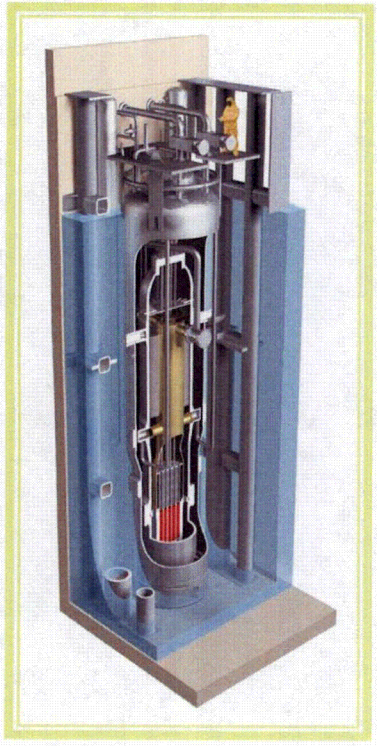
Enclosure 1:

"Multinational Design Evaluation Program Digital I&C Working Group Common Position Evaluations for NuScale Digital I&C Design," PM-0815-16440, Revision 0

NuScale Power, LLC
1100 NE Circle Blvd., Suite 200 Corvallis, Oregon 97330 Office 541.360-0500 Fax 541.207.3928
www.nuscalepower.com

Multinational Design Evaluation Program Digital I&C Working Group Common Position Evaluations for NuScale Digital I&C Design



Brian Arnholt
NuScale I&C Engineering

August 26, 2015

PM-0815-16440-NP
Revision: 0

NuScale Power™

Acknowledgement and Disclaimer

This material is based upon work supported by the Department of Energy under Award Number DE-NE0000633.

NuScale Power™

Meeting Purpose

- Compare Multinational Design Evaluation Program (MDEP) Digital I&C Working Group (DICWG) common positions to U.S. NRC regulations and guidance
- Highlight important aspects of MDEP common positions
- Discuss the NuScale Digital I&C Design and its relation to MDEP Common Positions

DICWG-01, Common Cause Failures

NRC Regulatory Guidance Applicable to NuScale I&C Design

- NUREG/CR-6303, "Method for Performing Diversity and Defense-in Depth Analyses of Reactor Protection Systems."
- IEEE-603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."
- IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."
- DSRS Chapter 7, Section 7.1.5, "Diversity and Defense-in-Depth."

Highlights and Takeaways

- Generally, consistent with NRC regulations and guidance
- MDEP Common Position only considers common cause failures (CCFs) introduced from a latent design deficiency during requirements, design, and implementation phases of the Digital I&C Development Life Cycle.
- Consistent guidance for analysis of CCFs concurrent with a design basis event (NRC goes further to define a best estimate analysis).
- Follows NRC guidance on use of manual/backup actuation.

Applicable NuScale Design Information

- Diversity and defense-in-depth compliance in DSRS Chapter 7, Section 7.1.5.
- NuScale Protection System Topical Report.
- Other information presented in DSRS Chapter 7.

DICWG-02, Software Tools

NRC Regulatory Guidance Applicable to NuScale I&C Design

- IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Section 5.3.2).
- RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants."
- RG 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

Highlights and Takeaways

- Generally, consistent with NRC regulations and guidance.
- Software tools are useful, efficient ways to improve the development process.
- Applies to tools used to: support the capture of requirements, support the translation of requirements into final system code and data (compilers, Verilog, etc.), V&V tools, and prepare/control application data (I/O database tools)
- V&V not required on tools if the target software is subject to V&V (RG 1.168)
- →MDEP Common Position does NOT apply to tools for complex programmable logic devices.

Applicable NuScale Design Information

- Software tools included in scope of review of NuScale design must follow RG 1.152 and IEEE 7-4.3.2.
- Development and application tools play a larger and different role in the V&V process, following guidance of IEEE-1012 and RG 1.168.

DICWG-03, Verification & Validation

NRC Regulatory Guidance Applicable to NuScale I&C Design

- RG 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."
- DSRS Chapter 7, Section 7.2.1, "Quality."
- IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations (Section 5.3.3).
- RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants."

Highlights and Takeaways

- MDEP Common Positions generally follow NRC guidance regarding scope, requirements for verification and validation (V&V), independence and processes, etc.
- MDEP position does not address software reliability verification (i.e., RG 1.168).
- NRC guidance more prescriptive regarding V&V independence.
- Scope of V&V should cover entire software life cycle and be specified in a V&V plan.

Applicable NuScale Design Information

- NuScale design conforms to NRC regulations and guidance as demonstrated in:
  - Digital I&C System V&V Plan – adapted to the NuScale Digital I&C Design Process.
  - IEEE 7-4.3.2 conformance assessments

NuScale Power™

DICWG-04, Data Communications

NRC Regulatory Guidance Applicable to NuScale I&C Design

- DSRS Chapter 7, Section 7.1.2, "Independence" (Also, DI&C-ISG-04[1]).
- RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants."
- IEEE Std. 7-4.3.2-2003, "IEEE Standard Criterial for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Section 5.6).

Highlights and Takeaways

- Generally, follows NRC guidance, although NRC guidance is more prescriptive and detailed.
- MDEP Common Position contains guidance on non-safety to safety communications consistent with NRC positions.
- Control of safety equipment from non-safety systems: One-way, must demonstrate safety benefit and that safety function is not compromised.

Applicable NuScale Design Information

- NuScale design conforms to NRC regulations and guidance.
- NuScale developing data communication conformance assessments consistent with DSRS 7.1.2 review criteria (DI&C-ISG-04 as guidance).

[1] Although not applicable to the NuScale application review, NRC guidance in DI&C-ISG-04 used to develop MDEP DCIWG-04 position.

NuScale Power™

DICWG-05, Treatment of HDL[1]

NRC Regulatory Guidance Applicable to NuScale I&C Design[2]

- DSRS Chapter 7, Section 7.2.1, "Quality."
- NUREG/CR-7006, "Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems Plant."

Highlights and Takeaways

- NRC review criteria (DSRS) treats programmable devices and micro-processors equally and follows rigorous safety system QA program.
- MDEP guidance on design and implementation recommends following technology rules of the supplier for design and implementation.
- Ensure PLDs demonstrate deterministic (predictable and repeatable) behavior.
- MDEP Common Position recommends NOT using intellectual property cores.

Applicable NuScale Design Information

- NuScale Safety Digital I&C Design based on use of programmable logic devices.
- NuScale Digital I&C Design Process documented in Digital I&C Quality Assurance Program and associated plans.
  - NuScale design life cycle processes account for both complex logics devices (no runtime software) and micro-processor devices.

[1] *Hardware Description Language*

[2] *Additional guidance in "EPRI Report, 1022983, Recommended Approaches and Design Criteria for Application of Field Programmable Gate Arrays in Nuclear Power Plant Instrumentation and Control Systems"*

NUSCALE POWER™

DICWG-06, Simplicity

NRC Regulatory Guidance Applicable to NuScale I&C Design

- DSRS Chapter 7, Appendix C, "Simplicity."

Highlights and Takeaways

- Generally, follows NRC guidance in DSRS.
- Avoid unnecessary complexity while still conforming to design requirements.
  - designs should be as simple as practicable
  - ensure initial requirements fully meet the safety objectives
- All features must be demonstrated to meet/support the intended safety function.

Applicable NuScale Design Information

- NuScale design principles incorporate simplicity elements into design.
- Rigorous requirements engineering process implements specific safety, operational, and other system functional requirements.
- Strict conformance to requirements assures no unnecessary functions or "features."

DICWG-07, Industrial Digital Devices

NRC Regulations and Guidance Applicable to NuScale I&C Design

- DSRS, Chapter 7, Section 7.1.5, "Diversity and Defense-in-Depth."
- U.S. Nuclear Regulatory Commission, Draft Regulatory Issue Summary (RIS) 2013-XX, "Embedded Digital Devices in Safety-Related Systems, Systems Important to Safety, and Items Relied on For Safety," Office of Nuclear Reactor Regulation, June, 2013.

Highlights and Takeaways

- Generally, follows NRC guidance in DSRS → treats embedded digital devices equally regardless of configuration of hardware/firmware/software
- Level of rigor applied to use of general, commercially available embedded devices should be commensurate with safety function (A1/A2/B1/B2 and SIL classification).
- Follow same rigorous digital I&C development processes for embedded digital devices. Commensurate with their quality and safety classification.
- MDEP Common Position good practices:
  - use information for use in safety applications in non-nuclear industries (pharma, aviation, etc.) to support use and application
  - include any restrictions on the use of the device in its intended application and do not contradict assumptions in the safety analysis (introduce new, unanalyzed failure modes).

Applicable NuScale Design Information

- NuScale following current regulatory issues related to use of embedded digital devices.
- NuScale Digital I&C System Quality Assurance Program uses graded approach based on Digital I&C component SIL classification, which equally applies to embedded digital devices.
- The NuScale Digital I&C Design will address use of embedded digital devices, if applicable, including failure modes and effects, common cause failures, and any contributing hazards to overall system safety.

DICWG-08, Cyber-Security in Digital I&C Designs

NRC Regulatory Guidance Applicable to NuScale I&C Design

- IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria For Digital Computers in Safety Systems of Nuclear Power Generating Stations" (Section 5.9).
- IEEE 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."
- RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants."
- DSRS Chapter 7, Section 7.2.9, "Control of Access."

Highlights and Takeaways

- MDEP Common Position consistent with NRC guidance with following relevant takeaways
- Software life cycle phases should account for security elements in each phase.
- Design should consider simplicity attributes when planning and developing features to address or mitigate security issues and justify the risk/benefit.
- Digital I&C QA program (requirements) should explicitly address requirements for security features.
- Demonstrate risk versus benefit for cyber-features in design and cyber-features must meet same quality requirements as resident system.

Applicable NuScale Design Information

- NuScale Digital I&C Secure Development and Operating Environment Plan will address cyber-security-related aspects of the Digital I&C design.
- Development of a Cyber-Security Plan (ref. 10 CFR 73.54) is scope of licensee. DCA will address control of access and SDOE plans.

DICWG-11, Digital I&C System Testing

NRC Regulatory Guidance Applicable to NuScale I&C Design

- RG 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."
- RG 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."
- IEEE Std. 1008-1987, "IEEE Standard for Software Unit Testing."

Highlights and Takeaways

- MDEP guidance consistent with NRC guidance. Scope of testing covers Integrated factory and site acceptance testing.
- Testing scenarios should cover full suite of the plant safety analyses.
- The testing program should be iterative with a feedback loop to include results from earlier design and development stages.
- All design requirements should be tested on a fully integrated system prior to on-site testing.

Applicable NuScale Design Information

- NuScale Digital I&C System QA Program includes following related to Digital I&C System Testing:
  - Digital I&C System Master Test Plan (follows guidance in RG 1.170 and IEEE-829)
  - Digital I&C System Configuration Management Plan (follows guidance in RG 1.169 and IEEE-828)
  - Digital I&C System Verification and Validation Plan (follows guidance of RG 1.168 and IEEE-1012)

DICWG-12, Automatic Surveillance Tests of Digital I&C Systems

NRC Regulatory Guidance Applicable to NuScale I&C Design

- DSRS Chapter 7, Section 7.2.15, "Capability for Test and Calibration."
- IEEE 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (Section 5.10, 6.5).
- RG 1.22, "Periodic Testing of Protection System Actuation Functions."
- RG 1.118, "Periodic Testing of Electric Power and Protection Systems."
- GDC 21, "Protection System Reliability and Testability."
- RIS 2006-17, 10 CFR 50.36(c)(3) (Technical Specification Surveillance Requirements).
- IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." (Sections 5.7, 5.5.2, 5.5.3).

Highlights and Takeaways

- Automatic testing should be a passive function and not impair performance of the safety functions.
- Surveillance testing should not compromise safety characteristics (independence, redundancy, etc.)
- Evaluate benefit of automatic tests against any increase in complexity of I&C design.
- Operators must be aware of faults identified through automatic testing (alarms, logs, etc.) and automatic system actions must be reflected in design.

Applicable NuScale Design Information

- NuScale will develop system testing methods as part of overall I&C system design and technical specification development.
- Interface with Operations and Human Factors is important to ensure consistency with control room operations and design.

Questions?

NuScale Power™

6650 SW Redwood Lane, Suite 210
Portland, OR 97224
503.715.2222

1100 NE Circle Blvd., Suite 200
Corvallis, OR 97330
541.360.0500

11333 Woodglen Ave., Suite 205
Rockville, MD 20852
301.770.0472

6060 Piedmont Row Drive South, Suite 600
Charlotte, NC 28287
704.526.3413

http://www.nuscalepower.com