Competencies Required for Engineering of Digital Systems in Nuclear Power Plant

Steven Arndt

Office of Nuclear Reactor Regulation

May 6, 2013

Agenda

- Introduction
- Critical aspects of the nuclear industry
- Digital systems in the nuclear industry
- Competencies
- Summary

NRC Mission

License and regulate the Nation's civilian use of source, byproduct, and special nuclear materials to ensure adequate protection of public health and safety, promote the common defense and security, and protect the environment.
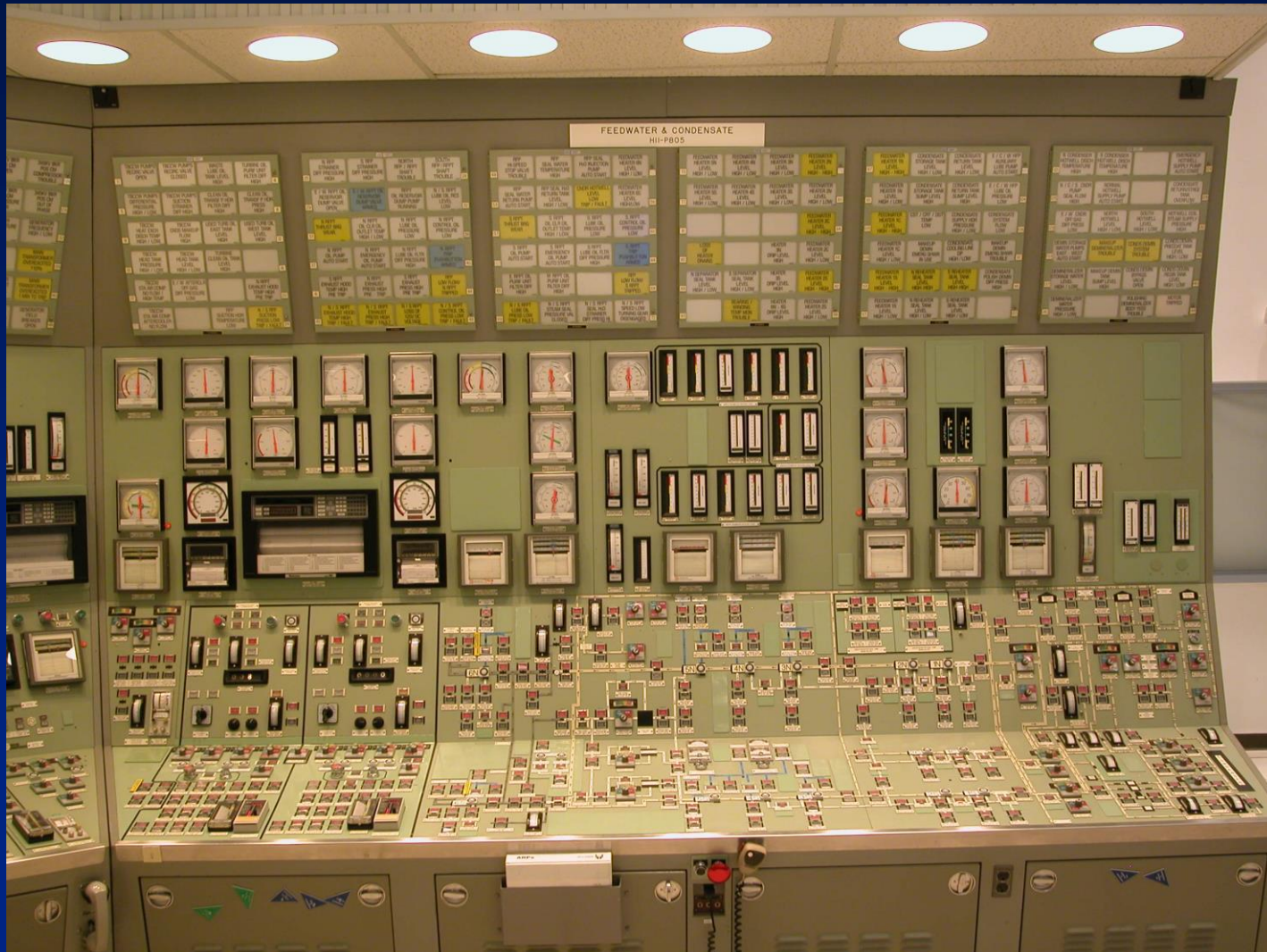
Nuclear Industry

- Highly regulated, safety critical industry
- Includes large and small equipment vendors, nuclear power plants, nuclear regulatory commission and other regulatory agencies
- Design and quality guided by industry standards and regulation
- Safety and non-safety systems treated differently

Digital Systems in Nuclear Power Plants

- In current plants combined with legacy analog systems, in new plants completely digital
- A number of different digital systems in same plant
- Very long lifecycles (development, licensing, and use)
- Slow to implement new technology
- Mix of systems developed specifically for nuclear and commercial off the shelf
- Significant public and stakeholder interactions

- Knowledge of industry
  - Nuclear plant design and operation
  - Interfaces with other professionals
- Knowledge of industry standards and regulation
  - Dozens of design, testing, qualification, V&V, etc., standards
  - Complex regulatory structure
  - Safety verse non-safety systems

Regulatory Framework

US.NRC — United States Nuclear Regulatory Commission
Protecting People and the Environment

IEEE 603-1991, Standard Criteria for Safety Systems for Nuclear Power Generating Stations

IEEE 279-1971 Criteria for Protection Systems for Nuclear Power Generating Stations

10CFR Part 50, Appendix A, General Design Criteria For Nuclear Power Plants

10 CFR Part 50, Domestic Licensing of Production and Utilization Facilities May 13, 1999

10CFR Part 50, Appendix B, Quality Assurance Criteria For Nuclear Power Plants And Fuel Reprocessing Plants

NUREG-0800 Rev. 5 March 2007, Standard Review Plan

USNRC Reg Guide 1.118, Periodic Testing of Electrical Power and Protection Systems

USNRC Reg Guide 1.152, Criteria for Programmable Digital Computer System Software in Safety Systems of Nuclear Power Plants

USNRC Reg Guide 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems

USNRC Reg Guide 1.168, Verification, Validation, Reviews, And Audits For Digital Computer Software used in Safety Systems of Nuclear Power Plants

USNRC RIS 2002-22, Use of NUMARC/EPRI TR-102348 in Determining the Acceptability of Performing Analog to Digital Replacements Under 10 CFR50.59

USNRC Reg Guide 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

USNRC Reg Guide 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

USNRC Reg Guide 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

USNRC Reg Guide 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

USNRC Reg Guide 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

Branch Technical Position HICB-14, Guidance on Software Reviews for Digital Computer Based Instrumentation and Control Systems.

IEEE 338-1987 Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Stations Safety Systems

IEEE 7-4.3.2-2003, Standard Criteria for Digital Computers in Safety Systems

IEEE 603-1991, Standard Criteria for Safety Systems for Nuclear Power Generating Stations

IEEE 1028-1988 Standard for Software Reviews and Audits

EPRI TR-102348, Guideline on Licensing Digital Upgrades

IEEE 828-1990, Standard for Software Configuration Management Plans

IEEE 829-1983, Standard for Software Test Documentation

IEEE 1008-1987, Standard for Software Unit Testing

IEEE 830-1993, Recommended Practice for Software Requirements Specification

IEEE 1074-1995, Standard for Developing Software Lifecycle Processes

EPRI TR-106439 Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications

ASME NQA-1-1983, Quality Assurance Program Requirements for Nuclear Facilities

ASME NQA-2a-1990, Part 2.7, Quality Assurance Requirements of Computer Software for Nuclear Facility Applications

IEEE 603-1991, Standard Criteria for Safety Systems for Nuclear Power Generating Stations

IEEE 1012-1986 Standard for Software Verification and Validation plans

IEEE 1012-1998 Standard for Software Verification and Validation

- System knowledge
  - System level requirements
  - Interfaces
  - Human Factors
- Digital system design alternatives
  - Analog verse digital
  - CPLDs and FPGAs
  - Diversity requirements
  - Redundancy requirements
  - Hardware options

Competencies

- Digital System Engineering
  - Engineering Processes
  - Requirements
  - Architecture
  - Design
  - Construction
  - Testing
  - Maintenance
  - Configuration Management
  - Quality Assurance
  - Cyber Security/Security Development and Operations Environment

- Software requirements fundamentals
- Requirements elicitation
- Requirements specification
- Requirements analysis
- Requirements verification and validation
- Requirements management

Software requirements fundamentals

- Concept of operations
- Types of requirements
- Product and process requirements
- Functional and nonfunctional requirements
- Quantifiable requirements
- System requirements
- Software requirements
- Derived requirements
- Constraints
- Requirements tracking

Construction

- Software construction fundamentals
  - Minimizing complexity
  - Constructing for verification
  - Standards in construction (coding standards)
- Construction methods
  - Construction measurement
  - Test-driven development
  - Tool selection and use
- Construction techniques
  - Error and exception handling,
  - Reuse,
  - Timing and synchronization

Qualifications Programs

- Plant Digital Engineer Qualification Program (INPO ADAD 98-04)

- Nuclear Regulatory Commission Technical Reviewer Qualification Program

- Digital System Vendor Qualifications

- Third party qualification programs (Software Engineering P.E., CSQE, etc.)

Plant Digital Engineer Qualification Program

Overview (1.1)

1.1-1*	Introduction
1.1-2*	Digital Delta
1.1-3*	Lifecycle Overview
1.1-4*	EPRI DI&C Program

Tech Basics (2.1)

2.1-1	Licensing Overview
2.1-2	Digital Component Architectures
2.1-3	Communication Architectures
2.1-4	Digital Delta Impact
2.1-5	Digital Risk
2.1-6	Software Risk
2.1-7	Process Variations
2.1-8	Cyber Security Overview
2.1-9*	DC/COL/DAC/ITAAC

Requirements Phase (3.1)

3.1-1	Req'ts. Characteristics
3.1-2	Safety Requirements
3.1-3	Requirements Expression

Related Processes (3.2)

3.2-1	Licensing
3.2-2	SW Safety Plans
3.2-3	SW V&V
3.2-4*	BTP 7-14 Software Lifecycle
3.2-5*	Vendor/Construction Oversight
3.2-6	Digital PRA
3.2-7	Failure Analysis Methods
3.2-8*	Cyber Security
3.2-9	Human Factors Engineering
3.2-10*	Configuration Management
3.2-11	COTS
3.2-12	COTS Compensation

Project Management (2.2)

New	Project Experience
New	Project Definition
New	Resources
New	Vendor Oversight
New	Scheduling, Dependancies
New	Training/Simulator/Lab
New	Cost Estimating

Design Phase (3.3)

3.3-1	Digital Characteristics 1
3.3-2	Digital Characteristics 2
3.3-3	CDR Intro
3.3-4	CDR Process
3.3-5	Architectural Concepts
3.3-6*	Interdivisional Communications
3.3-7	CCF Part 1
3.3-8	CCF Part 2
3.3-9	CCF Part 3

Program Management (2.3)

New	Regulatory Roadmap
New	NUREG 0800 (SRP), ISGs
New	MCR Modernization Trends
New	I&C Strategies (1015087)
New	Technical Programs
New	Resource Development
New	Organizational Models
New	Executive Buy-In

Implementation, Test, O&M Phases (3.4)

3.4-1	Testing Overview
3.4-2	IEEE 1012 (1998) Test Phase
3.4-3	O&M Support

Event (3.5) (Classroom Only)

New	Root Cause PJB
New	Event Reports
New	CARB

*Published in CBT format, available via CD-ROM under EPRI product # 1023013 (Dec 2011)

Nuclear Regulatory Commission Technical Reviewer Qualification

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

- Combination of study and OJT activities
- Combination of review and digital competencies
    - Regulation
    - Current licensing and design basis
    - Backfit process
    - Review and documentation process
    - Safety evaluations
    - Interfacing and exchange of Information with licensees and applicants, and vendors

Nuclear Regulatory Commission Technical Reviewer Qualification

- – Requirement and guidance document
- – Applicable codes and standards (primarily IEEE)
- – Setpoint methodology
- – Software quality assurance
- – Diversity and defense-in depth-principles
- – Digital equipment qualification
- – Digital technology and software development
- – Cyber security
- – Completion of safety function
- – Single failure
- – Etc.

![U.S.NRC logo - United States Nuclear Regulatory Commission - Protecting People and the Environment](logo)

Questions?