UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555-0001

April 24, 2017

Mr. Victor McCree
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: SAFETY EVALUATION OF THE NUSCALE POWER, LLC LICENSING TOPICAL REPORT TR-1015-18653-P, REVISION 1, "DESIGN OF THE HIGHLY INTEGRATED PROTECTION SYSTEM PLATFORM"

Dear Mr. McCree:

During the 642nd meeting of the Advisory Committee on Reactor Safeguards, April 6-7, 2017, we reviewed the NRC staff's safety evaluation report (SER) for the NuScale Power, LLC (NuScale) topical report TR-1015-18653-P, Revision 1, "Design of the Highly Integrated Protection System [HIPS] Platform." Our NuScale Subcommittee also reviewed this matter during a meeting on February 7, 2017. During these meetings, we had the benefit of discussions with NuScale and the staff. We also had the benefit of the referenced documents.

RECOMMENDATION

The HIPS platform is acceptable for use in plant safety-related instrumentation and control systems provided its implementation satisfies the staff application specific action items. The staff's safety evaluation report of NuScale topical report TR-1015-18653-P, Revision 1 should be issued.

BACKGROUND

In December 2015, NuScale submitted topical report TR-1015-18653-P, Revision 0 to the NRC staff for review. NuScale requested staff to review and confirm that the HIPS platform meets the applicable regulatory requirements associated with the fundamental digital instrumentation and control (DI&C) design principles. Revision 1 of the topical report (hereafter "topical report") was issued in October 2016 in response to NRC staff request for additional information with additional corrections and clarifications.

The topical report includes Appendices A through D that provide traceability matrices to identify levels of compliance with IEEE Std. 603-1991, IEEE Std. 7-4.3.2-2003, Digital I&C Interim Staff Guidance 04, and the Staff Requirements Memorandum for SECY-93-087.

NuScale stated that an applicant using the approved HIPS platform topical report could reference the generic approval for design concepts, as noted in the appendices. For concepts with full conformance, the applicant would need to demonstrate that the requirements have been implemented. The applicant could reference the generic approval for design concepts with partial conformance. However additional application-specific information would be needed to show how these HIPS platform design concepts were properly implemented in the system design. The applicant would then also need to address all other application-specific items that were not reviewed or not approved as part of the HIPS platform topical.

DISCUSSION

The topical report describes key design concepts for the generic DI&C platform cooperatively developed by Rock Creek Innovations, LLC and NuScale. It describes the design attributes and physical configuration of the HIPS platform standardized circuit boards and their chassis. When configured in the proper manner, HIPS is designed to provide the reactor trip system (RTS) and engineered safeguards actuation system (ESFAS) for a nuclear power plant. The topical report describes how the HIPS platform design meets the fundamental DI&C design principles of independence, redundancy, predictability and repeatability, and diversity and defense in depth. It also describes the testing and diagnostics concepts applied to the HIPS platform.

The HIPS platform is logic-based and does not use software or microprocessors for operation. The HIPS platform is implemented using discrete components and field programmable gate array technology (FPGA). An FPGA is an integrated circuit consisting of a set of programmable logic gates. This makes it possible to implement complex digital circuits that do not incorporate software for their operation.

The scope of the topical report is limited to the HIPS platform. It includes, as an example, a conceptual plant reactor trip and engineered safeguards design configuration to illustrate how HIPS meets the fundamental DI&C principles. However, it does not illustrate its interface with any other safety or non-safety systems, external power supplies, other details of plant monitoring, or communications external to the notional system (e.g., in-plant networks, support facilities, corporate offices, and external plant internet sources). Thus, design features that control access from internal networks or external sources are not described and have not been reviewed as part of this topical report SER.

The conceptual system consists of four separation groups representing four redundant plant-parameter monitoring channels. These groups independently monitor and produce reactor trip and engineered safeguards actuation signals. These four separation groups feed two divisions of RTS and two divisions of ESFAS, where 2-out-of-4 voting logic is performed.

The HIPS platform includes four different HIPS modules each capable of performing dedicated functions: (1) safety function module (SFM), (2) communication module, (3) equipment interface module (EIM), and (4) the hardwired module. Each HIPS module can be replaced while the system is operating. Each HIPS module consists of a base printed circuit board, a set of rear connectors, a front panel, and electronic components. In some modules, sub-modules may be added to the base circuit board.

The SFM is responsible for input signal conditioning and executing the safety function trip algorithm. Also, this module provides scaled values of input processes to non-safety controls and safety display for monitoring purposes. It has three functional areas: (1) signal conditioning/analog-to-digital conversion (input sub-module) and (2) FPGA-based digital logic circuits and (3) FPGA-based communications engines.

The safety function modules:

- Convert the output of input sub-modules into engineering units,
- Perform the safety function algorithm,
- Compare the safety function algorithm output to a protection actuation setpoint, and
- Generate permissives and control interlocks.

In addition to the 2-out-of-4 voting logic for protection actions, all safety function module tasks are processed using three independent, redundant signal paths internal to each module (referred to as triple modular redundant (TMR)) through to the EIM.

The communication modules are responsible for controlling, collecting, and transmitting information between HIPS modules or to external components. Each uses an FPGA device to implement the logic circuits, based on the specific functions each will perform. The three types of communication modules are: (1) the scheduling and bypass module (SBM), (2) the scheduling and voting module (SVM), and (3) the monitoring and indication bus.

The SBMs are responsible for scheduling the communications within their separation group. This module validates and transmits the data from the safety function modules through isolated one-way transmit-only fiber as 'Trip/No-Trip Information' to both divisions of the RTS and ESFAS and their respective scheduling and voting modules.

The SVMs are responsible for scheduling communications within each RTS division and each division of ESFAS. The SVMs in both the RTS and ESFAS platforms receive the data from the respective SBMs in the four separation groups as 'Trip/No-Trip Information' and independently perform 2-out-of-4 voting on the information. The 2 of 4 voted trip or actuate signal is passed to three data busses in the EIM as serial data for 2-out-of-3 TMR voting.

The EIM is responsible for voting on TMR signal paths. This module provides the final equipment actuation output and includes priority logic circuitry for automatic and manual actuation inputs.

The EIM is composed of the following circuits:

- an FPGA for communication logic and 2-out-of-3 voting logic,
- hard-wired signals logic,
- actuation and priority logic,
- switching output for component actuation, and
- position feedback.

The hard-wired module receives signals from manual switches in the main control room and the trip/bypass switch panel. It converts and transmits those signals to particular modules through a dedicated backplane.

This module is constructed of discrete logic components only. There are no programmable devices. All input signals to the hard-wired module are isolated from the field and routed on the backplane to modules that need the signals. This module provides isolation for the backplane and modules from the external manual switches and the non-safety-related control signals.

Diversity is incorporated in the HIPs modules through the use of two different FPGA architectures, one being a one time programmable (OTP) or flash-based FPGA and the other being a static random-access memory (SRAM) based FPGA. OTP FPGAs are used on two of the four protection channels, and SRAM FPGAs are used on the other two. The FPGA functional logic on any of the modules cannot be modified (for SRAM type) or replaced (for OTP type) while installed in the HIPS platform chassis.

The staff evaluated the suitability of the HIPS platform for use in safety systems based on how it incorporates the fundamental design principles of independence, redundancy, predictability and repeatability, and defense-in-depth, as well as important platform functionality, including the capability for testing and calibration. Because this platform is intended for use in safety systems and other safety-related applications, the staff evaluated the topical report against applicable regulations, industry standards, and staff review guidance.

The staff review did not consider the quality of the HIPS platform standardized circuit boards and their associated instrument chassis, the quality of the design process, and equipment qualification. These activities are application specific, and dependent on the equipment vendor to be used to implement the HIPS platform.

In the SER, the staff identified a number of application specific action items (ASAIs) that must be implemented for NRC approval of the HIPS platform for safety-related applications in any nuclear power plant. The determination of full compliance with the regulations remains subject to a plant-specific licensing review of a full system design based on the HIPS platform.

The staff determined that the four HIPS platform modules and their design features can be configured to meet the fundamental DI&C principles of independence, redundancy, predictability and repeatability, and diversity and defense in depth. The staff also concluded that the HIPS platform meets the applicable regulatory requirements for safety-related I&C systems when each plant-specific and application-specific use meets the limitations and conditions delineated in the ASAIs.

On this basis, the staff determined that the HIPS platform is acceptable for use in safety-related I&C systems. We concur with the staff conclusion and the SER for the NuScale topical report should be issued.

Dr. Peter Riccardella did not participate in the Committee's deliberations regarding this matter.

Sincerely,

/RA/

Dennis C. Bley
Chairman

REFERENCES:

1. NuScale Power, LLC, TR-1015-18653-NP, "Highly Integrated Protection System Platform," Revision 0, December 2015 (ML15363A115).

2. NuScale Power, LLC, TR-1015-18653-P, "Design of the Highly Integrated Protection System Platform," Revision 1, October 2016 (ML16309A614).

3. U.S. Nuclear Regulatory Commission, "Safety Evaluation by the Office of New Reactors Licensing Topical Report (TR) 1015-18653-P, (Revision 1) 'Design of the Highly Integrated Protection System Platform,'" March 14, 2017 (ML17069A138).

4. U.S. Nuclear Regulatory Commission, Safety Evaluation by the Office of New Reactors Licensing TR 1015-18653-P (Revision 1), "Design of Highly Integrated Protection System Platform", March 21, 2017 (ML17069A135). [PUBLIC VERSION]

5. Institute of Electrical and Electronics Engineers, Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," including the correction sheet, January 30, 1995.

6. Institute of Electrical and Electronics Engineers, Standard 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," December 19, 2003.

7. U.S. Nuclear Regulatory Commission, DI&C-ISG-04, "Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc)," Revision 1, March 6, 2009 (ML083310185).

8. U.S. Nuclear Regulatory Commission, Staff Requirements Memorandum SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs," July 21, 1993 (ML003708056).

9. U.S. Nuclear Regulatory Commission, "Design-Specific Review Standard for NuScale SMR Design," Chapter 7 - Instrumentation and Controls, June 2016 (ML15355A295).

-5-

On this basis, the staff determined that the HIPS platform is acceptable for use in safety-related I&C systems. We concur with the staff conclusion and the SER for the NuScale topical report should be issued.

Dr. Peter Riccardella did not participate in the Committee's deliberations regarding this matter.

Sincerely,

/RA/

Dennis C. Bley
Chairman

REFERENCES:

1. NuScale Power, LLC, TR-1015-18653-NP, "Highly Integrated Protection System Platform," Revision 0, December 2015 (ML15363A115).
2. NuScale Power, LLC, TR-1015-18653-P, "Design of the Highly Integrated Protection System Platform," Revision 1, October 2016 (ML16309A614).
3. U.S. Nuclear Regulatory Commission, "Safety Evaluation by the Office of New Reactors Licensing Topical Report (TR) 1015-18653-P, (Revision 1) 'Design of the Highly Integrated Protection System Platform,'" March 14, 2017 (ML17069A138).
4. U.S. Nuclear Regulatory Commission, Safety Evaluation by the Office of New Reactors Licensing TR 1015-18653-P (Revision 1), "Design of Highly Integrated Protection System Platform", March 21, 2017 (ML17069A135). [PUBLIC VERSION]
5. Institute of Electrical and Electronics Engineers, Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," including the correction sheet, January 30, 1995.
6. Institute of Electrical and Electronics Engineers, Standard 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," December 19, 2003.
7. U.S. Nuclear Regulatory Commission, DI&C-ISG-04, "Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc)," Revision 1, March 6, 2009 (ML083310185).
8. U.S. Nuclear Regulatory Commission, Staff Requirements Memorandum SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs," July 21, 1993 (ML003708056).
9. U.S. Nuclear Regulatory Commission, "Design-Specific Review Standard for NuScale SMR Design," Chapter 7 - Instrumentation and Controls, June 2016 (ML15355A295).

Accession No: **ML17108A433** **Publicly Available** **Y** **Sensitive** **N**
Viewing Rights: ☒ NRC Users or ☐ ACRS Only or ☐ See Restricted distribution

OFFICE	ACRS	SUNSI Review	ACRS	ACRS	ACRS
NAME	CAntonescu	CAntonescu	MLBanks	ADVeil	ADV for DCB
DATE	04/25/17	04/25/17	04/21/17	04/21/17	04/21/17

OFFICIAL RECORD COPY