30/07

❖ Factory Acceptance Test: 2/18/08 – 10/1/08

❖ Safety Evaluation requested by 3/31/09

❖ Site Acceptance Test: 1/5/09 – 5/11/09

❖ Unit 1 Installation – Fall 2009

❖ Quality Process

❖ Setpoint Methodology

❖ Level of detail in selected sections of the LAR

❖ Confirm

    ↗ Finding

    ↗ Regulatory Requirements

    ↗ Regulatory Guidance

    ↗ Format and Content of LAR

    ↗ Document Availability & Review Options

    ↗ Acceptance Review Checklist

    ↗ Digital LAR Review Plan

❖ Future Meetings

Regulatory Guide 1.206	Yes	No
Section C.I.7 – Instrumentation and Controls		

Appendix C.I.7-A, Digital Instrumentation and Control Systems Application Guidance

The application addresses the following topics:

	Yes	No
(1) The design criteria to be applied to the proposed system.	☐	☐
(2) The I & C design as applicable to the final safety analysis report.	☐	☐
(3) Defense in depth and diversity	☐	☐
(4) Functional requirements and commitments	☐	☐
(5) Life-cycle process planning (refers to BTP 7-14)	☐	☐
(6) Life-cycle process requirements (refers to BTP 7-14)	☐	☐
(7) Software life-cycle process design outputs (refers to BTP 7-14)	☐	☐

Appendix C.I.7-B, Conformance with IEEE Std 603;
C.I.7.B-1 Safety System Design Basis

The application addresses the following topics:

	Yes	No
(1) Single-Failure Criterion	☐	☐
(2) Completion of Protective Action	☐	☐
(3) Quality (refers to BTP 7-14 which is software quality even though this section is for hardware quality)	☐	☐
(4) Equipment Qualification	☐	☐
(5) System Integrity	☐	☐
(6) Independence	☐	☐
(7) Capability for Test and Calibration	☐	☐
(8) Information Displays	☐	☐
(9) Control of Access	☐	☐
(10) Repair	☐	☐
(11) Identification	☐	☐
(12) Human Factors Considerations	☐	☐
(13) Reliability	☐	☐

Regulatory Guide 1.206	Yes	No

Section C.I.7 – Instrumentation and Controls

Appendix C.I.7-B, Conformance with IEEE Std 603;
C.I.7.B-2 Functional and Design Requirements
The application addresses the following topics:

	Yes	No
(1) Automatic Control	☐	☐
(2) Manual Control	☐	☐
(3) Interaction between the Sense and Command Features and Other Systems	☐	☐
(4) Derivation of System Inputs	☐	☐
(5) Capability for Testing and Calibration of System Inputs	☐	☐
(6) Operating Bypasses	☐	☐
(7) Maintenance Bypass	☐	☐
(8) Setpoints (documents available for NRC audit)	☐	☐

Appendix C.I.7-C, Conformance with IEEE Std 7-4.3.2;
C.I.7.C-1 Computer-Based Safety System Design Basis
The application addresses the following topics:

	Yes	No
(1) Single-Failure Criterion	☐	☐
(2) Completion of Protective Action	☐	☐
(3) Quality (refers to BTP 7-14)	☐	☐
(4) Equipment Qualification	☐	☐
(4)(a) Computer System Testing	☐	☐
(4)(b) Qualification of Existing Commercial Computers	☐	☐
(5) System Integrity	☐	☐
(6) Independence	☐	☐
(7) Capability for Test and Calibration	☐	☐
(8) Information Displays (documentation to be available for staff audit)	☐	☐
(9) Control of Access	☐	☐
(10) Repair	☐	☐
(11) Identification	☐	☐
(12) Human Factors Considerations	☐	☐
(13) Reliability	☐	☐

Regulatory Guide 1.206	Yes	No
Section C.I.7 – Instrumentation and Controls		

C.I.7.C-2 Cyber Security Requirements
The digital safety system development process should address
potential security vulnerabilities in each phase of the digital
safety system life cycle.(Refers to regulatory positions 2.1
through 2.9 of RG 1.152) *Not clear what should be provided in
the LAR itself.*

☐　　　☐