Verification and Validation of Nuclear Chiller Digital Controls

James M. Dean
NPEC 2011 Summer Meeting
Dana Point, CA
July 27, 2011
Future Nuclear Technology
Future Nuclear Chiller Control Technology

- **UNIT STATUS**
  - "UNIT IS LOADING"

- **COMPRESSOR CONTROL STATE**
  - "CMP IS RUNNING"

- **RUN/STOP**
  - RUN

- **UNIT OK**
  - YES

- **EVAP PSI**: 33.0
  - **EVAP SF TEMP**: 39.0°F
  - **SAT SUCT TMP**: 34.0°F
  - **SUCT TEMP**: 44.0°F
  - **COND. PSI**: 140.0
  - **DISCH TEMP**: 107.0°F
  - **SAT DISC. TEMP**: 97.0°F

- **CONDENSER**
  - 85.0°F
  - 95.0°F

- **EVAPORATOR**
  - 54.0°F
  - 47.0°F

- **Micro Control Systems**

- **Preferred**
  - Metal Technologies Inc.
Digital Technology and the U.S. Nuclear Industry

- Plants Designed and Constructed 1960’s – 1980’s
- State of the Art I&C Technology was Analog, Transistor, Op-Amp, PCB
- Industry-Wide Obsolescence and Lack of Qualified Supplier Support in 1980’s-1990’s
- Integration of “Digital Equipment” in 1990’s
- Industry Recognized Need to Address Digital Equipment
- New NRC Regulatory Guides
- New NUREGS
- New Plants – All Digital
Why Digital Controls for Existing and New Nuclear Chillers

- Obsolescence (Spare Parts)
- Obsolescence (Technology)
- Obsolescence (Chillers)
- Solution to Operational Issues such as Hard Starting, Surging and Highly Variable Operating Conditions
- New Compressors and Other Chiller System Subcomponents are Optimized for Digital Controls
**verification**: Confirmation by examination and provisions of objective evidence that specified requirements have been fulfilled.

**validation**: Confirmation by examination and provisions of objective evidence that the particular requirements for a specific intended use are fulfilled.

**NOTES**

1—In design and development, verification concerns the process of examining the result of a given activity to determine conformity with the stated requirement for that activity.

2—“Verified” is used to designate the corresponding status. [ISO 8402: 1994]

3—In design and development, validation concerns the process of examining a product to determine conformity with user needs.

4—Validation is normally performed on the final product under defined operating conditions. It may be necessary in earlier stages.

5—“Validated” is used to designate the corresponding status.

6—Multiple validations may be carried out if there are different intended uses. [ISO 8402: 1994]
3.1.36 **verification**: (A) The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase. (B) The process of providing objective evidence that the software and its associated products conform to requirements (e.g., for correctness, completeness, consistency, accuracy) for all life cycle activities during each life cycle process (acquisition, supply, development, operation, and maintenance); satisfy standards, practices, and conventions during life cycle processes; and successfully complete each life cycle activity and satisfy all the criteria for initiating succeeding life cycle activities (e.g., building the software correctly).

3.1.35 **validation**: (A) The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements. (B) The process of providing evidence that the software and its associated products satisfy system requirements allocated to software at the end of each life cycle activity, solve the right problem (e.g., correctly model physical laws, implement business rules, use the proper system assumptions), and satisfy intended use and user needs.
3.1.49 validation: The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.

3.1.50 verification: (1) The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase. (2) Formal proof of program correctness.

3.1.51 verification and validation (V&V): The process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and the final system or component complies with specified requirements.
Prospective V&V

- Classic V&V Model (e.g. IEEE 1012-1998)
- V&V Activities Performed in Parallel with Software Development
- Multi-Phased, Total Life-Cycle Approach

NOTES—The numbered lines represent the flow of control and data as defined below:
1) Submittal of program documentation (e.g., concept, requirements, design, users manuals) source code, program status, program budgets, and development plans and schedules.
2) Approval, denial, and recommendations on development issues and deliverables listed in #1.
3) Submittal of V&V task results, anomaly reports, activity summary reports, and other special reports.
4) Approval, denial, and recommendations on V&V issues and deliverables listed in #3.
5) Submittal of V&V task results, anomaly reports, activity summary reports, and special reports as directed by the acquirer program management.
6) Submittal of program documentation (e.g., concept, requirements, design, users manuals, special reports, source code, and program schedules).
Retrospective V&V

- Typical Scenario for V&V of Nuclear Chiller A/D Controls Upgrades or New Replacement Chillers
- V&V of "Reusable Software" ..... "Legacy Software" .......... "COTS Software"
- Classic V&V Model Not Applicable
- V&V Activities Performed After Software has been Developed (and Installed)
- Typical Retrospective V&V Activities
  - Black Box/White Box Testing
  - Software Code Reverse Engineering
  - Software Requirements Reverse Engineering
  - Software Design Basis Reconstitution
  - Operational History Analysis
  - Critical Digital Review
  - Product Documentation (Artifacts) Review and Analysis
Dedication and V&V Activities

Source: EPRI TR-106439, Evaluating and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications, October 1996 (Endorsed by USNRC RG 1.152, Rev. 1 and 2)
Digital CGI Acceptance Process

Commercial Grade Digital Item

→

Technical Evaluation + Acceptance Process + V&V

→

Dedicated Commercial Grade Digital Item

=

Digital Item Designed and Developed as Basic Component to 10CFR50 App. B
U.S. Nuclear Digital Regulatory Framework

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

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

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

USNRC Reg Guide 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

IEEE 74.3.2-2003, Standard Criteria for Digital Computers in Safety Systems

IEEE 828-1990, Recommended Practice 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 1012-1995, Standard for Developing Software Lifecycle Processes

IEEE 1028-1988, Standard for Software Reviews and Audits
IEEE 1028-1988, Standard for Software Reviews and Audits


IEEE 1012-1986, Standard for Software Verification and Validation

EPRI TR-102348, Guidelines on Licensing Digital Upgrades

Source: Steven A. Arndt, USNRC, Key Issues and Lessons Learned Associated with the Licensing of U.S. Digital Instrumentation and Control System Upgrades, Presentation to IAEA Nov. 3-6, 2008
Generic V&V Process Implementation

1. 10 CFR 50 App. B
   - EPRI TR-106439
   - RG 1.152

2. 10 CFR 50 App. B
   - IEEE 7-4.3.2
   - RG 1.152

3. 10 CFR 50 App. B
   - IEEE 1012
   - RG 1.168
**NUC-Magnum Digital Control System Overview**

- **Hardware Components**
  - NUC-Magnum Controller Board (Master)
  - NUC-SI16-A04 Sensor Input Expansion Board (Slave)
  - NUC-R010 Relay Output Expansion Board (Slave)
  - NUC-Keypad Display
  - NUC-Magtouch Color LCD
  - NEMA 4 Enclosure
  - Customer Specified Components and Interfaces
NUC-Magnum Digital Control System Overview

Diagram showing the system overview with the main components:
- SENSORS
- NUC-MAGNUM MASTER
  - Analog Output
  - Relay (Digital) Output
- NUC-SI16 AO4
- NUC-MAGTOUCH LCD
- NUC-MAGNUM KEYPAD/DISPLAY
- Communication methods:
  - I2C
  - Ethernet

Diagram includes Preferred Metal Technologies, Inc. logo.
Why NUC-Magnum?

- COTS Hardware and Software Designed Specifically for Chiller Control and A/D Retrofits in Critical Industrial Applications
- 1000’s of Units Installed with 10,000,000’s of Verifiable/Reliable Operating Hours
- Relatively Simple, Application Specific Software Code and Control Logic
- Software Highly Configurable without Need for Base Software Changes
- COTS Supplier Willing to Create, Control and Freeze Software and Hardware Design for Nuclear End Use Applications
- COTS Supplier Willing to Provide Total Access to Software Code for V&V
- No Life-Cycle Issues
NUC-Magnum V&V Project
Goals & Objectives

- Demonstrate the COTS Design Suitability for Safety Related Applications Through Rigorous V&V Process
- Develop, Implement and Document “Generic” V&V Process that Meets Nuclear Power Industry Technical, Quality and Regulatory Requirements
- Develop and Implement “Generic” V&V Process that Applies to All Potential Chiller Installations
- Perform Project Within Budget and Schedule Requirements
IEEE 1012, 1998, “Software Verification and Validation”
USNRC RG 1.168, Rev 1 - Verification, Validation, Reviews, and Audits for Digital Computer Software used in Safety Systems of Nuclear Power Plants – Feb 2004
NUC-Magnum V&V Project Organization

- **Personnel**
  - V&V Project Manager
  - Lead V&V Engineer
  - 3 V&V engineers

- **Responsibilities**
  - Ensure Compliance With Industry and Regulatory Requirements and Customer Specs
  - Prepare Software V&V Plan, Associated Documents/Reports and Related SOPs
  - Execute Tasks Identified in Software V&V Plan
**NUC-Magnum V&V Project Deliverables**

- Critical Digital Review (CDR)
- Software V&V Plan (SVVP)
- Software Quality Assurance Plan (SQAP)
- Software Requirements Spec (SRS)
- Software Design Description (SDD)
- Software V&V Report (SVVR)
- Failure Modes & Effects Analysis (FMEA)
- Hazards Analysis (HA)
- Software Code Review Records
- Software Validation Test Cases and Reports
- Software Bug List
Software Code Review SOP, PMT 3.5.G
Software Validation SOP, PMT 3.7.1.G
Hazard Analysis SOP, PMT 3.7.2.G
Software Critical Digital Review SOP, PMT 3.6 G
Software Maintenance SOP, PMT 3.7.3.G
Software V&V SOP, PMT 3.7.4.G
Software Development SOP, N1637-MCS-SD-1
PMT Micro Control Systems, Magnum Controller “C” Coding Guidelines, PMT N1637-CCG-1
NUC-Magnum V&V Project

V&V Plan Activities

- Create a Software Requirements Specification (SRS) by Reverse Engineering Existing MCS Magnum Source Code
- Compare Source Code to other MCS Documents (e.g. Technical Manuals, Flow Charts, Logic Diagrams)
- Perform Detailed Code Reviews of Magnum Source Code
- Perform a Qualitative Hazard Analysis of the MCS Magnum Controller (Hardware and Software) Using FMEA and FTA Techniques
- Develop and Perform Validation Testing of ALL Software Code Modules and User Interfaces Using MCS Test Bed
- Create a Requirements Traceability Matrix (RTM) that Maps SRS to Validation Tests
- Perform Factory Acceptance Tests (FAT) of Integrated Hardware, Software and User Interfaces Using a Production Chiller
NUC-Magnum V&V Project
Software Code Reviews

- **SOP**
  - PMT Software Code Review SOP, PMT 3.5.G, Rev. 0

- **Coding Standards**
  - PMT Procedure N1637-CCG-1, Micro Control Systems, Magnum Controller C Coding Guidelines

- **Code Reviews**
  - Review Code Against Coding Guidelines AND Design Docs
  - Prepared Reports
Hazard Analysis SOP PMT 7.3.2.G
  - FMEA (Bottom Up) and FTA (Top Down)
  - Guidance:
NUC-Magnum V&V Project Validation Testing

- Software Validation Performed Against Design Input Documents
  - Reverse-Engineered SRS
  - Developed State Diagrams
  - Abnormal Conditions and Events (ACEs)
  - Relevant Software Design Documents
  - MCS Operation Manual and Design Information
- Performed >340 Validation Tests
NUC-Magnum V&V Project
Validation Testing

- ACEs Include:
  - Loss of Supply Power
  - Degraded Supply Voltage
  - Sensor Input Open/Shorted
  - Sensor Value Out of Range (High/Low)
  - Loss of Data Communication between Master and Slave Boards/HMI
  - Data/Broadcast Storm
  - NUC-Magtouch Modbus Write Command to NUC-Magnum Board
  - EMI/RFI*
  - Seismic Event (Including Relay Output Chatter)*

*Not Formally Considered Validation Tests
NUC-Magnum V&V Project Validation Testing

- MCS Test Bed
  - Same Hardware, Software and Configuration File as Installed in NUC-Magnum Production Digital Controller
  - Inputs Simulated with Potentiometers and Relays
  - Outputs Represented by Lights (Relays)
  - Keypad and LCD Touch Screen

- Automated Test Process by use of a Digital Potentiometer Test Tool (DPTT)
  - Developed Software to Automate Testing
  - Software Developed under Controlled Process (SVVR, SRS, etc)
  - Provide Discrete Control of Multiple Digital DPTT POT Outputs
  - Interface to Manually Set DPTT Output Value
  - Automated Set of DPTT Output Values via Scripts that Includes Timed and Manual Steps
 NU C-Ma gn u m V & V P ro ject
 Fa c t ory A c c e pt ance T est ing

- Complete Chiller System Test Including Plant System
  Design Temperature, Pressure, Flow, Current
- Includes Chiller Design Capacity Test (ARI, ASHRAE)
- Includes Operation and Tuning of NUC-Magnum
  Control, Alarm and Trip Setpoints
Observations, Lessons Learned and Recommendations

- Industry V&V Requirements are Complex and Difficult to Implement on a Generic Basis
- Plant/Customer Expectation that V&V Process and Documents will be Project Specific
- Nuclear Chiller Controls V&V Specification Requirements are Inconsistent Across the Industry... Nationally and Internationally
- Nuclear Chiller Controls V&V Specification Requirements Often Not Tied to Plant Licensing Commitments
- Nuclear Chiller V&V Specification Requirements Often Dependent Upon Plant Digital Expert
Observations, Lessons Learned and Recommendations

- Nuclear Chiller Controls V&V Specifications Often Invoke Conflicting Requirements

- Chiller Replacement/Upgrade Projects Often Implemented By Third Party (e.g. A/E) that may or may not be Cognizant of Industry or Plant V&V/Digital Dedication Requirements

- Open and Constant Communications Between the Supplier, A/E and Plant Personnel are Key to Project Success.... TEAM Attitude is Imperative

- Completely and Thoroughly Understand YOUR Customers Expectations