December 14, 2018 Docket No. 52-048

Annette L. Vietti-Cook
Secretary of the Commission
U.S. Nuclear Regulatory Commission
Mail Stop O-16G4
Washington, DC 20555-0001

TO: Chairman Kristine L. Svinicki
Commissioner Jeff Baran
Commissioner Stephen G. Burns
Commissioner Annie Caputo
Commissioner David A. Wright

SUBJECT: NuScale Power, LLC Request for Commission Clarification on the Application of the Single Failure Criterion to "Active-Passive" Components

Dear Chairman and Commissioners:

In SECY-77-439, "Single Failure Criterion," the NRC staff described how it was using the single failure criterion in reviewing reactor safety and discussed the distinction between active and passive failures of a system or component. In SECY-94-084, NRC Staff "examined current regulatory practice to determine how it will apply to check valve failures for the passive plant designs." The framework established by these documents is based on the understanding of system and component designs existing at the time each was published and may not provide adequate consideration for innovations in subsequent designs. NuScale Power, LLC (NuScale) requests that the Commission re-visit and clarify the single failure criterion as it applies to active components that can be treated as passive failures with respect to the single failure criterion.

Since the issuance of SECY-77-439, designs have both improved in safety performance and increasingly relied upon passive systems to achieve greater safety performance. NuScale has moved the reliance upon passive systems, and innovative devices within them, beyond what was contemplated in 1977, and as a result has a design of far greater safety. However, a difference of interpretation by the NRC staff and NuScale regarding the application of SECY-77-439 to these innovative devices is a concern as the NRC staff position imposes substantial burden upon NuScale. The staff's position would not improve safety as the design would not change. The staff's position would result in a different licensing basis than that in the design certification application, one that would come at high cost in terms of new analyses, revision to the design certification application, and revision to topical reports under review. NuScale and the NRC staff have discussed a range of design, analysis, and regulatory options, and continue to do so. All have disadvantages to varying degrees in terms of safety, cost, or regulatory risk. On balance, NuScale believes the policy interpretation offers the best possible path in terms of safety and cost, while involving equivalent regulatory risk to other options.

The component of interest is the "inadvertent actuation block" (IAB) device. This component ensures both that the passive, fail-safe emergency core cooling system (ECCS) does not actuate at an unnecessarily high reactor coolant system pressure, and that the ECCS valves ensure core cooling via natural circulation indefinitely.

NuScale developed its design on the basis that the closing of the IAB is a passive function after careful consideration of the 1977 Commission paper and subsequent re-visits (e.g., SECY-94-084,"Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems in Passive Plant Designs") as described in the attachment to this letter. The NRC staff, in conducting its review of the DCA, reached a different conclusion. This difference was not reached lightly. To the contrary, the

NRC staff and NuScale conducted extensive communications. These include numerous meetings, focused licensing audits, and dialog at staff, management, and executive levels. NuScale and the NRC staff using the same documents and design information, reached different conclusions as to the classification of the IABs, which indicates that the policy may be ambiguous and would benefit from clarity by the Commission.

The attachment to this letter discusses the history of the single failure criterion with respect to devices that involve mechanical movement but that are considered as passive single failures in the Chapter 15 safety analysis. It provides an evaluation of the IAB against other active components that have been treated as passive, and addresses concerns expressed by the NRC staff as documented in meeting summaries and audit reports.

NuScale believes this issue has generic policy implications as future designs are likely to similarly consider new types of devices passive with respect to the single failure criterion. Therefore, these vendors would benefit from clarity of the "active-passive" single failure criterion so they can incorporate it into their designs as early as possible. This interpretation would be relevant to NuScale and other advanced reactor applicants that use the existing licensing framework. NuScale understands that in the near future the NRC staff will recommend endorsement of the Licensing Modernization Project (LMP) Licensing Basis Development guidance document.[1] Under the LMP approach, the concept of single failure criterion does not exist. Had the LMP been available at the time NuScale developed its application, the IABs would not be an issue as there are negligible safety consequences associated with their failure.

NuScale recognizes that it is most desirable to resolve the issue generically. However, given the breadth of designs that could be affected by the Commission's decision, NuScale is concerned whether a generic policy could be developed in time to support NuScale's design certification application review. Therefore, NuScale requests that the Commission address the application of the single failure criterion to the IABs in the near term, and engage with other stakeholders in a broader solution.

NuScale wants to reiterate that the NRC staff has engaged in open dialog with NuScale regarding their concerns with the IABs, and NuScale's interpretation of the single failure criterion as it applies to the IABs. Clarification of this policy is of critical importance to NuScale, and we appreciate the Commission's attention to this matter.

Sincerely,

Thomas A. Bergman
Vice President, Regulatory Affairs
NuScale Power, LLC

[1] NEI 18-04, "Risk-Informed Performance-Based Guidance for Non-Light Water Reactor Licensing Basis Development," developed as part of the Licensing Modernization Project (see https://www.nrc.gov/about-nrc/regulatory/risk-informed/rpp/reactor-safety-advanced.html). NuScale understands the LMP approach was developed for non-LWRs. However, there appears no technical reason why NEI 18-04 and DG-1353 should be limited to non-LWRs and exclude advanced LWRs such as NuScale.

Distribution: Margaret Doane, OWFN-16E15, Executive Director for Operations
Michael R. Johnson, OWFN-16E15, Deputy Executive Director for Reactor and Preparedness Programs
Frederick Brown, OWFN-4D4, Director, Office of New Reactors
John Monninger, OWFN-2H10, Director, Division of Safety Systems, Risk Assessment, and Advanced Reactors
Robert Taylor, OWFN-7H4, Director, Division of Licensing, Siting, and Environmental Analysis, Office of New Reactors
Anna H. Bradford, OWFN-4F00, Director (Acting), Division of Engineering and Infrastructure
Samuel Lee, NRC, OWFN-8G9A
Gregory Cranston, NRC, OWFN-8G9A
Rani Franovich, NRC, OWFN-8G9A
Prosanta Chowdhury, NRC, OWFN-8G9A
Bruce Bavol, NRC, OWFN-8G9A
Marieliz Vera, NRC, OWFN-8G9A
Omid Tabatabai, NRC, OWFN-8G9A
Getachew Tesfaye, NRC, OWFN-8H12

Attachment: Application of the Single Failure Criterion to the NuScale Inadvertent Actuation Block Valves, nonproprietary

Application of the Single Failure Criterion to the NuScale Inadvertent Actuation Block Valves

1.0 Purpose and Summary

In SECY-77-439, "Single Failure Criterion," the NRC staff described how it was using the single failure criterion in reviewing reactor safety and discussed the distinction between active and passive failures of a system or component. In SECY-94-084, NRC Staff "examined current regulatory practice to determine how it will apply to check valve failures for the passive plant designs." The framework established by these documents is based on the understanding of system and component designs existing at the time each was published and may not provide adequate consideration for innovations in subsequent designs. NuScale requests that the Commission re-visit and clarify the single failure criterion (SFC) as it applies to certain mechanical components that can be treated as passive components with respect to the SFC. Specifically, NuScale and NRC Staff are unable to reach agreement on the proper treatment of NuScale's inadvertent actuation block (IAB) devices.

The IAB is a simple block-valve device with a spring-loaded disc. The IAB operates on differential fluid pressure acting against a spring, which closes the IAB to prevent inadvertent actuation of the associated ECCS valve. Although the IAB is a new component, NuScale believes the IAB design and its closing function are similar to valve designs and functions that are currently postulated as passive failures. Thus, NuScale believes that under existing regulations, guidance, and precedent the function in question should be treated as a passive failure. NRC Staff have evaluated the IAB design and concluded it should be treated as an active failure because the device lacks test or operational data to demonstrate its reliability.

NuScale and the NRC staff, using the same guidance documents and design information, reached different conclusions as to the classification of the IABs, which may indicate that the current policy is ambiguous and would benefit from clarity by the Commission. Therefore, NuScale requests Commission clarification on a series of Policy interpretations that together will establish the appropriate classification of the IABs: first, that SECY-77-439 is the applicable guidance under which the IAB's classification is to be addressed; second, that under SECY-77-439, reliability data is not required to justify the treatment of the IAB's function as passive; and third, that a qualitative evaluation of a component's design and function, including a comparison to other components that have been and are treated as passive, is sufficient to demonstrate the component function's expected reliability. Under this framework, NuScale then shows that the IAB satisfies the SECY-77-439 guidance to be considered a passive component. Additionally, NuScale presents an alternative evaluation under a set of criteria that further clarify the SECY-77-439 policy, which also would establish the IAB closing function as a passive failure.

2.0 Background

Under the existing SFC framework, safety systems must perform their safety function even if a component within the system were to fail, thereby promoting redundancy within the system design. "Passive failures," however, are generally not postulated to occur in the short term response to a transient. Although failure of a valve to move is usually treated as an active failure, some postulated valve failures are treated as passive failures. This is because, although the function entails movement, that function has been judged as sufficiently reliable as compared to a passive component, based on a review of the component design.

NuScale's emergency core cooling system (ECCS) consists of five ECCS valves that open on demand to ensure core cooling following certain postulated events. In order to ensure passive safety, the ECCS valves also fail to an open (safe) position upon a total loss of electric power, which would occur only if both ac and dc power were to fail. The IABs are components of the NuScale ECCS. The primary function

of the IABs is to prevent inadvertent ECCS operation while the reactor coolant system (RCS) is at operational pressures.

IAB closure is not required for the ECCS to actuate, and failure of the IAB to close would not prevent the ECCS from performing its core cooling safety function. In the unlikely scenario of certain initiating events concurrent with a total loss of electric power (ac and dc), the NuScale design would rely on the IABs moving to a closed position to prevent the ECCS valves from opening at high reactor coolant system pressure. Successful closure of the IABs delays the actuation of ECCS to prevent rapid and excessive RCS depressurization, which may challenge the critical heat flux (CHF) success criterion NuScale established for those events.

While the IAB is a new component developed for the NuScale design, it is a simple block-valve device with a spring-loaded disc. The IAB operates on differential fluid pressure acting against the spring; when the RCS to containment vessel (CNV) differential pressure is above a predetermined threshold, the pressure pushes the IAB closed to prevent inadvertent actuation of the associated ECCS valve.

NuScale's current licensing basis treats failure of the IAB to close as a passive failure, and thus IAB failure-to-close is not analyzed as part of the design basis transient response. Thus, the IABs are credited to prevent inadvertent or premature actuation of the ECCS valves. Although failure of an IAB to close is not within the design basis events currently analyzed in Chapter 15, NuScale has shown in beyond-design-basis analysis, FSAR Chapter 19, that core damage is avoided even in the event of an IAB failure.

NuScale developed its ECCS design on the basis that the closing of the IAB is a passive function after careful consideration of the existing SFC guidance, primarily set forth in SECY-77-439 and re-visited in SECY-94-084. NuScale determined that the IAB is a simple mechanical device similar in design and function to other valves that are currently postulated as passive failures. NuScale interprets the scope of SECY-77-439 to include the IABs, and that under that guidance, failures of mechanical valves other than "simple check valves" can be treated as passive failures. NuScale believes the attributes of the IAB—including the simplicity of the mechanical design, the lack of control signal or external motive power to actuate it, and the quality assurance applied to its design and manufacturing—as well as relevant operational data for similar valves justify treatment as a passive function under that guidance.

The NRC staff have determined that the IAB closing function must be considered a potential active failure. NRC and NuScale staff engaged in an audit and held several public meetings on the issue, concluding with a discussion of the IAB design on August 22, 2018.[2] The key outcomes of that meeting, relevant herein, are:

- NuScale only considers the closing function of the IAB valve would be considered a passive function with respect to the single failure criterion.[3] Thus, previous discussions concerning multiple movements of the IAB are no longer relevant.
- The NRC staff considers the IAB valve to be a spring-loaded differential pressure valve. As such, it is not a "simple check valve" as explicitly addressed by SECY-77-439. NuScale believes that passive valve failures under SECY-77-439 are not limited to simple check valves.
- NuScale interprets SECY-77-439 as applicable to the IAB valve without the need for the quantitative reliability demonstration specified in SECY-94-084. The NRC staff did not agree

[2] Summary of the August 22, 2018, Category 1 Public Teleconference with NuScale Power, LLC to Discuss the Inadvertent Actuation Block of the Design Certification Application, Oct. 19. 2018, Accession No. ML18285A032 [hereafter "Summary of the August 22, 2018 Meeting"].

[3] The NuScale FSAR currently describes both the IAB failure to close and failure to open as passive failures. In the public meetings on this topic, NuScale has clarified that only the first valve motion—its closure to prevent inadvertent ECCS valve operation—will be considered as a passive failure. Single failures of the IAB opening function, which would prevent an ECCS valve from opening, are bounded by design basis safety analysis.

with this distinction in the two Commission papers for justifying the assumption of a passive failure of a component.

- The NRC staff believes that the specific functions of other valves treated as passive failures do not match the design, application, and function of the IAB valve.

Taken together, NuScale believes that the basic differences of opinion appear due to which NRC guidance document applies, what that document requires, and how the IAB should be evaluated thereunder. In reviewing the various guidance documents associated with the issue, NRC Staff noted "the common provision is that the assumption that the function of a specific component is a passive function with respect to the single failure criterion needs to be justified by an evaluation of the reliability of the component to perform that function."[4] NuScale performed a reliability evaluation of the IAB that concluded the IAB met the quantitative reliability threshold established by SECY-94-084,[5] but NRC staff do not accept the applicability of the operational data that NuScale used to perform that evaluation. Accordingly, NRC Staff believe that NuScale has not sufficiently justified the reliability of the IAB, pointing to SECY-94-084 and its position that specific reliability data is necessary for that justification.

3.0 Discussion

3.1 Regulatory Framework

The SFC is "one of several tools applied in systems design and analysis to promote reliability of the systems which are needed in a nuclear power plant for safe shutdown and cooling, and for mitigation of the consequences of postulated accidents."[6] The SFC is primarily codified in the General Design Criteria (GDCs), Appendix A to 10 CFR Part 50. The GDCs require that certain systems that perform safety functions[7] have "suitable redundancy...to assure...the systems safety function can be accomplished." For the purposes of the General Design Criteria:

> *A single-failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single-failure. Fluid and electric systems are considered to be designed against an assumed single-failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single-failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions.*

As summarized in SECY-77-439, "Simply stated, application of the Single Failure Criterion requires that a system which is designed to perform a defined safety function must be capable of meeting its objectives assuming the failure of any major component within the system or in an associated system which supports its operation." Beyond the requisite application of the SFC to assure reliability of specific safety systems, NRC guidance also more broadly considers single failures in analyzing plant transients, "directed toward demonstrating adequate design margins based upon defined acceptance criteria."[8]

The GDC definition of single failure includes the footnote, "The conditions under which a single failure of a passive component in a fluid system should be considered in designing the system against a single

---

[4] Summary of the August 22, 2018 Meeting.
[5] NuScale Power, LLC Response to NRC Request for Additional Information No. 36 (eRAI No. 8815) on the NuScale Design Certification Application, RAIO-0717-55033, July 21, 2017.
[6] SECY-77-439, p.1.
[7] The SFC is required for the onsite electric power system (GDC 17), the protection system (GDC 21), the residual heat removal and emergency core cooling systems (GDCs 34 and 35), the containment heat removal and containment atmosphere cleanup systems (GDCs 38 and 41), and the cooling water system (GDC 44).
[8] SECY-05-0138, p.3.

failure are under development." That development effort was later summarized in SECY-77-439, an information paper detailing the agency's practice with respect to the SFC and its application.

SECY-77-439 defines an active failure in a fluid system as "(1) the failure of a component which relies on mechanical movement for its operation to complete its intended function on demand, or (2) an unintended movement of the component." It defines a passive failure in a fluid system as "a breach in the fluid pressure boundary or a mechanical failure which adversely affects a flow path. Examples include the failure of a simple check valve to move to its correct position when required...."

From the outset, then, SECY-77-439 has contained an apparent ambiguity: a simple check valve failing to move to its correct position is a "mechanical failure which adversely affects a flow path," a passive failure. But a simple check valve failing to move is also the "failure of a component which relies on mechanical movement for its operation to complete its intended function on demand," which would otherwise classify it as an active failure.

The AEC/NRC's determinations of active versus passive failures, originally on a case-by-case basis and culminating in SECY-77-439, appear to reflect the Staffs' qualitative judgment of the likelihood of such failure occurring. As noted in SECY-77-439, the SFC "was developed without the benefit of numerical assessments on the probabilities of component failure."[9] The explicit recognition of a simple check valve as a passive failure appears to have derived from that qualitative judgment: although technically a failed mechanical movement, it was judged unlikely enough to be treated as a passive failure. Although simple check valves are the only example called out in SECY-77-439, historically other mechanical valve motions have been treated as passive failures as well, such as the failure of safety valves to open.[10]

In SECY-94-084, NRC Staff "examined current regulatory practice to determine how it will apply to check valve failures for the passive plant designs." As addressed in Section 3.4 below, NuScale believes that SECY-94-084 is not applicable here and the postulated IAB failure should be categorized based on the definitions, criteria, and rationale established in SECY-77-439.

3.2 The IAB function

The IAB is a component of the NuScale ECCS. Its primary function is to prevent inadvertent ECCS operation while the RCS is at operational pressures. In the design basis analysis of some transients, the IAB is credited to perform this function. For example, in an inadvertent operation of the ECCS transient, described in NuScale FSAR 15.6.6, an undefined failure is assumed that causes one ECCS valve to open at the initiation of the event. The highly-reliable dc power system is assumed to fail, which would de-energize and open the trip valves on the remaining ECCS valves. This depressurizes the line downstream of the IAB. Each IAB would then move to the closed position based on the differential pressure between the RCS and the open trip line to prevent those ECCS valves from opening immediately. Within this sequence, only that IAB moving to its closed position is at issue—NuScale's position is that function should be considered as a potential passive failure, which, under NRC guidance, is not assumed in analyzing the ECCS response.[11]

It should be noted that the IAB devices do not have the safety significance of the overall ECCS. The ECCS safety function contemplated by the GDCs is that of accident mitigation--to prevent extensive core

---

[9] SECY-77-439, p.1. See also Backfit Appeal, p.10: "SECY-77-439 also stresses the use of engineering judgment relating to the probability of component failure and does not suggest that valve "certification" or "qualification" in accordance with ASME standards should be invoked as the basis for such decisions."

[10] American National Standard ANSI/ANS-58.9-1981 (Reaffirmed 2015), Single Failure Criteria for Light Water Reactor Safety-Related Fluid Systems, p.3.

[11] Passive failures are only generally postulated only during the long-term (e.g. beyond 24 hours) event response. The IAB only has a function immediately following event initiation, so neither a short- or long-term failure is considered.

damage in the event of a design basis loss of coolant accident (LOCA).[12] NuScale credits the IABs only to meet more-stringent anticipated operational occurrence (AOO) acceptance criteria; failure of an IAB to close would challenge only the minimum critical heat flux limit due to faster RCS depressurization.[13] As discussed above, NuScale's Chapter 19 analysis shows that core damage is prevented even in the event of IAB failure.

3.3 The IAB design

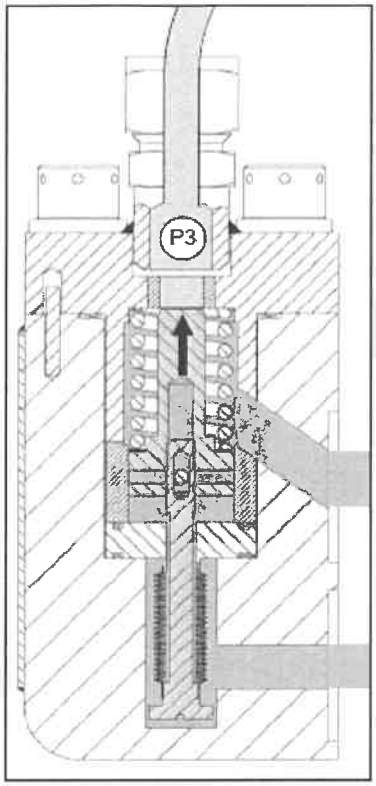
The IAB is a spring-loaded normally open valve. It consists of a rod that pushes against a spring and travels based on differential pressure between the chambers at the top and bottom of the rod. The spring provides a force pushing the rod away from the vent line seating surface. Under normal operating conditions, the rod inside the IAB is exposed to equivalent RCS pressure at the top and bottom of the rod. The IAB functions when an ECCS trip valve opens and places the IAB valve rod in a condition with RCS pressure at the bottom (under the rod, acting against the spring) and containment pressure at the top. The RCS pressure pushes the rod to the closed position with the equivalent of approximately 750 psi differential pressure[14] to move the IAB to the closed position. The closed IAB keeps the main ECCS valve closed until RCS pressure drops below the release threshold, when the IAB spring force will overcome the lower differential pressure and the IAB will reopen, permitting the ECCS main valve to open.

The left figure below is a diagram of the IAB, showing the rod, spring, and pressure ports and chambers. On the right is a diagram of the pilot valve portion of a safety relief valve (SRV) from an NRC Technology Manual.[15] As depicted, such pilot valves also consist of a valve disc that positions in response to spring force versus differential pressure. The design and operation of the pilot valve is described in the Technology Manual as follows:

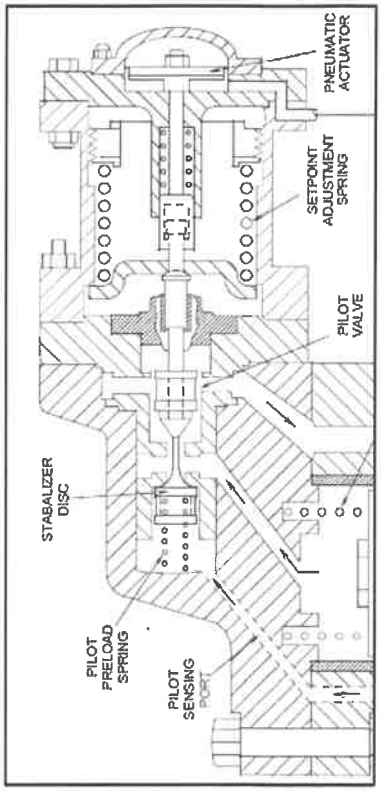
> *[The pilot valve] consists of a pilot stabilizer disc assembly with a means for remote actuation, via the attached pneumatic actuator. The pilot valve is the pressure sensing member to which the stabilizer disc movement is coupled. Though not mechanically connected, a small spring (pilot preload spring) keeps the stabilizer in contact with the pilot. The setpoint adjustment spring permits setpoint adjustment (lifting pressure) of the pilot valve and provides pilot valve seating force.... When the reactor is at operating pressure, below the setpoint of the valve, the pilot valve is seated with system pressure acting on the stabilizer disc side.... As system pressure increases to the setpoint of the SRV, the pressure acting on the pilot valve produces a force great enough to overcome the opposing force of the setpoint adjustment spring and lifts the pilot valve from its seat. As the pilot valve moves to full open (to the right), the stabilizer disc follows the pilot until the stabilizer is seated. With the pilot valve full open and the stabilizer seated, the area above the main valves piston is vented to the discharge piping via the main valve piston vent passage.*[16]

---

[12] GDC 35 provides, in part, "A system to provide abundant emergency core cooling shall be provided. The system safety function shall be to transfer heat from the reactor core following any loss of reactor coolant at a rate such that (1) fuel and clad damage that could interfere with continued effective core cooling is prevented and (2) clad metal-water reaction is limited to negligible amounts." The LOCA acceptance criteria are further defined by 10 CFR 50.46.
[13] Containment peak pressure would also increase, but NuScale has performed sensitivity analyses that demonstrate containment peak pressure would remain within applicable acceptance criteria.
[14] During a spurious ECCS valve opening with a reactor operating pressure of 1850 psia, a differential pressure of 1850 psid acts to move the IAB to the closed position. This differential pressure is countered by the IAB spring force (equivalent to ~1100 psid differential pressure). The net closing pressure is equivalent to approximately 750 psid.
[15] Source: NRC, "General Electric Advanced Technology Manual, Chapter 6.8, Safety Relief Valve Differences," ML11232A362.
[16] *Id.* [Internal references omitted].



NuScale IAB



SRV Pilot Valve

Failure of such spring-driven pilot valves have not typically been postulated as a single active failure.[17] NuScale believes that the IAB is similar, though simpler, in design and function to these existing pilot valve designs.

3.4 NuScale Position

3.4.1 SECY-77-439 is the applicable guidance to address the single failure classification of the IABs

Two NRC guidance documents define the SFC for current licensing practice: SECY-77-439 and SECY-94-084. NuScale believes SECY-77-439 is the controlling guidance here.

As discussed above, a "failure of a simple check valve to move to its correct position" is one of the functions identified in SECY-77-439 as a passive failure. In SECY-94-084, NRC Staff "examined current regulatory practice to determine how it will apply to check valve failures for the passive plant designs." Staff's rationale for revisiting the treatment of check valve failures was that

> *These safety-related check valves in the passive designs will operate under different conditions (low flow and pressure without pump discharge pressure to open valves) than current generation reactors and evolutionary designs. Check valves have high safety significance in the operation of the passive safety systems, and operating experience of check valves suggests that they may have a lower reliability than originally anticipated.*

[17] See discussion of the U.S. EPR below.

Staff's subsequently-approved recommendation was to "redefine check valves, except for those whose proper function can be demonstrated and documented, in the passive safety systems as active components subject to single failure consideration."[18] However, for components outside the scope of SECY-94-084, SECY-77-439 remains in force. Per NRC Regulatory Guide 1.206:

> *The applicant should provide a discussion of how the definitions for active and passive failures, as described in SECY-77-439, "Single-Failure Criterion," issued August 1977 have been applied to the analyses. For passive system designs, applicants should follow the guidance of the SECY-94-84, and ensure that low differential pressure check valves that perform a safety function are considered active components subject to single active failure consideration, except when their proper function can be demonstrated and documented.*[19]

Thus, Regulatory Guide 1.206 clarifies that the passive failure position in SECY-94-084 is limited to low differential pressure check valves in a passive safety system, consistent with the Staff's concerns in development of that position. Accordingly, except for "low differential pressure check valves" in "passive system designs," component failures continue to be categorized based on the definitions established in SECY-77-439. Indeed, in the AP1000 DCD, low differential pressure check valves in the passive core cooling system were treated as active failures, while check valves in the passive ECCS accumulator injection lines were treated as passive failures, consistent with SECY-77-439 practice.[20]

NuScale believes the IABs do not fit the criteria for applying SECY-94-084. First, while the IAB is part of a passive safety system, the IAB will move to its closed position under the equivalent of approximately 750 psi differential pressure,[21] more akin to the pressures seen by check valves in high-pressure pumped systems and RCS accumulators. Second, NRC Staff have concluded that the IAB is not a check valve.[22] Third, the IABs lack the "high safety significance" that underpinned Staff's rationale for developing the SECY-94-084 position. For these reasons, SECY-94-084 does not apply. Therefore the IABs should be evaluated under SECY-77-439.

3.4.2 Reliability data is not required to consider a component failure as passive under SECY-77-439

Under SECY-77-439, reliability data was not the basis of Staff's determination that a component can be considered a passive failure. Application of the SFC prior to and under SECY-77-439 was based on Applicant and Staff judgment[23] of the component's reliability. The SFC "was developed without the benefit of numerical assessments on the probabilities of component failure..."[24]

NRC addressed this issue head-on in NUREG-0153, Issue 17. Therein, NRC addressed a staff member's position that "a failure rate criterion should be specified for single failures," and that a "single passive mechanical failure of a valve" in a safety system should be considered in the system design where "the failure rate of the given valve is in excess of the failure rate criterion." The agency declined to establish a numerical failure rate criterion, instead relying on their "present judgment regarding the likelihood of

---

[18] SECY-94-084/95-132 consolidation, p. 11.
[19] RG 1.206, Rev. 0, C.I.15-6. RG 1.206 was recently updated to Revision 1, which has been reformatted to remove technical discussion, instead relying on the Standard Review Plan for that discussion. Chapter 15.0 of the Standard Review Plan does not provide the same statement, but NuScale has no reason to believe this reflects a change in NRC position.
[20] NUREG-1793, Vol. 1, Section 6.3.2.7.
[21] See footnote 14.
[22] Summary of the August 22, 2018 Meeting, p.5.
[23] SECY-77-439 includes numerous statements supporting the notion that subjective judgment was the basis for development of the SFC. For example, "In general only those systems or components which are judged to have a credible chance of failure are assumed to fail when the Single Failure Criterion is applied," and that only certain long-term passive failures in fluid systems "are required to be assumed because it is judged that compounding of probabilities associated with other types of passive failures...results in probabilities sufficiently small."
[24] SECY-77-439, p.1.

passive mechanical valve failures." NUREG-0153 discusses plans to confirm that judgment via a systematic review of valve failure data. However, SECY-77-439, issued the following year, declined to specify a failure rate criterion.

NuScale is unaware of any numeric failure rate criterion subsequently established until the promulgation of SECY-94-084. As discussed above, for the specific components addressed thereunder—low differential pressure check valves in passive safety systems—SECY-94-084 changes the presumptive classification from passive failure to active failure. In order to demonstrate that such a check valve function is a passive failure, the plant designer must "perform a comprehensive evaluation of check valve test data or operational data" for similar valves to show that "reliability of the particular check valve application is such that the probability of failure is comparable to those of passive components." The policy further establishes that "a failure probability on the order of 1E-4 per year or less would be low enough."

Because SECY-94-084 established a quantitative reliability criterion for the specific components addressed by that policy, it necessarily follows that such a reliability criterion does not otherwise exist under SECY-77-439. Accordingly, under SECY-77-439, NuScale believes a specific failure probability is not required to be demonstrated in order to conclude that a mechanical valve function is a passive failure mechanism. As discussed below, however, NuScale acknowledges that relevant, available reliability data is one factor to consider in evaluating sufficient reliability of a component.

3.4.3 A qualitative evaluation of a component's design and function, including a comparison to other component functions that have been and are treated as passive, is sufficient to demonstrate the component's expected reliability.

The movements of both a simple check valve and an SRV meet the definitions of both an active[25] and passive[26] failure under SECY-77-439. However, SECY-77-439 does not provide explicit guidance on categorizing the functions of such components as potential active or passive failures. Lacking explicit criteria to make such a determination, then, NuScale believes that a component such as the IAB should be assessed for sufficient reliability on a qualitative basis, considering the attributes that precedent indicate have underpinned determinations that a mechanical component function may be treated as passive.

In Section 3.3, above, NuScale compared the design of the IAB to an SRV pilot valve. NRC guidance and precedent addresses treatment of such valves as passive failures. SRP 5.2.2 provides that with respect to reactor coolant pressure boundary overpressure protection:

> *"A single malfunction or failure of an active component should not preclude safety-related portions of the system from functioning as required during normal operations, adverse environmental occurrences, and accident conditions, including loss of offsite power. Full credit is allowed for spring-loaded safety valves designed in accordance with the requirements of ASME Code Article NB-7511.1."*

ASME NB-7511.1 states in its entirety:

> *Spring Loaded Valves. Valves shall open automatically by direct action of the fluid pressure as a result of forces acting against a spring.*

As a recent example of this position, the U.S. EPR Final Safety Analysis Report,[27] Section 15.0.0.3.8, states that pressurizer safety relief valves (PSRVs), when actuated by a spring-driven pilot, are

---

[25] "the failure of a component which relies on mechanical movement for its operation to complete its intended function on demand"
[26] "a mechanical failure which adversely affects a flow path"
[27] ML13220A925

considered passive devices and therefore not subject to single failure. NRC's Safety Evaluation Report with Open Items concurs:

> *The spring operated pilot valves are designed in accordance with the requirements of ASME Section III, NB-7511.1. With successful operation of the pilot valve, a large differential pressure reliably opens the main relief disk, which relieves RCS pressure. A single failure is not postulated because the PSRVs do not require additional motive force to perform their design safety function during RCS hot conditions. The staff finds the response acceptable, since it complies with the ASME B&PV Code, Section III."*[28]

Considering the treatment of both simple check valves and pressure-and-spring actuated valves, NuScale observes that the essential characteristics that define mechanical valves treated as passive failures appear to be simplicity in the design, a lack of external motive power source to operate, and the quality of the design and construction. Together, these characteristics appear to provide sufficient justification to judge a mechanical valve function as a passive failure.

As addressed above, NuScale does not believe that a quantitative reliability criterion for passive failures is required under SECY-77-439. To be clear, NuScale does not believe reliability data, including operational data, is wholly irrelevant to an evaluation of whether a given component function should be treated as a passive failure. If operational data exists to indicate that a component's treatment as passive is inappropriate, it would be appropriate to revisit that determination for similar components in future licensing reviews. NuScale's position, however, is that the formal requirements for highly-specific reliability data and the bright-line threshold established under SECY-94-084 are not appropriate to impose under SECY-77-439.

Rather, NuScale believes that a more flexible consideration of reliability data is appropriate when evaluating a new component under SECY-77-439. NuScale believes the applicant and NRC staff can reasonably consider component reliability using operational data for components that are sufficiently similar to the new component, relying on component vendor expertise to determine that the operational data is relevant. NuScale also believes there is no predetermined threshold for passive reliability, but rather that the reliability data should be considered in the broader qualitative evaluation of the component's reliability. For example, the safety significance of the new component would be relevant in considering the available reliability data.

3.4.4 Evaluating the IAB under this SECY-77-439 framework demonstrates that IAB closure function is sufficiently reliable to be considered a passive failure

As with a simple check valve or SRV, failure of the IAB closing function appears to meet the definitions of both an active and passive failure under SECY-77-439. Thus, NuScale evaluated the IAB under the above framework: by evaluating the attributes of the design for inherent reliability, by comparing the closing function to other component functions that are normally treated as passive under SECY-77-439, and by considering relevant operational reliability data. Based on that evaluation, NuScale concludes that the IAB should be considered a passive failure under SECY-77-439.

As discussed in Section 3.3 above, the IAB closely resembles an SRV pilot valve. The IAB is being designed and manufactured by Target Rock, a proven manufacturer of safety-related SRV spring-driven pilot valves. The IAB supports the same conclusions as Staff's preliminary conclusions on the U.S. EPR PSRVs. The IAB is an ASME Section III Class 1 component and it "opens automatically by direct action of the fluid pressure as a result of forces acting against a spring."[29] Like the U.S. EPR PSRVs, a large

---

[28] "Safety Evaluation Report with Open Items for the U.S. EPR," ML090900096.

[29] ASME NB-7511.1 does not directly apply because it is an ASME code requirement specifically for SRVs, so the IAB is not designed to ASME NB-7511.1 in the strict sense. However, NuScale views the attributes described as the pertinent consideration here.

differential pressure would actuate the valve disk, and no additional motive force is required to perform the safety function.

NuScale also evaluated possible failure modes of the IAB and concluded that all are sufficiently unlikely. The IAB valve design utilizes a rod which slides up and down in a small clearance channel. The rod is normally held open by a spring with fluid pressures acting on either side of the rod. The valve disc is integral to the end of the rod and a bellows is incorporated on the other side. The bellows helps to isolate the RCS reference pressure boundary which acts on one side of the rod. Without the bellows, leakage through the rod and channel clearances could reduce the precision of the intended block and release differential pressures.

Accordingly, failure modes of the IAB that could affect the blocking function[30] are:

- Valve body failure
- Seat leakage
- Bellows pressure boundary failure
- O-ring/gasket failure
- Fastener failure (fasteners attach the IAB to the main valve body, and affix the upper and lower IAB valve body)

These potential failures modes are similar in nature to failures treated as passive in safety analyses for other parts of the reactor such as the reactor and containment vessel. These potential failure modes are addressed by appropriate quality assurance—designing, constructing, and testing per ASME Section III Class 1 rules, analyzing clearances at the range of operating temperatures and pressures, selecting suitable component materials and seals, etc.

With respect to reliability data, in response to an NRC request for additional information[31] NuScale provided a quantitative evaluation of IAB reliability. NuScale performed an evaluation using Target Rock main steam safety relief valves (MSSRVs) in use at boiling water reactors as a surrogate for the IAB. The pilot assembly of the Target Rock MSSRV is of similar design to the IAB valve, is made by the same manufacturer, and operates on the same principle of differential pressure. NuScale reviewed the operating experience for these valves to identify specific failure events involving the MSSRV pilot that would be applicable to the IAB, and the results were used to estimate a failure probability for the IAB valve. This evaluation determined the IAB to have a mean failure-to-close probability of 3.5E-4 per demand. When combined with the frequency of initiating events determined in the PRA that would demand the IAB, the failure frequency for any of the five IAB valves to close is 1.2E-5 per module critical year. While the operational data is not for the actual IAB, NuScale believes that under SECY-77-439 it is an acceptable surrogate to consider in evaluating the reliability of a new component. In light of the low safety significance of the IAB in the NuScale design, NuScale concludes that the reliability data supports categorization of the IAB closing function as a potential passive failure.

In summary, although the IAB is a new component developed for the NuScale design, NuScale believes it is similar, albeit even simpler, in design and simplicity to an SRV spring-driven pilot valve. The IAB meets the same criteria—actuated by fluid pressure against a spring and an ASME Section III component—that such a valve must meet to be treated as a passive component. NuScale also determined that surrogate operational data supports treatment as a passive function. Thus, the simplicity and operating principles of the IAB, the failure modes of the IAB, the design, fabrication, and testing quality assurance requirements

[30] Three additional failure modes—spring failure, disc sticking, and Swagelok tubing connector failure—would only impact the IAB open function (staying open or re-opening).
[31] NuScale Power, LLC Response to NRC Request for Additional Information No. 36 (eRAI No. 8815) on the NuScale Design Certification Application, RAIO-0717-55033, July 21, 2017.

as an ASME Class 1 component, and relevant reliability data demonstrate that the IAB will perform adequately in service, commensurate with the IAB's importance to safety.

3.4.5 Alternatively, NuScale considered new criteria that clarify the SECY-77-439 policy, which would also establish the IAB closing function as a passive failure.

NuScale carefully considered the letter and spirit of SECY-77-439 to conclude that IAB failure-to-close is a passive failure thereunder, and developed the NuScale design and licensing basis from that determination. NRC staff, however, reviewed the same information and reached the opposite conclusion, indicating the existing guidance needs clarification to address this and future instances that are likely to arise in other advanced designs. Specifically, if NRC staff believe SECY-77-439 cannot be applied or does not resolve the issue, then additional direction is requested from the Commission in classifying new components as passive or active failures. The scope of the new guidance should address components, such as the IAB, that fall into both the passive and active failure definitions of SECY-77-439.

Consistent with SECY-77-439, NuScale believes it is unnecessary to provide reliability data to justify treatment of a new component as a passive failure. Staff's position in SECY-94-084 addresses a particular concern over low-differential pressure check valves in passive safety systems with high safety significance. NuScale's IABs are not similarly situated.[32]

Instead, NuScale believes the 2016 Backfit Appeal Review Panel report[33] also suggests an appropriate framework for clarifying the classification of mechanical valve functions as passive or active failures that is consistent with the qualitative evaluation approach of SECY-77-439. Therein, the Panel observed that

> *In general… the classification of a component as "active" or "passive" depends on its design, application, and function. For example, passive components almost always do not need external power; usually do not need an external actuator (e.g., signal); sometimes do not involve any mechanical motion (e.g., movement of a valve disc); and sometimes do not involve any motion, either fluid or mechanical (e.g., piping).*[34]

The Panel went on to evaluate the opening function of a PSV under the applicable standard of SECY-77-439.[35] The Panel noted the ambiguity of SECY-77-439 with respect to safety valves, and observed

> *the opening function of check valves and PSVs to be similar in that they both open through the motion of the valve disk under differential pressure with no external signal or motive power. The Panel also recognized that the ambiguity with respect to "passive" versus "active" component definitions and nomenclature exists for safety valves. In addition, the passive or active classification of check valves or safety valves may differ based on design considerations, inservice testing, or accident analyses.*[36]

The Panel then concluded:

> *[I]t is appropriate to consider the potential failure of a PSV to reclose following water discharge as a passive failure (consistent with the treatment of check valve failures for the operating fleet), supported by the EPRI testing associated with TMI Action Plan Item II.D.1 that gave confidence in the capability of the valves.*[37]

---

[32] NuScale acknowledges that the rationale of the SECY-94-084 policy could be extended beyond merely check valves. Even so, NuScale believes that the other concerns underpinning the policy—low differential pressure and high safety significance—do not apply to the IABs.
[33] Report of the Backfit Appeal Review Panel Chartered by the Executive Director for Operations to Evaluate the June 2016 Exelon Backfit Appeal, August 23, 2016, ADAMS Accession No. ML16236A208.
[34] *Id.*, p. 7 (emphasis added; citations omitted).
[35] *Id.*, p. 13.
[36] *Id.*, p. 13.
[37] *Id.*, p. 13.

The Panel's conclusion is not directly applicable to the NuScale IABs, but provides a useful framework to address it and other ambiguous cases under SECY-77-439. NuScale suggests that criteria derived from that framework may help clarify such cases. Based on that framework, NuScale believes the following criteria, if satisfied, would result in a conclusion that a mechanical component function may be treated as a passive failure:

- Design:
  - The postulated failure must be a mechanical function. The function must not rely on an external signal or external motive power.
  - The component operation must be similar to other component functions judged to be passive failures.
- Application:
  - The component must perform a function for which it is designed and will be qualified to perform.
  - The component must have inherent "margin" to overcome unexpected challenges (e.g. high differential pressure).
- Function:
  - A failure modes and effects analysis shows that only passive mechanisms (e.g., mechanical binding, spring failure, etc.) can lead to a failure to function.
  - Functional testing demonstrates that the component will perform under design conditions.

In addition to those elements, it may be appropriate to qualitatively consider additional factors in their evaluation: (1) the safety significance of the individual component function in performing the system safety function (i.e., the consequences of failure), and (2) the importance of the component function with respect to the reliability of a system to perform its safety function. With respect to the safety significance of the component function, NuScale believes that the design certification PRA is adequate to inform that consideration.

Applying such a framework to the IABs would yield a conclusion that their failure to close on demand is a passive failure:

- Closure of the IAB is a mechanical failure; the IAB does not rely on an external signal or external motive power to function. The IAB only relies on differential pressure against a spring force to move to its closed position.
- The IAB closes when increased differential pressure overcomes the spring force and causes the valve disc to seat, as with to the opening of a SRV pilot that has historically been treated as a passive failure.
- The IAB is safety-related, designed for, and will be qualified to perform its required function.
- The IAB acts on high differential pressures causing it to close.
- The only failure modes that could cause the IAB to fail to close are passive mechanisms.
- The IAB will be functionally tested to demonstrate its performance.
- Chapter 19 of the PRA demonstrates that even with failure of the IAB to close, the ECCS performs its safety function of preventing core damage.

Therefore, under this proposed framework, the IAB closing function would likewise be categorized as a postulated passive failure, subject to completion of performance testing and qualification testing at the applicable points in the licensing sequence.

4.0 Conclusion

NuScale and NRC Staff have been unable to reach agreement on the proper treatment of NuScale's inadvertent actuation block devices under the single failure criterion. NuScale requests that the Commission revisit and clarify the single failure criterion as it applies to mechanical components that can be treated as potential passive failures in NuScale's and other advanced reactor designs. With some clarification from the Commission, the existing SECY-77-439 guidance should support resolution of this issue for the IABs. In NuScale's judgment, the IAB is similar in design and function to existing valve components which have been treated as passive failures, and thus should be treated as such without the need for reliability data to justify that conclusion. However, NuScale has also evaluated the IAB under suggested new criteria that could enhance the framework for evaluating such components.

McCloskey, Bridin

Attachments: LO-1218-63707_IAB Single Failure Criterion_121418 Signed .pdf

From: "Bergman, Tom" <tbergman@nuscalepower.com>
Subject: [External_Sender] Submittal of IAB Single Failure Criterion Letter
Date: 14 December 2018 21:22
To: "Taylor, Robert" <Robert.Taylor@nrc.gov>

Rob,

The final letter.

Tom Bergman
Vice President, Regulatory Affairs
email: tbergman@nuscalepower.com
web: www.nuscalepower.com
office: 541.360.0740