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

COMMISSION MEETING WITH THE ADVISORY COMMITTEE ON REACTOR SAFEGUARDS (ACRS)

October 8, 2021

Agenda

- Joy Rempe, Vice-Chair, ACRS
  - Overview
- David Petti, Member, ACRS
  - Advanced Reactor Activities: 10 CFR Part 53, Fuel Qualification, and Source Term
- Charles Brown, Member, ACRS
  - Uni-Directional Communications from High Safety to Lower Safety Systems and Internal Plant to External Systems Connected to the Internet
- Matt Sunseri, Chair, ACRS
  - NuScale Control Room Staffing Plan Topical Report

Overview

Issued 14 reports since the last meeting with the Commission in December 2020:

- Non-LWR Activities
  - 10 CFR Part 53 (Interim Letter)
  - Advanced Reactor Computer Codes
  - KAIROS Fuel Performance Topical Report
- Small Modular LWR Activities
  - BWRX-300 Reactivity Control Topical Report
  - BWRX-300 Containment Performance Topical Report
  - NuScale Control Room Staffing Plan Topical Report

Overview (Cont'd)

- Digital I&C topics
  - Regulatory Guide 1.105 Setpoints for Safety-Related Instrumentation
  - Uni-directional Communications from Higher Safety-Significance Systems
  - Non-LWR I&C Design Review Guide
- Additional review topics
  - NRC Human Reliability Methods (IDHEAS-G)
  - Vogtle Units 1 and 2 LARs for Risk-Informed GSI-191 Resolution
  - Rulemaking Plan on Revision of IST and ISI Program Update Frequencies
  - Regulatory Guide 1.9 Application and Testing of Onsite AC Power Sources
  - Regulatory Guide 4.26 Volcanic Hazard Assessments

Other ACRS Activities

- Keeping abreast of selected Agency efforts
  - Embark and Be riskSMART efforts
  - Advanced LWR and non-LWR preparations and applications
  - ACRS staff follow and provide summaries of selected agency activities
- Identifying and implementing our own process improvements while continuing to focus on safety-significant issues
  - Updating bylaws and guidance to promote operational efficiencies
  - Evaluating the benefit/impact of optional ACRS letters
  - Continuing focused reviews with RES to provide more timely input
- Membership changes

Advanced Reactor Activities: 10 CFR Part 53, Fuel Qualification and Source Term

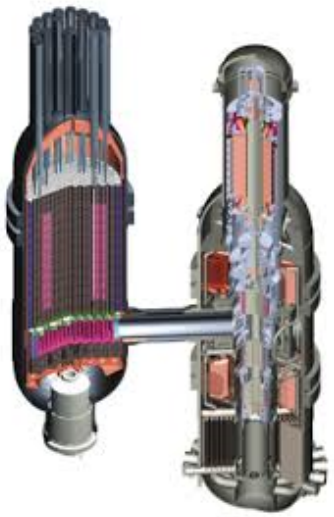
David Petti, Chair

Future Plant Designs Subcommittee

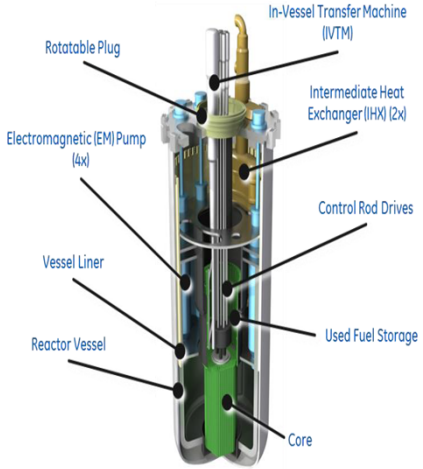
Advanced Reactor Technologies and Sizes Vary

- Many different reactor technologies derived from Generation IV and other government studies. Also includes fusion.
- A range of sizes from < 10 MWt to 600 MWt with the potential of multiple reactors on a single site.

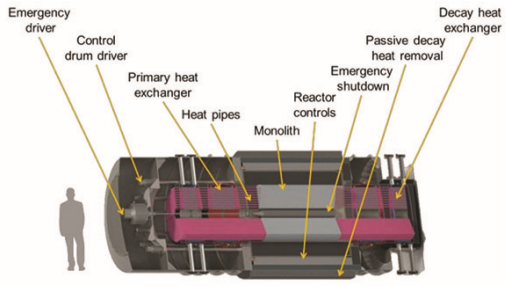
High Temperature Gas-Cooled Reactors



Sodium Fast Reactors



Heat Pipe Reactor



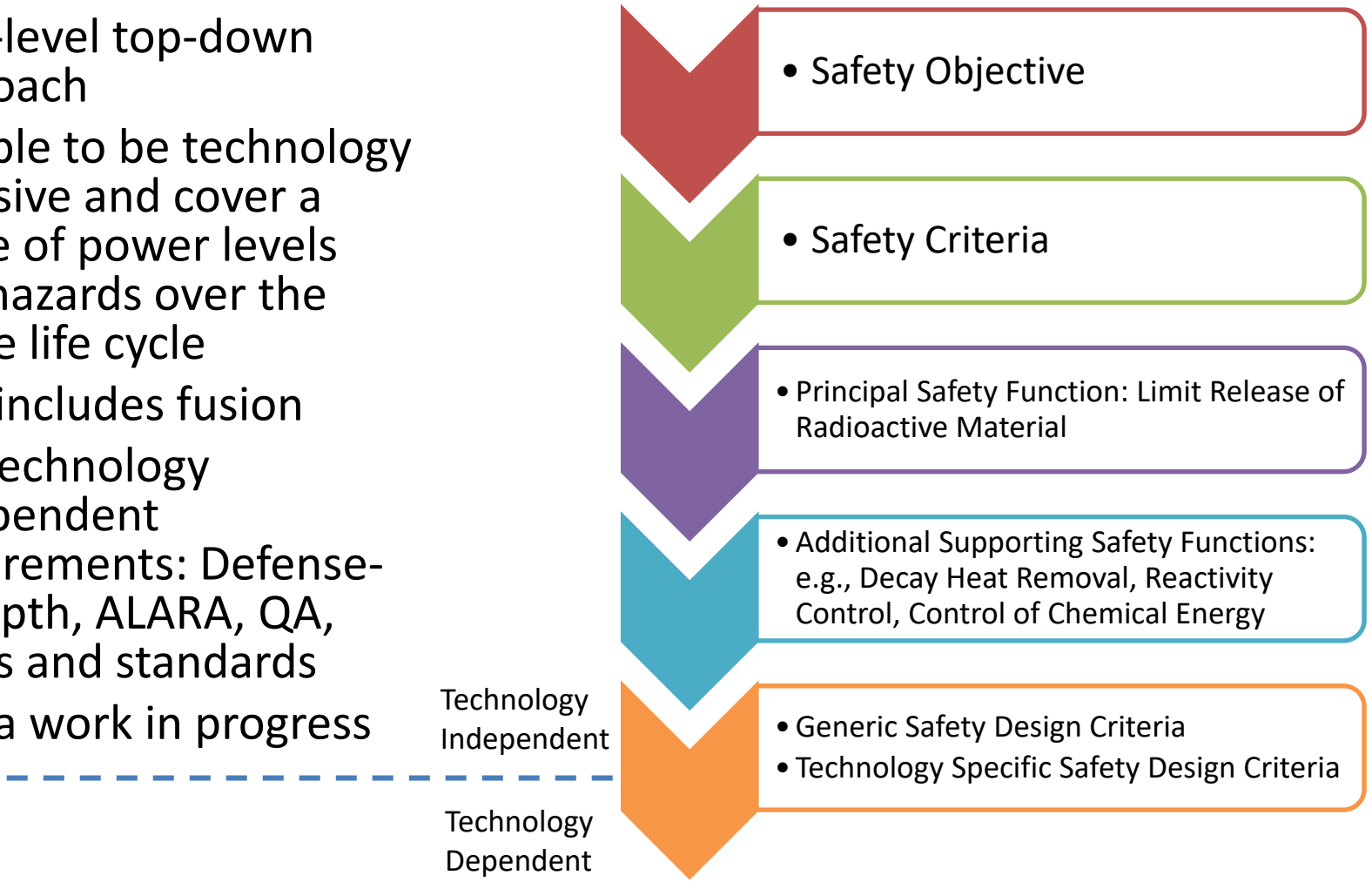
Advanced Reactor Characteristics

- Hazards vary with power level and radionuclide inventory
- Reduced source terms anticipated (affects siting and emergency planning with small EPZ and LPZ)
- Passive systems
  - Inherent characteristics
  - No need for AC power to operate safety systems
- More prevention/less mitigation
  - Defense-in-depth different than current fleet
  - Role of operator is different

These characteristics drive need for a flexible approach to development of 10 CFR Part 53.

10 CFR Part 53: Approach

- High-level top-down approach
- Flexible to be technology inclusive and cover a range of power levels and hazards over the entire life cycle
- Also includes fusion
- Key technology independent requirements: Defense-in-depth, ALARA, QA, codes and standards
- Still a work in progress



Many detailed comments from ACRS. Approach is logical and coherent. ACRS supports the approach taken by staff.

10 CFR Part 53: Further ACRS Comments (1/2)

- Flexibility versus Regulatory Certainty
- Embed more of the rationale into the rule itself
- Better definition of risk-based approach to reliability of SSCs that replaces the Single Failure Criterion
- Advanced reactor based surrogate metrics needed for Quantitative Health Objectives (QHOs)
- More clarity in wording related to safety analysis requirements

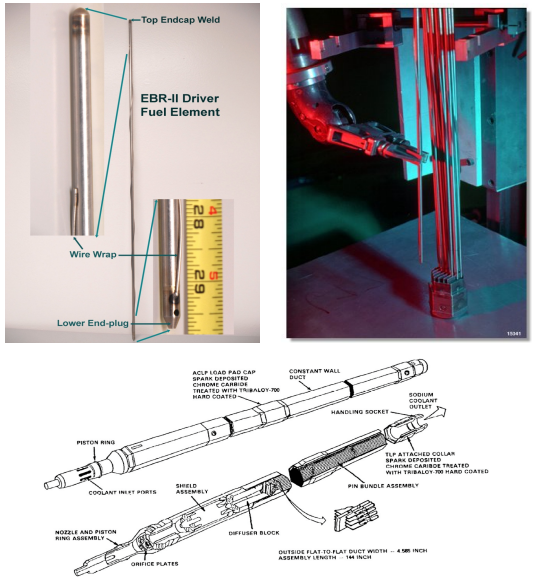
10 CFR Part 53: Further ACRS Comments (2/2)

- Systematic searches for hazards, initiating events, and accident scenarios should be required
- A licensing pathway like prototype testing should be available
- Schedule to issue needed detailed guidance looks very ambitious
- The staff's ability to graciously accept comments from all sources and to seek resolution of competing requests is commendable

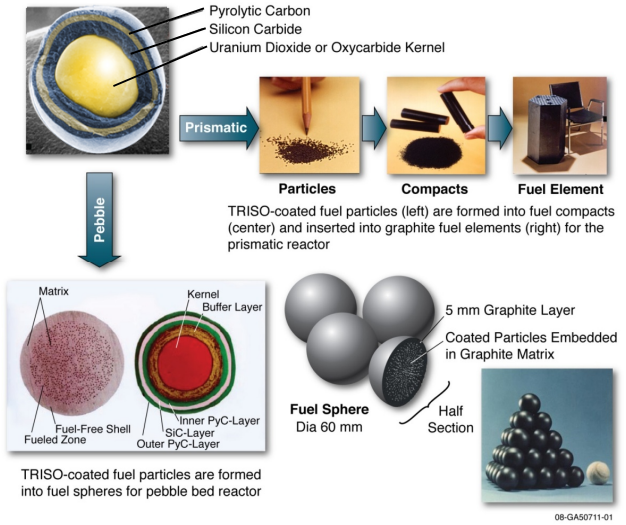
Fuel Qualification Activities

- Fuel Qualification for Advanced Reactors (NUREG -2246)
  - Outlines requirements and assessment framework, focusing on the need for data
  - Planned applications include high and low technology readiness fuels
- KAIROS TRISO Fuel Performance Model Topical Report
- TRISO Fuel Particle Performance Topical Report
- Legacy Metallic Fuel Qualification Data

Metal Fuel for Sodium Fast Reactors

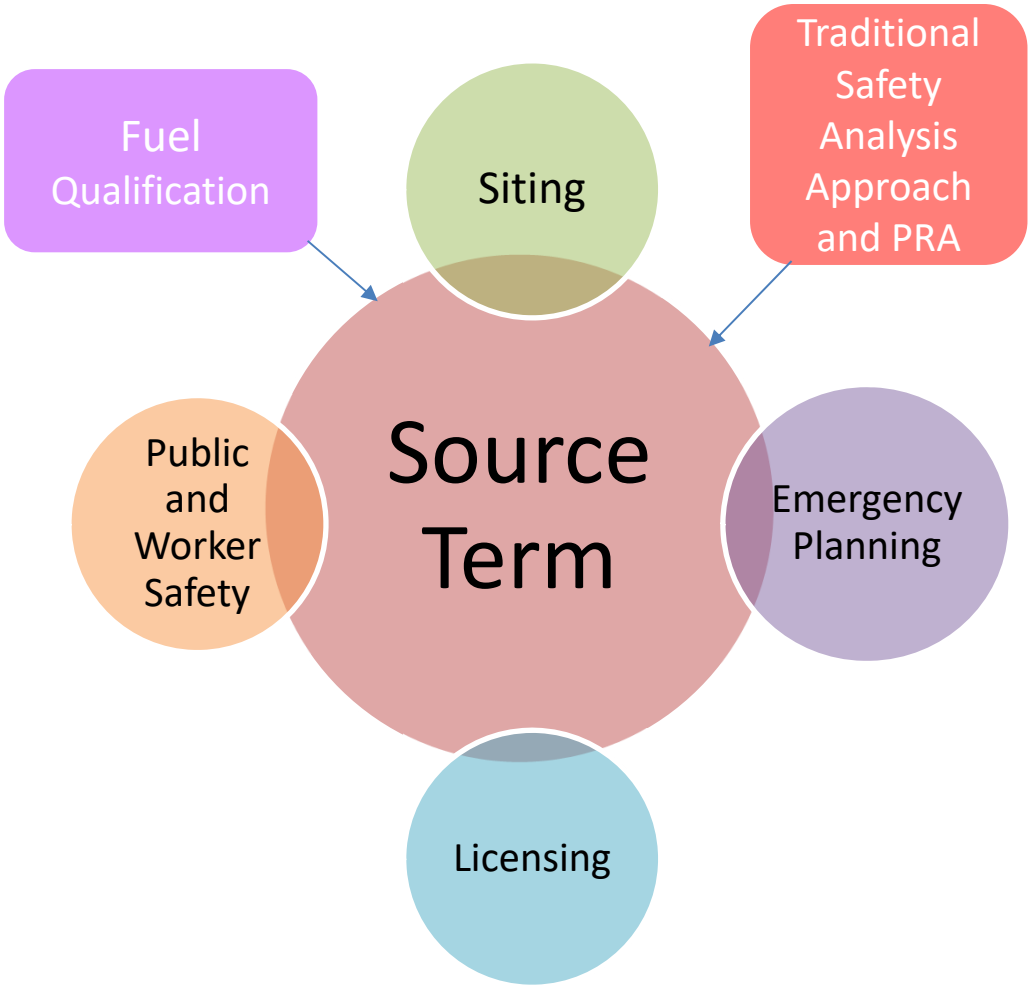


TRISO Fuel for High Temperature Gas-cooled Reactors



Source Term is at the Heart of Many Regulatory Activities

- Key part of fuel qualification, traditional safety analysis approach and PRA
- Source term for advanced reactors differ from LWRs
- Numerous recent and upcoming source term related activities
  - A roadmap showing how all the pieces fit together would be worthwhile



Many different pieces are coming together. ACRS plans an integrated review later this year

Summary

- Regulatory activities related to advanced reactors are in full gear
- 10 CFR Part 53 is a major undertaking by the staff
  - Approach is coherent and logical
  - Schedule to issue detailed guidance that will be needed looks very ambitious
- Fuel qualification and source term activities, key parts of the regulatory process, are also underway

Uni-Directional Communications from High Safety to Lower Safety Systems and Internal Plant to External Systems Connected to the Internet

Charles Brown, Chair

DI&C Systems Subcommittee

Background

- Our letter report of November 23, 2020, on Branch Technical Position (BTP) 7-19, Revision 8, "Guidance for Evaluation of Defense-in-Depth and Diversity to Address Common Cause Failure Due to Latent Defects in Digital Safety Systems," noted that:
  - The November 2019 version emphasized that interconnections between High Safety-Significance and Lower Safety-Significance systems should be through one-way digital communication devices rather than bi-directional devices that reduce independence and defense-in-depth and compromise control of access.
  - Thus, external plant access and compromised software in Lower Safety-Significance systems or in-plant networks do not compromise High Safety-Significance systems.
  - This language was deleted in all later versions of the draft BTP including Revision 8.
  - Revision 8 should be revised to ensure that interconnections between High Safety-Significance systems and those of Lower Safety-Significance are one-way, uni-directional (not implemented in software) digital communication devices.

Background (continued)

- The staff response disagreed stating that BTP 7-19, Revision 8, is guidance for staff reviewers and cannot prescribe or impose specific design requirements such as those described in our recommendation.
- We strongly disagree that our recommendation unnecessarily imposes either specific design requirements or a specific component design.
- In previous discussions, the staff has stated that:
  - They cannot review electronic control of access and uni-directional data communications for internal DI&C systems or in-plant to external systems during the design review phase.
  - Instead, it is viewed as an operational issue and cyber security concern during licensee programmatic review under 10 CFR 73.54, where guidance is provided by Regulatory Guide (RG) 5.71, “Cyber Security Programs for Nuclear Facilities.”

March 31, 2021, follow-up ACRS letter to the Chairman—Main Points

- Computer-based digital instrumentation and controls (DI&C) for reactor protection systems (RPS), engineered safeguards, and other reactor/steam plant control and monitoring systems result in significant improvements in plant performance.
- Computer-based DI&C systems drastically increase the vulnerability for control of access to critical RPS, safeguards systems, and in-plant networks through communication of digital data and control signals.
- With DI&C architectures and networks configured for bi-directional data communication using software, control of access is gravely threatened and is not an abstract consideration.
- In-plant systems and networks that control all plant operations are now susceptible to attacks from external plant sources that connect to the internet.
- This results in compromise of independence, defense-in-depth (DID), and control of access, three of the fundamental DI&C design principles.

Main points (continued)

- The problem is that cyber-security and other security controls are not addressed and applied until the latter phases of the lifecycle that occur at a licensee's site (i.e., site installation, operation, maintenance). By then:
  - The DI&C digital data communications architecture is potentially already designed and ready for manufacture or in the installation phase.
  - Incorporation of uni-directional (not implemented in software) hardware-based data communication devices into the architecture at this late juncture in the process would possibly require a license amendment request (since it would be a licensing basis change) with its inherent delay and cost implications.

Main points (continued)

- RG 5.71 should be used during the design and design review phase to ensure a strong defensive architecture is part of the design licensing basis.
- RG 5.71 describes a defensive architecture that is strong and to the point noting that:
  - All digital safety systems should be in the highest defensive level.
  - Only permits one way data flow from higher level digital safety systems to lower-level systems in the defensive architecture.
  - Prohibits communication from digital assets in lower security levels to digital assets in higher security levels.
  - Notes that one-way communications should be enforced using hardware mechanisms.

Main points (continued)

- The alternative of incorporating cyber security software into operating system software for in-plant systems and networks involved in protection, control and monitoring is problematic on two counts.
- First, cyber security software is primarily reactive; it mostly protects against attacks that have already been observed.
- Second, it would disrupt all critical functions by:
  - Imperiling plant systems timely completion of program cycle operation.
  - Requiring constant software upgrades to maintain currency.
  - Increasing the possibility of introducing malware during the upgrades that allows cyber compromise.

Summary of Main Points

- Allowing the use of computer-based DI&C architectures and networks configured for bi-directional data communication or software configured uni-directional data communications, threatens control of access and compromises independence and defense-in-depth.
- They compromise plant safety by leaving High and Low Safety-Significance systems open to the kinds of attacks that have seriously impacted other industries and government agencies.

Summary (continued)

- We recommended that Commission direction is needed for the staff to assure, during design reviews, that only uni-directional hardware-based data communications mechanisms (not implemented in software) are used between High Safety-Significance systems and those of Lower Safety-Significance.
- Consistent with Be riskSMART, guidance to the staff would help cases where regulations provide flexibility, but overly rigid interpretation can be detrimental.
- This ensures, at the design review stage, there are not any software deficiencies or backdoors within in-plant networks and systems that can be exploited by internet connected sources to access in-plant systems and networks. Thus, independence, redundancy, and defense-in depth are not compromised.

Activities following the ACRS Letter

- We have not yet received a response from the staff
- What we have observed in public documents:
  - In a memorandum to the EDO, dated April 14, 2021, the Chairman directed the NRC staff to undertake a review and within 90 days provide the Commission information on how the issues raised by the ACRS have been addressed.
  - The EDO established an independent team of experts (Team) to respond to the matters raised in the ACRS' letter.
  - In a memorandum to the Commissioners, dated July 14, 2021, the EDO reported the results of the Team evaluation as follows:
    - The concerns identified by the ACRS' letter do not identify a safety issue not currently covered by the NRC's regulations.
    - Mandating hardware for uni-directional communication devices would not increase the level of cyber security protection.

Post ACRS Letter (continued)

- Mandating hardware uni-directional devices would add a regulatory burden, reduce flexibility, and make the NRC's regulations more prescriptive in an area where performance-based regulations have proven effective, however,
- The Team concluded that specific guidance documents could be revised to encourage design certification applicants to consider the cyber security requirements during the design phase for a future operating license or COL.

- Team recommendation:
  - Revise RGs 5.71 and 1.152, Revision 3, "Criteria for Use of Computers in Safety Systems of NPPs," to make applicants for design certifications aware of cyber security requirements and cyber security controls to be considered during the design phase of the nuclear power reactor design.

Post ACRS Letter (continued)

- Revise BTP 7-19 to clarify how the inclusion of uni-directional digital communications in a design could reduce the scope of its review of defense-in-depth and diversity.

- EDO Evaluation:
  - The Team's recommendations and conclusions are accepted.
  - The staff will be directed to revise these regulatory documents as soon as possible
- ACRS Position
  - We stand by our letters of November 23, 2020, and March 31, 2021
  - We cannot evaluate proposed staff actions until we see the changes to the Regulatory Guides and Branch Technical Position

NuScale Control Room Staffing Plan Topical Report

Matthew Sunseri, Chair

ACRS

NuScale Design

NuScale Power Module (NPM)

- Small modular, natural circulation PWRs
- 160 MWt/50 MWe per module, 37 half-length, commercial PWR fuel assemblies
- Reactor core, riser, pressurizer, and two helical-coil steam generators integral to a reactor vessel in a high-strength steel containment vessel
- Passive emergency core coolant system (ECCS) and decay heat removal system (DHRS)
- NPMs immersed in a large reactor building pool that serves as a passive ultimate heat sink
- Up to 12 modules in a nuclear power plant (NPP)

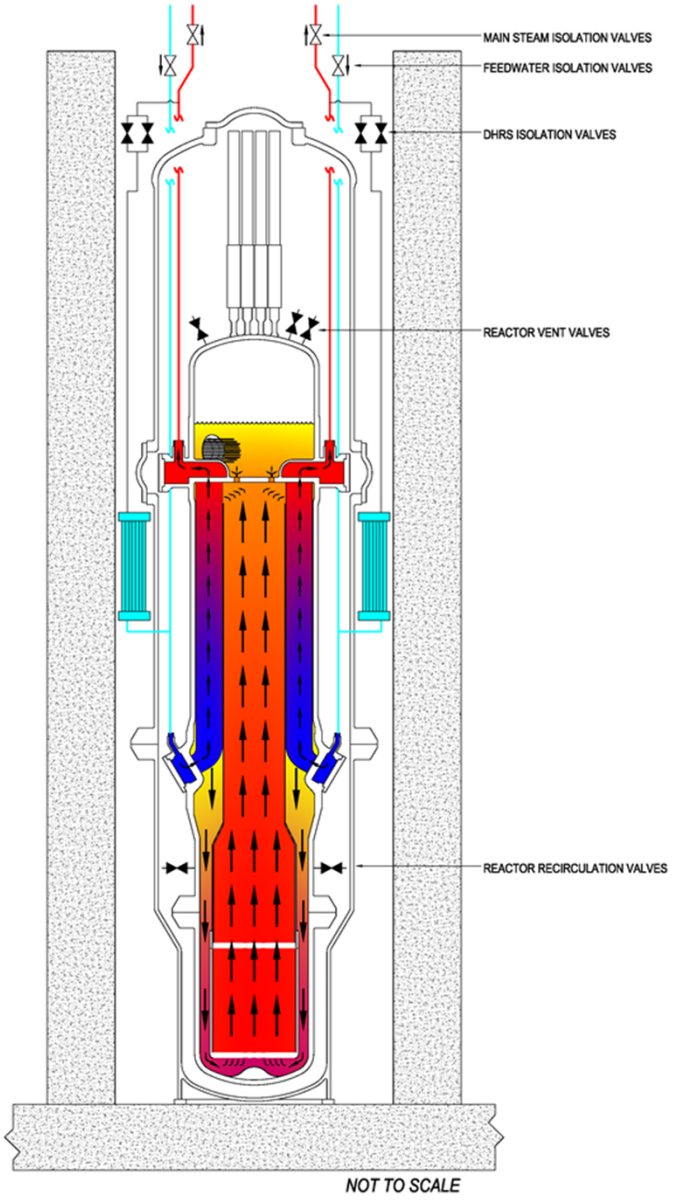


Figure courtesy of NuScale

NuScale Features

NuScale NPMs have several features that enable consideration of reduced staffing levels:

- Passive safety characteristics and enhanced safety margins of design
- Simplicity of tripping a module and placing it in a passive cooling mode
- Minimal operator intervention required within 72 hours for a wide spectrum of design basis events (DBEs)
- Improved human-system interfaces in main control room (MCR) design, functionality, and displays (“at a glance” displays, tiered alarms, multi-module trending, direct links to procedures, etc.)

ACRS Review of NuScale Control Room Staffing

- ACRS issued final letter report review on Design Certification Application (DCA) on July 29, 2020
- NuScale proposed in DCA a MCR minimum shift crew of six licensed operators
- In its revised Control Room Staffing (CRS) Plan, December 17, 2020, NuScale proposed operating up to twelve modules with a MCR minimum shift crew of three licensed operators (two SROs and one RO)
- NuScale also proposed eliminating the separate Shift Technical Advisor (STA) position, combining its functions with shift manager (SRO) and crew

Control Room Staffing Background

- Current staffing requirements are specified in 10 CFR 50.54(m) – a 12 module NPP was not anticipated
- Staff recognized evolving issues for number of licensed operators for multi-module SMRs in SECY-11-0098
- Path forward was to process exemption requests using the general framework of:
  - Standard Review Plan (NUREG-0800) Chapter 18
  - Human factors engineering review (NUREG-0711)
  - Guidance for assessing exemption requests (NUREG-1791)

NuScale Staffing Plan Validation Exercises (1)

- NuScale conducted two staffing plan validation exercises
- First with two crews of 6-person shift as specified in DCA
- Scenarios included a spectrum of challenging, high-workload operating conditions, including DBEs, BDBEs, multi-module transients and upset events, and large-scale loss of MCR displays
- Acceptance criteria included performance within in specified task completion times, established human performance indicators, and situational awareness questionnaires

NuScale Staffing Plan Validation Exercises (2)

- In revised staffing plan validation exercises a three-person shift crew of an SRO as shift shift manager, an SRO, and an RO was used
- Testing was repeated for a similar spectrum of events, but *different* scenarios
- The two operating crews were able to successfully operate a plant with up to 12 modules, meeting all task performance and evaluation criteria
- No high-priority human engineering discrepancies, retesting, or corrective actions were identified

Staff's Safety Evaluation

- Staff determined that the NuScale simulator test-bed was adequately representative of an as-designed MCR (10 CFR 55.46 and RG 1.149)
- Test scenarios were audited, evaluated, and found sufficiently representative
- Successful performance of task assignments in spectrum of test scenarios for two different crews of three determined to be a satisfactory demonstration
- Concluded that a 12-module plant can be operated safely and reliably operated by a shift of 3-licensed operators from a single control room under high-workload conditions

ACRS Evaluation

- Factors considered by ACRS in support of NuScale's proposed minimum 3-licensed operator shift crew:
  - Passive safety characteristics and enhanced safety margins of design
  - Simplicity of tripping a module and placing it in a passive cooling mode
  - No operator intervention required within 72 hours for a wide spectrum of DBEs
  - Improved human-system interfaces in MCR design, functionality, and displays ("at a glance" displays, tiered alarms, multi-module trending, direct links to procedures, etc.)
  - Pilot operator training programs and high-fidelity simulator validation exercises
  - Provision for an additional SRO on plant floor during refueling operations and evolutions, consistent with 10 CFR 50.54(m)

ACRS Evaluation – MCR Design Validation

- Staffing validation activities were highly dependent on the simulated control room design attributes such as:
  - Critical safety functions and defense-in-depth monitoring and display,
  - Tiered alarm scenario scheme,
  - 12 module trend monitoring.
- The as-built Main Control Room will need to be thoroughly tested to ensure that the same features used to validate the staffing requirements exist and function as intended

Shift Technical Advisor (STA)

- Post TMI, NRC required establishment of an STA position at all plants to provide independent engineering expertise and advice to shift supervisor (NUREG-0737)
- It was recognized that when qualifications of operators were upgraded, and human-system interfaces were upgraded in MCRs, the STA position could be eliminated
- In policy statements (SECY-84-355 and GL-86-04) the Commission encouraged licensees to move to a dual SRO/STA position
- We agree that for the NuScale design, sufficient justification exists to eliminate the STA position

Summary

- NuScale's design, the simplicity with which modules can be placed in a safe, stable, passive-cooling state, and successful staffing plan validation exercises provide confidence that up to 12 modules can be safely operated with the proposed minimum 3-licensed operator crew
- We recommended that the staff's SER be issued
- We suggested that the minimum operating crew be supplemented with additional independent engineering expertise until sufficient experience is gained with multi-module operations
- We look forward to reviewing licensee submittals that reference this NuScale Control Room Staffing TR, and associated deployment issues noted in our letter report

Acronyms

- AC – Alternating Current
- ACRS – Advisory Committee on Reactor Safeguards
- ALARA – As Low As Reasonably Achievable
- BDBE – Beyond Design Basis Event
- BTP – Branch Technical Position
- CFR – Code of Federal Regulations
- COL – Combined License
- CRS – Control Room Staffing
- DBE – Design Basis Event
- DCA – Design Certification Application
- DHRS – Decay Heat Removal System
- DI&C – Digital Instrumentation and Control
- DID – Defense-in-Depth
- ECCS – Emergency Core Cooling System
- EDO – Executive Director for Operations
- EPZ – Emergency Planning Zone
- GL – Generic Letter
- GSI – Generic Safety Issue
- IDHEAS-G – General Methodology of an Integrated Human Event Analysis System
- ISI – Inservice Inspection
- IST – Inservice Testing
- LWR – Light Water Reactor
- LPZ – Low Population Zone
- MCR – Main Control Room
- MWe – Megawatt (electric)
- MWt – Megawatt (thermal)
- NPM – NuScale Power Module
- NPP – Nuclear Power Plant
- NRC – U.S. Nuclear Regulatory Commission
- PRA – Probabilistic Risk Assessment
- QA – Quality Assurance
- QHO – Quantitative Health Objectives
- RES – Office of Nuclear Regulatory Research
- RG – Regulatory Guide
- RO – Reactor Operator
- RPS – Reactor Protection System
- SMR – Small Modular Reactor
- SRM – Staff Requirements Memorandum
- S-R – Safety-related
- SRO – Senior Reactor Operator
- SSC – Structure, System, or Component
- STA – Shift Technical Advisor
- TMI – Three Mile Island
- TRISO – Tri-structural Isotopic