

February 23, 2018

Docket: PROJ0769

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
One White Flint North
11555 Rockville Pike
Rockville, MD 20852-2738

SUBJECT: NuScale Power, LLC Submittal of the Approved Version of NuScale Topical Report TR-0815-16497, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 1 (CAC No. RQ6002)

REFERENCE: Letter from Frank Akstulewicz (NRC) to Thomas Bergman (NuScale), "Safety Evaluation for Topical Report: 0815-16497, Revision 1, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," dated December 13, 2017 (ML17339A533).

By the referenced letter dated December 13, 2017, the NRC issued a final safety evaluation report documenting the NRC staff conclusion that the NuScale topical report TR-0815-16497, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 1, is acceptable for referencing in licensing applications for the NuScale small modular reactor design. The referenced NRC letter requested that NuScale publish the approved version of TR-1015-18653, within three months of receipt of the letter.


Accordingly, Enclosure 1 to this letter provides the approved version of TR-0815-16497-P-A, Revision 2. This enclosure includes the December 13, 2017 NRC letter and its final safety evaluation report, the NuScale response to NRC requests for additional information, and documentation of the final Topical Report submittal, Revision 1.

Enclosure 1 contains proprietary information. NuScale requests that the proprietary enclosure be withheld from public disclosure in accordance with the requirements of 10 CFR § 2.390. The enclosed affidavit (Enclosure 3) supports this request. Enclosure 2 contains the nonproprietary version of the approved topical report package.

This letter makes no regulatory commitments and no revisions to any existing regulatory commitments.

Please contact Jennie Wike at 541-360-0539 or at jwike@nuscalepower.com if you have any questions.

Sincerely,



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

Distribution: Frank Akstulewicz, NRC, OWFN-8H4A
Greg Cranston, NRC, OWFN-8G9A
Omid Tabatabai, NRC, OWFN-8G9A
Samuel Lee, NRC, OWFN-8G9A

Enclosure 1: NuScale Topical Report, TR-0815-16497-P-A, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 1, proprietary version

Enclosure 2: NuScale Topical Report, TR-0815-16497-NP-A, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 1, nonproprietary version

Enclosure 3: Affidavit of Thomas A. Bergman, AF-0118-58310

Enclosure 1:

NuScale Topical Report, TR-0815-16497-P-A, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 1, proprietary version

Enclosure 2:

NuScale Topical Report, TR-0815-16497-NP-A, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 2, nonproprietary version

Contents

<u>Section</u>	<u>Description</u>
A	Letter from Frank Akstulewicz (NRC) to Thomas Bergman (NuScale), "Safety Evaluation for Topical Report: 0815-16497, Revision 1, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," (CAC No RQ6002)," dated December 13, 2017.
B	NuScale Topical Report: Safety Classification of Passive Nuclear Power Plant Electrical Systems, TR-0815-16497-NP-A, Revision 1.
C	Letter from Thomas A. Bergman (NuScale) to NRC, "NuScale Power, LLC Submittal of Response to Request for Additional Information Letter No. 8 for the Review of NuScale Topical Report, TR-0815-16497, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 0," dated December 5, 2016 (ML 16340D339).
D	Letter from Thomas Bergman (NuScale) to NRC, "NuScale Power, LLC, Submittal of Topical Report TR-0815-16497, "Safety Classification of Passive Nuclear Power Plant Electrical Systems, Revision 1 (CAC No. RQ6002)," dated February 17, 2017.

Section A



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

December 13, 2017

Mr. Thomas Bergman
Vice President, Regulatory Affairs
NuScale Power, LLC
1100 NE Circle Boulevard, Suite 200
Corvallis, OR 97330

SUBJECT: SAFETY EVALUATION FOR TOPICAL REPORT 0815-16497, REVISION 1,
"SAFETY CLASSIFICATION OF PASSIVE NUCLEAR POWER PLANT
ELECTRICAL SYSTEMS" (CAC NO. RQ6002)

Dear Mr. Bergman:

By letter dated October 29, 2015, NuScale Power, LLC (NuScale), submitted Topical Report (TR) 0815-16497, Revision 0, "Safety Classification of Passive Nuclear Power Plant Electrical Systems" (Agencywide Documents Access and Management System (ADAMS) Accession No. ML15306A263). On February 7, 2017, NuScale submitted proprietary and nonproprietary versions of TR-0815-16497, Revision 1 (ADAMS Accession No. ML17048A459).

The U.S. Nuclear Regulatory Commission (NRC) staff has found that the TR 0815-16497, Revision 1, is acceptable for referencing in licensing applications for the NuScale small modular reactor design to the extent specified and under the conditions and limitations delineated in the enclosed safety evaluation report (SER). The SER defines the basis for acceptance of the TR.

The NRC's acceptance applies only to matters approved in the subject TR. We do not intend to repeat our review of the acceptable matters described in the TR. When the report appears as a reference in license applications, our review will ensure that the material presented applies to the specific plant involved. Regulatory licensing action requests that deviate from this TR will be subject to additional staff reviews in accordance with applicable review standards.

In accordance with the guidance provided on the NRC's TR website (<http://www.nrc.gov/about-nrc/regulatory/licensing/topical-reports.html>), we request that NuScale publish an accepted version of this TR within three months of receipt of this letter. The accepted version shall incorporate this letter and the enclosed safety evaluation between the title page and the abstract. It must be well indexed such that the information is readily located. Also, it must contain in its appendices historical review information, such as questions and accepted responses, and original report pages that were replaced. The accepted version shall include an "-A" (designated accepted) following the report identification symbol.

T. Bergman

2

If the NRC's criteria or regulations change so that its conclusion in this letter, that the TR is acceptable, is invalidated, NuScale and/or the applicant referencing the TR will be expected to revise and resubmit its respective documentation, or submit justification for the continued applicability of the TR without revision of the respective documentation.

Sincerely,

Francis M. Akstulewicz, Director **/RA Anna Bradford Acting for/**
Division of New Reactor Licensing
Office of New Reactors

Docket No. PROJ0769

Enclosure:
Safety Evaluation

cc w/encl: DC NuScale Power LLC Listserv

NUSCALE POWER, LLC
SAFETY EVALUATION FOR TOPICAL REPORT TR-0815-16497,
REVISION 1, “SAFETY CLASSIFICATION OF PASSIVE NUCLEAR POWER PLANT
ELECTRICAL SYSTEMS”
(CAC. NO. RQ6002)

1.0 Introduction

By letter dated October 29, 2015 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML15306A263), NuScale Power, LLC (the applicant or NuScale), submitted Topical Report (TR)-0815-16497, Revision 0, “Safety Classification of Passive Nuclear Power Plant Electrical Systems.” By letter dated February 7, 2017, NuScale submitted Revision 1 to TR-0815-16497 in proprietary (-P) and nonproprietary (-NP) versions (letter and -NP version available at ADAMS Accession No. ML17048A459).

Section 1.1, “Purpose,” of TR-0815-16497-NP, Revision 1, states the purpose of the submittal and describes the review and approval that the applicant seeks from the U.S. Nuclear Regulatory Commission (NRC or Commission) staff, as follows:

The purpose of this topical report is to request Nuclear Regulatory Commission (NRC) review and approval of what are termed herein as “conditions of applicability,” and the methodology and bases used in their development. The conditions of applicability comprise a set of passive reactor plant design and operational attributes that, if met in full by a reactor design or license applicant, justify the applicant’s determination that none of the plant electrical systems fulfill functions that, per the regulatory definitions of “safety-related” and “Class 1E,” would warrant a Class 1E classification. The conditions of applicability are presented in Table 3-1, “Conditions of applicability.”

This topical report also seeks NRC review and approval of augmented design, qualification, and quality assurance (QA) provisions that are an extension of the conditions of applicability (via Item II.1 of Table 3-1). The augmented provisions are described in Table 3-2. For reasons detailed in Section 3.2, these augmented design, qualification, and QA provisions would be applied as minimum requirements to electrical systems that have been determined to be nonsafety-related but yet are essential to the post-accident monitoring of Type B and Type C variables. Provided the conditions of applicability are fully satisfied, the approved augmented provisions would represent an acceptable alternative to the portion of Regulatory Guide 1.97, Revision 4 (Reference 4.39), that specifies a Class 1E power source for instrumentation associated with Type B and Type C variables.

Based on its review of the TR, the NRC staff issued requests for additional information (RAIs) via letter dated October 7, 2016 (ADAMS Accession No. ML16281A298); in particular, the RAIs addressed the direct current (dc) equipment and system, postaccident monitoring, and reactor coolant pressure boundary (RCPB) integrity and safe shutdown. In response to these RAIs, NuScale provided supplemental information in a letter dated December 5, 2016 (ADAMS Accession No. ML16340D339).

2.0 Regulatory Evaluation

The electric power systems for power plants include onsite electrical power systems providing alternating current (ac) power and dc power. Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," refers to safety-related electrical equipment as "Class 1E" equipment. As defined therein, the safety-related or "Class 1E" classification is the safety classification of the electrical equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or otherwise are essential in preventing a significant release of radioactive material to the environment. As used in IEEE Std. 323-1974, Class 1E equipment includes appropriate interfaces.

If a reactor was designed so that no electrical equipment was "essential" such that it met the definition of Class 1E (i.e., the reactor plant design did not include safety-related equipment dependent on electric power), then the design would not require Class 1E ac or dc power systems. Where no Class 1E equipment is used, the basic requirements for qualifying Class 1E equipment and interfaces, which are provided in IEEE Std. 323-1974, are inapplicable. In TR-0815-16497, NuScale provided a method to justify that the plant electric power supplies need not be classified as Class 1E.

In TR Section 3.1, "Methodology Used to Develop Conditions of Applicability," the applicant stated that "the application of augmented provisions is consistent with the process established in the NRC regulatory framework for 'special treatment' of nonsafety-related SSCs that are determined to have risk-significance."

In TR Table 3-2, "Augmented Design, Qualification, and Quality Assurance Provisions," the applicant listed the regulatory requirements and guidance documents that a future passive plant applicant would need to apply or consider for the augmented design, qualification, and QA provisions of the non-Class 1E electrical systems—termed the "highly reliable DC electrical system(s)"—for powering the postaccident monitoring instrumentation for Type B and Type C variables and for the plant emergency lighting systems.

The NRC staff evaluated the conditions of applicability in TR Table 3-1, "Conditions of Applicability," by first identifying the design-basis information, as defined in Title 10 of the *Code of Federal Regulations* (10 CFR) 50.2, "Definitions." As defined in 10 CFR 50.2, "design basis" means that information that identifies the specific functions to be performed by an SSC of a facility, and the specific values or ranges of values chosen for controlling parameters as reference bounds for design. The staff then ensured that Table 3-1 addressed these specific functions by the conditions of applicability.

In accordance with 10 CFR 52.47(a)(3), an application for a design certification must include the design of the facility, including the following:

- (i) The principal design criteria for the facility. Appendix A to 10 CFR part 50, general design criteria (GDC), establishes minimum requirements for the principal design criteria for water-cooled nuclear power plants similar in design and location to plants for which construction permits have

previously been issued by the Commission and provides guidance to applicants in establishing principal design criteria for other types of nuclear power units;

- (ii) The design bases and the relation of the design bases to the principal design criteria;
- (iii) Information relative to materials of construction, general arrangement, and approximate dimensions, sufficient to provide reasonable assurance that the design will conform to the design bases with an adequate margin for safety;

The staff's review considered if the design would meet the following minimum requirements in Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," for principal design criteria even if no electrical equipment was classified as Class 1E:

- GDC 10, "Reactor Design," requires that the reactor core and associated coolant, control, and protection systems be provided with appropriate margin to assure that specified acceptable fuel design limits (SAFDLs) are not exceeded during any condition of normal operation, including the effect of anticipated operational occurrences (AOOs).
- GDC 13, "Instrumentation and Control," requires, in part, that the applicant provide instrumentation to monitor variables and systems over their anticipated ranges for normal operation, AOOs, and accident conditions as appropriate to assure adequate safety.
- GDC 15, "Reactor Coolant System Design," requires that the reactor coolant system and associated auxiliary, control, and protection systems be designed with sufficient margin to assure that the design conditions of the RCPB are not exceeded during any condition of normal operation, including AOOs.
- GDC 16, "Containment Design," requires that the reactor containment and associated systems shall be provided to establish an essentially leak-tight barrier against the uncontrolled release of radioactivity to the environment and to assure that the containment design conditions important to safety are not exceeded for as long as postulated accident conditions require.
- GDC 19, "Control Room," requires, in part, that a control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents (LOCAs).
- GDC 20, "Protection System Functions," requires, in part, that the protection system be designed to automatically initiate the operation of appropriate systems, including the reactivity control systems, to assure that SAFDLs are not exceeded as a result of AOOs.

- GDC 26, “Reactivity Control System Redundancy and Capability,” requires, in part, that the control rods be capable of reliably controlling reactivity changes to assure that SAFDLs are not exceeded under conditions of normal operation, including AOOs, and with appropriate margin for stuck rods.
- GDC 27, “Combined Reactivity Control Systems Capability,” requires that the reactivity control systems be designed to have a combined capability, in conjunction with poison addition by the emergency core cooling system (ECCS), of reliably controlling reactivity changes to assure that the capability to cool the core is maintained under postulated accident conditions and with appropriate margin for stuck rods.
- GDC 34, “Residual Heat Removal,” requires, in part, that a residual heat removal system be provided. The system safety function shall be to transfer fission product decay heat and other residual heat from the reactor core at a rate such that SAFDLs and the design conditions of the RCPB are not exceeded.
- GDC 35, “Emergency Core Cooling,” requires, in part, that a system to provide abundant core cooling 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.
- GDC 38, “Containment Heat Removal,” requires, in part, the provision of a system to remove heat from the reactor containment. The system safety function shall be to rapidly reduce, consistent with the functioning of other associated systems, the containment pressure and temperature following any LOCA and to maintain them at acceptably low levels.
- GDC 41, “Containment Atmosphere Cleanup,” requires, in part, systems to control fission products, hydrogen, oxygen, and other substances that may be released into the reactor containment as necessary to reduce, consistent with the functioning of other associated systems, the concentration and quality of fission products released to the environment following postulated accidents and to control the concentration of hydrogen or oxygen and other substances in the containment atmosphere following postulated accidents to assure that containment integrity is maintained.
- GDC 50, “Containment Design Basis,” requires, in part, that the reactor containment structure, including access openings, penetrations, and the containment heat removal system, shall be designed so that the containment structure and its internal compartments can accommodate, without exceeding the design leakage rate and with sufficient margin, the calculated pressure and temperature conditions resulting from any LOCA.
- GDC 54, “Piping Systems Penetrating Containment,” requires, in part, that piping systems penetrating primary reactor containment shall be provided with leak detection, isolation, and containment capabilities that have redundancy, reliability, and performance capabilities that reflect the importance to safety of isolating these piping systems.

- GDC 55, "Reactor Coolant Pressure Boundary Penetrating Containment," requires, in part, that each line that is part of the RCPB and that penetrates primary reactor containment shall be provided with containment isolation valves.
- GDC 56, "Primary Containment Isolation," requires, in part, that each line that connects directly to the containment atmosphere and penetrates the primary reactor containment shall be provided with containment isolation valves.
- GDC 57, "Closed System Isolation Valves," requires each line that penetrates primary reactor containment and is neither part of the RCPB nor connected directly to the containment atmosphere to have at least one containment isolation valve that shall be either automatic or locked closed, or capable of remote manual operation. This valve shall be outside containment and located as close to the containment as practical. A simple check valve may not be used as the automatic isolation valve.
- GDC 61, "Fuel Storage and Handling and Radioactivity Control," requires, in part, that fuel storage and handling, radioactive waste, and other systems that may contain radioactivity be designed to assure adequate safety under normal and postulated accident conditions. This criterion specifies that such systems shall be designed to include appropriate containment, confinement, and filtering systems.
- GDC 63, "Monitoring Fuel and Waste Storage," requires, in part, appropriate systems in fuel storage and radioactive waste systems and handling areas to detect conditions that may cause a loss of residual heat removal capability and excessive radiation levels and to initiate appropriate safety actions.
- GDC 64, "Monitoring Radioactive Releases," requires, in part, the means for monitoring the reactor containment atmosphere, spaces containing components for recirculation of LOCA fluids, effluent discharge paths, and the plant environs for radioactivity that may be released as a result of postulated accidents.

The NRC staff also determined that the following regulatory requirements and guidance documents are applicable to the review of this TR:

- In accordance with the requirements in 10 CFR 52.47(a)(8), an application for a design certification must include the information necessary to demonstrate compliance with any technically relevant portions of the Three Mile Island requirements set forth in 10 CFR 50.34(f), 10 CFR 50.34(f)(1)(xii), (f)(2)(ix), and (f)(3)(v). In turn, 10 CFR 50.34(f)(2) states that to satisfy the requirements in 10 CFR 50.34(f)(2)(i)–(xxviii), the application shall provide sufficient information to demonstrate that the required actions will be satisfactorily completed by the operating license stage. Those required actions under 10 CFR 50.34(f)(2) include the following:
 - (viii) Provide a capability to promptly obtain and analyze samples from the reactor coolant system and containment that may contain accident source term radioactive materials without radiation exposures to any individual exceeding 5 rems to the whole body or 50 rems to the extremities. Materials to be analyzed and

quantified include certain radionuclides that are indicators of the degree of core damage (e.g., noble gases, radioiodines and cesium, and nonvolatile isotopes), hydrogen in the containment atmosphere, dissolved gases, chloride, and boron concentrations.

- (xvii) Provide instrumentation to measure, record and readout in the control room: (A) containment pressure, (B) containment water level, (C) containment hydrogen concentration, (D) containment radiation intensity (high level), and (E) noble gas effluents at all potential, accident release points. Provide for continuous sampling of radioactive iodines and particulates in gaseous effluents from all potential accident release points, and for onsite capability to analyze and measure these samples.
 - (xix) Provide instrumentation adequate for monitoring plant conditions following an accident that includes core damage.
 - (xx) Provide power supplies for pressurizer relief valves, block valves, and level indicators such that: (A) Level indicators are powered from vital buses; (B) motive and control power connections to the emergency power sources are through devices qualified in accordance with requirements applicable to systems important to safety; and (C) electric power is provided from emergency power sources. (Applicable to PWR's only.)
- In accordance with the requirements in 10 CFR 52.47(a)(12), an application for a design certification must include an analysis and description of the equipment and systems for combustible gas control as required in 10 CFR 50.44, "Combustible Gas Control for Nuclear Power Reactors." In turn, 10 CFR 50.44 requires, in part, that an applicant must perform an analysis that demonstrates containment structural integrity. The analysis must address an accident that releases hydrogen generated from a 100-percent fuel clad-coolant reaction accompanied by the hydrogen burning. The applicant must demonstrate that systems necessary to ensure containment integrity are able to perform their function under these conditions.
- In accordance with the requirements in 10 CFR 52.47(a)(4), an application for a design certification must include an analysis and evaluation of the design and performance of structures, systems, and components (SSCs) with the objective of assessing the risk to public health and safety resulting from operation of the facility and including determination of the margins of safety during normal operations and transient conditions anticipated during the life of the facility, and the adequacy of SSCs provided for the prevention of accidents and the mitigation of the consequences of accidents. The applicant shall perform analysis and evaluation of ECCS cooling performance and the need for high-point vents following postulated LOCA in accordance with the requirements in 10 CFR 50.46, "Acceptance Criteria for Emergency Core Cooling Systems for Light-Water Nuclear Power Reactors," and 10 CFR 50.46a, "Acceptance Criteria for Reactor Coolant System Venting Systems." In turn, 10 CFR 50.46 sets forth

acceptance criteria for ECCS for light-water nuclear power reactors, and 10 CFR 50.46a sets forth acceptance criteria for reactor coolant system venting systems.

- In accordance with the requirements in 10 CFR 50.55a(h)(3), an application for design certification must meet the requirements for safety systems in IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995.
- In accordance with the requirements in 10 CFR 52.47(a)(16), an application for a design certification must include a coping analysis, and any design features necessary to address station blackout, as required in 10 CFR 50.63, "Loss of All Alternating Current Power." In turn, 10 CFR 50.63(a)(1) requires that each design for a light-water-cooled nuclear power plant approved under a standard design certification must be able to withstand a station blackout for a specified duration and recover from a station blackout, as defined in 10 CFR 50.2. The specified station blackout duration shall be based on the following factors:
 - the redundancy of the onsite emergency ac power sources
 - the reliability of the onsite emergency ac power sources
 - the expected frequency of loss of offsite power
 - the probable time needed to restore offsite power

The requirements in 10 CFR 50.63(a)(2) state that the reactor core and associated coolant, control, and protection systems, including station batteries and any other necessary support systems, must provide sufficient capacity and capability to ensure that the core is cooled and appropriate containment integrity is maintained in the event of a station blackout for the specified duration. The capability for coping with a station blackout of specified duration shall be determined by an appropriate coping analysis. Applicants are expected to have the baseline assumptions, analyses, and related information used in their coping evaluations available for NRC review.

In accordance with the requirements in 10 CFR 52.47(a)(2), an application for standard design certification for nuclear power reactors shall present a safety analysis of the facility design in terms of site parameters postulated for the design. Specifically, 10 CFR 52.47(a)(2)(iv) requires that an analysis of the radiological consequences of postulated accidents include the following:

The safety features that are to be engineered into the facility and those barriers that must be breached as a result of an accident before a release of radioactive material to the environment can occur. Special attention must be directed to plant design features intended to mitigate the radiological consequences of accidents. In performing this assessment, an applicant shall assume a fission product release from the core into the containment assuming that the facility is operated at the ultimate power level contemplated. The applicant shall perform an evaluation and analysis of the postulated fission product release, using the expected demonstrable containment leak rate and any fission product cleanup systems intended to mitigate the consequences of the accidents, together

with applicable postulated site parameters, including site meteorology, to evaluate the offsite radiological consequences. The evaluation must determine that:

(A) An individual located at any point on the boundary of the exclusion area for any 2-hour period following the onset of the postulated fission product release, would not receive a radiation dose in excess of 25 rem total effective dose equivalent (TEDE);

(B) An individual located at any point on the outer boundary of the low population zone, who is exposed to the radioactive cloud resulting from the postulated fission product release (during the entire period of its passage) would not receive a radiation dose in excess of 25 rem TEDE.

Applications for combined licenses (COLs), construction permits, and operating licenses that reference the subject TR have similar requirements to evaluate the radiological consequences of postulated accidents in accordance with 10 CFR 52.79(a)(1)(vi) and 10 CFR 50.34(a)(1). The siting requirements in 10 CFR 100.21, "Non-Seismic Site Criteria," also reference the criteria in 10 CFR 50.34(a)(1).

- In accordance with the requirements in 10 CFR 52.47(a)(2)(iii), as part of its review of an application for a design certification, the Commission will consider the extent to which the reactor incorporates unique, unusual, or enhanced safety features having a significant bearing on the probability or consequences of accidental release of radioactive materials.
- As discussed in 10 CFR Part 50, Appendix E, "Emergency Planning and Preparedness for Production and Utilization Facilities," Section VI, "Emergency Response Data System," the Emergency Response Data System (ERDS) is a direct near real-time electronic data link between the applicant's onsite computer system and the NRC Operations Center that provides for the automated transmission of a limited data set of selected parameters. While it is recognized that ERDS is not a safety system, it is conceivable that an applicant's ERDS interface could communicate with a safety system, and thus would require appropriate isolation devices at these interfaces. Section VI.2.a.(i) of Appendix E requires, for pressurized-water reactors (PWRs), that the selected plant parameters to be transmitted include those from radiation monitoring systems (i.e., reactor coolant radioactivity, containment radiation level, condenser air removal radiation level, effluent radiation monitors, and process radiation monitor levels).
- Regulatory Guide (RG) 1.97, Revision 4, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," issued June 2006, describes a method that the NRC staff considers acceptable for use in complying with the agency's regulations with respect to satisfying criteria for accident monitoring instrumentation in nuclear power plants. Specifically, the method described RG 1.97 relates to GDC 13, 19, and 64. RG 1.97 endorses (with certain clarifying regulatory positions specified in Section C of the RG) IEEE Std. 497-2002, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations."

- NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports: LWR Edition,” Branch Technical Position 7-10, “Guidance on Application of Regulatory Guide 1.97,” Revision 6, issued August 2016, provides additional guidelines for reviewing an applicant’s accident monitoring instrumentation.

SECY-94-084, “Policy and Technical Issues Associated with the Regulatory Treatment of Non-safety Systems in Passive Plant Designs,” dated March 28, 1994 (ADAMS Accession No. ML003708068), presented the Commission with recommended positions pertaining to policy and technical issues affecting passive advanced light-water reactor (ALWR) designs and requested that the Commission approve certain staff positions stated in the SECY, including the Electric Power Research Institute’s proposed alternative to the cold-shutdown condition called for by RG 1.139, “Guidance for Residual Heat Removal,” as a safe, stable condition that the passive decay heat removal systems must be capable of achieving and maintaining following non-LOCA events. This recommendation was predicated on an acceptable passive safety system performance and an acceptable resolution of the issue of regulatory treatment of nonsafety systems. In its staff requirements memorandum (SRM) on SECY-94-084, “Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems,” and COMSECY-94-024, “Implementation of Design Certification and Light-Water Reactor Design Issues,” dated June 30, 1994, the Commission, among other things, approved the staff’s recommendation on this item. In doing so, the Commission stated that, with respect to the 72-hour capacity of the passive residual heat removal system water pool, the requirements for replenishing the water in the pool should be based on design-specific attributes, and the applicant’s justification of these requirements should not be based solely on the 72-hour criterion of the utility requirement document. Further, the Commission stated that the staff should be receptive to arguments for longer periods if technically justified. On May 22, 1995, the staff issued SECY-95-132, “Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems (RTNSS) in Passive Plant Designs” (ADAMS Accession No. ML003708005), in response to SRM-SECY-94-084 and presented a corresponding revision of SECY-94-084 for Commission review and approval. On June 28, 1995, the Commission approved the staff’s recommendations in SECY-95-132 (ADAMS Accession No. ML003708019).

3.0 Staff Evaluation

TR Section 1.2, “Scope,” gives the scope of review specific to the safety classification of plant electrical systems for which the conditions of applicability and augmented provisions apply, as follows:

- offsite and onsite ac electrical power systems
- onsite dc electrical power systems.

In the TR, NuScale stated that the above scope does not include instrumentation and control equipment and circuits, which include both Class 1E and non-Class 1E systems, that serve to monitor and control power to and operation of safety-related and nonsafety-related loads.

The TR contains four appendices that describe the methodology and procedures to be applied to an example power system design to ensure that a dc power system design can be “highly reliable”:

- (1) Appendix A, “Example Overview of Electrical Systems and Instrumentation and Control (I&C) Systems Design,” gives an overall description of an onsite power system that could serve a passive plant design that meets the conditions of applicability. In addition, Appendix A includes a set of typical one-line diagrams to facilitate an overall understanding of the concepts as applied to a passive plant electrical system.
- (2) Appendix B, “Example Safety Classification Assessment for Electrical Systems,” describes how a hypothetical complete loss of all electric power (both ac and dc) would affect the various safety functions and explains how the applicant can satisfy the attributes of the conditions of applicability. However, Appendix B does not describe how the requirements of 10 CFR Part 50, Appendix E, Section VI.2.a.(i); 10 CFR 50.34(f)(2)(viii); or 10 CFR 50.34(f)(2)(xvii) would be met.
- (3) Appendix C, “Example Failure Modes and Effects Analysis—Highly Reliable DC Power System,” provides an example failure modes and effects analysis of the example onsite dc power system described in Appendix A. The effects of failure modes and mechanisms for components in the example analysis establish that no single failure exists that could prevent safety-related functions from being achieved and maintained.
- (4) Appendix D, “Example Safety Analysis Results,” provides example safety analysis results of a passive plant that has the design attributes described in Appendices A and B. The analysis shows that, in each postulated design-basis event (DBE) analyzed, none of the systems credited for mitigating the event requires electric power or operator action.

TR Section 1.2 states the following:

The information provided in the appendices is provided to facilitate: (1) the NRC’s review of the conditions of applicability and augmented provisions for which approval is sought; and (2) an understanding of how this topical report would be implemented by future applicants (including NuScale). As part of the scope of this topical report, NuScale is not seeking NRC approval of the information in the appendices. Information is provided in this report to demonstrate applicability of the methodology and to aid the reader’s understanding of the application of these methodologies.

NuScale TR further stated that its design certification application (DCA) will present the final design information and will confirm that the final design meets the conditions of applicability described in TR Table 3-1, which lists the attributes to be satisfied as conditions of applicability.

The TR Table 3-1 has two sections:

- (1) Section I contains the specific conditions that, if fully met, would adequately justify that no Class 1E electrical supply systems (power sources) are required.

(2) Section II contains additional conditions to be applied (after meeting Section I).

TR Table 3-1, Section II, requires augmented design, qualification, and QA provisions. The provisions in Table 3-2 are the minimum requirements to be applied to non-Class 1E electrical systems (termed as “highly reliable DC electrical system(s)”) that will be used to power postaccident monitoring instrumentation for Type B and Type C variables and to power the plant emergency lighting system. If a passive nuclear plant can meet all the conditions listed in Table 3-1 without the need for any electrical power, Class 1E ac or dc power supply systems may not be necessary. This is subject to satisfying the capability [REDACTED]

The NRC staff review of the information in the appendices does not constitute approval of the information in the appendices. Therefore, the NRC staff limited its review to the main body of the TR and focused on the design criteria considered in the conditions of applicability, not an actual design.

Concept of “Highly Reliable” Non-Class 1E Direct Current System

With regard to a fully non-Class 1E dc power system for a completely passive nuclear power plant design, the NRC staff was concerned whether the dc power system would have high reliability. More specifically, the NRC staff was concerned that the valve-regulated, lead-acid (VRLA) battery life could be seriously and suddenly reduced by exposure to prolonged periods of high temperatures, the magnitude and frequency of discharge cycles, or overcharging. The NRC staff devised a three-pronged review approach (i.e., performance, QA, and quantification) to determine the relative reliability of the conceptual dc power system design (presented in TR Appendix A) compared to a Class 1E dc power system.

To date, conventional large light-water nuclear power plants have not used VRLA batteries for onsite power. Therefore, the NRC staff requested information on battery life, QA, performance, qualification, and reliability.

RAI 08.03.02-01

In a letter dated December 5, 2016 (ADAMS Accession No. ML16340D339), NuScale acknowledged the NRC staff’s concerns with VRLA battery life and stated that these effects can be mitigated by following the recommendations in IEEE Std. 1187-2013, “IEEE Recommended Practice for Installation Design and Installation of Valve-Regulated Lead-Acid Batteries for Stationary Applications,” and IEEE Std. 1188-2005 (R2010), “IEEE Recommended Practice for Maintenance, Testing, and Replacement of Valve-Regulated Lead-Acid (VRLA) Batteries for Stationary Applications,” as noted in TR Table 3-2. Additionally, IEEE Std. 1187-2013 refers to IEEE Std. 1491-2012, “IEEE Guide for Selection and Use of Battery Monitoring Equipment in Stationary Applications,” and IEEE Std. 1635-2012, “IEEE/ASHRAE Guide for the Ventilation and Thermal Management of Batteries for Stationary Applications.”

In addition to the use of the industry standard procedures mentioned above for design, testing, and implementation of the VRLA battery-powered dc system, the applicant stated the following:

- The backup power supply system delivers backup power to heating, ventilation, and air conditioning systems serving the battery and associated charger rooms to avoid prolonged periods of high ambient temperature.
- For design consideration for magnitude and frequency of discharge cycle related monitoring, the applicant will follow the guidance in IEEE Std. 1187-2013, IEEE Std. 1188-2005, and specifically IEEE Std. 1491-2012, which provides criteria to detect and monitor a battery for degradation.
- Following the guidance in IEEE Std. 1187-2013, as supplemented by IEEE Std. 1491-2012, provides reasonable assurance that the VRLA batteries will not be overcharged and that instances of potential overcharging will be detected before degrading a battery to a point where it is not able to perform its intended function.

The electrical power system presented in TR Appendix A depicts an onsite power system design with no Class 1E power sources, assuming the reactor design does not require any safety-related electrical loads to support the safety analyses. The NRC staff reviewed the RAI response and determined that the use of VRLA batteries in a nonsafety dc power system design for a passive nuclear power plant, construction and monitoring will follow the guidance in IEEE Std. 1187-2013 and IEEE Std. 1188-2005, as supplemented by IEEE Std. 1491-2012 and IEEE Std. 1635-2012. These IEEE standards provide widely established industry guidance for design, testing, and performance of VRLA batteries.

The NRC staff determined that, based on the IEEE standards mentioned above, the design will give reasonable assurance that a dc power system that uses a VRLA battery will not be exposed to prolonged periods of high temperatures, will be monitored for potential overcharging, and will be monitored for magnitude and frequency of discharge cycles that may degrade the battery performance.

For the reasons discussed above, the NRC staff concludes that, for a nonsafety dc system that uses VRLA batteries, the applicant's response gives reasonable assurance that the dc system will be monitored for degradation and the use of VRLA batteries will not adversely affect the dc system's intended function.

The NRC staff asked the applicant to include its response to RAI 08.03.02-01 in the next revision of the TR. In Revision 1 to the TR, the applicant included the applicable year for the following IEEE standards as requested in the RAI: IEEE Std. 1491-2012 and IEEE Std. 1635-2012. This action satisfies the NRC staff's request.

RAI 08.03.02-02

In TR Table 3-2, NuScale stated that a graded QA program will be applied to the dc electrical system that will meet or exceed the augmented QA guidance in Appendix A, "Quality Assurance Guidance for Non-Safety Systems and Equipment," to RG 1.155, "Station Blackout." The NRC staff asked NuScale to describe the proposed QA program in sufficient detail to enable the NRC staff to verify whether it meets or exceeds the guidance in RG 1.155.

In its December 5, 2016, response to RAI 08.03.02-02, NuScale stated that a COL applicant that references TR-0815-16487 will be required to follow the guidance in RG 1.155, Appendix A. The NRC staff finds NuScale's response reasonable.

The NRC staff has placed Condition 4.1 in Section 4.0 of this safety evaluation to ensure that all future applicants that reference TR-0815-16497 address the guidance in RG 1.155, Appendix A, in sufficient detail to verify whether the relevant QA program would meet or exceed the guidance in RG 1.155.

RAI 08.03.02-03

In TR Table 3-2, under "Batteries," NuScale stated that the VRLA batteries have augmented design, QA, and qualification provisions. The NRC staff asked NuScale to describe the methods and processes that a passive reactor nuclear power plant will use to verify that VRLA batteries will perform their intended functions during normal operation, AOOs, and postulated DBEs.

In its response dated December 5, 2016 (ADAMS Accession No. ML16340D339), NuScale stated that the VRLA batteries used in a passive reactor nuclear power plant design are not credited for use in mitigating the consequences of postulated DBEs. NuScale also stated that an applicant using this TR shall implement a testing and monitoring program, as described in IEEE Std. 1188-2005 and IEEE Std. 1491-2012, to ensure that VRLA batteries will perform their intended functions when called upon. These standards provide for a wide variety of operating parameters to be monitored on a continuous basis, including cell-specific parameters.

Furthermore, NuScale stated that applicants would be required to environmentally qualify their VRLA batteries in accordance with IEEE Std. 323-1974, as appropriate, and IEEE Std. 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," and to seismically qualify their batteries in accordance with IEEE Std. 344-2004, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations," as appropriate, to give further assurance that the batteries will perform their intended functions.

The NRC staff also asked NuScale to identify the industry standards or applicable references that will be used for verification purposes. NuScale identified the following industry standards:

- IEEE Std. 323-1974, as endorsed by RG 1.89, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants," for harsh environments
- IEEE Std. 323-2003 for mild environments
- IEEE Std. 344-2004, as endorsed by RG 1.100, "Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants"
- IEEE Std. 1188-2005
- IEEE Std. 1491-2012

The NRC staff reviewed the applicant's response to RAI 08.03.02-03 and determined that the design of the VRLA batteries used as a non-Class 1E dc power source in a passive reactor nuclear power plant design, in accordance with the widely accepted industry practices IEEE Std. 1188-2005 and IEEE Std. 1491-2012 for testing and monitoring; IEEE Std. 323-1974, as appropriate, and IEEE Std. 323-2003, as appropriate, for environmental qualification; and IEEE Std. 344-2004 for seismic qualification provide reasonable assurance that the VRLA batteries will perform their intended functions.

The NRC staff concludes that NuScale's response is acceptable with regard to the methods and processes used to verify that the VRLA batteries will perform as intended.

The TR states that the VRLA batteries will be seismic Category 1; therefore, an applicant using the TR shall provide a qualification testing plan that includes an environmental and seismic qualification, and also a technical functional requirement for the VRLA batteries to provide reasonable assurance that VRLA batteries will perform their intended functions. For this reason, the NRC staff has established Condition 4.2 on the TR for the applicant to confirm that the VRLA batteries and their structures are seismic Category 1. To give reasonable assurance that the VRLA batteries will perform as intended, the applicant that references the TR must provide a COL action item to support that the VRLA batteries and their structures are seismic Category 1.

RAI 08.03.02-04

In the TR, NuScale described its dc power system as "highly reliable" and substantially equal in reliability to that of an analogous Class 1E dc power system. However, the TR did not fully justify these statements. Therefore, to complete its review, the NRC staff asked the applicant to provide additional quantitative information. Specifically, the NRC staff asked the applicant to describe the methodology that it will use to compare the highly reliable dc system that it will describe in its DCA to a Class 1E dc power system to show that the highly reliable dc system is substantially equal in reliability to a typical Class 1E dc power system.

NuScale provided a two-part response. The first part describes the methodology in the TR that design certification applicants would use to perform a quantitative analysis. This methodology comprises the following five steps needed to compare the reliability of the highly reliable dc system to that of a typical Class 1E dc power system:

- (1) [REDACTED]
- (2) [REDACTED]
- (3) [REDACTED]
- (4) [REDACTED]

(5)

The second part of NuScale's response gave the results of its comparative analysis using the above methodology. NuScale indicated that its results were favorable in that the augmented non-Class 1E design indicated a reliability greater than that of the Class 1E design. In its response, NuScale further concluded that amending the TR to include the methodology presented is not necessary.

NuScale and the NRC staff held a conference call on January 6, 2017, to address the RAIs. First, the staff asked for clarification on whether NuScale's referenced probabilistic risk analysis (PRA) model included common-cause failures among each of the two-battery-in-parallel configurations. NuScale stated that the model included common-cause failure of the two-battery configurations. The concern was that any battery operating in parallel could experience certain common-cause events. Any further questions on PRA methodology would be part of the PRA review of the referencing DCA or COL application.

Second, the NRC staff requested clarification about the statement at the end of the response that the response does not require a revision to the licensing document (i.e., TR-0815-16497). The NRC staff questioned this statement because TR-0815-16497 is a methodology document and the response to RAI 08.03.02-04 provides additional methodology necessary for use of the TR by any applicant referencing it. NuScale added this methodology to Table 3-1, Section II, of Revision 1 to the TR. This action satisfies the NRC staff's request.

Based on the review of this response, the NRC staff concludes that the five-step process outlined in the applicant's response provides an acceptable approach for demonstrating the relative reliability of a non-Class 1E system with that of an analogous Class 1E system.

3.1 Postaccident Monitoring

The primary purpose of postaccident monitoring instrumentation is to display plant variables that provide information required by the control room operator during and after an accident.

GDC 13, GDC 19, GDC 64, 10 CFR 50.34(f)(2)(xix), 10 CFR 50.34(f)(2)(xx), and 10 CFR 50.55a(h) contain regulatory requirements governing postaccident monitoring instrumentation. The NRC provides the primary guidance for implementing these regulatory requirements in RG 1.97, which describes a method acceptable to the NRC staff for complying with the Commission's regulations to provide instrumentation for monitoring plant variables and systems during and after an accident. RG 1.97, which endorses IEEE Std. 497-2002, with certain clarifying regulatory positions specified in Section C of RG 1.97, specifies that a Class 1E electrical system should be provided to supply the instrumentation that monitors Type A, B, and C variables under postaccident conditions. Under 10 CFR 50.34(f)(2)(xx), the NRC requires that electric power for pressurizer level indicators must be powered by vital buses.

RG 1.97 defines Type A, B, and C variables as follows:

- Type A variables provide the primary information required to allow main control room operators to take manual actions for which no automatic control is provided.
- Type B variables provide primary information to the control room operators to assess the plant safety functions.
- Type C variables provide primary information to the control room operators to indicate the potential for breach or the actual breach of fission product barriers (e.g., fuel cladding, RCPB, and containment pressure boundary).

During its review, the NRC staff considered whether the safety system design to provide accident monitoring instrumentation would require instrumentation to be powered by a Class 1E electrical system for Type B and C variables.

IEEE Std. 603-1991, Clause 5.8.1, "Displays for Manually Controlled Actions," specifies that monitoring instrumentation be part of the safety systems and meet the requirements of IEEE Std. 497-2002. For monitoring instrumentation used for these operations, IEEE Std. 603-1991 and IEEE Std. 497-2002 specify a Class 1E electrical power supply.

The NRC staff's evaluation considered the following:

- Regulatory requirements in GDC 13, 19, and 64 are applicable to postulated DBEs and do not specify a Class 1E electrical power supply. Therefore, a Class 1E electrical power supply is not required to meet GDC 13, 19, and 64.
- In accordance with the requirements in 10 CFR 52.47(a)(8), an application for a design certification must include the information necessary to demonstrate compliance with any technically relevant portions of the Three Mile Island requirements as stated in 10 CFR 50.34(f), except for 10 CFR 50.34(f)(1)(xii), (f)(2)(ix), and (f)(3)(v). The requirements in 10 CFR 50.34(f)(2)(xix) call for the design to provide instrumentation adequate for monitoring plant conditions following an accident that includes core damage. This includes core damage that may be more extensive than a postulated DBE. Finally, 10 CFR 50.34(f)(2)(xix) does not specify the quality of the electrical supply; therefore, a Class 1E electrical power supply is not required to meet 10 CFR 50.34(f)(2)(xix).
- In accordance with the requirements in 10 CFR 50.34(f)(2)(xx), which are applicable to PWRs only, the design must provide power supplies for pressurizer relief valves, block valves, and level indicators such that (1) level indicators are powered from vital buses, (2) motive and control power connections to the emergency power sources are through devices qualified in accordance with requirements applicable to systems important to safety, and (3) electric power is provided from emergency power sources. On its face,

NUREG- 0737, "Clarification of TMI Action Requirements," issued November 1980, states that the instrument channels for pressurizer level indication instrument channels shall be powered from the vital instrument buses and does not specify a Class 1E electrical power supply requirement; therefore, a Class 1E electrical power supply is not required to meet 10 CFR 50.34(f)(2)(xix).

- Clause 5.8.2 of IEEE Std. 603-1991 states, in part, that the display instrumentation provided for safety-system status indication need not be part of the safety systems; therefore, a Class 1E electrical power supply is not required to meet Clause 5.8.2 of IEEE Std. 603-1991.

Type B and Type C accident monitoring instrumentation is required to perform its intended function under postulated accident conditions. As such, the reliability of the electrical power supply for these instruments should be substantially similar to that of a Class 1E electrical system (see Section 3.0 of this safety evaluation).

In TR Section 3.2.1, the applicant provided an alternative to RG 1.97 that uses a highly reliable dc power system in lieu of a Class 1E electrical system to supply electrical power to the postaccident monitoring instrumentation. When performing this review, the NRC staff considered the electrical system reliability of the highly reliable dc electrical system. The NRC staff established a three-pronged approach to establish whether the highly reliable dc electrical system provides a substantially equal reliability to that of a Class 1E design. The three-pronged approach consisted of (1) evaluation of the augmented design, qualification, and QA provisions, (2) consideration of the rigor of the highly reliable dc power system as demonstrated by the failure modes and effect analysis, and (3) quantification via fault tree analysis to compare the NuScale design with an approved passive PWR dc system design. Section 3.0 of this safety evaluation evaluates the electrical system reliability of the highly reliable dc power system. Based on its evaluation of the electrical system reliability, the staff concluded that the highly reliable dc electrical system provides a substantially equal reliability to that of a Class 1E design; thus, the dc electrical system provides additional assurance that postaccident monitoring capability is maintained during and following a DBE.

Based on the NRC staff's review of the TR and the regulatory requirements governing accident monitoring instrumentation, the staff found that the augmented design, qualification, and QA provisions of the power sources for Type B and Type C variables represent an acceptable alternative to the guidance in RG 1.97. [REDACTED]

[REDACTED], the staff has established Condition 4.3 (see Section 4.0 of this safety evaluation) for the applicants referencing this safety evaluation to confirm that operator actions are not necessary to ensure safety-related functions for any postulated DBE (i.e., the design does not include Type A variables as defined in IEEE Std. 497-2002, as modified in RG 1.97, Regulatory Position C.4).

Spent Fuel Pool Considerations

The spent fuel pool (SFP) has the safety function of maintaining the spent fuel assemblies in a safe and subcritical array during all credible storage conditions. GDC 63 for spent fuel storage facilities requires monitoring systems to (1) detect conditions that may cause the loss of residual

heat removal capability and excessive radiation levels and (2) indicate when to take action to initiate appropriate safety actions.

In TR Appendix B, Section B.2.2, “Fuel Assembly Cooling—Spent Fuel and Module Core Refueling,” the applicant described [REDACTED]

In TR Table 3-1, Conditions of Applicability 3 and 4 specify that for the TR to be applicable to a design, the applicant must demonstrate the following:

- [REDACTED]
- [REDACTED]

The NRC staff determined that Conditions of Applicability 3 and 4, as stated above, are consistent with the staff guidance in NUREG-0800, Section 19.3, “Regulatory Treatment of Non-Safety Systems (RTNSS) for Passive Advanced Light Water Reactors,” and, therefore, if a design met these conditions, Class 1E power would not be required for monitoring SFP conditions.

3.2 Safe Shutdown, Core Cooling, and Reactor Coolant Pressure Boundary Integrity

The NRC staff used the review guidance in the NUREG-0800 to identify the Commission’s regulations associated with safe shutdown, core cooling, and RCPB integrity. In accordance with 10 CFR 52.47(a)(3)(i), the staff identified, as minimum requirements, GDC 10, 15, 20, 26, 27, and 34 and 10 CFR 50.46 as associated with safety-related SSCs (in accordance with the definition in 10 CFR 50.2) that need to be addressed by the conditions of applicability in TR Table 3-1.

Condition of Applicability I.1.a, [REDACTED] and Condition of Applicability I.1.c., [REDACTED] require, in part, [REDACTED]

[REDACTED] The NRC staff finds these requirements to be consistent with GDC 20. Accordingly, the NRC staff finds that Conditions of Applicability I.1.a and I.1.c are necessary and sufficient for determining that no Class 1E power is required to satisfy GDC 20.

Condition of Applicability I.1.b states, [REDACTED]

██████████ The NRC staff describes safe-shutdown requirements in SECY-94-084. In SRM-SECY-94-084, the Commission approved the staff's recommendation on safe-shutdown requirements. SECY-94-084 clarifies the conditions that constitute a safe-shutdown condition as reactor subcriticality, decay heat removal, and radioactive material containment. Additionally, SECY-94-084 states that an appropriate safety analysis can be used to demonstrate passive system capabilities to bring the plant to a safe, stable condition and to maintain this condition. The staff's views on safe shutdown were not changed in SRM-SECY-95-132 (updating the Commission on matters in SECY-94-084).

TR Appendices B and D provide clarifying examples to illustrate how the conditions of applicability can be demonstrated. The examples did not include a quantitative safety analysis to demonstrate the ability to insert sufficient negative reactivity during and following a DBE to achieve and maintain safe shutdown. This omission caused the NRC staff to question the interpretation of safe shutdown as applied to Condition of Applicability I.1.b. Accordingly, the NRC staff issued RAI 08.03.02-05, dated October 7, 2016 (ADAMS Accession No. ML16281A298), asking the applicant to (1) specify the criteria that constitute a safe shutdown as applied to Condition of Applicability I.1.b, and (2) describe how a future applicant for a passive plant will demonstrate that electric power is not necessary to achieve and maintain a safe shutdown for a minimum of 72 hours.

In its December 5, 2016, response (ADAMS Accession No. ML16340D339), NuScale stated that the criteria that constitute a safe shutdown are subcriticality and decay heat removal in order to maintain fuel clad integrity (radioactive material containment). The NRC staff finds this response acceptable because it is more restrictive than the criteria in SECY-94-084.

The applicant's response to RAI 08.03.02-05 further discussed the following approach to demonstrating Condition of Applicability I.1.b:

...an applicant will evaluate the reactivity control systems to ensure sufficient shutdown function capability and evaluate the decay heat removal system to ensure sufficient heat removal capability. To ensure that safe shutdown capability is sufficient to address the safety issue of heat removal reliability, a probabilistic risk assessment is used to ensure that the reliability of systems used to achieve and maintain safe shutdown supports conformance to the commission's safety goal guidelines.

The applicant further explained that safety analyses of DBEs (as typically presented in Chapter 15 of a final safety analysis report (FSAR)) may not be suitable for demonstrating the ability to achieve and maintain a safe shutdown following a DBE. Specifically, the applicant's response stated the following:

Conservative assumptions are applied to Chapter 15 safety analysis of DBEs appropriate for the intended purpose of ensuring appropriate margins to protect fuel integrity and core coolability. Although these safety analyses can be used to demonstrate adequate shutdown capability per SECY-94-084, application of the same conservative assumptions may lead to excessive margin with respect to shutdown capability.

The NRC staff previously communicated positions on shutdown margin during and following DBEs in letters discussing GDC 26 and 27, dated December 5, 2016 (ADAMS Accession No. ML16292A589), and September 8, 2016 (ADAMS Accession No. ML16116A083), respectively. These letters clarify that shutting down the reactor and maintaining a subcritical reactor are safety functions considered in GDC 26 and 27, both of which require margin for malfunctions such as stuck rods. In the letter addressing GDC 27, the NRC staff stated the following:

Criterion 27 requires that the reactor be reliably controlled and that the reactor achieve and maintain a safe, stable condition, including subcriticality beyond the short term, using only safety related equipment following a postulated accident with margin for stuck rods.

Based on the shutdown margin requirements of GDC 26 and 27, the NRC staff established Condition 4.5 to require a demonstration or appropriate justification of shutdown margin. Based on the applicant's criteria for safe shutdown and pursuant to Condition 4.5, the NRC staff finds that Condition of Applicability I.1.b is necessary and sufficient for determining that no Class 1E power is required to satisfy GDC 26 and 27.

Condition of Applicability I.1.c, [REDACTED] is a high-level requirement associated with core cooling. GDC 10, 34, and 35 and 10 CFR 50.46 are design requirements associated with safety-related SSCs that perform core cooling functions. In accordance with the requirements in 10 CFR 50.34, "Contents of Applications; Technical Information"; 10 CFR 52.47, "Contents of Applications; Technical Information"; and 10 CFR 52.79, "Contents of Applications; Technical Information in Final Safety Analysis Report," applicants are required to provide a description and analysis of the safety-related SSCs credited to perform core cooling functions, with emphasis upon performance requirements. The information provided by an applicant under these regulations must be sufficient to demonstrate compliance with GDC 10, 34, and 35 and 10 CFR 50.46. Additionally, an applicant referencing the TR is required to perform these evaluations to show that safety functions will be accomplished in the absence of electrical power to demonstrate compliance with Condition of Applicability I.1.c. Accordingly, the NRC staff finds that Condition of Applicability I.1.c is necessary and sufficient for determining that Class 1E power is not required to satisfy GDC 10, 34, and 35 and 10 CFR 50.46.

Condition of Applicability I.1.g states, [REDACTED]
[REDACTED] This statement supports Condition of Applicability I.1, which states, [REDACTED]
[REDACTED]

[REDACTED] TR Appendices B and D provide clarifying examples to illustrate how the conditions of applicability can be demonstrated. The example safety analysis in Appendix D shows that the example passive plant response to an AOO includes establishing a direct coolant flowpath between the reactor core and the containment, thereby removing a fission product barrier. This caused the NRC staff to question whether Condition of Applicability I.1.g is sufficient for demonstrating RCPB integrity. Accordingly, the NRC staff issued RAI 08.03.02-06, dated October 7, 2016 (ADAMS Accession No. ML16281A298), asking the applicant to (1) specify the criteria that constitute RCPB integrity as applied to Condition of Applicability I.1, and (2) explain why the removal of a fission product barrier during an AOO is not considered an event escalation.

In its December 5, 2016, response (ADAMS Accession No. ML16340D339), NuScale stated that a loss of RCPB integrity involves a mechanical failure in an RCPB component, but it does not include the opening of a valve. The applicant further stated that considering the RCPB to be lost when a valve opens is problematic because (1) it would preclude advanced designs that offer improvements in safety by relying on valves to depressurize the reactor coolant system for safe shutdown, (2) it is not consistent with the licensing basis for PWRs and boiling-water reactors (BWRs), as these designs rely on safety relief valves for overpressure protection, and (3) the GDC address maintaining structural integrity of RCPB components rather than preventing the opening of valves to allow fluid to pass into or out of the RCPB.

Additionally, the applicant stated that opening a valve to depressurize the reactor coolant system and establish long-term cooling is not considered a removal of a fission product barrier, and thus not event escalation, because the functions of the reactor coolant system barrier are not lost. The applicant further stated that events that do not result in unacceptable consequences or significantly increase the risk for radiological release do not challenge the intent of the nonescalation criterion specified in NUREG-0800, Section 15.0, "Introduction—Transient and Accident Analyses."

The NRC staff's evaluation of the applicant's response considered the examples from operating PWRs and BWRs. The applicant's response included examples in which valves connected to the reactor coolant system opened and allowed fluid to pass through the RCPB and included the opening of safety relief valves, shutdown cooling, and the reactor core isolation cooling system in BWRs. The NRC staff finds these examples to differ from the scenario that was the basis for RAI 08.03.02-06. In particular, the staff identifies that a rapid discharge of reactor coolant directly to the containment atmosphere, in response to an AOO, can result in significant pressurization of the containment, which is required to retain coolant and establish a return path to the reactor pressure vessel. The AOO scenario in TR Appendix D appears to rely on the containment to retain the reactor coolant necessary to ensure fuel cladding integrity during an AOO. Because an AOO, by definition, is expected to occur one or more times during the life of the nuclear power plant, the NRC staff is concerned that such reliance upon the containment may not be consistent with the underlying defense-in-depth purpose of GDC 15, which expects the RCPB to remain available as a fission product barrier during AOOs. Accordingly, the NRC staff established Condition 4.4 on the TR to address reliability requirements for the systems necessary to retain reactor coolant within the RCPB. Condition 4.4 requires a probabilistic determination of the expected frequency of ECCS actuation during AOO mitigation (e.g., dc power system failure that causes ECCS actuation, ECCS pilot valve failure, spurious ECCS actuation). Opening of the ECCS valves during normal, planned plant operations, including recovery from an AOO, is acceptable once a safe, stable state has been established. Based on the overpressure protection of the RCPB and pursuant to Condition 4.4, the NRC finds that Condition of Applicability I.1.g is necessary and sufficient for determining that Class 1E power is not required to satisfy GDC 15.

3.3 Containment Isolation

TR Condition of Applicability I.1.d specifies that for [REDACTED] The provisions in GDC 54, 55, 56, and 57 in part require containment isolation capabilities. Based on consideration of the relevant GDC above, the staff determined that a plant design that is able to

satisfy Condition I.1.d should be able to meet the minimum design requirements in GDC 54, 55, 56, and 57. The NRC staff finds that the condition is necessary to enable the staff to determine that Class 1E electrical power is not required to achieve the containment isolation function.

3.4 Containment Integrity

TR Condition of Applicability I.1.e specifies that for [REDACTED]

[REDACTED] The provisions in GDC 16, 38, 41, and 50 in part require that the containment safety function can be achieved and maintained during DBEs. The provisions in 10 CFR 50.44 address the control of combustible gases in the containment. Based on consideration of the relevant GDC and 10 CFR 50.44, the staff determined that a plant design that is able to satisfy Condition of Applicability I.1.e should be able to meet the minimum design requirements in GDC 16, 38, 41, and 50 and 10 CFR 50.44. The staff finds that the condition is necessary to enable the staff to determine that Class 1E electrical power is not required to assure that containment integrity is achieved and maintained.

3.5 Fission Product Control

TR Condition of Applicability I.1.f specifies that for [REDACTED]

[REDACTED] The provisions in GDC 41 in part require systems to control fission products. Based on consideration of the relevant GDC and applicable guideline exposure requirements, the staff determined that a plant design that is able to satisfy Condition of Applicability I.1.f should be able to meet the minimum design requirements in GDC 41 and applicable guideline exposure requirements. The staff finds that the condition is necessary to enable the staff to determine that Class 1E electrical power is not required to satisfy GDC 41 and the applicable guideline exposures in 10 CFR 100.21, 10 CFR 50.34(a)(1)(ii)(D), and 10 CFR 52.47(a)(2)(iv).

3.6 Control Room Habitability

TR Condition of Applicability I.5 specifies that electrical power is not necessary [REDACTED]

[REDACTED] The provisions in GDC 19 in part require that a control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including LOCAs. Based on consideration of the relevant GDC, the staff determined that a plant design that is able to satisfy Condition of Applicability I.5 should be able to meet the minimum design requirements in GDC 19. The staff finds that the condition is necessary to enable the staff to determine that Class 1E electrical power is not required to satisfy GDC 19.

3.7 Cooling for Building Areas Containing Safety-Related Equipment

TR Condition of Applicability I.6 specifies that [REDACTED]

[REDACTED] The provisions in 10 CFR 50.63 in part require that the reactor core and associated coolant, control, and protection systems, including station batteries and any other necessary support systems, must provide sufficient capacity and capability to ensure that the core is cooled and appropriate containment integrity is maintained in the event of a station blackout for the specified duration. Based on consideration of the 10 CFR 50.63 requirement, the staff determined that a plant design that is able to satisfy Condition of Applicability I.5 should be able to meet the requirements in 10 CFR 50.63. The staff finds that the condition is necessary to enable the staff to determine that Class 1E electrical power is not required to satisfy 10 CFR 50.63.

3.8 Building Ventilation

TR Condition of Applicability I.7 specifies that [REDACTED]

[REDACTED] The provisions in GDC 61 in part require that fuel storage and handling, radioactive waste, and other systems that may contain radioactivity shall be designed to assure adequate safety under normal and postulated accident conditions. Based on consideration of the relevant GDC and the applicable guideline exposure requirements, the staff determined that a plant design that is able to satisfy Condition of Applicability I.7 should be able to meet the minimum design requirements in GDC 61 and applicable guideline exposure requirements. The NRC staff finds that the condition is necessary to enable the staff to determine that Class 1E electrical power is not required to satisfy GDC 61 and the applicable guideline exposures in 10 CFR 100.21, 10 CFR 50.34(a)(1)(ii)(D), and 10 CFR 52.47(a)(2)(iv).

3.9 Emergency Lighting

TR Section 3.2.2, "Emergency Lighting," states that the highly reliable dc electrical system provides power to portions of the emergency lighting system, and that the emergency lighting system is classified as non-Class 1E. Additionally, TR Condition of Applicability II.3 (Section II of Table 3-1) specifies that the applicant's emergency lighting capability [REDACTED]

[REDACTED] The NRC staff finds that TR Condition of Applicability II.3 is consistent with the NRC staff's guidance on the classification of the emergency lighting system as non-Class 1E and, therefore, is acceptable.

4.0 Limitations and Conditions

In its letter dated July 26, 2017 (ADAMS Accession No. ML17205A380), the Advisory Committee on Reactor Safeguards indicated that TR-0815-16497-P, Revision 1, is acceptable for use only as a reference document for the NuScale plant electrical systems design subject to the staff limitations and conditions. The staff responded to the committee on September 11, 2017 (ADAMS Accession No. ML17221A058), agreeing with its recommendation. Therefore, the NRC staff's conclusions on this TR are limited to the NuScale passive nuclear plant design.

If NuScale chooses to incorporate by reference TR-0815-16497 as part of its application, it must demonstrate that the reactor design meets all the conditions of applicability in Table 3-1 and all the augmented design, qualification, and QA provisions in Table 3-2.

Additionally, any applicant referencing this TR must take the following actions:

- 4.1 Address the guidance in RG 1.155, Appendix A, in sufficient detail to enable the NRC staff to verify that the relevant QA program would meet or exceed the guidance in RG 1.155.
- 4.2 Confirm that the VRLA batteries and their structures are seismic Category 1. To provide reasonable assurance that the VRLA batteries will perform as intended, an applicant that references the TR shall provide a COL action item to support that the VRLA batteries and their structures are seismic Category 1. A qualification testing plan includes environmental and seismic qualification and a technical functional requirement for VRLA batteries to show they can perform as intended.
- 4.3 Demonstrate that operator actions are not necessary to ensure the performance of safety-related functions for any postulated DBE (i.e., the design does not include Type A variables as defined in IEEE Std. 497-2002, as modified in RG 1.97, Regulatory Position C.4), as presented in Chapter 15 of its FSAR and the human factors analysis in Chapter 18 of its FSAR.
- 4.4 Evaluate the frequency for which a combination of an AOO and an actuation of the NuScale ECCS is realistically expected to occur, and show that such a combination of events is not expected to occur during the lifetime of the module.
- 4.5 Demonstrate that the reactor can be brought to a safe shutdown using only safety-related equipment in the absence of electrical power following a DBE, with margin for stuck rods. Alternatively, an applicant addressing this condition may provide justification, for NRC review, for a less restrictive approach.

5.0 Conclusions

The NRC staff approves the use of NuScale TR-0815-16497 as a reference document only to the NuScale passive nuclear plant design, subject to the conditions and limitations specified in Section 4.0 of this safety evaluation report. Specifically, based on its review of TR-0815-16497, the NRC staff finds that if the NuScale reactor design can meet the conditions of applicability and the augmented design, qualification, and QA provisions, Class 1E power sources would not be necessary. This approval of the concepts discussed in the TR does not constitute approval of any specific design.

Any applicant referencing this TR in support of a design other than the NuScale passive nuclear plant design must submit information, for NRC staff review, that justifies the applicability of this TR, or a variation of it, to the respective design.

Section B

Licensing Topical Report

Safety Classification of Passive Nuclear Power Plant Electrical Systems

January 2018

Revision 1

Docket: PROJ0769

NuScale Power, LLC

1100 NE Circle Blvd., Suite 200

Corvallis, Oregon 97330

www.nuscalepower.com

© Copyright 2018 by NuScale Power, LLC

Licensing Topical Report

PROPRIETARY INFORMATION NOTICE

This document contains information proprietary to NuScale Power, LLC. A nonproprietary version of this report has also been prepared and provided to the U.S. Nuclear Regulatory Commission (NRC) for release to the public. To conform to the requirements of the Commission's regulations (10 CFR 2.390) concerning the protection of proprietary information submitted to the NRC, the proprietary information in the proprietary version of this document is contained within double braces; where the proprietary information has been deleted in the nonproprietary versions, only the braces remain (to indicate that the information contained within the braces in the proprietary versions has been deleted). Pursuant to 10 CFR 2.390(b)(1), justification for claiming the information being so designated as proprietary is indicated in both versions by means of a superscripted entry containing either (2)(a), (2)(b), (2)(c), (2)(d), or (2)(e), or a combination thereof, located immediately following the closed braces of each set. These superscripted entries refer to paragraphs (2)(a) through (2)(e) of the affidavit accompanying this transmittal. These paragraphs provide the bases for proposing that the information be withheld from public disclosure.

COPYRIGHT NOTICE

This document bears a NuScale Power, LLC, copyright notice. No right to disclose, use, or copy any of the information in this document, other than by the U.S. Nuclear Regulatory Commission (NRC), is authorized without the express, written permission of NuScale Power, LLC.

The NRC is permitted to make the number of copies of the information contained in these reports needed for its internal use in connection with generic and plant-specific reviews and approvals, as well as the issuance, denial, amendment, transfer, renewal, modification, suspension, revocation, or violation of a license, permit, order, or regulation subject to the requirements of 10 CFR 2.390 regarding restrictions on public disclosure to the extent such information has been identified as proprietary by NuScale Power, LLC, copyright protection notwithstanding. Regarding nonproprietary versions of these reports, the NRC is permitted to make the number of additional copies necessary to provide copies for public viewing in appropriate docket files in public document rooms in Washington, DC, and elsewhere as may be required by NRC regulations. Copies made by the NRC must include this copyright notice in all instances and the proprietary notice if the original was identified as proprietary.

Licensing Topical Report

Department of Energy Acknowledgement and Disclaimer

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

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Licensing Topical Report**List of Affected Pages**

Revision Number	Page	Explanation
1	2, 4, 8, 11, 16, 38, 68, 89, 96	Update of NuScale Project Status and clarification of methodology use.
1	3, 5, 6, 13, 19, 21, 23, 43, 84, 87,	RAI No. 8 Question 08.03.02-04 Response
1	22	Spent Fuel Pool Makeup clarification regarding operator action
1	26, 36	RAI No. 8 Question 08.03.02-01 Response

Licensing Topical Report

CONTENTS

1.0	Introduction	7
1.1	Purpose	7
1.2	Scope	7
1.3	Abbreviations.....	8
2.0	Background	11
2.1	Regulatory Requirements and Guidance	11
3.0	Conditions of Applicability	13
3.1	Methodology Used to Develop Conditions of Applicability.....	14
3.2	Supporting Bases for Conditions of Applicability	16
3.2.1	Post-Accident Monitoring	17
3.2.2	Emergency Lighting.....	20
3.3	Implementation/Use	21
4.0	References	30
5.0	Appendices	37
Appendix A.	Example Overview of Electrical Systems and Instrumentation and Control (I&C) Systems Design	38
Appendix B.	Example Safety Classification Assessment for Electrical Systems	68
Appendix C.	Example Failure Modes and Effects Analysis – Highly Reliable DC Power System	89
Appendix D.	Example Safety Analysis Results	96

TABLES

Table 1-1.	Abbreviations.....	8
Table 3-1.	Conditions of applicability	22
Table 3-2.	Augmented design, qualification, and quality assurance provisions	24
Table A-1.	ELVS power supply connections to EDNS	49
Table A-2.	ELVS power supply connections to EDSS-C.....	51
Table B-1.	Example overview of plant response to simultaneous loss of all electrical power.....	88
Table C-1.	Example failure modes and effects analysis for highly reliable DC power system (EDSS) – sample summary results	90

Licensing Topical Report

FIGURES

Figure A-1.	High voltage electrical system and connections to onsite AC power system (Sheet 1 of 2).....	52
Figure A-2.	Onsite AC power system – medium voltage electrical system (Sheet 1 of 2)	54
Figure A-3.	Onsite AC power system – low voltage electrical system (Sheet 1 of 3).....	56
Figure A-4.	Onsite AC power system – BDG portion of backup power supply system	59
Figure A-5.	Highly reliable DC power system–common (EDSS-C).....	60
Figure A-6.	Highly reliable DC power system–module-specific (EDSS-MS) (Sheet 1 of 2) ...	61
Figure A-7.	Legend and general notes for Figures A-1 through A-6.....	63
Figure A-8.	Overall I&C system architecture	64
Figure A-9.	Data display and associated electrical power sources	65
Figure A-10.	Power supply power monitors – EDSS-MS	66
Figure A-11.	Power supply power monitors – EDSS-C	67
Figure D-1.	Loss of DC electrical power event diagram – common to all design basis events	122
Figure D-2.	Decrease in feedwater temperature event diagram	123
Figure D-3.	Increase in feedwater flow event diagram	124
Figure D-4.	Increase in steam flow event diagram	125
Figure D-5.	Steam line break inside containment event diagram.....	126
Figure D-6.	Steam line break outside containment event diagram.....	127
Figure D-7.	Loss of containment vacuum event diagram.....	128
Figure D-8.	Loss of external load event diagram	129
Figure D-9.	Turbine trip event diagram.....	130
Figure D-10.	Loss of condenser vacuum event diagram.....	131
Figure D-11.	Inadvertent closure of an MSIV event diagram	132
Figure D-12.	Inadvertent closure of the turbine throttle valve event diagram.....	133
Figure D-13.	Loss of AC power event diagram.....	134
Figure D-14.	Loss of normal feedwater flow event diagram	135
Figure D-15.	Inadvertent actuation of DHRS event diagram	136
Figure D-16.	Feedwater line break inside containment event diagram	137
Figure D-17.	Feedwater line break outside containment event diagram	138
Figure D-18.	PZR heater malfunction event diagram	139
Figure D-19.	PZR level control malfunction (PZR spray available) event diagram	140
Figure D-20.	PZR level control malfunction (PZR spray not available) event diagram	141
Figure D-21.	PZR spray control malfunction event diagram.....	142
Figure D-22.	Uncontrolled control rod bank withdrawal in low power or subcritical conditions event diagram	143
Figure D-23.	Uncontrolled control rod bank withdrawal at power event diagram	144
Figure D-24.	Single control rod withdrawal event diagram.....	145
Figure D-25.	Control rod drop event diagram.....	146
Figure D-26.	Inadvertent cold water addition to the RCS event diagram	147
Figure D-27.	Inadvertent boron dilution event diagram	148
Figure D-28.	Control rod ejection event diagram.....	149
Figure D-29.	Spurious RSV, RVV, or RRV event diagram.....	150
Figure D-30.	Small line break outside containment event diagram	151
Figure D-31.	Steam generator tube failure event diagram	152
Figure D-32.	Loss of coolant accident event diagram	153

Licensing Topical Report

Figure D-33.	LOFW event sequence diagram.....	154
Figure D-34.	RPV pressure for LOFW (30 minutes).....	154
Figure D-35.	RPV pressure for LOFW (24 hours)	155
Figure D-36.	RPV pressure for LOFW (72 hours)	155
Figure D-37.	DHRS flowrate for LOFW (24 hours).....	156
Figure D-38.	CNV pressure for LOFW (24 hours).....	156
Figure D-39.	Inadvertent RRV opening event sequence diagram.....	157
Figure D-40.	Peak cladding temperature for inadvertent RRV opening event	157
Figure D-41.	RPV liquid level for inadvertent RRV opening event	158
Figure D-42.	RPV pressure for inadvertent RRV opening event	158
Figure D-43.	CNV pressure for inadvertent RRV opening event.....	159

Abstract

The purpose of this topical report is to request Nuclear Regulatory Commission (NRC) review and approval of what are termed herein as “conditions of applicability,” and the methodology and bases used in their development. The conditions of applicability comprise a set of passive reactor plant design and operational attributes that, if met in full by a reactor design or license applicant, justify the applicant’s determination that no plant electrical supply systems fulfill functions that per the regulatory definitions of “safety-related” and “Class 1E” would warrant a Class 1E classification. This topical report also seeks NRC review and approval of augmented design, qualification, and quality assurance (QA) provisions that are an extension of the conditions of applicability. These augmented provisions would be applied as minimum requirements to electrical systems that have been determined to be nonsafety-related but yet are essential to the post-accident monitoring of Type B and Type C variables. Provided the conditions of applicability are fully satisfied, the approved augmented provisions would represent an acceptable alternative to the portion of Regulatory Guide 1.97, Revision 4 (Reference 4.39), that specifies a Class 1E power source for instrumentation associated with Type B and Type C variables. With the successful demonstration that all of the conditions of applicability and augmented provisions are met, an applicant would use this topical report as supporting basis for the acceptability of a non-Class 1E classification of its electrical supply systems.

Executive Summary

NuScale is currently in the application phase of design certification (DC) pursuant to 10 CFR 52, Subpart B (Reference 4.9). 10 CFR 52.47 (Reference 4.10) requires that an application for design certification (DCA) include certain technical information that identifies the design bases and provides reasonable assurance that the design will conform to those design bases. Consistent with NUREG-0800, Sections 3.2.1 and 3.2.2 (References 4.13 and 4.14, respectively), and Regulatory Guide 1.206, Section C.I.3.2 (Reference 4.47), this information includes identifying the appropriate safety (including seismic and quality group) classifications for plant structures, systems, and components (SSCs). Accordingly, as part of its DCA, NuScale has conducted safety classification assessments for plant SSCs, including electrical systems.

Based on the regulatory definitions of “safety-related” and “Class 1E,” it is expected that design and operational attributes of new passive light water reactor designs – including the NuScale power plant design – may support a determination that no Class 1E electrical systems¹ are warranted. The acceptability of this determination and its underlying assumptions and interpretations has substantive implications on the NuScale power plant design and content of the NuScale DCA. Thus, NuScale is seeking Nuclear Regulatory Commission (NRC) review and approval of certain conditions and provisions supporting this determination (summarized below), via the topical report process established in NRC Office of Nuclear Reactor Regulation (NRR) Office Instruction LIC-500 (Reference 4.26).

With consideration for the above, this topical report requests NRC review and approval of what are termed herein as “conditions of applicability,” and the methodology and bases used in their development. The conditions of applicability comprise a set of passive reactor plant design and operational attributes that, if met in full, justify the applicant’s determination that no plant electrical supply systems fulfill functions that would warrant a Class 1E classification. The conditions of applicability are presented in two separate categories indicated as Section I and Section II of Table 3-1. All of the conditions of applicability in Table 3-1 (i.e., both Section I and Section II) must be fully satisfied for an applicant to use this topical report as supporting basis for a determination that its plant electrical systems do not warrant a Class 1E classification.

Section I of Table 3-1 includes reactor plant design and operational attributes that support a determination that plant electrical systems do not fulfill functions that, per the regulatory definitions of “safety-related” and “Class 1E,” justify a Class 1E classification. Section II of Table 3-1 includes additional conditions that apply to an applicant that has successfully demonstrated that the Section I conditions of applicability are fully satisfied. These additional conditions include augmented design, qualification, and quality assurance (QA) provisions that

¹ This conclusion and the scope of this topical report for which NRC approval is sought are specific to the safety classification of reactor plant electrical systems. This scope does not include instrumentation and control (I&C) equipment and circuits, which comprise both Class 1E and non-Class 1E systems that serve to monitor and control power to and operation of safety-related and nonsafety-related loads.

would be prescribed as minimum requirements on electrical systems that, although determined to be nonsafety-related (via fully meeting Table 3-1, Section I), are essential to the post-accident monitoring of Type B and Type C variables.² Table 3-1, Section II conditions also specify a reliability comparison between the highly reliable DC electrical system(s) and typical Class 1E DC electrical system(s). The augmented provisions to be applied to such electrical system(s) – termed the “highly reliable DC electrical system(s)” – are detailed in Table 3-2.

The methodology NuScale used to develop the conditions of applicability in Section I of Table 3-1 is the same as that used historically by the nuclear industry in establishing whether the appropriate safety classification of an electrical system is Class 1E or non-Class 1E. The foundation of this methodology is the 10 CFR 50.2 definition of “safety-related” and the associated definition of “Class 1E” in NRC-endorsed industry standards. As safety-related and Class 1E are functional terms, the assessment of an electrical system for appropriate safety classification focuses on determining whether electrical power is necessary to fulfill any of the functions included in the definitions of “safety-related” and “Class 1E.”

Thus, the safety classification assessment involves first identifying those safety functions contemplated within these regulatory definitions, and then a methodical “function-by-function” evaluation of the role electrical power plays in the fulfillment of each function. If electrical power provided by one or more electrical systems is necessary to achieve and maintain the function (i.e., is an auxiliary supporting feature), then the electrical system(s) or portions thereof that are essential to the performance of the function would be appropriately classified as Class 1E. Conversely, if electrical power is not necessary to achieve and maintain the function, then the electrical power would not need to be provided from a Class 1E electrical supply.

The methodology used to develop the additional conditions in Section II of Table 3-1 and the augmented design, qualification, and QA provisions of Table 3-2 also is not new. Specifically, the application of augmented provisions is consistent with the process established in the NRC regulatory framework for “special treatment” of nonsafety-related SSCs that are determined to have risk-significance. This well-established framework includes previous Commission policy (SECY-94-084 and SECY-95-132 and their associated Staff Requirements Memorandums [References 4.24 and 4.25]) as implemented further in NUREG-0800, Section 19.3, “Regulatory Treatment of Nonsafety Systems for Passive Advanced Light Water Reactors” (Reference 4.20). Regulatory Guide 1.155 (Reference 4.45), which implements the station blackout (SBO) rule (10 CFR 50.63 [Reference 4.6]) requirements, also specifies the use of augmented design, qualification, and QA provisions for nonsafety-related SSCs that due to their role in station blackout (SBO) coping warrant special treatment. The application of the augmented provisions described in Table 3-2 via Section II of Table 3-1 (Item II.1) is consistent with the approach of these regulatory policy and guidance documents.

² IEEE Std. 497-2002 does not specify a Class 1E electrical power supply for instrumentation used to monitor variables other than those identified as Type A, Type B, and Type C. {{

}}^{2(a),(c)}

To illustrate how the conditions of applicability would be used by future applicants, an example safety classification assessment is included in Appendix B. This assessment provides an example of how the Table 3-1 conditions of applicability would be demonstrated. The other appendices to this topical report provide example plant design and safety analysis information that supports the Appendix B example assessment. The information provided in the appendices is provided to facilitate: (1) the NRC's review of the conditions of applicability and augmented provisions for which approval is sought; and (2) an understanding of how this topical report would be implemented by future applicants (including NuScale). NuScale is not seeking NRC approval of the information in the appendices. Information is provided in this report to demonstrate applicability of the methodology and to aid the reader's understanding of the application of these methodologies.

As illustrated in the example safety classification assessment provided in Appendix B, the Table 3-1, Section I, conditions of applicability may be satisfied largely by demonstrating that plant safety-related functions are achieved and maintained for a minimum duration with no reliance on electrical power (whether AC or DC). This concept is not new. For example, it is not uncommon for the control rod drive mechanism coils (even for existing and evolutionary light water reactor designs) to be powered from a non-Class 1E electrical power source. This is justified by the fact that upon a loss of the electrical supply to the coils, the safety-related reactor trip function of the control rods – i.e., control rod insertion – is achieved via gravity and/or stored energy. For advanced passive plant designs such as the NuScale power plant, this non-reliance on electrical power is a common attribute not only for the reactor trip safety function, but for other plant safety-related functions.

{{

}}^{2(a),(c)}

{{

}}^{2(a),(c)}

³ Electrical system(s) that supply power to monitoring instrumentation are typically DC electrical systems; thus, the augmented provisions presented in Table 3-2 are directed towards DC electrical systems.

This determination does not rely on other plant-specific electrical system design features that may be applied – beyond those specified in IEEE Std. 308-2001 and listed in Table 3-2 – and that would further enhance DC electrical system reliability. For instance, the example highly reliable DC power system design described in Appendix A, Section A.1.2, does not include inverters; rather, the system provides DC electrical power directly to loads without inverting the power to AC. According to operational experience data (Reference 4.28), the elimination of inverters in the design results in approximately a factor of 10 increase in system reliability as compared to a comparable DC electrical system that includes inverters. The use of plant-specific design features such as this in an electrical system design would further enhance the already “Class 1E-like” reliability of an electrical system that meets the augmented provisions described in Table 3-2. Based on the above, the augmented design, qualification, and QA provisions represent an acceptable alternative to the provision in Regulatory Guide 1.97, Revision 4 (Reference 4.39), specifying a Class 1E power source for instrumentation associated with Type B and Type C variables.

As described in detail in Section 3.2.2, a conclusion similar to that reached for the post-accident monitoring function also is justified for the emergency lighting function. That is, for a passive plant design that fully meets Table 3-1, Section I, emergency lighting does not serve the role in ensuring adequate illumination for operator safe shutdown actions to the extent it does for existing reactor designs. However, an important distinction is that unlike certain post-accident monitoring, the emergency lighting function is not normally considered to fall within the scope of functions contemplated in the IEEE standard definitions of Class 1E. This is reflected in that the emergency lighting fixtures, controllers, dimmers, etc., for existing reactor designs typically are not Class 1E, and that NRC requirements and guidance do not prescribe a Class 1E power source for emergency lighting.⁴

{{

}}^{2(a),(c)}

⁴ As discussed further in Section 3.2.2, the design of nuclear plant emergency lighting systems are typically not Class 1E, although some existing designs may elect to power the emergency lighting systems from a Class 1E power source to improve reliability.

1.0 Introduction

1.1 Purpose

The purpose of this topical report is to request Nuclear Regulatory Commission (NRC) review and approval of what are termed herein as “conditions of applicability,” and the methodology and bases used in their development. The conditions of applicability comprise a set of passive reactor plant design and operational attributes that, if met in full by a reactor design or license applicant, justify the applicant’s determination that none of the plant electrical systems fulfill functions that, per the regulatory definitions of “safety-related” and “Class 1E,” would warrant a Class 1E classification. The conditions of applicability are presented in Table 3-1.

This topical report also seeks NRC review and approval of augmented design, qualification, and quality assurance (QA) provisions that are an extension of the conditions of applicability (via Item II.1 of Table 3-1). The augmented provisions are described in Table 3-2. For reasons detailed in Section 3.2, these augmented design, qualification, and QA provisions would be applied as minimum requirements to electrical systems that have been determined to be nonsafety-related but yet are essential to the post-accident monitoring of Type B and Type C variables. Provided the conditions of applicability are fully satisfied, the approved augmented provisions would represent an acceptable alternative to the portion of Regulatory Guide 1.97, Revision 4 (Reference 4.39), that specifies a Class 1E power source for instrumentation associated with Type B and Type C variables.

1.2 Scope

The conditions of applicability and augmented provisions for which NRC review and approval are sought via this topical report are specific to the safety classification of reactor plant electrical systems, as follows:

- Offsite and onsite alternating current (AC) electrical power systems
- Onsite direct current (DC) electrical power systems

This scope does not include instrumentation and control (I&C) equipment and circuits, which include both Class 1E and non-Class 1E systems that serve to monitor and control power to and operation of safety-related and nonsafety-related loads.

This topical report includes four appendices, as follows:

- Appendix A – Example Overview of Electrical Systems and Instrumentation and Control (I&C) Systems Design
- Appendix B – Example Safety Classification Assessment for Electrical Systems
- Appendix C – Example Failure Modes and Effects Analysis – Highly Reliable DC Power System
- Appendix D – Example Safety Analysis Results

Appendix A provides an overview of an example small modular reactor advanced passive plant electrical system and I&C system design. Appendix B contains an example safety classification assessment that illustrates how the conditions of applicability could be met by a future passive plant applicant. Appendix C and Appendix D provide example details of plant design and safety analysis information that support the example descriptions in Appendix A and Appendix B.

The information provided in the appendices is provided to facilitate: (1) the NRC's review of the conditions of applicability and augmented provisions for which approval is sought; and (2) an understanding of how this topical report would be implemented by future applicants (including NuScale). As part of the scope of this topical report, NuScale is not seeking NRC approval of the information in the appendices. Information is provided in this report to demonstrate applicability of the methodology and to aid the reader's understanding of the application of these methodologies.

1.3 Abbreviations

Table 1-1. Abbreviations

Term	Definition
AAPS	auxiliary AC power source
AC	alternating current
ADAMS	Agencywide Documents Access and Management System
ASME	American Society of Mechanical Engineers
BAS	boron addition system
BDG	backup diesel generator
BPSS	backup power supply system
B&PV	boiler and pressure vessel
BTP	branch technical position
CRB	control building
CCF	common-cause failure
CES	containment evacuation system
CFDS	containment flood and drain system
CFR	Code of Federal Regulations
CIV	containment isolation valve
COL	combined license application
CNV	containment vessel
CRDM	control rod drive mechanism
CRE	control room envelope
CRHS	control room habitability system
CRVS	control room ventilation system
CVCS	chemical and volume control system
DC	direct current
DC	design certification
DCA	design certification application
DCD	design control document
DHRS	decay heat removal system

Term	Definition
DRAP	design reliability assurance program
DSRS	design-specific review standard
EDNS	normal DC power system
EDSS	highly reliable DC power system
EDSS-C	EDSS – Common
EDSS-MS	EDSS – Module-Specific
ECCS	emergency core cooling system
EHVS	high voltage electrical system
ELAP	extended loss of AC power
ELVS	low voltage electrical system
EMVS	medium voltage electrical system
EPRI	Electric Power Research Institute
EQ	environmental qualification
ESF	engineered safety features
ESFAS	engineered safety features actuation system
FERC	Federal Energy Regulatory Commission
FMEA	failure modes and effects analysis
FSAR	final safety analysis report
FWIV	feedwater isolation valve
FWLB	feedwater line break
FWS	condensate and feedwater system
GDC	general design criterion
GQA	graded quality assurance
HEPA	high efficiency particulate air
HFE	human factors engineering
HVAC	heating, ventilation, and air conditioning
I&C	instrumentation and control
IEEE	Institute of Electrical and Electronics Engineers
LOCA	loss of coolant accident
LOFW	loss of normal feedwater
LTOP	low-temperature overpressure protection
MCC	motor control center
MCR	main control room
MCS	module control system
MPS	module protection system
MPT	main power transformer
MSIV	main steam isolation valve
MSS	main steam system
NMS	neutron monitoring system
NERC	North American Electric Reliability Corporation
NRC	Nuclear Regulatory Commission
NRR	Nuclear Reactor Regulation, Office of
NUREG	NRC technical report designation (<u>N</u> uclear <u>R</u> egulatory Commission)
NuScale	NuScale Power LLC
PAM	post-accident monitoring

Term	Definition
PCS	plant control system
PDC	power distribution center
PPS	plant protection system
PRA	probabilistic risk assessment
PSPM	power supply power monitor
QA	quality assurance
QAPD	quality assurance program description
RXB	reactor building
RBVS	reactor building ventilation system
RCCWS	reactor component cooling water system
RCPB	reactor coolant pressure boundary
RCS	reactor coolant system
RG	regulatory guide
RPV	reactor pressure vessel
RRV	reactor recirculation valve
RSV	reactor safety valve
RTNSS	regulatory treatment of nonsafety systems
RTS	reactor trip system
RVV	reactor vent valve
RWB	radioactive waste (radwaste) building
SAFDLs	specified acceptable fuel design limits
SBO	station blackout
SC-I	seismic category I
SC-II	seismic category II
SC-III	seismic category III (i.e., non-seismic)
SCR	silicon-controlled rectifier
SDIS	safety display and indication system
SECY	Secretary of the Commission, Office of the
SFP	spent fuel pool
SPAR	standardized plant analysis risk
SRM	staff requirements memorandum/memoranda
SRP	standard review plan
SSCs	structures, systems, and components
SSE	safe shutdown earthquake
SST	station service transformer
Std.	standard
TGB	turbine generator building
UAT	unit auxiliary transformer
UHS	ultimate heat sink
V	volts
Vdc	volts direct current
VLA	vented lead acid
VRLA	valve-regulated lead acid
VRT	voltage regulating transformer
XSW	transfer switch

2.0 Background

NuScale is currently in the application phase of design certification (DC) pursuant to 10 CFR 52, Subpart B (Reference 4.9). 10 CFR 52.47 (Reference 4.10) requires that an application for design certification (DCA) include certain technical information that identifies safety design bases and demonstrates that those bases are assured. Consistent with NUREG-0800, Sections 3.2.1 and 3.2.2 (References 4.13 and 4.14, respectively), and Regulatory Guide 1.206, Section C.I.3.2 (Reference 4.47), this information includes identifying the appropriate safety (including seismic and quality group) classifications for plant SSCs. Accordingly, as part of its DCA, NuScale has conducted safety classification assessments for plant SSCs, including electrical systems.

Based on the regulatory definitions of “safety-related” and “Class 1E,” it is expected that design and operational attributes of some new passive light water reactor designs – including the NuScale power plant design – may support a determination that no Class 1E electrical systems are warranted. The acceptability of this determination and its underlying assumptions and interpretations has substantial implications on the NuScale power plant design and content of the NuScale DCA. Thus, NuScale is seeking NRC review and approval of those matters detailed in Section 3 in advance of the NuScale DCA, via the topical report process established in NRC Office of Nuclear Reactor Regulation (NRR) Office Instruction LIC-500 (Reference 4.26).

2.1 Regulatory Requirements and Guidance

As described in Section 3, the methodology used to develop the conditions of applicability (described in Table 3-1) is consistent with that used historically within the nuclear industry to determine the appropriate classification of structures, systems, and components (SSCs). This methodology and the NuScale electrical system safety classification efforts that will use the results in Section 3 conform to applicable regulatory requirements, including but not limited to 10 CFR 50.55a (Reference 4.5); 10 CFR 50, Appendix A; and 10 CFR 50, Appendix B (Reference 4.8). The safety classification conclusions ensure the appropriate application of: (1) regulatory requirements intended to ensure the performance of important-to-safety SSCs; and (2) regulatory guidance and industry codes and standards implementing those requirements.

The methodology used to develop Table 3-1 and Table 3-2 is consistent with the guidance provided in IEEE Standard (Std.) 603-1991 (Reference 4.69) as endorsed by Regulatory Guide 1.153 (Reference 4.44) and codified in 10 CFR 50.55a, and with IEEE Std. 308-2001 (Reference 4.53) as endorsed by Regulatory Guide 1.32 (Reference 4.31). The foundation of this process is the definition of safety-related provided in 10 CFR 50.2. Footnote 3 of 10 CFR 50.49 (Reference 4.4) states that safety-related electrical equipment is referred to as “Class 1E” in IEEE 323-1974 (Reference 4.54). This and more recent NRC-endorsed industry standards provide a definition of Class 1E that (as would be expected) is consistent with the 10 CFR 50.2 definition of safety-related.

These and other standards describe design criteria for Class 1E power systems that provide clarification when determining whether a system or component should be classified as Class 1E. In addition, Regulatory Guide 1.29 (Reference 4.30) provides additional guidance related to seismic classification that is related to safety classification. The methodology and bases used in the development of the Table 3-1 conditions of applicability and Table 3-2 augmented provisions conforms to the above-described requirements and codes and standards.

Regulatory requirements governing reactor plant monitoring instrumentation are contained in GDCs 13, 19, and 64, and 10 CFR 50.34(f)(2)(xix) (Reference 4.2). The primary NRC guidance that implements these regulatory requirements is contained in Regulatory Guide 1.97. Revision 4 of Regulatory Guide 1.97 (Reference 4.39) provides guidance specific to new reactor applicants/licensees, and endorses IEEE Std. 497-2002 (Reference 4.67) subject to clarifications and modifications specified in the guide's regulatory positions. This guidance represents an acceptable method for providing post-accident monitoring instrumentation to satisfy GDCs 13, 19, and 64, and 10 CFR 50.34(f)(2)(xix). Branch Technical Position (BTP) 7-10 (Reference 4.16) provides additional guidance clarifying acceptable means of applying Regulatory Guide 1.97.

3.0 Conditions of Applicability

NuScale has performed an assessment to identify what is termed herein as “conditions of applicability,” which justify an applicant’s determination that the appropriate classification of plant electrical systems is non-Class 1E per the regulatory definitions of “safety-related” and “Class 1E.”⁵ The conditions of applicability are presented in Table 3-1, and comprise two categories segregated as Section I and Section II of Table 3-1. All of the conditions of applicability in Table 3-1 (i.e., both Section I and Section II) must be fully satisfied for an applicant to use this topical report as supporting basis for its electrical system safety classification assessments.

Section I of Table 3-1 includes reactor plant design and operational attributes that, if met in full by a reactor design or license applicant, justify the applicant’s determination that plant electrical systems do not fulfill functions that per the regulatory definitions of “safety-related” and “Class 1E” would warrant a Class 1E classification. Section II of Table 3-1 includes additional conditions of applicability that apply to an applicant that has successfully demonstrated that the Section I conditions of applicability are fully satisfied. These additional conditions include augmented design, qualification, and quality assurance (QA) provisions that would be prescribed as minimum requirements on electrical systems that, although determined to be nonsafety-related, are essential to the post-accident monitoring of Type B and Type C variables.⁶ Table 3-1, Section II conditions also specify a reliability comparison between the highly reliable DC electrical system(s) and typical Class 1E DC electrical system(s). The augmented provisions to be applied to such electrical system(s) – termed the “highly reliable DC electrical system(s)” – are detailed in Table 3-2.

⁵ Regulatory definitions” refers to the 10 CFR 50.2 definition of “safety-related,” and the definition of “Class 1E” inferred by Footnote 3 of 10 CFR 50.49 (Reference 4.4) and detailed in a number of NRC-endorsed industry standards. These standards include IEEE Std. 603-1991 (Reference 4.69) as endorsed by Regulatory Guide 1.153 (Reference 4.44) and codified in 10 CFR 50.55a; IEEE Std. 308-2001 (Reference 4.53) as endorsed by Regulatory Guide 1.32 (Reference 4.31); and IEEE Std. 323-1974 (Reference 4.54) as endorsed by Regulatory Guide 1.89 (Reference 4.38).

⁶ IEEE Std. 497-2002 does not specify a Class 1E electrical power supply for instrumentation used to monitor variables other than those identified as Type A, Type B, and Type C. {{

}}^{2(a),(c)}

3.1 Methodology Used to Develop Conditions of Applicability

The methodology used to develop the Table 3-1, Section I, conditions of applicability is consistent with that used historically within the nuclear industry to determine the appropriate classification of structures, systems, and components (SSCs). The foundation of this methodology is the 10 CFR 50.2 definition of “safety-related” and the associated definition of “Class 1E” in NRC-endorsed industry standards (see Footnote 5). These definitions are centered on ensuring that plant safety-related functions – including safe shutdown, core cooling, and containment and reactor coolant pressure boundary (RCPB) integrity – are achieved and maintained during design basis events, including postulated accidents.

As safety-related and Class 1E are functional terms, the assessment of an electrical system for appropriate safety classification focuses on determining whether electrical power is necessary to fulfill any of the functions included in the definitions of “safety-related” and “Class 1E.” Thus, the safety classification assessment involves first identifying those safety functions contemplated within these regulatory definitions, and then a methodical “function-by-function” evaluation of the role electrical power plays in the fulfillment of each function. If electrical power provided by one or more electrical systems is necessary to achieve and maintain the function (i.e., is an auxiliary supporting feature), then the electrical system(s) or portions thereof that are essential to the performance of the function would be appropriately classified as Class 1E. Conversely, if electrical power is not necessary to achieve and maintain the function, then the electrical power would not need to be provided from a Class 1E electrical supply.

Existing and evolutionary light water reactors rely on active safety-related systems that require electrical power for the performance of safety-related functions. Enough similarity exists amongst the various existing and evolutionary reactor designs that the safety classification of each plant’s electrical systems has been substantially similar and relatively consistent over the years. For example, the prevailing expectation has been that at least a portion of a plant’s main AC electrical supply system, as well as its emergency diesel generators and backup (emergency) DC electrical system, would be vital to the performance of safety-related active systems and thus would be classified as Class 1E. Specific to nuclear plant AC power systems, this expectation changed with the advent of passive light water reactor designs, as reflected in SECY-94-084 and its associated staff requirements memorandum (Reference 4.24).

Specifically, in Section F of SECY-94-084, the Staff addressed the concern that the Electric Power Research Institute (EPRI) and passive plant designers had not made the same provisions for certain AC power system features found in existing or evolutionary advanced reactor plant designs. One of these passive plant design features included the use of non-Class 1E (rather than Class 1E) AC electrical systems. The Staff recommended the acceptability of nonsafety-related AC power system features for passive plants, provided these features are evaluated for risk-significance and RTNSS consideration. In a Staff Requirements Memorandum (SRM) dated June 30, 1994, the Commission approved the Staff’s recommendation.

The AP1000 passive design, as approved and certified in 10 CFR 52, Appendix D (Reference 4.11), reflects this approach. Specifically, the NRC approved the classification of the AP1000 onsite AC electrical system (including standby AC electrical generators) as non-Class 1E based on its not being necessary for the performance of safety-related functions. The Staff concluded that:

The AP1000 design as presented does not require Class 1E alternating current (ac) electrical power, except that provided by the Class 1E direct current (dc) batteries and their inverters, to accomplish the plant's safety-related functions. --NUREG-1793, Section 8.1 (Reference 4.23)

With further advancements in passive design methods, it is expected that new passive light water reactor design applicants – including NuScale – may reach this same conclusion not only for the main and backup AC power systems, but also for other electrical systems (such as the backup DC electrical system) that traditionally have been Class 1E systems. The Table 3-1 conditions of applicability are intended to facilitate such applicants by encompassing those plant design and operational attributes that if met would confirm a reactor design's complete non-reliance on electrical power (whether AC or DC) or operator action to achieve and maintain safety-related functions for any design basis event.

As described in Section 3.0 above, Section I of Table 3-1 includes reactor plant design and operational attributes that, if met in full, justify a determination that plant electrical systems do not require a Class 1E classification. The methodology used to identify these conditions of applicability is the same as that described above that has been and continues to be used by the nuclear industry in establishing whether the appropriate safety classification of an electrical system is Class 1E or non-Class 1E. The methodology used to develop the additional conditions in Section II of Table 3-1 and the augmented design, qualification, and QA provisions of Table 3-2 also is not new.

Specifically, the application of augmented provisions is consistent with the process established in the NRC regulatory framework for “special treatment” of nonsafety-related SSCs that are determined to have risk-significance. This well-established framework includes previous Commission policy (SECY-94-084 and SECY-95-132 and their associated Staff Requirements Memorandums [References 4.24 and 4.25]) as implemented further in NUREG-0800, Section 19.3, “Regulatory Treatment of Nonsafety Systems for Passive Advanced Light Water Reactors” (Reference 4.20). Regulatory Guide 1.155 (Reference 4.45), which implements the station blackout (SBO) rule (10 CFR 50.63 [Reference 4.6]) requirements, also specifies the use of augmented design, qualification, and QA provisions for nonsafety-related SSCs that due to their role in station blackout (SBO) coping warrant special treatment. The application of the augmented provisions described in Table 3-2 via Section II of Table 3-1 (Item II.1) is consistent with these regulatory policy and guidance documents.

To illustrate how the conditions of applicability would be used, an example safety classification assessment is included in Appendix B to this topical report. The Appendix B assessment provides an example of how the Table 3-1 conditions of applicability would be demonstrated. The other appendices to this report provide example design and safety analysis information that support the Appendix B example

assessment. The information provided in the appendices is provided to facilitate: (1) the NRC's review of the conditions of applicability and augmented provisions for which approval is sought; and (2) an understanding of how this topical report would be implemented by future applicants (including NuScale). NuScale is not seeking NRC approval of the information in the appendices. Information is provided in this report to demonstrate applicability of the methodology and to aid the reader's understanding of the application of these methodologies.

3.2 Supporting Bases for Conditions of Applicability

As illustrated in the example safety classification assessment provided in Appendix B, the Table 3-1, Section I, conditions of applicability may be satisfied largely by demonstrating that plant safety-related functions are achieved and maintained for a minimum 72-hour duration with no reliance on electrical power (whether AC or DC) or operator action. The minimum 72-hour duration is consistent with that addressed in SECY-94-084 and established in Revision 13 of the EPRI Utility Requirements Document (URD) for passive light water reactors as the minimum duration that passive systems should be able to perform their safety functions, independent of AC electrical power, operator action, or offsite support, after an initiating event. With an advanced passive plant design's complete non-reliance on electrical power (whether AC or DC) or operator action for design basis events, it is expected that the ability to maintain safety-related functions without any electrical power or operator actions would in many instances far exceed the 72-hour minimum duration specified in Table 3-1 (e.g., see example safety classification assessment in Appendix B). However, the use of the 72-hour minimum duration in Table 3-1 is appropriate given its consistency with the previously established minimum duration for passive plants as described above.

This concept – where an SSC having a safety-related function is shown to have no reliance on electrical power and thus the SSC is powered from a non-Class 1E source – is not new. For example, it is not uncommon for the control rod drive mechanism coils (even for existing and evolutionary light water reactor designs) to be electrically powered from a non-Class 1E electrical power source. This is justified by the fact that upon a loss of the electrical supply to the coils, the safety-related reactor trip function of the control rods – i.e., control rod insertion – is achieved via gravity and/or stored energy. For advanced passive plant designs such as the NuScale power plant, this non-reliance on electrical power (whether AC or DC) is a common attribute not only for the reactor trip safety function, but for other plant safety-related functions.

{

}}^{2(a),(c)}

3.2.1 Post-Accident Monitoring

Regulatory Guide 1.97, Revision 4, endorses IEEE Std. 497-2002 as an acceptable method of providing instrumentation to monitor variables for accident conditions, subject to clarifications and modifications specified in the guide's regulatory positions. IEEE Std. 497-2002 states that a Class 1E electrical system shall be provided to supply instrumentation that monitors Types A, B, and C variables. This guidance was developed with consideration for existing and evolutionary light water reactor designs in which operator actions that depend on post-accident monitoring data are essential to ensuring safety-related function performance.

Specifically, existing and evolutionary light water reactor designs rely on active components (e.g., pumps) and may rely on operator actions during and following design basis events to ensure that safe shutdown conditions are achieved and maintained. For these designs, electrical power is an auxiliary supporting feature as defined in IEEE Std. 603-1991, i.e., it is required for safety systems to accomplish their safety functions. These designs often have monitoring instrumentation associated with Type A variables, i.e., variables providing the primary information required to allow main control room (MCR) operators to take manual actions for which no automatic control is provided.

In addition, instrumentation associated with Type B and Type C variables may be necessary to respond to long-term failures of active components that are automatically actuated and used to maintain safe shutdown conditions for the duration of the event. For example, a long-term failure of the electrical supply to an active engineered safety feature (ESF) component such as an emergency core cooling system [ECCS] pump during a design basis event would require action(s) by plant operators to ensure that the safety-related function of the component is restored/maintained. Any credited operator actions would be driven by MCR safety system display readings indicating that a safety system failure occurred.

{{

}}^{2(a),(c)}

Unlike a traditional reactor plant design, these passive designs would not rely on pumps and other active components that require electrical power to achieve and maintain safety functions in response to design basis events. Once actuated via stored energy or other passive means, safety-related systems rely solely on natural passive mechanisms based on fundamental physical and thermodynamic principles – e.g., gravity; natural circulation; convective, radiative, and conductive heat transfer; condensation; and evaporation. Following system actuation, these passive mechanisms ensure that safe shutdown, core cooling, containment isolation and integrity, and RCPB integrity are maintained passively with no reliance on electrical power for the minimum duration specified in Table 3-1, Section I.

{{

}}^{2(a),(c)}

{{

}}^{2(a),(c)} The sample safety classification assessment contained in Appendix B of this topical report, Section B.2.7, describes for illustration purposes how this conclusion would be justified.

{{

}}^{2(a),(c)}

⁷ Electrical system(s) that supply power to monitoring instrumentation are typically DC electrical systems; thus, the augmented provisions presented in Table 3-2 are directed towards DC electrical systems.

3.2.2 Emergency Lighting

Reactor plant emergency lighting is used to provide acceptable levels of illumination throughout the plant upon loss of normal lighting. The NRC guidance relevant to new reactor plant lighting systems, including emergency lighting, includes Standard Review Plan (SRP) (or Design-Specific Review Standard [DSRS], as applicable) Section 9.5.3 (References 4.17 and 4.21); Regulatory Guide 1.189 (Reference 4.46); and NUREG-0700 (Reference 4.27). The objective of this guidance, as noted in Reference 4.17, Acceptance Criterion II.3, is that adequate emergency lighting capability be provided as necessary to support fire suppression actions and safe-shutdown operations during any plant operating condition.

SRP Section 9.5.3, Regulatory Guide 1.189, and NUREG-0700 do not prescribe that emergency lighting be provided with Class 1E power. Rather, the guidance specifies various measures that demonstrate acceptable emergency lighting capability. These measures include design, performance, and operability provisions; maintenance and testing; failure analyses; and comparison to equipment and lighting systems provided on previously approved plants.

Traditional reactor designs typically provide certain portions of the emergency lighting system (e.g., MCR lighting) with electrical power from a Class 1E source. This is appropriate, since at these reactor plants electrical power is an auxiliary supporting feature as defined in IEEE Std. 603-1991, such that one or more Class 1E electrical systems must be provided to ensure that safety-related systems will accomplish their safety functions. With a Class 1E electrical supply required and installed to serve safety-related SSCs, this Class 1E supply also is available for use as a reliable source of electrical power to the emergency lighting system.

As described in Section 3.2.1, existing and evolutionary light water reactor designs typically rely on operator actions to achieve and/or maintain safe shutdown conditions during and following design basis events. Thus, emergency lighting can serve an important role in ensuring that adequate illumination is provided for these operator actions. Such actions – including control and maintenance/repairs of active equipment – would require adequate illumination in the equipment areas, and the access routes to and from these areas.

Even with consideration for the role emergency lighting plays in a traditional reactor design to support operator actions for safe shutdown and fire fighting, the emergency lighting function typically is not considered to fall within the scope of functions contemplated in the IEEE standard definitions of Class 1E. This is reflected in that the emergency lighting fixtures, controllers, dimmers, etc., even for a traditional reactor design typically are not classified as Class 1E. Rather, acceptable emergency lighting capability is demonstrated by implementing the aforementioned measures specified in SRP Section 9.5.3; Regulatory Guide 1.189; and NUREG-0700, combined with providing a Class 1E electrical power source to select portions (e.g., MCR) of the emergency lighting system. In addition, although the lighting fixtures, controllers, and cable are not Class 1E, they commonly are mounted such that there is reasonable assurance that they will remain functional following a safe shutdown earthquake.

As explained in detail in Section 3.2.1, for a passive plant design that fully satisfies the conditions of applicability in Table 3-1, Section I, plant operator actions are not necessary to achieve and maintain safe shutdown conditions during and following a postulated design basis event. Thus, for these designs, emergency lighting does not serve the role in ensuring adequate illumination for operator actions to the extent it does for existing and evolutionary light water reactor designs. The sample safety classification assessment contained in Appendix B of this topical report, Section B.2.6, describes for illustration purposes how the conclusions reached above would be justified.

{{

}}^{2(a),(c)}

3.3 Implementation/Use

An applicant that uses this topical report as a basis for demonstrating that Class 1E electrical systems are not required would perform an assessment that demonstrates that the conditions of applicability described in Table 3-1 are fully satisfied. As part of demonstrating that the conditions of applicability are satisfied, the applicant would be required to impose as minimum requirements the augmented provisions of Table 3-2 on those electrical systems specified in Table 3-1, Section II and perform the reliability comparison specified by condition of applicability Item II.2. With the successful demonstration that all of the conditions of applicability in Table 3-1 are met, an applicant would use this topical report as supporting basis for the acceptability of a non-Class 1E classification of its electrical systems.

Condition No.	Attributes to be Satisfied as “Conditions of Applicability”
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	
31	
32	
33	
34	
35	
36	
37	
38	
39	
40	
41	
42	
43	
44	
45	
46	
47	
48	
49	
50	
51	
52	
53	
54	
55	
56	
57	
58	
59	
60	
61	
62	
63	
64	
65	
66	
67	
68	
69	
70	
71	
72	
73	
74	
75	
76	
77	
78	
79	
80	
81	
82	
83	
84	
85	
86	
87	
88	
89	
90	
91	
92	
93	
94	
95	
96	
97	
98	
99	
100	

Condition No.	Attributes to be Satisfied as “Conditions of Applicability”
{ {	
	}} ^{2(a),(c)}

Table 3-2. Augmented design, qualification, and quality assurance provisions

(([REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
			}} ^{2(a),(c)}

{{ [REDACTED] }}	[REDACTED]	[REDACTED]	[REDACTED]
			}}2(a),(c)

{{ [REDACTED]	[REDACTED]		[REDACTED]
			}} ^{2(a),(c)}

(([REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
			}} ^{2(a),(c)}

{} <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
			}} ^{2(a),(c)}

{{ [REDACTED] }}	[REDACTED]	[REDACTED]	[REDACTED]
			}} ^{2(a),(c)}

{{

}}^{2(a),(c)}

4.0 References

- 4.1 *U.S. Code of Federal Regulations*, “Definitions,” Section 50.2, Part 50, Chapter I, Title 10, “Energy” (10 CFR 50.2).
- 4.2 *U.S. Code of Federal Regulations*, “Contents of applications; technical information,” Section 50.34, Part 50, Chapter I, Title 10, “Energy” (10 CFR 50.34).
- 4.3 *U.S. Code of Federal Regulations*, “Combustible gas control for nuclear power reactors,” Section 50.44, Part 50, Chapter I, Title 10, “Energy” (10 CFR 50.44).
- 4.4 *U.S. Code of Federal Regulations*, “Environmental qualification of electric equipment important to safety for nuclear power plants,” Section 50.49, Part 50, Chapter I, Title 10, “Energy” (10 CFR 50.49).
- 4.5 *U.S. Code of Federal Regulations*, “Codes and standards,” Section 50.55a, Part 50, Chapter I, Title 10, “Energy” (10 CFR 50.55a).
- 4.6 *U.S. Code of Federal Regulations*, “Loss of all alternating current power,” Section 50.63, Part 50, Chapter I, Title 10, “Energy” (10 CFR 50.63).
- 4.7 *U.S. Code of Federal Regulations*, “General Design Criteria for Nuclear Power Plants,” Appendix A, Part 50, Chapter I, Title 10, “Energy” (10 CFR 50, Appendix A).
- 4.8 *U.S. Code of Federal Regulations*, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants,” Appendix B, Part 50, Chapter I, Title 10, “Energy” (10 CFR 50, Appendix B).
- 4.9 *U.S. Code of Federal Regulations*, “Standard Design Certifications,” Subpart B, Part 52, Chapter I, Title 10, “Energy” (10 CFR 52, Subpart B).
- 4.10 *U.S. Code of Federal Regulations*, “Contents of applications; technical information,” Section 52.47, Part 52, Chapter I, Title 10, “Energy” (10 CFR 52.47).
- 4.11 *U.S. Code of Federal Regulations*, “Design Certification Rule for the AP1000 Design,” Appendix D, Part 52, Chapter I, Title 10, “Energy” (10 CFR 52, Appendix D).
- 4.12 *U.S. Code of Federal Regulations*, “Determination of exclusion area, low population zone, and population center distance,” Section 100.11, Part 100, Chapter I, Title 10, “Energy” (10 CFR 100.11).
- 4.13 U.S. Nuclear Regulatory Commission, “Standard Review Plan, Seismic Classification,” NUREG-0800, Chapter 3, Section 3.2.1, Revision 2, March 2007.

-
- 4.14 U.S. Nuclear Regulatory Commission, "Standard Review Plan, System Quality Group Classification," NUREG-0800, Chapter 3, Section 3.2.2, Revision 2, March 2007.
 - 4.15 U.S. Nuclear Regulatory Commission, "Standard Review Plan, Environmental Qualification of Mechanical and Electrical Equipment," NUREG-0800, Chapter 3, Section 3.11, Revision 3, March 2007.
 - 4.16 U.S. Nuclear Regulatory Commission, "Standard Review Plan, Guidance on Application of Regulatory Guide 1.97," NUREG-0800, Branch Technical Position 7-10, Revision 5, March 2007.
 - 4.17 U.S. Nuclear Regulatory Commission, "Standard Review Plan, Lighting Systems," NUREG-0800, Chapter 9, Section 9.5.3, Revision 3, March 2007.
 - 4.18 U.S. Nuclear Regulatory Commission, "Standard Review Plan, Initial Plant Test Program – Design Certification and New License Applicants," NUREG-0800, Chapter 14, Section 14.2, Revision 3, March 2007.
 - 4.19 U.S. Nuclear Regulatory Commission, "Standard Review Plan, Reliability Assurance Program," NUREG-0800, Chapter 17, Section 17.4, Revision 1, May 2014.
 - 4.20 U.S. Nuclear Regulatory Commission, "Standard Review Plan, Regulatory Treatment of Nonsafety Systems for Passive Advanced Light Water Reactors," NUREG-0800, Chapter 19, Section 19.3, Revision 0, June 2014.
 - 4.21 U.S. Nuclear Regulatory Commission, "Design Specific Review Standard for NuScale SMR Design, Lighting Systems," Chapter 9, Section 9.5.3, Draft Revision 0 (for comment), June 2015.
 - 4.22 U.S. Nuclear Regulatory Commission, "Design Specific Review Standard for NuScale SMR Design, Initial Plant Test Program – Design Certification and New License Applicants," Chapter 14, Section 14.2, Draft Revision 0 (for comment), June 2015.
 - 4.23 U.S. Nuclear Regulatory Commission, "Final Safety Evaluation Report Related to Certification of the AP1000 Standard Design," Chapter 8, "Electric Power Systems," NUREG-1793 (Initial Report), September 2004.
 - 4.24 U.S. Nuclear Regulatory Commission, "Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems in Passive Plant Designs," SECY-94-084, March 28, 1994, (ADAMS Accession No. ML003708068), Approved in Staff Requirements Memorandum dated June 30, 1994 (ADAMS Accession No. ML003708098).
 - 4.25 U.S. Nuclear Regulatory Commission, "Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems (RTNSS) in Passive Plant Designs," SECY-95-132, May 22, 1995 (ADAMS Accession No. ML003708005),

Approved in Staff Requirements Memorandum dated June 28, 1995 (ADAMS Accession No. ML003708019).

- 4.26 U.S. Nuclear Regulatory Commission, "Processing Requests for Reviews of Topical Reports," NRR Office Instruction LIC-500, Revision 4, December 21, 2009 (ADAMS Accession No. ML091520370).
- 4.27 U.S. Nuclear Regulatory Commission, "Human-System Interface Design Review Guidelines," NUREG-0700, Revision 2, May 2002.
- 4.28 U.S. Nuclear Regulatory Commission, "Summary of SPAR Component Unreliability Data and Results, 2010 Parameter Estimation Update."
<http://nrcoe.inl.gov/resultsdb/publicdocs/AvgPerf/ComponentUR2010.pdf>
- 4.29 U.S. Nuclear Regulatory Commission, "Control of Combustible Gas Concentrations in Containment," Regulatory Guide 1.7, Revision 3, March 2007.
- 4.30 U.S. Nuclear Regulatory Commission, "Seismic Design Classification," Regulatory Guide 1.29, Revision 4, March 2007.
- 4.31 U.S. Nuclear Regulatory Commission, "Criteria for Power Systems for Nuclear Power Plants," Regulatory Guide 1.32, Revision 3, March 2004.
- 4.32 U.S. Nuclear Regulatory Commission, "Preoperational Testing of Redundant On-Site Electric Power Systems to Verify Proper Load Group Assignments," Regulatory Guide 1.41, March 16, 1973.
- 4.33 U.S. Nuclear Regulatory Commission, "Application of the Single-Failure Criterion to Safety Systems," Regulatory Guide 1.53, Revision 2, November 2003.
- 4.34 U.S. Nuclear Regulatory Commission, "Electric Penetration Assemblies in Containment Structures for Nuclear Power Plants," Regulatory Guide 1.63, Revision 3, February 1987.
- 4.35 U.S. Nuclear Regulatory Commission, "Initial Test Programs for Water-Cooled Nuclear Power Plants," Regulatory Guide 1.68, Revision 4, June 2013.
- 4.36 U.S. Nuclear Regulatory Commission, "Criteria for Independence of Electrical Safety Systems," Regulatory Guide 1.75, Revision 3, February 2005.
- 4.37 U.S. Nuclear Regulatory Commission, "Share Emergency and Shutdown Electric Systems for Multi-Unit Nuclear Power Plants," Regulatory Guide 1.81, Revision 1, January 1975.
- 4.38 U.S. Nuclear Regulatory Commission, "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants," Regulatory Guide 1.89, Revision 1, June 1984.

-
- 4.39 U.S. Nuclear Regulatory Commission, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," Regulatory Guide 1.97, Revision 4, June 2006.
 - 4.40 U.S. Nuclear Regulatory Commission, "Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants," Regulatory Guide 1.100, Revision 3, September 2009.
 - 4.41 U.S. Nuclear Regulatory Commission, "Periodic Testing of Electric Power and Protection Systems," Regulatory Guide 1.118, Revision 3, April 1995.
 - 4.42 U.S. Nuclear Regulatory Commission, "Installation Design and Installation of Vented Lead-Acid Storage Batteries for Nuclear Power Plants," Regulatory Guide 1.128, Revision 2, February 2007.
 - 4.43 U.S. Nuclear Regulatory Commission, "Maintenance, Testing, and Replacement of Vented Lead-Acid Storage Batteries for Nuclear Power Plants," Regulatory Guide 1.129, Revision 3, September 2013.
 - 4.44 U.S. Nuclear Regulatory Commission, "Criteria for Safety Systems," Regulatory Guide 1.153, Revision 1, June 1996.
 - 4.45 U.S. Nuclear Regulatory Commission, "Station Blackout," Regulatory Guide 1.155, August 1988.
 - 4.46 U.S. Nuclear Regulatory Commission, "Fire Protection for Nuclear Power Plants," Regulatory Guide 1.189, Revision 2, October 2009.
 - 4.47 U.S. Nuclear Regulatory Commission, "Combined License Applications for Nuclear Power Plants (LWR Edition)," Regulatory Position Part I, "Standard Format and Content of Combined License Applications," Section C.I.3.2, "Classification of Structures, Systems, and Components," Regulatory Guide 1.206, June 2007.
 - 4.48 U.S. Nuclear Regulatory Commission, "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," Regulatory Guide 1.209, March 2007.
 - 4.49 U.S. Nuclear Regulatory Commission, "Qualification of Safety-Related Battery Chargers and Inverters for Nuclear Power Plants," Regulatory Guide 1.210, June 2008.
 - 4.50 U.S. Nuclear Regulatory Commission, "Qualification of Safety-Related Cables and Field Splices for Nuclear Power Plants," Regulatory Guide 1.211, April 2009.
 - 4.51 U.S. Nuclear Regulatory Commission, "Sizing of Large Lead-Acid Storage Batteries," Regulatory Guide 1.212, November 2008.

-
- 4.52 U.S. Nuclear Regulatory Commission, "Qualification of Safety-Related Motor Control Centers for Nuclear Power Plants," Regulatory Guide 1.213, May 2009.
 - 4.53 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations," IEEE Standard 308-2001, Piscataway, NJ.
 - 4.54 Institute of Electrical and Electronics Engineers, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," IEEE Standard 323-1974, Piscataway, NJ.
 - 4.55 Institute of Electrical and Electronics Engineers, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," IEEE Standard 323-2003, Piscataway, NJ.
 - 4.56 Institute of Electrical and Electronics Engineers, "IEEE Standard for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems," IEEE Standard 338-1987, Piscataway, NJ.
 - 4.57 Institute of Electrical and Electronics Engineers, "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations," IEEE Standard 344-2004, Piscataway, NJ.
 - 4.58 Institute of Electrical and Electronics Engineers, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," IEEE Standard 379-2000(R2008), Piscataway, NJ.
 - 4.59 Institute of Electrical and Electronics Engineers, "IEEE Standard for Qualifying Class 1E Electric Cables and Field Splices for Nuclear Power Generating Stations," IEEE Standard 383-2003, Piscataway, NJ.
 - 4.60 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," IEEE Standard 384-1992(R1998), Piscataway, NJ.
 - 4.61 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Diesel-Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations," IEEE Standard 387-1995, Piscataway, NJ.
 - 4.62 Institute of Electrical and Electronics Engineers, "IEEE Guide for Planning of Preoperational Testing Programs for Class 1E Power Systems for Nuclear Power Generating Stations," IEEE Standard 415-1986 (withdrawn), Piscataway, NJ.
 - 4.63 Institute of Electrical and Electronics Engineers, "IEEE Recommended Practice for Maintenance, Testing, and Replacement of Vented Lead-Acid Batteries for Stationary Applications," IEEE Standard 450-2010, Piscataway, NJ.

-
- 4.64 Institute of Electrical and Electronics Engineers, "IEEE Recommended Practice for Installation Design and Installation of Vented Lead-Acid Batteries for Stationary Applications," IEEE Standard 484-2002, Piscataway, NJ.
 - 4.65 Institute of Electrical and Electronics Engineers, "IEEE Recommended Practice for Sizing Vented Lead-Acid Batteries for Stationary Applications," IEEE Standard 485-1997, Piscataway, NJ.
 - 4.66 Institute of Electrical and Electronics Engineers, "IEEE Standard Method for Identification of Documents Related to Class 1E Equipment and Systems for Nuclear Power Generating Stations," IEEE Standard 494-1974 (withdrawn), Piscataway, NJ.
 - 4.67 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations," IEEE Standard 497-2002, Piscataway, NJ.
 - 4.68 Institute of Electrical and Electronics Engineers, "IEEE Standard for Qualification of Class 1E Lead Storage Batteries for Nuclear Power Generating Stations," IEEE Standard 535-2006, Piscataway, NJ.
 - 4.69 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Standard 603-1991, Piscataway, NJ.
 - 4.70 Institute of Electrical and Electronics Engineers, "IEEE Standard for Qualifying Class 1E Motor Control Centers for Nuclear Power Generating Stations," IEEE Standard 649-2006, Piscataway, NJ.
 - 4.71 Institute of Electrical and Electronics Engineers, "IEEE Standard for Qualification of Class 1E Static Battery Chargers and Inverters for Nuclear Power Generating Stations," IEEE Standard 650-2006, Piscataway, NJ.
 - 4.72 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for the Protection of Class 1E Power Systems and Equipment in Nuclear Power Generating Stations," IEEE Standard 741-1997(R2002), Piscataway, NJ.
 - 4.73 Institute of Electrical and Electronics Engineers, "IEEE Recommended Practice for Installation Design and Installation of Valve-Regulated Lead-Acid Batteries for Stationary Applications," IEEE Standard 1187-2013, Piscataway, NJ.
 - 4.74 Institute of Electrical and Electronics Engineers, "IEEE Recommended Practice for Maintenance, Testing, and Replacement of Valve-Regulated Lead-Acid (VRLA) Batteries for Stationary Applications," IEEE Standard 1188-2005(R2010), Piscataway, NJ.
 - 4.75 Institute of Electrical and Electronics Engineers, "IEEE Recommended Practice for Maintenance, Testing, and Replacement of Valve-Regulated Lead-Acid

(VRLA) Batteries for Stationary Applications, Amendment 1: Updated VRLA Maintenance Considerations,” IEEE Standard 1188a-2014, Piscataway, NJ.

- 4.76 Institute of Electrical and Electronics Engineers, “IEEE Guide for Selection of Valve-Regulated Lead-Acid (VRLA) Batteries for Stationary Applications,” IEEE Standard 1189-2007, Piscataway, NJ.
- 4.77 Electric Power Research Institute, “Advanced Nuclear Technology: Advanced Light Water Reactor Utility Requirements Document,” Final Report, Revision 13, December 2014.
- 4.78 American Society of Mechanical Engineers, “Qualification of Active Mechanical Equipment Used in Nuclear Power Plants,” ASME QME-1-2007, New York, NY.
- 4.79 American Society of Mechanical Engineers, “Rules for Construction of Nuclear Facility Components,” ASME Code Section III, Division 1, New York, NY.
- 4.80 Institute of Electrical and Electronics Engineers, “IEEE Guide for Selection and Use of Battery Monitoring Equipment in Stationary Applications,” IEEE Standard 1491-2012, Piscataway, NJ.
- 4.81 Institute of Electrical and Electronics Engineers, “IEEE/ASHRAE Guide for the Ventilation and Thermal Management of Batteries for Stationary Applications,” IEEE Standard 1635-2012, Piscataway, NJ.

5.0 Appendices

Appendix A. Example Overview of Electrical Systems and Instrumentation and Control (I&C) Systems Design

This appendix provides an example overview of a small modular reactor passive plant electrical and I&C system design. Section A.1 provides details on the design and operation of plant electrical systems, and Section A.2 provides details on the design and operation of primary I&C systems.

The information provided in this appendix is only an example of a design provided to facilitate: (1) the NRC's review of the conditions of applicability and augmented provisions for which approval is sought; and (2) an understanding of how this topical report would be implemented by future applicants (including NuScale). As part of the scope of this topical report, NuScale is not seeking NRC approval of the information in this appendix, as the details specific to the final NuScale electrical and I&C systems design are presented in the NuScale design certification application (DCA).

A.1 Electrical System Overview

Similar to a typical reactor design, the small modular reactor passive plant onsite electrical power systems include both an AC power system and a DC power system. These systems are described in the following subsections.

A.1.1 AC Power System

The AC power system includes an offsite AC power system and an onsite AC power system. For reasons detailed below, the term "high voltage electrical system" (EHVS) may be used to indicate what commonly is termed an "offsite power system." The scope of the EHVS is consistent with that contemplated by GDC 17 for an offsite power system, except that connections to an offsite transmission grid would be provided at the discretion of the license applicant referencing a design certification.

The scope of the EHVS includes the switchyard, transmission connection(s) (if provided) and associated breakers to the switchyard, main power transformers (MPTs), MPT supply breakers, and 13.8kV switchgear, breakers, and cable buses. The EHVS ends at the high-side terminals of the unit auxiliary transformers (UATs), which is the interface between the EHVS and the medium voltage AC electrical system. The design configuration of the EHVS and its interfaces with the onsite AC power system are depicted in Figure A-1.

The transmission grid would not be the normal preferred power source for a small modular reactor passive power plant. As described below, the normal source of electrical power to plant electrical loads would be the operating power module main generators. If a transmission grid connection is provided, except for periods when no power modules are operating, the grid normally would be used only for transportation of the electrical power generated by the plant to electricity consumers. A transmission grid connection would not be necessary during any design basis conditions as a source of electrical power for the performance of plant safety functions. Thus, the transmission grid is more representatively described as an electrical load rather than a power source. It is for this reason that the term “high voltage electrical system” may be used to indicate what commonly is referred to as an “offsite power system.”

The onsite AC power system includes the following:

- Normal AC power system
 - Medium voltage electrical system (EMVS) with nominal bus voltage of 4.16kV.
 - Low voltage electrical system (ELVS) with nominal bus voltages of 480 V and 120V.
- Backup power supply system (BPSS)
 - Backup diesel generators (BDGs) with nominal output voltage of 480 V.
 - Auxiliary AC power source (AAPS) with nominal output voltage of 13.8kV.

The normal source of electrical power to the onsite AC power system is the operating power module main generators via the EHVS 13.8kV generator buses. Power generated by the main turbine generators is provided as needed to the plant auxiliary and service loads through the UATs; the remaining power is supplied to the grid via the MPTs. The transmission grid connection (if provided) and the AAPS provide capability to power the onsite AC power system via the EHVS during periods when no power modules are operating. Whether power is provided from the main generators, a transmission grid, or the AAPS, the power flow is from the EHVS 13.8kV main generator buses to the high-side terminals of the UATs, which is the interface between the EHVS and the EMVS.

The voltage of the power supplied from the EHVS is reduced by the UATs to the EMVS nominal bus voltage of 4.16kV. The EMVS is graphically depicted in Figure A-2. The power at the EMVS buses is distributed to large auxiliary (nonsafety-related) pump motor loads, and to the high-side terminals of the station service transformers (SSTs), which is the interface between the EMVS and the ELVS. The SSTs reduce the voltage further to ELVS nominal bus voltage of 480V, the voltage at which the majority of plant AC loads is supplied. As shown in the simplified ELVS one-line diagram provided in Figure A-3, the power is then distributed by the ELVS to the following:

- Onsite DC power system
 - Normal DC power system (EDNS)
 - Highly reliable DC power system (EDSS)

- AC equipment load motor control centers (MCCs) and 480V/120V transformers
- Other plant static loads including the plant lighting system (PL).

The onsite AC power system does not interface directly with plant safety-related equipment – i.e., the design has no safety-related AC loads. Rather, as described further below, plant safety-related equipment, as well as post-accident monitoring instrumentation and emergency lighting, are powered from the EDSS.

The BPSS provides backup sources of AC electrical power when the normal AC power sources are not available. Such a condition would occur only if none of the power modules was operating and a connection to a transmission grid is not provided as part of the site-specific design or if provided, is lost. The BPSS power generation sources include two BDGs and an AAPS (e.g., combustion turbine generator, hydroelectric power plant, etc., to be determined by the COL applicant).

It is noted that each power module is designed to sustain a load rejection from 100 percent reactor power with its turbine generator continuing stable operation while supplying plant electrical loads. Thus each of the operating power modules represents an additional source of AC power for plant electrical loads in the event that an offsite transmission grid connection is not available. This capability, combined with the BPSS power generation sources, results in a significantly reduced likelihood of a loss of all AC power (i.e., station blackout) as compared to existing reactor designs.

The primary function of the BDGs is to provide backup electrical power to equipment loads that are determined to be risk-significant. These loads include nonsafety-related, risk-significant equipment that may be determined to meet RTNSS Criterion B such that electrical power would be required in the post-72 hour period following a hypothetical SBO event. The BDG portion of the BPSS and its connections to the ELVS is shown in Figure A-4. As shown in Figure A-4, two divisions of BDG backup power are provided (one division assigned to each BDG), with each division consisting of two separate BDG switchgear buses. As indicated in Figure A-3 and Figure A-4, the 480V output of the BDGs is connected via the BDG buses to “BDG-backed MCCs.” The BDG-backed MCCs are part of the ELVS (see Figure A-3), and the ELVS equipment and circuits downstream of these MCCs are used to route the power to the selected loads.

The primary BDG load is the EDSS, since it is the normal power source for post-accident monitoring (PAM) instrumentation, portions of the emergency lighting system, and control circuits for some other BDG loads. Other systems and equipment preliminarily designated as BDG loads include the EDSS battery and module protection system (MPS) room ventilation systems, and equipment needed to support the post-72 hour control room habitability function.

The BDGs are conservatively sized to accommodate the full capacity of the EDSS battery chargers and all “non-EDSS” BDG loads. This allows for providing electrical power to post-72 hour loads while simultaneously recharging the EDSS batteries. Although not necessary to operate in the first 72 hours following a loss of all AC power, the BDGs start automatically upon sensing a loss of voltage on the 13.8kV EHVS buses. Thus, the BDGs are available for manual loading within minutes of starting, providing plant operators additional flexibility in the unlikely event of a loss of normal AC power sources.

The AAPS provides the capability to power plant auxiliary and service loads during periods when no other AC power sources are available. This capability includes sufficient electrical power for startup of the first power module (i.e., black start), and for controlled shutdown and cooldown of plant power modules in the unlikely event involving a simultaneous loss of all operating main generators and the transmission grid connection. The AAPS is connected directly to the EHVS 13.8kV generator buses through its generator circuit breaker as shown in Figure A-1. The EHVS then provides the power to plant auxiliary and service loads via the EMVS and ELVS, the same flowpath as when power is provided from the power module main generators or transmission grid.

A.1.2 DC Power System

The onsite DC power systems include the normal DC power system (EDNS) and the highly reliable DC power system (EDSS). The EDNS design is analogous to a typical non-Class 1E DC power system, in that it serves no safety-related loads and is not required for nuclear safety. The EDNS is shared between the plant power modules, and provides DC power and AC power via inverters to nonsafety-related loads that support functions related to investment protection and power generation (i.e., loads considered part of the plant permanent nonsafety systems). The EDNS battery chargers are supplied from the ELVS, as indicated in Figure A-3 and Table A-1. The EDNS batteries are sized to supply the continuous full load for a runtime period of 40 minutes, based on the most limiting load profile without load shedding.

The EDSS design consists of two separate and independent portions. One portion, termed the EDSS-Common (EDSS-C), serves plant common loads – i.e., loads with functions not specific to any single power module. The other portion, termed the EDSS-Module-Specific (EDSS-MS), consists of 12 separate and independent DC electrical power supply systems, one for each of the plant’s 12 power modules. The EDSS-MS for a power module provides electrical power for the module protection system (MPS) and other important-to-safety loads associated with that power module. Figure A-5 and Figure A-6 provide a graphical overview of the EDSS-C and EDSS-MS designs, respectively, and indicate the demarcation between the EDSS and the Class 1E equipment served by the EDSS. As shown in Figure A-3, Figure A-5 (with clarification in Table A-2), and Figure A-6, the source of electrical supply to the EDSS-C and EDSS-MS battery chargers is the ELVS via the BDG-backed MCCs described above in Section A.1.1.

The EDSS design incorporates significant redundancy and independence that provides protection from single failures substantially similar to a typical Class 1E DC electrical system. An example failure modes and effects analysis (FMEA) for the EDSS is documented in Appendix C (Table C-1) of this report. This FMEA is the first general step of a reliability analysis effort intended to confirm that the final EDSS design adequately satisfies single failure criterion guidance to the extent described in Table 3-2 within the main body of this topical report. The FMEA results would indicate the effect of various failures within an EDSS-MS or within the EDSS-C on the ability of that system to perform its function. It is noted that with separate and independent EDSS-C and EDSS-MSs, a postulated failure of an EDSS-MS component would not affect the EDSS-MS of other power modules, and also would not affect the EDSS-C. Similarly, a postulated failure within the EDSS-C would not adversely affect any of the EDSS-MSs. In summary, providing an EDSS-C portion and 12 separate EDSS-MS portions – all independent from each other – makes a complete loss of DC power improbable.

The EDSS-C and the 12 EDSS-MSs each have two separate divisions as indicated in Figure A-5 and Figure A-6. Each division of the EDSS-MS comprises two separate and independent channels – one channel having redundant full-load 24-hour batteries, and the other channel having redundant full-load 72-hour batteries. Similarly, each division of the EDSS-C has redundant full-load 72-hour batteries. Thus, if a battery is not functional or taken out of service for maintenance, the other redundant battery is capable of serving the full load of the EDSS-MS channel or EDSS-C division for the designated design duration (i.e., 24 hours for EDSS-MS Channels A and D, and 72 hours for the two EDSS-C divisions and EDSS-MS Channels B and C).

The 24-hour battery duty cycle of EDSS-MS Channels A and D is specified to ensure the ECCS valves are held shut for a minimum of 24 hours following a postulated loss of AC power unless a valid ECCS actuation signal is received (see Appendix B, Section B.2.1.3, for additional information on ECCS operation). The 72-hour battery duty cycle for EDSS-MS Channels B and C and the EDSS-C is specified to ensure a minimum of 72 hours of electrical supply for post-accident monitoring instrumentation (see Section A.2). Battery monitors are used to provide continuous monitoring of EDSS battery performance.

The EDSS design provides the same redundancy in battery chargers as that for the EDSS batteries. Specifically, each EDSS-MS channel and EDSS-C division has redundant battery chargers, each of which is capable of supplying electrical power to its associated loads while simultaneously recharging its associated batteries from their design minimum charge state to 95 percent of full charge within 24 hours. Unlike the EDNS, the design of the EDSS does not include inverters. Rather, the EDSS provides DC electrical power directly to loads without inverting the power to AC. According to operational experience data (Reference 4.28), the elimination of inverters in the design results in approximately a factor of 10 increase in system reliability as compared to a comparable DC power system that includes inverters.

Notwithstanding the features described above, as a result of the safety classification assessment provided in Appendix B, Section B.2.7 of this report, the augmented design, qualification, and QA provisions described in Table 3-2 within the main body of this topical report would be applied to the EDSS design. These provisions and the reliability comparison specified by condition of applicability Item II.2 in Table 3-1, Section II – in addition to those features described above – ensure an EDSS reliability substantially similar to that of a Class 1E DC electrical system. Additional details on the augmented provisions that ensure the EDSS is a highly reliable DC power source are provided in Section 3 (Table 3-2) of this topical report.

The battery chargers between the ELVS and the EDSS provide nonsafety-related electrical isolation between the AC power system and the EDSS. The battery chargers are not relied upon to achieve the electrical isolation of safety-related loads. Rather, Class 1E electrical isolation of safety-related equipment from the non-Class 1E EDSS is provided within the Class 1E instrumentation and controls (I&C) equipment for each load. Specifically, a Class 1E power supply power monitor (PSPM) is installed at each interface between the EDSS and downstream Class 1E equipment and circuits. The PSPM monitors incoming power quality and provides electrical isolation of the Class 1E circuits and components in the event of degradation in the electrical supply that would have the potential to adversely impact safety functions. This ensures that a power fluctuation on either the AC or DC power system will not adversely affect the ability to achieve and maintain safety functions. Section A.2.1 provides additional detail on the design and operation of the PSPMs.

A.2 Instrumentation and Controls (I&C) Equipment Overview

The assessment provided in Appendix B describes an example of the role that electrical power plays in small modular reactor passive plant functions to demonstrate the appropriate classification for electrical systems is non-Class 1E. The plant functions addressed in Appendix B include but are not limited to those performed by I&C systems, some of which are safety-related and thus comprise Class 1E equipment. To facilitate a full understanding of the Appendix B assessment, this section provides an overview of an example I&C architecture and primary I&C systems that would be used for power module and plant monitoring and control.

The design philosophy for I&C systems is based on providing clear interconnections for plant systems, system separation, and simplification of system functions. A simplified block diagram of an example I&C system architecture is shown in Figure A-8. As indicated, there are Class 1E protection systems and non-Class 1E systems that are used to perform monitoring and control functions. The Class 1E protection systems include 12 separate and independent module protection systems (MPSs) – one for each of the power modules. These protection systems, and other Class 1E systems and equipment, are described in Section A.2.1. The non-Class 1E monitoring and control systems include: (1) a common plant protection system (PPS); (2) 12 separate and independent module control systems (MCSs) – one for each of the power modules; and (3) a common plant control system (PCS) independent of the MCSs. These systems are described in Section A.2.2.

As indicated in Figure A-8 and Figure A-9, the protection and control systems described in Sections A.2.1 and A.2.2 provide sensor data for display in the main control room (MCR). MCR display and indication includes that provided by the safety display and indication system (SDIS) and associated displays, as well as by the MCS and PCS displays. Section A.2.3 provides a description of this display and indication equipment and its interfaces with the protection and control systems described in Sections A.2.1 and A.2.2.

A.2.1 Module Protection Systems and Other Class 1E I&C Equipment

Each power module has its own dedicated (i.e., not shared with other modules) MPS as indicated in Figure A-8. Each MPS has four redundant separation groups of sensors, signal conditioning, monitoring and indication, and trip determination circuitry and two redundant divisions of reactor trip system (RTS) and engineered safety features actuation system (ESFAS).

The MPS interfaces with the power module's dedicated Class 1E neutron monitoring system (NMS) and power module sensors and execute devices (e.g., valve actuator solenoids). The NMS measures the reactor core power level using ex-core detectors, provides power to the detectors, and sends the parameter values to each MPS separation group. The power module's redundant sensors provide the required plant parameters to each separation group. Each separation group independently evaluates each safety function parameter to determine if a setpoint has been exceeded. If a setpoint has been exceeded, the separation group sends an actuate signal to both divisions of RTS and ESFAS where it is compared to the other three separation groups. If two of the four separation groups request an actuation of a safety function, both redundant divisions of RTS and ESFAS actuate (de-energize) the associated execute devices.

The safety-related functions executed by the MPS include reactor trip, containment isolation, decay heat removal system (DHRS) actuation, chemical and volume control system (CVCS) isolation, pressurizer heater trip, emergency core cooling system (ECCS) actuation, and low-temperature overpressure protection (LTOP) actuation. The parameters monitored by the MPS include reactor coolant system (RCS) flow and temperatures; pressurizer pressure and level; containment vessel pressure and water level and temperature; neutron flux levels through the NMS; and other parameters as identified through safety analysis. The MPS also monitors the positions of safety-related valves. As indicated in Figure A-8 and Figure A-9, the MPS supplies parameter data inputs to the SDIS and to the MCS (for MCS displays in the MCR). The SDIS and MCS displays are described in Section A.2.3.

As indicated in Figure A-6 and Figure A-10, a separate and independent EDSS-MS provides two divisions (four channels) of electrical power to each power module MPS' four separation groups,⁸ NMS, and sensors, and two divisions of RTS and ESFAS. A Class 1E PSPM is shown in Figure A-10 and Figure A-11 at each interface between the non-Class 1E EDSS electrical supply and downstream Class 1E equipment. The PSPMs ensure appropriate independence between safety systems and the EDSS (as an interconnected non-Class 1E system) as required by IEEE Std. 603-1991. Each PSPM provides a redundant isolated DC-to-DC interface between the EDSS and Class 1E equipment and circuits. Additionally, the PSPM monitors the input voltage, with triple redundant monitoring circuits, and alarms on both a high input voltage and low input voltage. The alarm outputs are provided to the protection system circuitry to implement any necessary protection functions to ensure Class 1E equipment and circuits respond in a controlled manner given a degraded input voltage condition.

A.2.2 Plant Protection System, Module Control System, and Plant Control System

The PPS is a non-Class 1E protection system used to monitor and control common plant functions. The PPS consists of two redundant divisions of sensors, signal conditioning, monitoring and indication, and trip determination circuitry. It includes the equipment used for monitoring parameters at the plant level and executing functions in response to out-of-normal parameter values. The parameters monitored by the PPS include radiation detectors in the normal air intake for the MCR, ultimate heat sink (including reactor and spent fuel pool) level, and other parameters as identified by plant analyses. The functions executed by the PPS include isolation of the control room envelope (CRE) and actuation of the control room habitability system (CRHS).

Two separate and independent divisions of the EDSS-C provide electrical power to the two divisions of the PPS (see Figure A-5 and Figure A-11). As indicated in Figure A-8 and Figure A-9, the PPS supplies parameter data inputs to the SDIS and to the PCS (for PCS displays). The SDIS and PCS displays are described in Section A.2.3.

As indicated in Figure A-8, each power module has its own dedicated (i.e., not shared with other modules) MCS. The principal function of each MCS is to control and monitor the nonsafety-related control system components associated with its respective power module. This includes all the necessary nonsafety-related primary and secondary systems – e.g., chemical, utility, and support process systems to a power module. The MCS also provides control and monitoring of safety-related components that are specific to a power module. The monitoring of the safety-related components is achieved by receiving one-way communications from the MPS to the MCS through isolation devices. As shown in Figure A-8 and detailed further in Section A.2.3, each MCS sends these signals to its respective MCS displays.

⁸ Each of the EDSS-MS power channels provides power to one of the four MPS separation groups. For example, power channel A serves MPS separation group A, etc.

The MCS control of its power module safety-related valves is not for the purposes of safety function initiation (i.e., is not a safety-related function). Rather, it involves manual component level manipulation used for valve maintenance, testing, or alignment following refueling or valve actuation. The non-Class 1E control signal from the MCS is sent through a qualified isolation device to a dedicated priority logic circuit in the MPS, which requires a safety-related enable signal prior to allowing control of the device from the MCS. The dedicated analog priority logic circuit ensures that both the automatic actuation signal as well as the manual actuation signal are the highest priority. Therefore, the priority circuit will ensure an actuation is performed when either an automatic actuation signal or a manual actuation signal are present, regardless of whether non-Class 1E MCS control of the safety-related component is enabled.

The principal function of the PCS is to control and monitor the nonsafety-related control system components which are common to multiple power modules and are not in the scope of control by the MCS. The PCS also provides monitoring and nonsafety-related control capability for testing and routine operation of components that are controlled by PPS (e.g., CRHS air delivery valves and CRE isolation dampers; see Appendix B, Section B.2.3). As shown in Figure A-8 and detailed further in Section A.2.3, each PCS sends these signals to its respective PCS displays. As described above, the 12 MCSs and the PCS do not perform a safety function. Accordingly, as shown on Figure A-9, these systems are powered from the nonsafety-related normal DC power system (EDNS).

A.2.3 Display and Indication

The MCR indication of power module and plant status is provided on the SDIS displays and the PCS and MCS displays as shown in Figure A-8 and Figure A-9. The scope of the SDIS is from the isolated outputs of the MPS and PPS up to and including the SDIS displays. The SDIS is designed to provide information for display of post-accident monitoring variables as defined in IEEE Std. 497-2002 and safety system status including execute device position. The displayed variables include power module and common plant parameters that are provided as output from the MPS and PPS, respectively. The SDIS is display only and does not initiate automatic protective actions or have any control functions.

As indicated in Figure A-8 and Figure A-9, each MPS sends data associated with its power module to its respective (module-specific) SDIS displays, and each MCS sends its data to its associated module's MCS displays. The data from the PPS is sent to a common SDIS MCR display and the data from PCS is sent to a common PCS MCR display separate from the module-specific displays. Based on human factors engineering (HFE) and parameters needed for operation and plant procedures, select MPS and PPS parameters displayed on the SDIS displays are available on the PCS and MCS displays for routine monitoring by the MCR operator. The SDIS data not routinely displayed on the PCS and MCS displays is retrievable for display on the PCS and MCS displays via the plant historian which archives all required data from MPS, MCS, PPS, and PCS.

Figure A-9 shows the sources of electrical power to the various display and indication equipment and the control and monitoring systems that send parameter data to that equipment. Electrical power to the SDIS is provided from two separate and independent divisions of the EDSS-C, the same electrical power source as that for the PPS. As shown in Figure A-9, the 12 MCSs, the PCS, and the MCS and PCS displays are powered from the EDNS. The following summarizes the various independent and separate electrical power sources reflected in Figure A-9:

- EDSS-MS (x12) – Module Protection System (x12)
- EDSS-C –
 - Plant Protection System
 - Safety Display and Indication System, including SDIS displays
- EDNS –
 - Module Control System (x12), including MCS displays
 - Plant Control System, including PCS displays

As described in Appendix B, Section B.2.7, although not necessary for reactor safety, post-accident monitoring capability is an important defense-in-depth element of the plant design. Furthermore, post-accident monitoring serves an important role in providing plant status information to stakeholders during and following a postulated design basis event. Based on these operational considerations, as well as other commercial and investment protection reasons, maintaining post-accident monitoring capability, while not necessary for safety-related function performance, is desirable and important. Thus, augmented design, qualification, and QA provisions are applied to the SDIS and the electrical system (i.e., the EDSS) that provides electrical power to the SDIS and the protection systems that send data signals to the SDIS. The augmented design, qualification, and QA provisions applied to the EDSS are described in Section 3 (Table 3-2) of this report (main body). These provisions are intended to ensure an EDSS reliability substantially similar to that of a Class 1E DC power system.

Given the highly reliable “Class 1E-like” design of the EDSS, a complete loss of electrical power (i.e., the EDSS-C or one or more EDSS-MSs) to the systems sending data for MCR display (i.e., the MPSs and PPS) is improbable. Further, the availability of MPS and PPS data output on both the SDIS displays and MCS/PCS displays that are powered from separate electrical systems provides additional assurance that MCR monitoring capability is maintained. The following summarizes the effects that a postulated loss of various electrical systems would have on MCR monitoring capability.

With electrical power available from the EDSS (including both the EDSS-C and EDSS-MS) and the EDNS, MCR operators have the SDIS displays and the MCS/PCS displays with which to monitor power module and plant parameters during normal operations and during and following a design basis event. A postulated loss of the EDNS would result in a loss of the MCS/PCS displays, but would have no adverse effect on accident monitoring capability via the SDIS. A postulated loss of both divisions of the EDSS-C would result in the unavailability of the PPS and the SDIS until at least one division of the EDSS-C was restored. In this unlikely scenario, each power module MPS would remain powered from its respective EDSS-MS, and the MCS and PCS displays would remain powered from the EDNS. Thus, power module monitoring data (from each module's MPS) would be available to MCR operators via the MCS displays (powered from the EDNS).

A postulated loss of both divisions of a power module's EDSS-MS would result in a loss of electrical power to the affected module's MPS and to the actuation devices powered and controlled by the MPS. This would result in the power module safety functions actuating via stored energy and continuing to be maintained passively as described in Appendix B. In this unlikely scenario, the SDIS displays would remain powered from the EDSS-C, and the MCS and PCS displays would remain powered from the EDNS. Thus the MCR displays for the unaffected power modules and for PPS common plant parameters would remain available to the operators. However, the affected power module's MPS would no longer be sending output signals for MCR display and indication until at least one of the four channels of the affected EDSS-MS was restored.

In summary, the postulated scenarios described above are intended to facilitate an understanding of the plant monitoring architecture as related to the example safety classification evaluations in Appendix B. Section B.2.7 provides additional detail regarding the post-accident monitoring function and the role it and its electrical power supplies fulfill in a small modular reactor passive power plant operations. The augmented design, qualification, and QA provisions to be applied to the EDSS are described in Section 3 (Table 3-2) within the main body of this topical report.

Table A-1. ELVS power supply connections to EDNS

EDNS Equipment	ELVS Power Source to EDNS Equipment		EDNS Equipment Location
	Low Voltage Bus	Motor Control Center (MCC)	
EDNS SUBSYSTEM 1			
Battery Charger 1	Bus 1 – Module 6	Bus 1 Reactor Building (RXB) MCC	RXB North 100' el.
Voltage Regulating Transformer (VRT) 1	Bus 3 – Module 6	Bus 3 RXB MCC	RXB North 100' el.
EDNS SUBSYSTEM 2			
Battery Charger 2	Bus 1 – Module 7	Bus 1 RXB MCC	RXB South 100' el.
VRT 2	Bus 3 – Module 7	Bus 3 RXB MCC	RXB South 100' el.
EDNS SUBSYSTEM 3			
Battery Charger 3A	Bus 1 – Module 4	Bus 1 TGB MCC	Turbine Generator Building (TGB) A (North)
Battery Charger 3B	Bus 3 – Module 4	Bus 3 TGB MCC	TGB A (North)
VRT 3	Bus 3 – Module 4	Bus 3 TGB MCC	TGB A (North)
EDNS SUBSYSTEM 4			
Battery Charger 4A	Bus 1 – Module 10	Bus 1 TGB MCC	TGB B (South)
Battery Charger 4B	Bus 3 – Module 10	Bus 3 TGB MCC	TGB B (South)
VRT 4	Bus 3 – Module 10	Bus 3 TGB MCC	TGB B (South)
EDNS SUBSYSTEM 5			
Battery Charger 5	Bus 1 – Module 6	Bus 1 RXB MCC	Control Building (CRB) 50' el.
VRT 5	Bus 3 – Module 6	Bus 3 RXB MCC	CRB 50' el.
EDNS SUBSYSTEM 6			
Battery Charger 6	Bus 1 – Module 11	Bus 1 RWB MCC	Radwaste Building (RWB)
VRT 6	Bus 3 – Module 11	Bus 3 RWB MCC	RWB
EDNS SUBSYSTEM 7			
Battery Charger 7A	Bus 1 – Common 6A	Bus 1 Yard MCC	Yard Power Distribution Center (PDC) #7
Battery Charger 7B	Bus 2 – Common 6A	Bus 2 Yard MCC	Yard PDC #7
EDNS SUBSYSTEM 8			
Battery Charger 8A	Bus 1 – Common 6B	Bus 1 Yard MCC	Yard PDC #8
Battery Charger 8B	Bus 2 – Common 6B	Bus 2 Yard MCC	Yard PDC #8
EDNS SUBSYSTEM 9			
Battery Charger 9A	Bus 1 – Module 4	Bus 1 TGB MCC	Yard PDC #3
Battery Charger 9B	Bus 3 – Module 4	Bus 3 TGB MCC	Yard PDC #3

EDNS Equipment	ELVS Power Source to EDNS Equipment		EDNS Equipment Location
	Low Voltage Bus	Motor Control Center (MCC)	
EDNS SUBSYSTEM 10			
Battery Charger 10A	Bus 1 – Module 3	Bus 1 TGB MCC	Yard PDC #1
Battery Charger 10B	Bus 3 – Module 3	Bus 3 TGB MCC	Yard PDC #1
EDNS SUBSYSTEM 11			
Battery Charger 11A	Bus 1 – Module 4	Bus 1 TGB MCC	Yard PDC #2
Battery Charger 11B	Bus 3 – Module 4	Bus 3 TGB MCC	Yard PDC #2
EDNS SUBSYSTEM 12			
Battery Charger 12A	Bus 1 – Module 10	Bus 1 TGB MCC	Yard PDC #4
Battery Charger 12B	Bus 3 – Module 10	Bus 3 TGB MCC	Yard PDC #4
EDNS SUBSYSTEM 13			
Battery Charger 13A	Bus 1 – Module 9	Bus 1 TGB MCC	Yard PDC #5
Battery Charger 13B	Bus 3 – Module 9	Bus 3 TGB MCC	Yard PDC #5
EDNS SUBSYSTEM 14			
Battery Charger 14A	Bus 1 – Module 9	Bus 1 TGB MCC	Yard PDC #6
Battery Charger 14B	Bus 3 – Module 9	Bus 3 TGB MCC	Yard PDC #6

NOTES:

1. This table supports Figure A-3, Note 4.

Table A-2. ELVS power supply connections to EDSS-C

EDSS-C Equipment	ELVS Power Source to EDSS-C Equipment		EDSS-C Equipment Location
	Low Voltage Bus	Motor Control Center (MCC)	
Division 1, Charger 1	Bus 1 – Module 6	BDG-backed CRB MCC 1	CRB 50' el.
Division 1, Charger 2	Bus 2 – Module 7	BDG-backed CRB MCC 2	CRB 50' el.
Division 2, Charger 1	Bus 3 – Module 6	BDG-backed CRB MCC 3	CRB 50' el.
Division 2, Charger 2	Bus 4 – Module 7	BDG-backed CRB MCC 4	CRB 50' el.

NOTES:

1. This table supports Figure A-3, Note 5; Figure A-4, Note 4; and Figure A-5, Note 2.

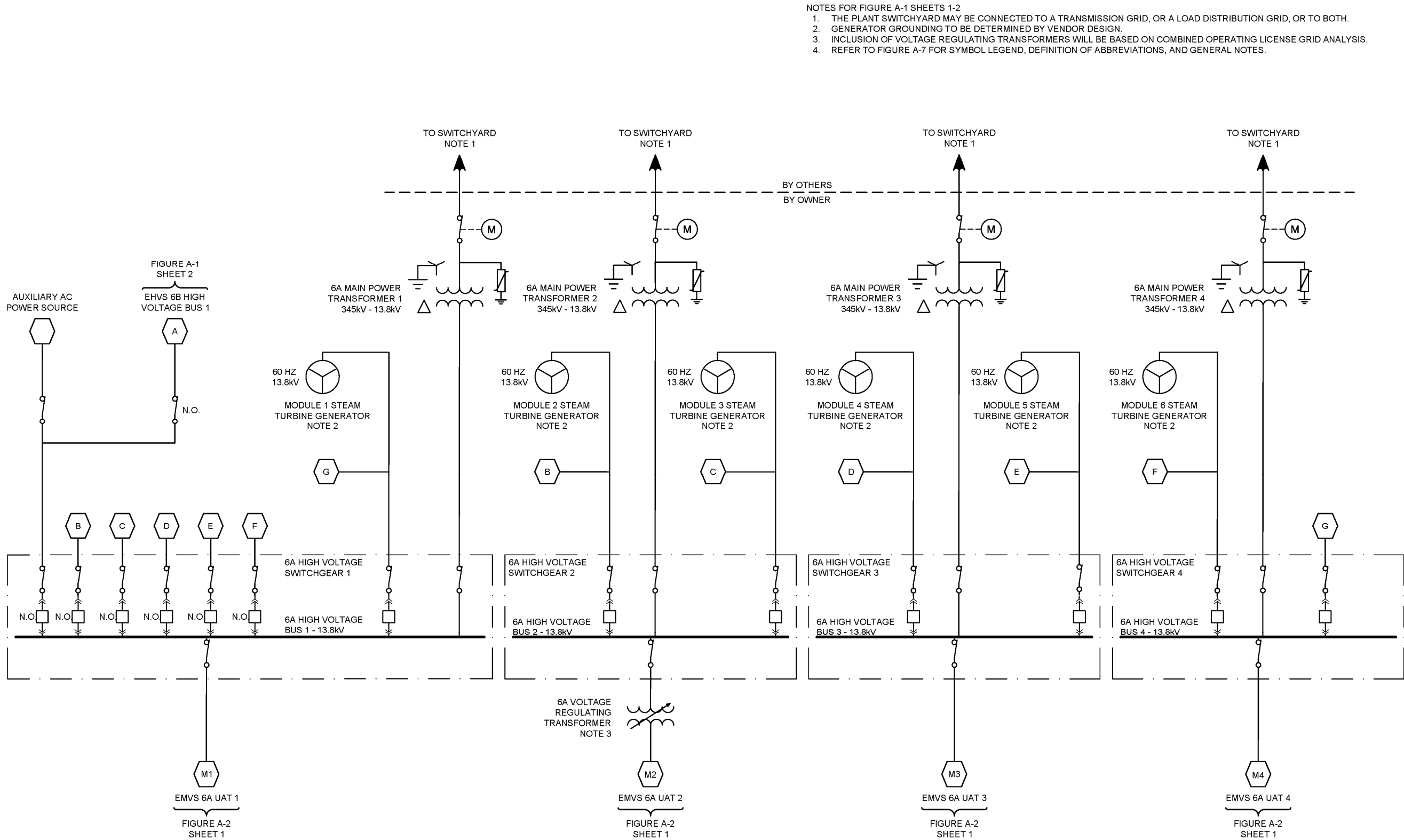


Figure A-1. High voltage electrical system and connections to onsite AC power system (Sheet 1 of 2)



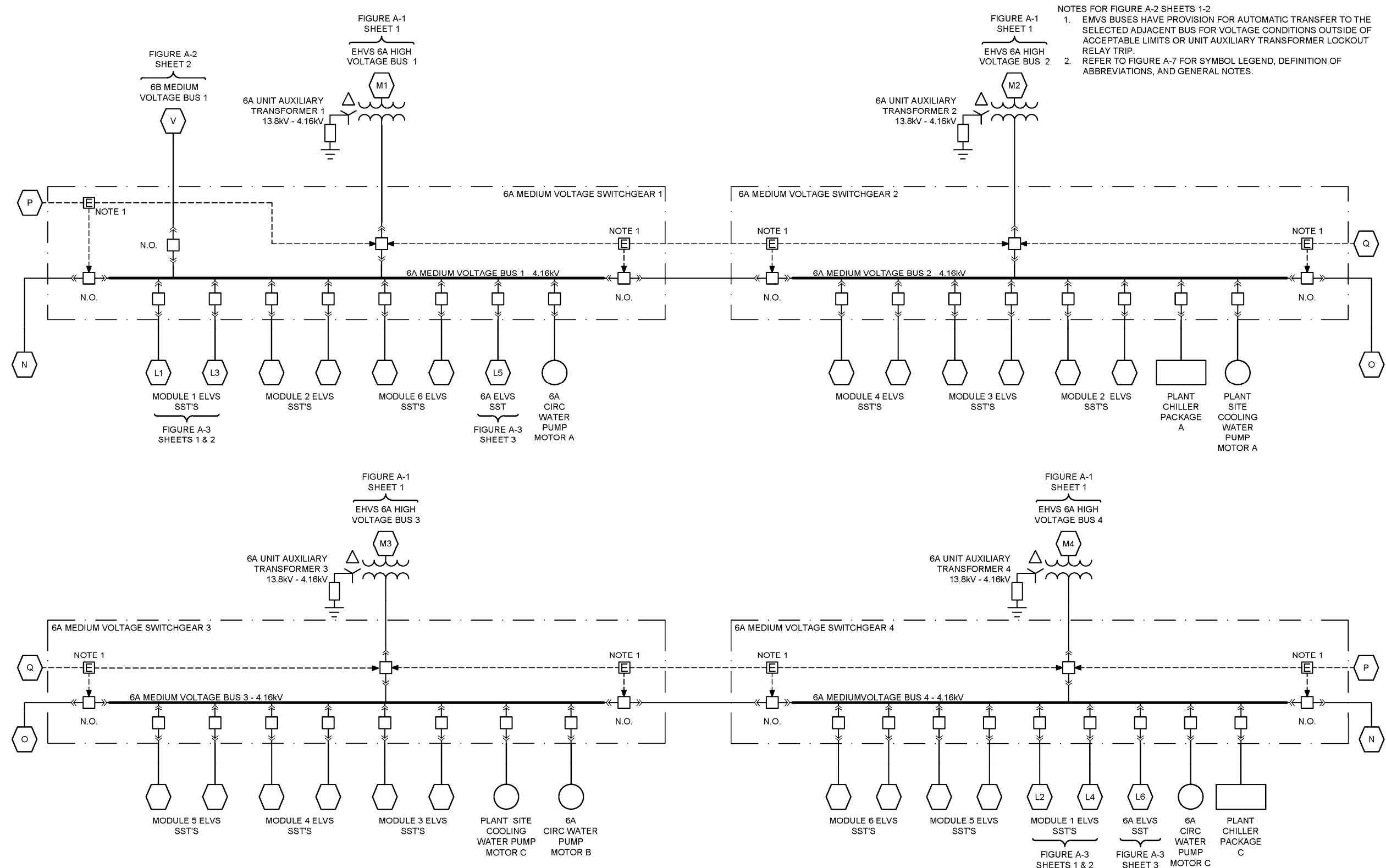
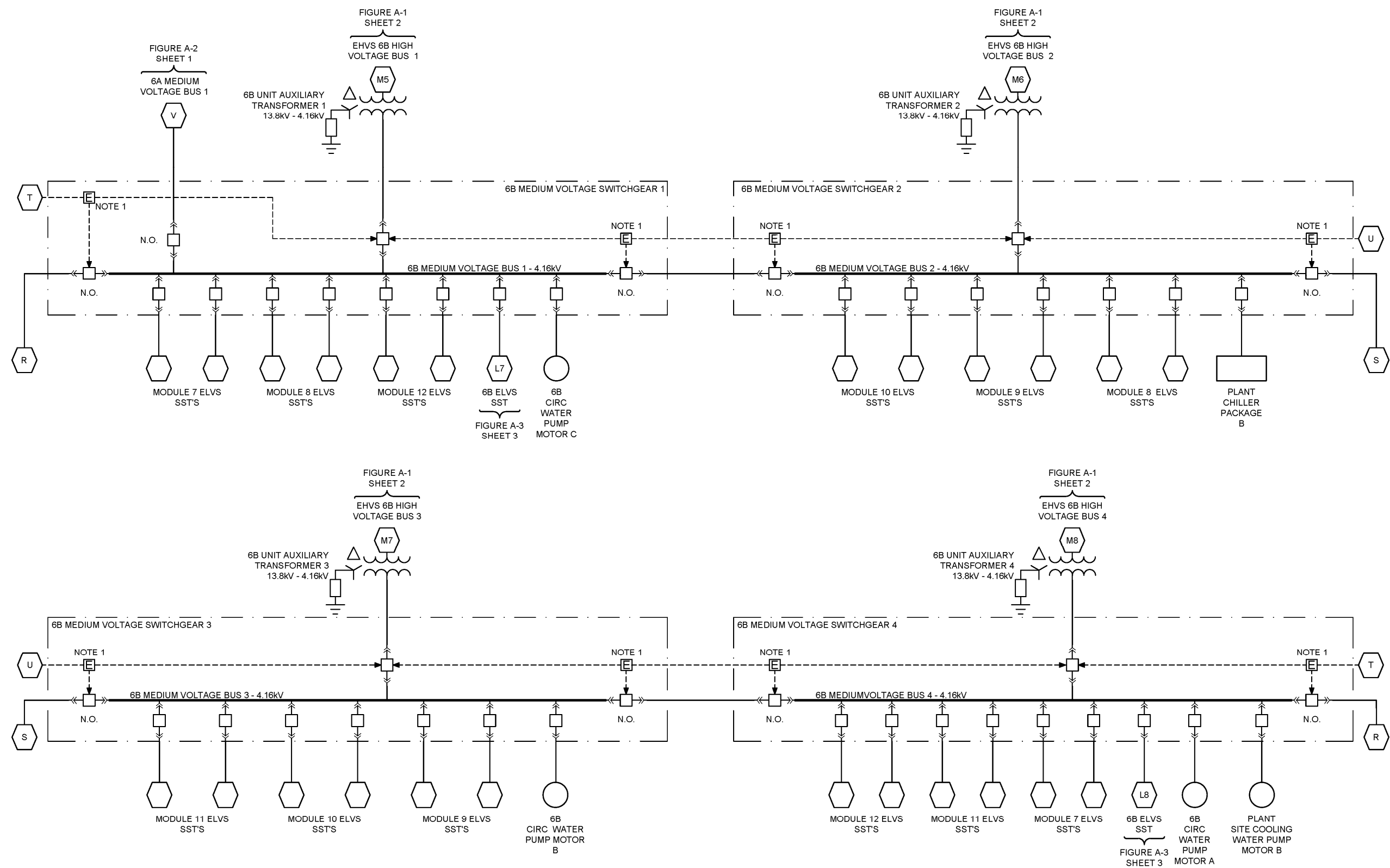


Figure A-2. Onsite AC power system – medium voltage electrical system (Sheet 1 of 2)



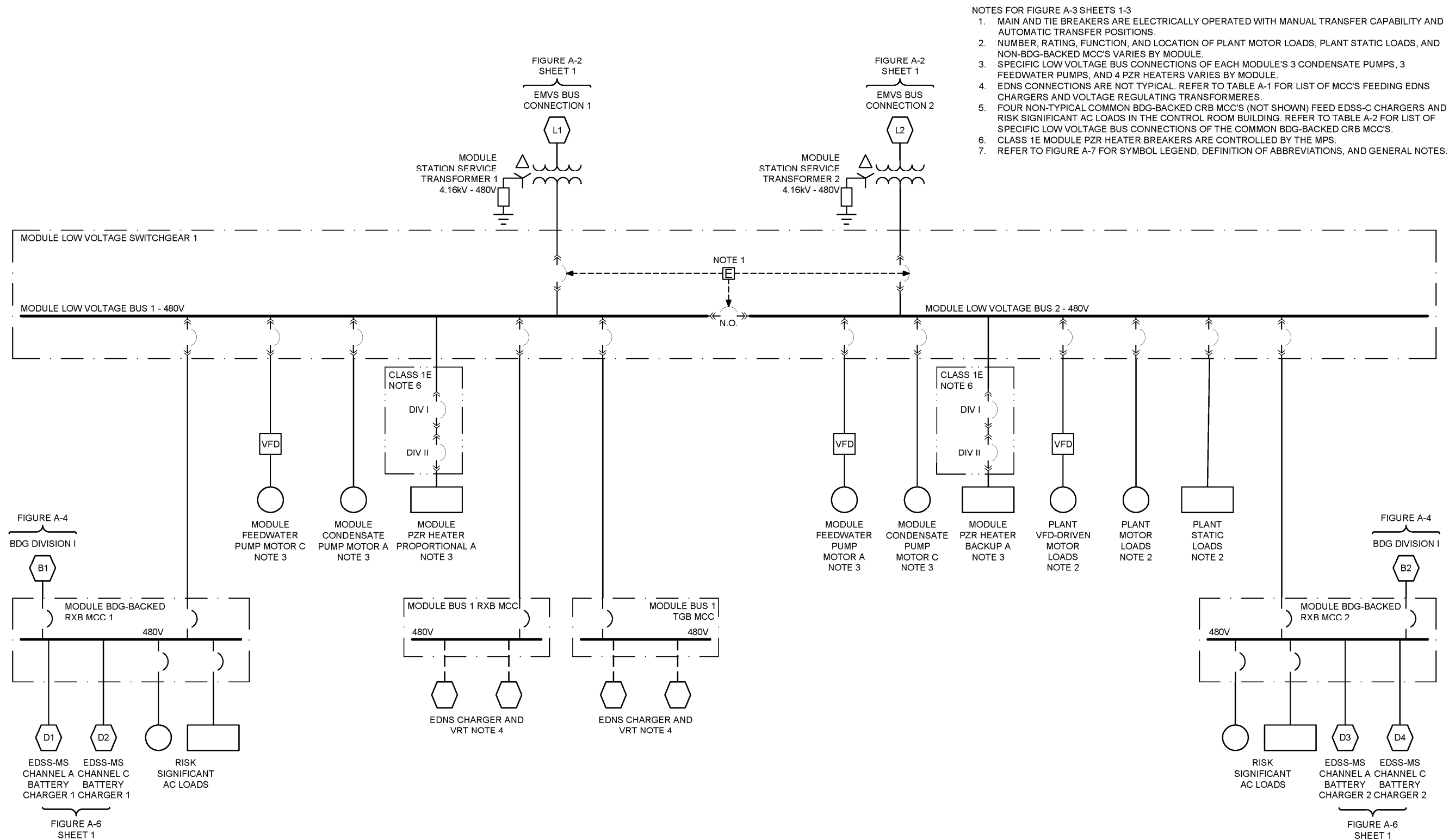


Figure A-3. Onsite AC power system – low voltage electrical system (Sheet 1 of 3)

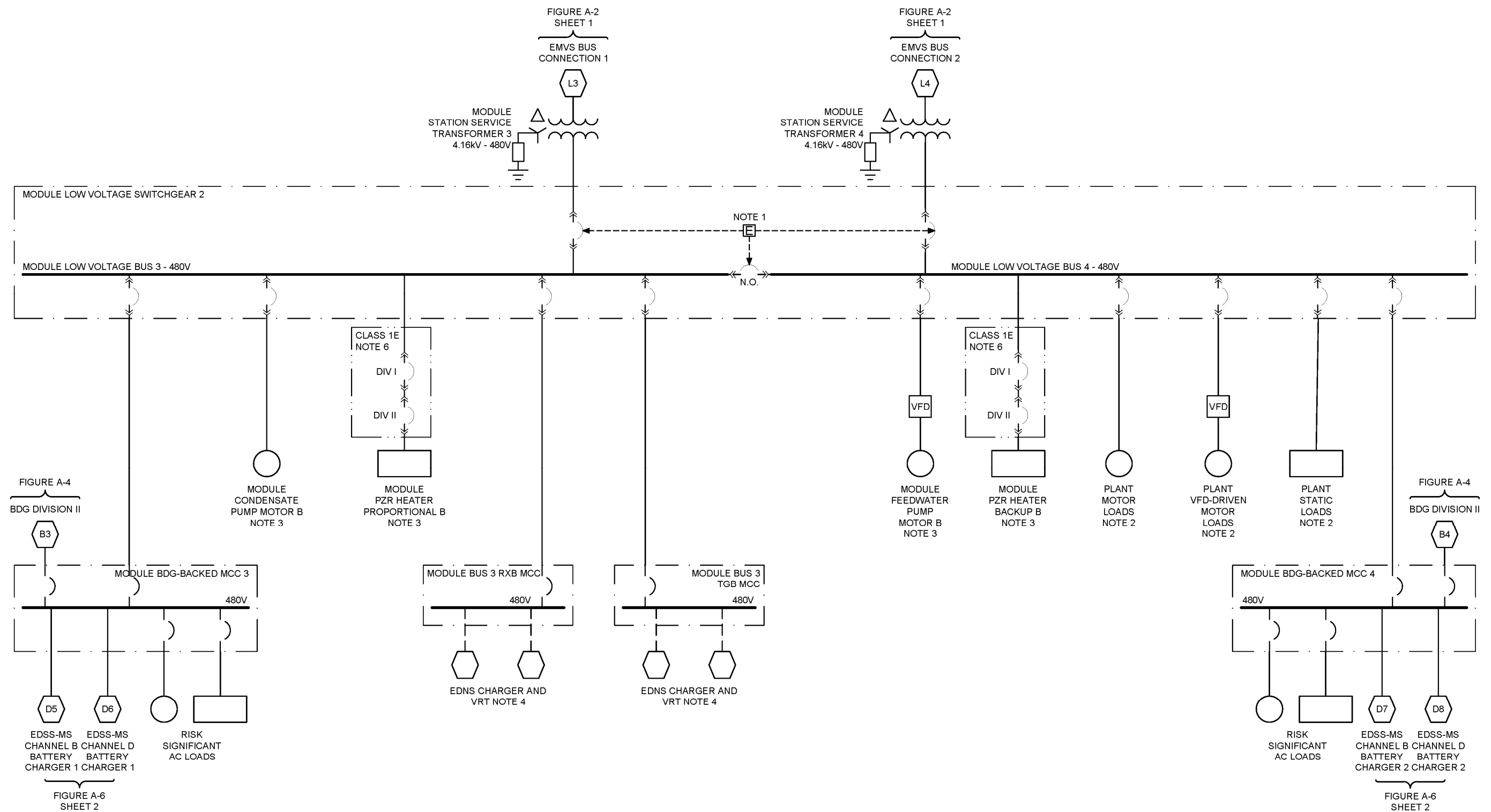


Figure A-3. Onsite AC power system – low voltage electrical system (Sheet 2 of 3)

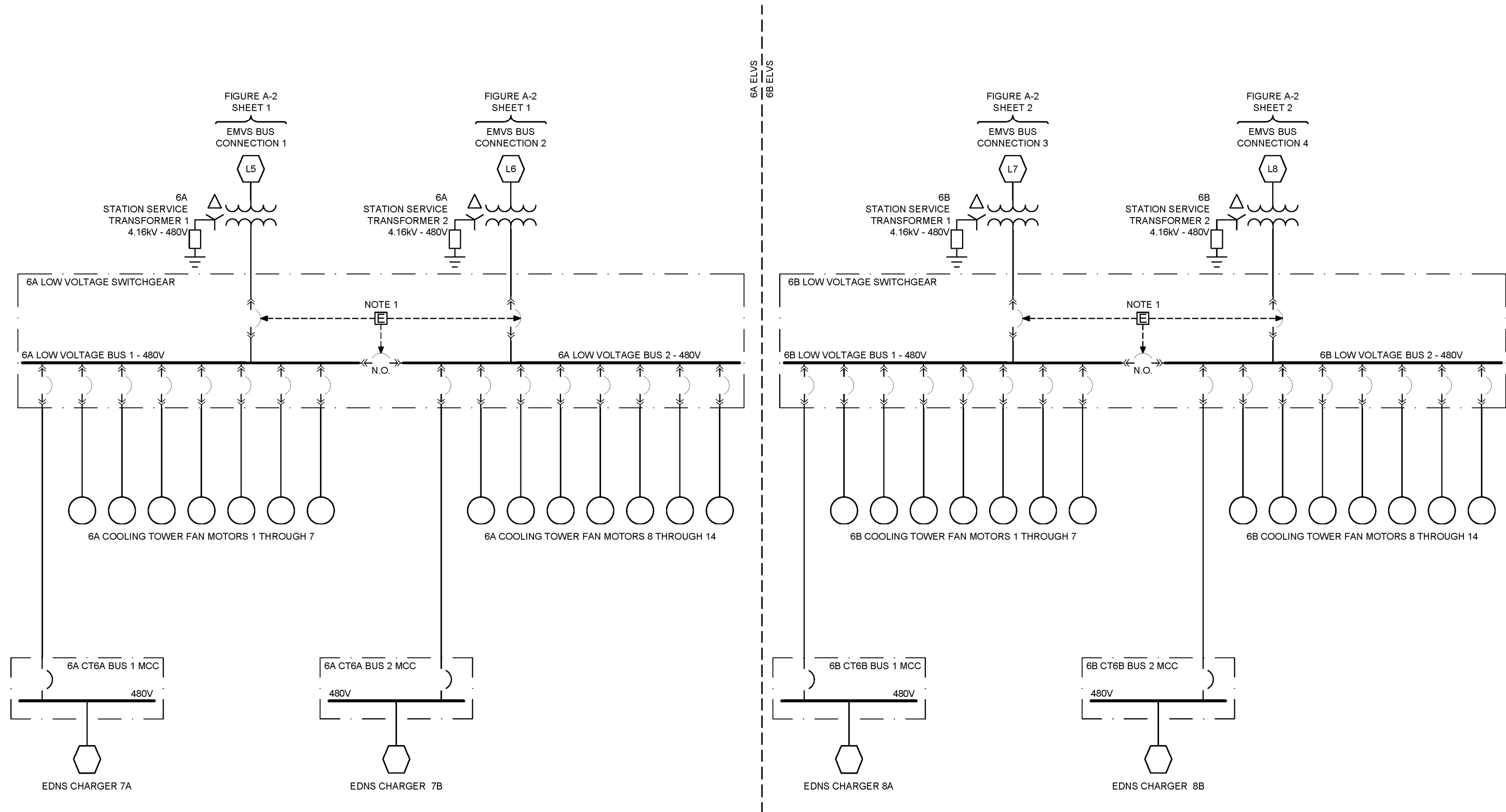


Figure A-3. Onsite AC power system – low voltage electrical system (Sheet 3 of 3)

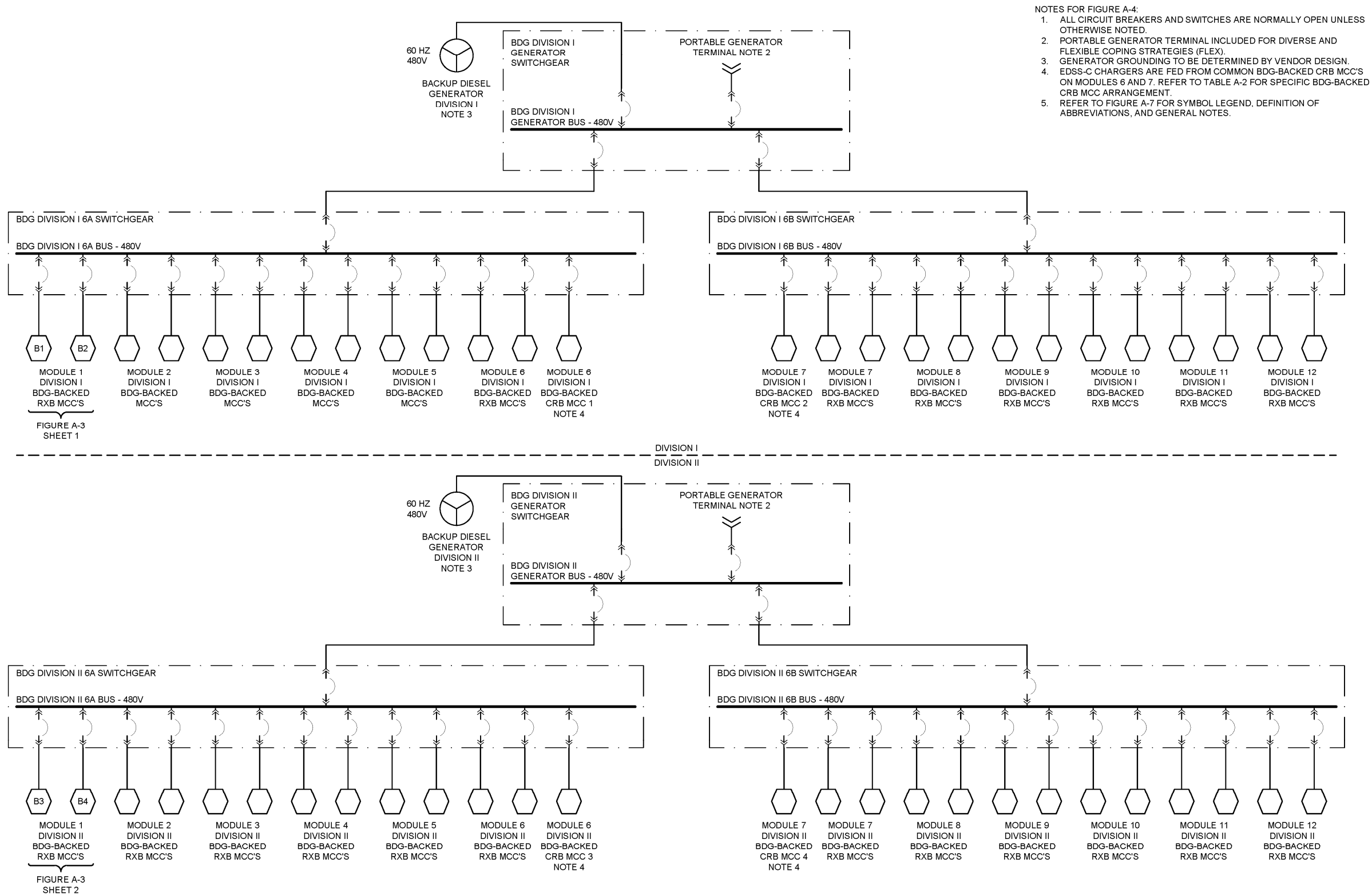


Figure A-4. Onsite AC power system – BDG portion of backup power supply system

- NOTES FOR FIGURE A-5:
- 1. EDSS-C EQUIPMENT IS LOCATED IN THE CRB.
 - 2. REFER TO TABLE A-2 FOR LIST OF COMMON BDG-BACKED MCC'S FEEDING EDSS-C CHARGERS.
 - 3. REFER TO FIGURE A-7 FOR SYMBOL LEGEND, DEFINITION OF ABBREVIATIONS, AND GENERAL NOTES.

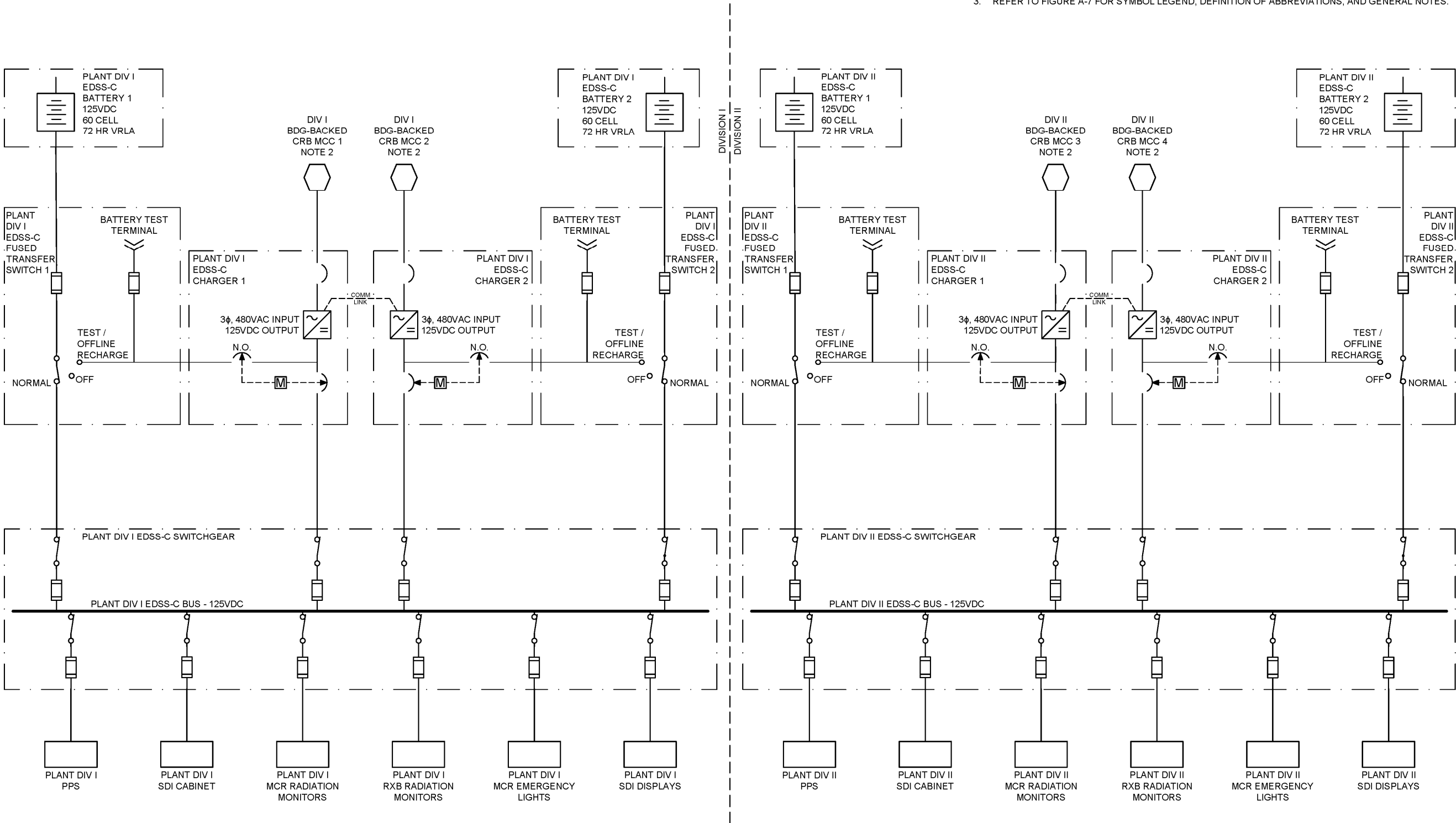


Figure A-5. Highly reliable DC power system—common (EDSS-C)

- NOTES FOR FIGURE A-6 SHEETS 1-2:
- 1. THIS DRAWING IS TYPICAL FOR 12 MODULES.
 - 2. POWER SUPPLY POWER MONITORS PROVIDE CLASS 1E ELECTRICAL ISOLATION OF SAFETY-RELATED LOADS FROM THE NONSAFETY-RELATED EDSS.
 - 3. SPECIFIC VENDOR-SUPPLIED POWER SOURCE REQUIRED FOR UNIQUE SENSORS NOT POWERED VIA MPS OR NMS.
 - 4. REFER TO FIGURE A-7 FOR SYMBOL LEGEND, DEFINITION OF ABBREVIATIONS, AND GENERAL NOTES.

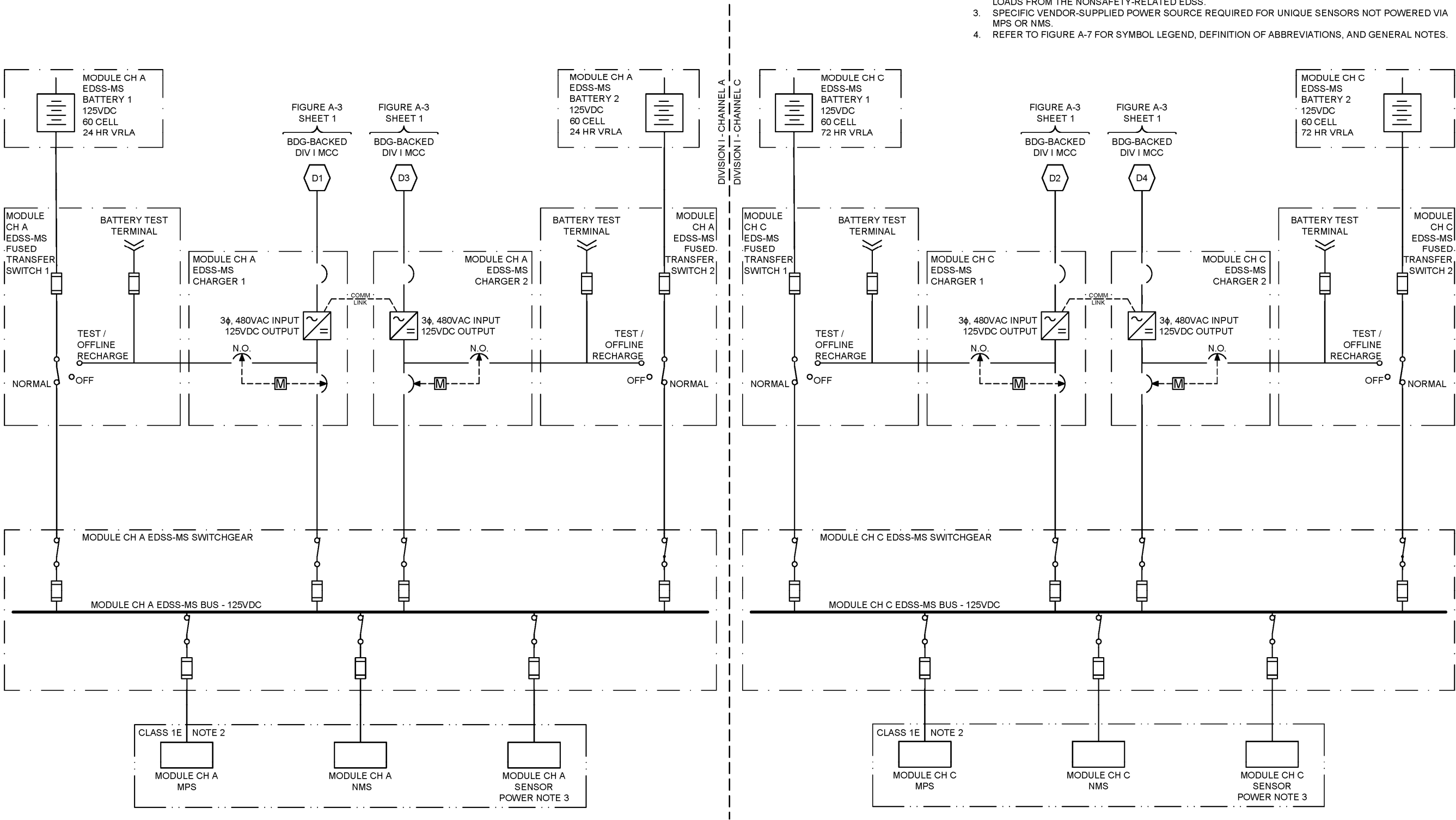


Figure A-6. Highly reliable DC power system—module-specific (EDSS-MS) (Sheet 1 of 2)

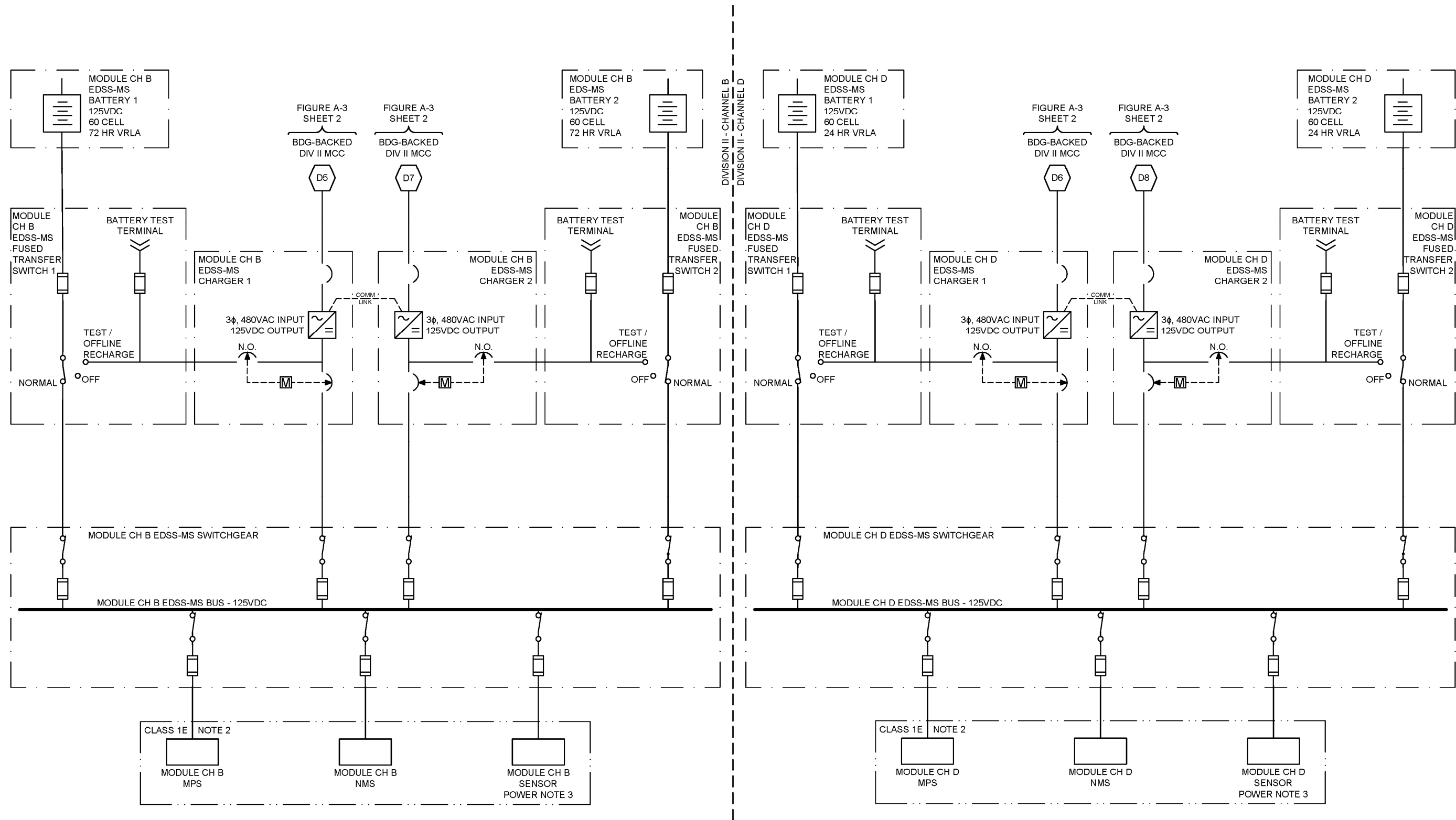
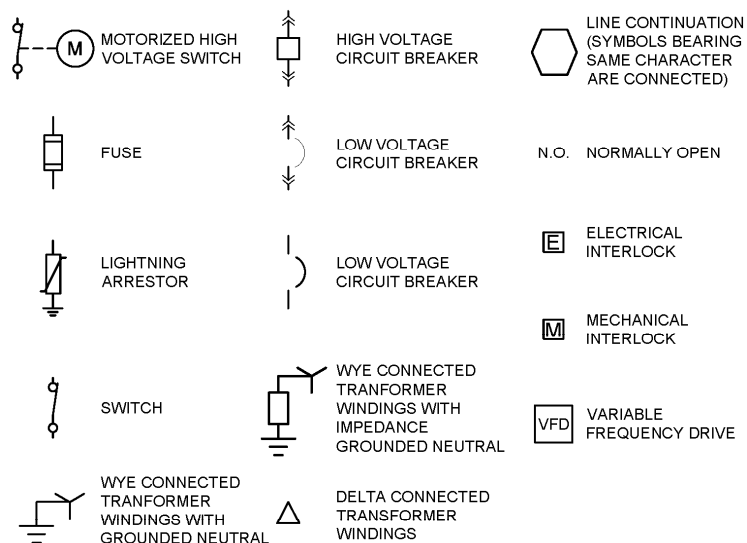


Figure A-6. Highly reliable DC power system – module-specific (EDSS-MS) (Sheet 2 of 2)

LEGEND FOR FIGURES A-1 THROUGH A-6



GENERAL NOTES FOR FIGURES A-1 THROUGH A-6

1. ALL CIRCUIT BREAKERS AND SWITCHES ARE NORMALLY CLOSED UNLESS OTHERWISE NOTED.
2. ADEQUATE NUMBER OF SPARE BREAKERS, FUSED SWITCHES, EQUIPPED SPACES, AND BLANKS SPACES IN ALL SWITCHGEAR AND MCC'S WILL BE PROVIDED TO ALLOW FOR FUTURE CHANGES.
3. LOADS AND EQUIPMENT PREFIXED WITH "PLANT" ARE COMMON TO THE 12-UNIT PLANT AND ARE NOT MODULE SPECIFIC.
4. LOADS AND EQUIPMENT PREFIXED WITH "6A" OR "6B" ARE COMMON TO UNITS 1-6 OR 7-12, RESPECTIVELY, AND ARE NOT MODULE SPECIFIC. "6A" LOADS AND EQUIPMENT ARE TYPICAL TO "6B" LOADS AND EQUIPMENT.
5. LOADS AND EQUIPMENT PREFIXED WITH "MODULE" ARE MODULE SPECIFIC. "MODULE" LOADS AND EQUIPMENT ARE TYPICAL TO ALL 12 MODULES.

DEFINITION OF ABBREVIATIONS

ABBREVIATION	DEFINITION
3 ϕ	3-PHASE
CIRC	CIRCULATING
CH	EDSS-MS CHANNEL
CT6A	6A (NORTH) COOLING TOWER
CT6B	6B (SOUTH) COOLING TOWER
COMM	COMMUNICATION
DIV	DIVISION
HZ	HERTZ
HR	HOUR
KV	KILO-VOLT
PZR	PRESSURIZER
RAD	RADIATION
V	VOLT
VAC	AC VOLTS (RMS)
VDC	DC VOLTS
VFD	VARIABLE FREQUENCY DRIVE

Figure A-7. Legend and general notes for Figures A-1 through A-6

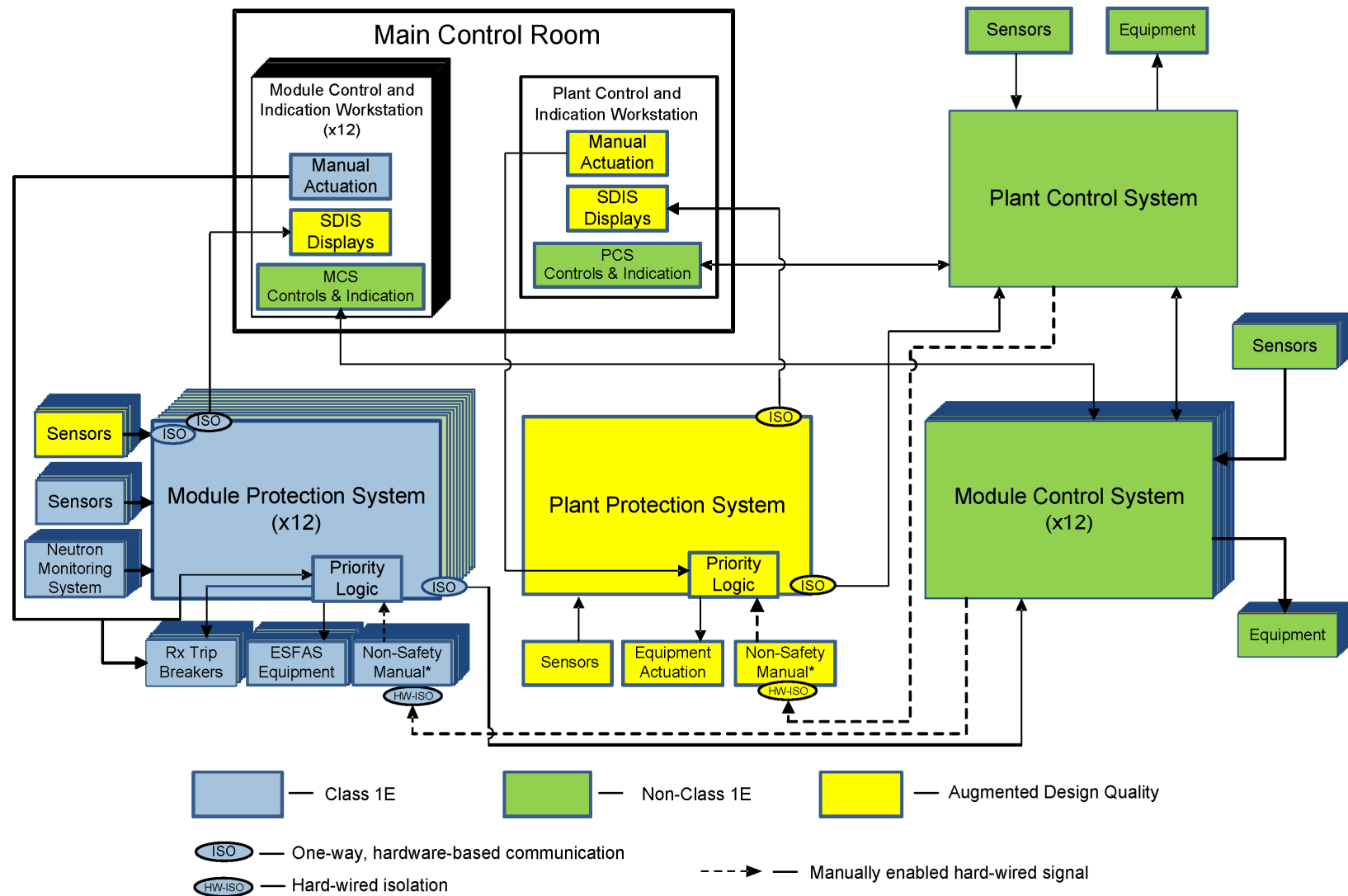


Figure A-8. Overall I&C system architecture

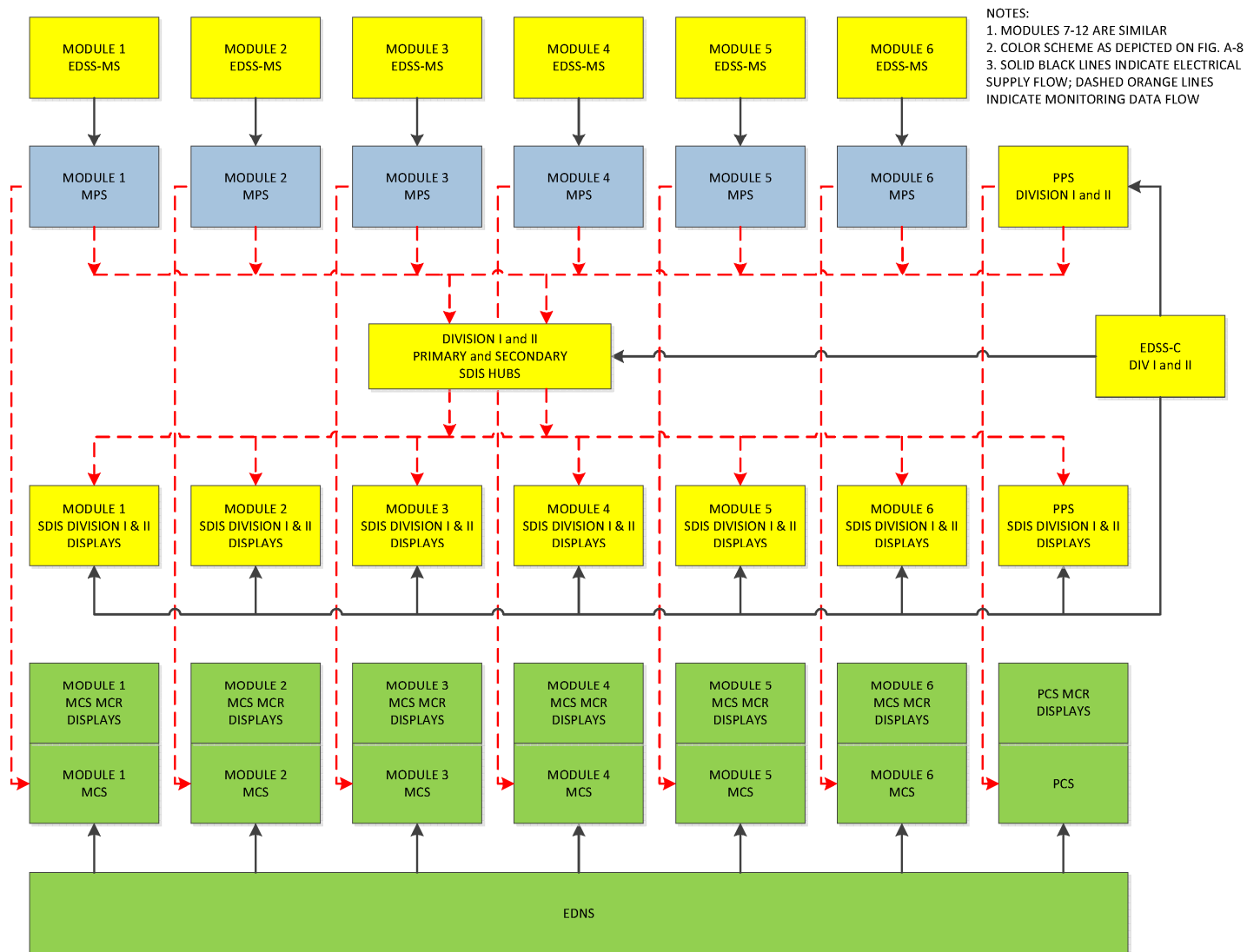


Figure A-9. Data display and associated electrical power sources

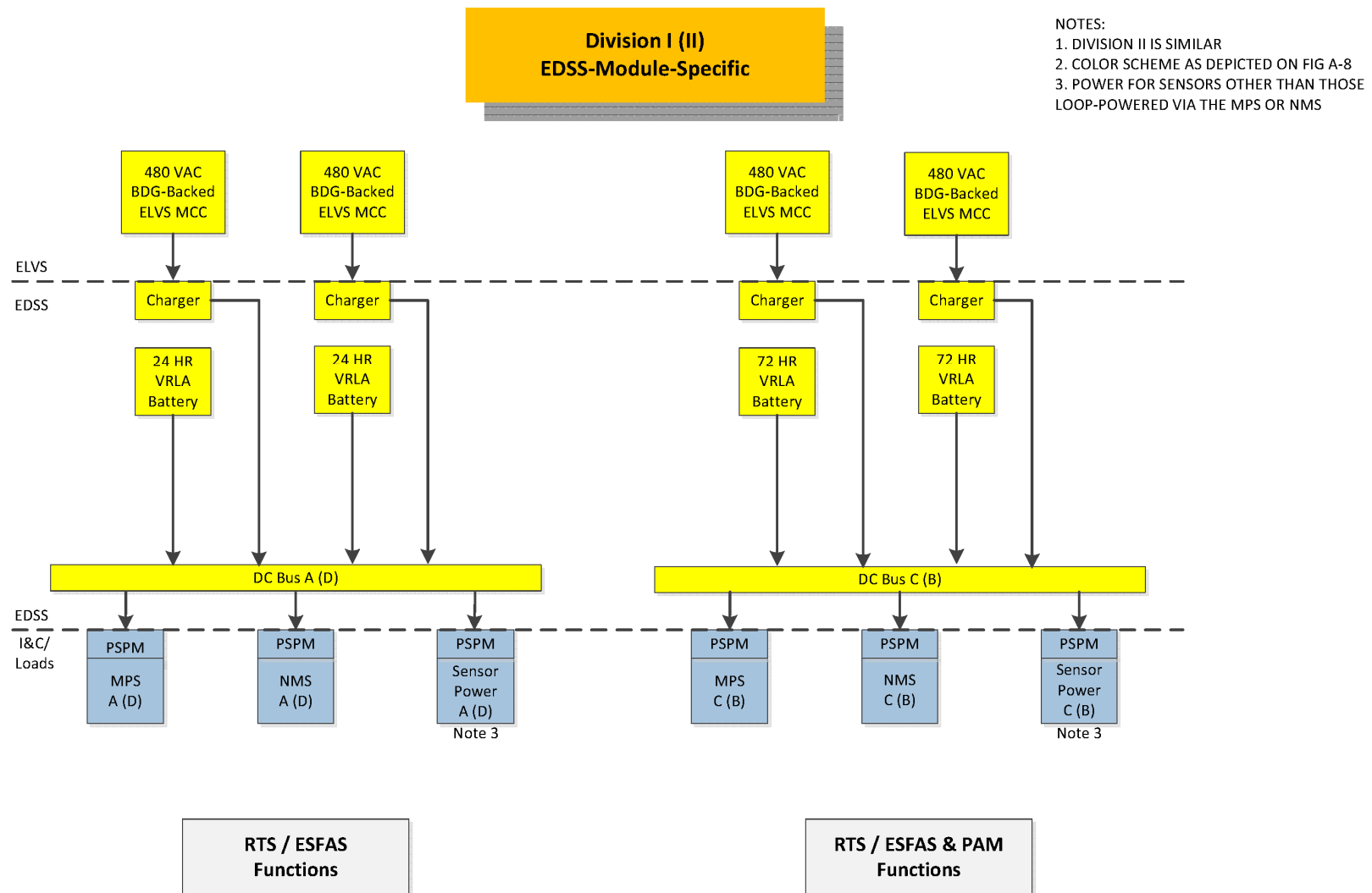


Figure A-10. Power supply power monitors – EDSS-MS

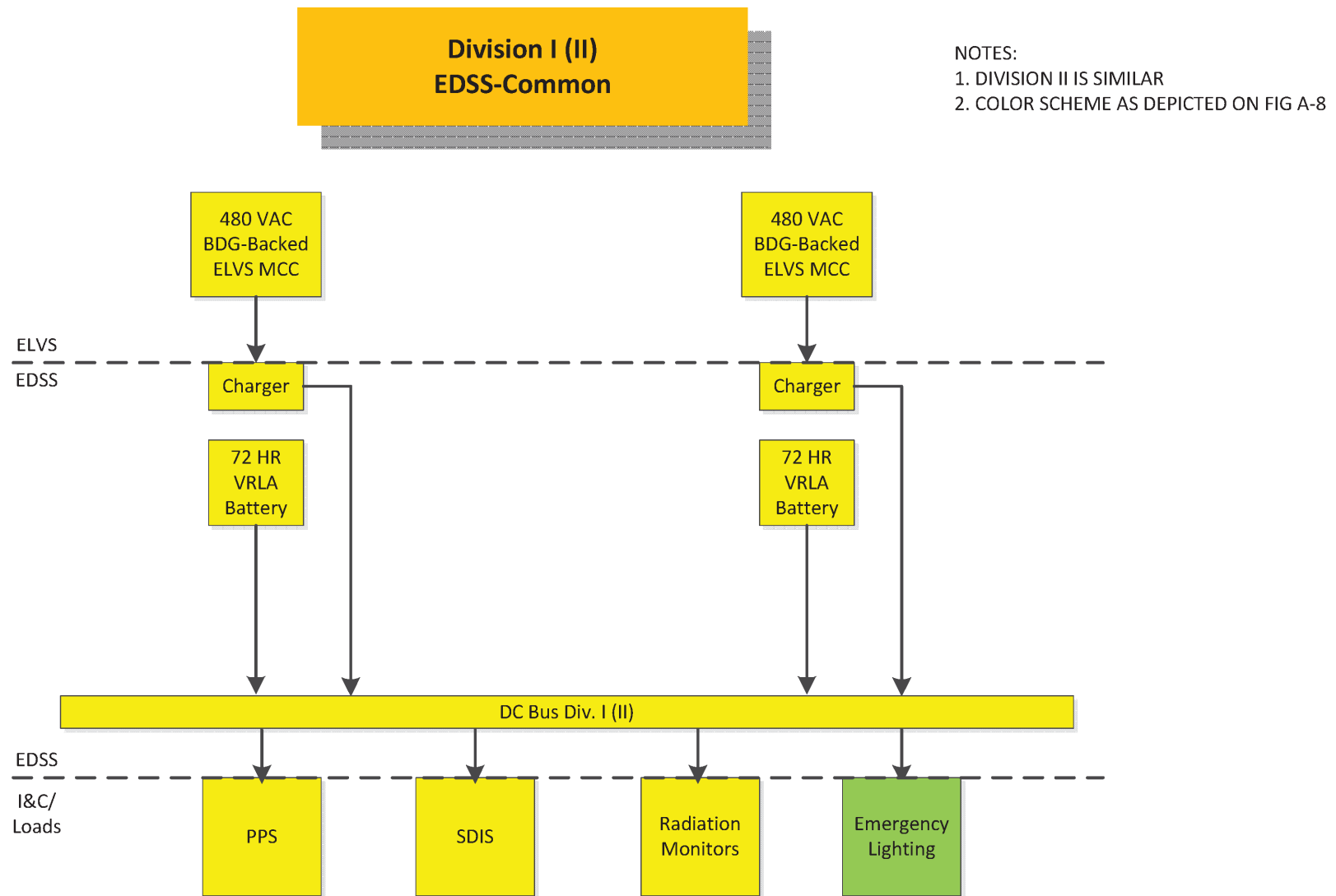


Figure A-11. Power supply power monitors – EDSS-C

Appendix B. Example Safety Classification Assessment for Electrical Systems

This appendix contains an example safety classification assessment to illustrate how the conditions of applicability included as Table 3-1 of the main body of this topical report would be used by future applicants, including NuScale. Specifically, this assessment provides an example of how the Table 3-1 conditions of applicability would be demonstrated based on an example small modular reactor passive power plant design. The safety classification assessment comprises the evaluation descriptions presented in Section B.2.

The information provided in this appendix is only an example of a safety classification assessment provided to facilitate: (1) the NRC's review of the conditions of applicability and augmented provisions for which approval is sought; and (2) an understanding of how this topical report would be implemented by future applicants (including NuScale). As part of the scope of this topical report, NuScale is not seeking NRC approval of the information in this appendix, as the details specific to the final NuScale power plant design are presented in the NuScale design certification application (DCA).

B.1 Approach/Methodology

The methodology applied in the example safety classification assessment (Section B.2) is as described in Section 3 in the main body of this topical report..

B.2 Assessment Evaluations

The “function-by-function” safety classification evaluations are described in Subsections B.2.1 through B.2.7. These assessment evaluations demonstrate that the design fully meets the Table 3-1, Section I, conditions of applicability. Specifically, with the passive power plant's non-reliance on electrical power and operator action, the electrical power systems do not fulfill functions that per the regulatory definitions of “safety-related” and “Class 1E” justify a Class 1E classification.

To properly assess the role of electrical power for each system/function, the evaluation process inherently involves consideration of the impact that a hypothetical complete loss of all electrical power – both AC and DC – would have on the system/function being evaluated. This process requires a general understanding of the response of plant systems during such a scenario. To facilitate the assessment, Table B-1 provides a concise overview of the response of plant systems or components to a hypothetical scenario in which all AC and DC power is lost simultaneously. The system response actions compiled in Table B-1, as well as overall plant response detail, are further described in Appendix D of this topical report. Appendix D confirms the conclusions reached in the safety classification evaluations provided in this section.

B.2.1 Power Module Safety Functions

Power module safety functions include the processes or conditions essential to maintaining the following within acceptable limits established for a design basis event:

- Safe shutdown
- Core cooling
- Containment vessel isolation and integrity
- Reactor coolant pressure boundary integrity

B.2.1.1 Reactor Trip

{{

}}^{2(a),(c)}

{{

}}^{2(a),(c)}

B.2.1.2 Reactor Coolant Makeup and Poison Addition

{{

}}^{2(a),(c)}

B.2.1.3 Core Cooling

{{

}}^{2(a),(c)}

{{

}}^{2(a),(c)}

{{

}}^{2(a),(c)}

{{

}}^{2(a),(c)}

{{

}}^{2(a),(c)}

B.2.1.4 Containment Isolation

{{

}}^{2(a),(c)}

{{

}}^{2(a),(c)}

B.2.1.5 Containment Vessel Integrity

{{

}}^{2(a),(c)}

{{

}}^{2(a),(c)}

B.2.1.6 Fission Product Control

{{

}}^{2(a),(c)}

B.2.1.7 Reactor Coolant Pressure Boundary Integrity

{{

}}^{2(a),(c)}

{{

}}^{2(a),(c)}

B.2.2 Fuel Assembly Cooling – Spent Fuel and Module Core Refueling

{{

}}^{2(a),(c)}

{{

}}^{2(a),(c)}

B.2.3 Control Room Habitability

{{

}}^{2(a),(c)}

B.2.4 Cooling for Building Areas Containing Safety-Related Equipment

{{

}}^{2(a),(c)}

B.2.5 Reactor Building Ventilation

{{

}}^{2(a),(c)}

{{

}}^{2(a),(c)}

B.2.6 Emergency Lighting

{{

}}^{2(a),(c)}

{{

}}^{2(a),(c)}

{{

}}^{2(a),(c)}

B.2.7 Post-Accident Monitoring

{{

}}^{2(a),(c)}

{{

}}^{2(a),(c)}

{{

}}^{2(a),(c)}

{{

}}^{2(a),(c)}

B.3 Conclusions

Based on the example safety classification assessment described in Section B.2 above, it is concluded that the example design fully meets the conditions of applicability in Table 3-1 in the main body of this topical report. This conclusion is based on the advanced passive design wherein neither electrical power nor operator action is necessary to ensure safety-related functions in response to a design basis event. With this non-reliance on electrical power and operator action, the electrical power systems do not fulfill functions that per the regulatory definitions of “safety-related” and “Class 1E” justify a Class 1E classification.

© Copyright 2018 by NuScale Power, LLC

Appendix C. Example Failure Modes and Effects Analysis – Highly Reliable DC Power System

C.1 Introduction

Table C-1 documents an example failure modes and effects analysis (FMEA) of the highly reliable DC power system (EDSS). The FMEA documented in Table C-1 is the first general step of a reliability analysis effort intended to confirm that the EDSS design adequately satisfies single failure criterion guidance to the extent described in Table 3-2 of the main body of this report. The FMEA considers the effect of conceivable failures within an EDSS-MS or within the EDSS-C on the ability of that system to perform its function (i.e., to provide electrical power to EDSS loads). Also addressed is the effect of each failure on the performance of plant safety-related system functions.

The information provided in this appendix is only an example of an FMEA provided to facilitate: (1) the NRC's review of the conditions of applicability and augmented provisions for which approval is sought; and (2) an understanding of how this topical report would be implemented by future applicants (including NuScale). As part of the scope of this topical report, NuScale is not seeking NRC approval of the information in this appendix, as the details specific to the final NuScale power plant design are presented in the NuScale design certification application (DCA).

C.2 Summary Conclusions

The FMEA documented in Table C-1 conservatively assumes that each component single failure occurs concurrently with the unavailability of the redundant EDSS channel (for EDSS-MS) or division (for EDSS-C). However, the FMEA results show that even with this conservative assumption, there is no conceivable failure that could prevent safety-related functions from being achieved and maintained. With the redundant EDSS channel/division conservatively assumed to be unavailable, there are certain failures that have the potential to result in actuation of safety-related systems. However, under normal operating conditions wherein all EDSS channels/divisions are available, there is no conceivable failure that would result in potential actuation of safety-related functions.

The example EDSS FMEA results are provided in the following Table C-1.

Table C-1. Example failure modes and effects analysis for highly reliable DC power system (EDSS) – sample summary results

Component Identification	Function	Failure Description (Note 1)		Effects Description (Note 2)		Method of Failure Detection	Remarks
		Failure Mode	Failure Mechanism	Effect on EDSS	Effect on Interfacing Safety-Related Systems		
Battery Charger 00-EDS-BYC-1003A 00-EDS-BYC-1003B 01-EDS-BYC-1003A 01-EDS-BYC-1003B 01-EDS-BYC-2003A 01-EDS-BYC-2003B 01-EDS-BYC-3003A 01-EDS-BYC-3003B 01-EDS-BYC-4003A 01-EDS-BYC-4003B	Provide 125 Vdc power to DC switchgear while maintaining battery charge.	No output	Charger fault; failure of internal components including AC input breaker, DC output breaker, resistors, silicon-controlled rectifiers (SCRs), transformer, relays, fuses, diodes, voltage regulators, etc.; misuse; design deficiency; quality defect.	(A) System load supplied by redundant charger of affected channel/division.	(A, B) None.	Main control room (MCR) alarm for battery charger AC power failure, DC output failure, and low DC output voltage; local indication of battery charger output voltage and current	Acceptable. No conceivable single failures result in loss of interfacing safety-related system functions. All failures are detectable. * Conservatively assumes worst-case condition described in Note 1; else, this failure would not result in actuation of safety-related functions. ** Assumes worst-case loss of both linked chargers to account for differences in manufacturer designs. Final design may result in the loss of a single battery charger following failure of communication link.
		Loss of input		(B) None.			
		Low output		(A) Redundant charger available to compensate on affected channel/division. (B) None.	(A, B) None.		
		Erratic output		(A) If fluctuations are outside the capability of redundant charger to compensate, EDSS channel/division operates at abnormal voltage levels. (B) None.	(A) If fluctuations exceed power supply power monitor (PSPM) setpoints, EDSS channel/division isolated from safety-related loads, and safety-related functions are actuated.* (B) None.	Fluctuating local/MCR indication; periodic testing.	
		High output voltage		(A) Associated channel/division operates at elevated voltage. (B) None.	(A) If voltage exceeds PSPM setpoints, EDSS channel/division isolated from safety-related loads, and safety-related functions are actuated.* (B) None.	MCR high DC bus voltage alarm; elevated local/MCR bus voltage indication; periodic testing.	
		Loss of communication link		(A) Battery chargers on affected channel/division nonfunctional, batteries begin discharging.** (B) None.	(A, B) None. Uninterrupted power provided to safety-related loads from the batteries.	MCR battery charger failure alarm; battery discharge alarm from battery monitor.	

Component Identification	Function	Failure Description (Note 1)		Effects Description (Note 2)		Method of Failure Detection	Remarks
		Failure Mode	Failure Mechanism	Effect on EDSS	Effect on Interfacing Safety-Related Systems		
Battery 00-EDS-BTY-1001A 00-EDS-BTY-1001B 01-EDS-BTY-1001A 01-EDS-BTY-1001B 01-EDS-BTY-2001A 01-EDS-BTY-2001B 01-EDS-BTY-3001A 01-EDS-BTY-3001B 01-EDS-BTY-4001A 01-EDS-BTY-4001B	Supply power to 125 Vdc switchgear and various loads.	No output	Battery fault; container cracks; dryout of cell; excessive temperature; thermal runaway; high cycling rates; defective post seals; strap corrosion; excessive plate sulfation/growth; post/connection hardware problems; personnel error; design deficiency; quality defect.	(A) None. Uninterrupted power provided to safety-related loads from the battery chargers. (B) System load supplied by redundant battery of affected channel/division.	(A, B) None.	MCR DC bus undervoltage and low battery voltage alarms; local and MCR battery voltage/current indication; periodic testing.	Acceptable. No conceivable single failures result in safety-related system actuation or loss of interfacing safety-related system functions. All failures are detectable.
125Vdc Switchgear/Bus 00-SWG-S-4001 00-SWG-S-4002 01-SWG-S-4011A 01-SWG-S-4011B 01-SWG-S-4011C 01-SWG-S-4011D 00-BUS-S-4001 00-BUS-S-4002 01-BUS-S-4011A 01-BUS-S-4011B 01-BUS-S-4011C 01-BUS-S-4011D	Supply 125 Vdc to various loads.	No input	Grounding of positive or negative leg; bus fault; personnel error; design deficiency; quality defect.	(A, B) Affected channel/division becomes nonfunctional.	(A, B) Affected channel/division no longer supplies power to loads, and safety-related functions are actuated.*	MCR alarm for DC system ground; periodic testing.	Acceptable. No conceivable singe failures result in loss of interfacing safety-related system functions. All failures are detectable. Power remains available with a single ground. * Conservatively assumes worst-case condition described in Note 1; else, this failure would not result in actuation of safety-related functions.
		Bus failure					
Fused Transfer Switch (XSW) 00-EDS-XSW-1001A 00-EDS-XSW-1001B 01-EDS-XSW-1001A 01-EDS-XSW-1001B 01-EDS-XSW-2001A 01-EDS-XSW-2001B 01-EDS-XSW-3001A 01-EDS-XSW-3001B 01-EDS-XSW-4001A 01-EDS-XSW-4001B	Provide continuity or point isolation from battery, test connection, or battery charger.	Inadvertent opening (blown fuse)	Wear, fatigue, deformation, degradation of fuse holder; corrosion; oxidation; equipment load cycling; heat generated by surrounding components; embrittlement of fuse element; personnel error; design deficiency; quality defect.	(A) Reduced load on battery chargers. (B) System load supplied by redundant battery of affected channel/division.	(A, B) None.	MCR alarm on XSW open.	Acceptable. No conceivable single failures result in safety-related system actuation or loss of interfacing safety-related system functions. All failures are detectable.
		Fails to interrupt		(A, B) Fusible disconnect located between XSW and DC bus available to clear/interrupt.		MCR alarm on disconnect switch open; periodic testing.	

Component Identification	Function	Failure Description (Note 1)		Effects Description (Note 2)		Method of Failure Detection	Remarks
		Failure Mode	Failure Mechanism	Effect on EDSS	Effect on Interfacing Safety-Related Systems		
Battery Monitor 00-EDS-CP-1001A 00-EDS-CP-1001B 01-EDS-CP-1001A 01-EDS-CP-1001B 01-EDS-CP-2001A 01-EDS-CP-2001B 01-EDS-CP-3001A 01-EDS-CP-3001B 01-EDS-CP-4001A 01-EDS-CP-4001B	Continuously monitor performance characteristics of battery system.	High output parameter/ indication/ alarm	Device failure; misuse; design deficiency; quality defect.	(A, B) Erroneous local and MCR indication/alarms related to affected battery. Affected battery and unaffected battery and its monitor remain available to the channel/division.	(A, B) None.	Abnormal battery indication; periodic testing.	Acceptable. No conceivable single failures result in safety-related system actuation or loss of interfacing safety-related system functions. All failures are detectable.
		Low output parameter/ indication/ alarm					
		Output parameter/ indication fails as-is					
		Loss of output/ indication/ alarm function		(A, B) Loss of local and MCR indication/alarms related to affected battery. Affected battery and unaffected battery and its monitor remain available to the channel/division.			
Fusible Disconnect Division I, Bus-to-Load Division II, Bus-to-Load	Provide circuit continuity and protection between DC bus and associated loads.	Spurious operation (blown fuse)	Wear, fatigue, deformation, degradation of fuse holder; corrosion; oxidation; equipment load cycling; heat generated by surrounding components; embrittlement of fuse element; misuse; design deficiency; quality defect.	(A, B) Loss of ability of the channel/division to supply power to loads on the affected circuit.	(A, B) Channel/division no longer supplies power to loads on affected circuit. Safety-related functions may be actuated.*	Inspection of disconnect switch; periodic testing.	Acceptable. No conceivable single failures result in loss of interfacing safety-related system functions. All failures are detectable. * Conservatively assumes worst-case condition described in Note 1; else, this failure would not result in potential actuation of safety-related functions. ** Does not consider failure of fusible disconnect concurrent with a fault/failure outside the boundaries of the EDSS (e.g. downstream of qualified PSPM).
		Fails to close		(A) Continued loading on battery chargers.** Upstream protection devices available to open/ interrupt.		(A, B) None. Affected channel/division isolated from safety system by PSPM, if required.	
		Fail to open		(B) Continued loading on batteries.** Upstream protection devices available to open/interrupt.		Inspection of associated plant load; periodic testing.	
		Fails to interrupt on opening					

Component Identification	Function	Failure Description (Note 1)		Effects Description (Note 2)		Method of Failure Detection	Remarks
		Failure Mode	Failure Mechanism	Effect on EDSS	Effect on Interfacing Safety-Related Systems		
Fusible Disconnect Division I, Charger-to-Bus Division II, Charger-to-Bus	Provide circuit continuity and protection between battery charger and DC bus.	Spurious operation (blown fuse)	Wear, fatigue, deformation, degradation of fuse holder; corrosion; oxidation; equipment load cycling; heat generated by surrounding components; embrittlement of fuse element; misuse; design deficiency; quality defect.	(A) Loss of ability to supply channel/division DC bus from affected battery charger. DC bus remains powered from redundant battery charger.	(A, B) None.	MCR alarm on switch open and low/no battery charger output; Local indication of battery charger output voltage and current.	Acceptable. No conceivable single failures result in safety-related system actuation or loss of interfacing safety-related system functions. All failures are detectable.
		Fails to close		(B) None.		Personnel attention while operating (manual) disconnect switch.	
		Fail to open		(A) Continued loading on battery charger. Upstream battery charger output breaker available to open/interrupt.		MCR alarm on battery charger output breaker open. Local indication of battery charger output voltage and current; periodic testing.	
		Fails to interrupt on opening		(B) None. Upstream battery charger output breaker available to open/interrupt.			
Fusible Disconnect Division I, XSW-to-Bus Division II, XSW-to-Bus	Provide circuit continuity and protection between battery XSW and DC bus.	Spurious operation (blown fuse)	Wear, fatigue, deformation, degradation of fuse holder; corrosion; oxidation; equipment load cycling; heat generated by surrounding components; embrittlement of fuse element; misuse; design deficiency; quality defect.	(A) Reduced load on battery chargers.	(A, B) None.	MCR alarm on switch open. Local indication of battery (charge) current.	Acceptable. No conceivable single failures result in safety-related system actuation or loss of interfacing safety-related system functions. All failures are detectable.
		Fails to close		(B) System load supplied by redundant battery of affected channel/division.		Personnel attention while operating (manual) disconnect switch.	
		Fail to open		(A) Continued float charging of battery. Upstream XSW located between battery and fusible disconnect available to open/interrupt.		MCR alarm on XSW open; periodic testing.	
		Fails to interrupt on opening		(B) Continued loading on battery. Upstream XSW located between battery and fusible disconnect available to open/interrupt.			

Component Identification	Function	Failure Description (Note 1)		Effects Description (Note 2)		Method of Failure Detection	Remarks
		Failure Mode	Failure Mechanism	Effect on EDSS	Effect on Interfacing Safety-Related Systems		
Conductor Division I (EDSS-C), Bus-to-Load Division II (EDSS-C), Bus-to-Load Channel A (EDSS-MS), Bus-to-Load Channel B (EDSS-MS), Bus-to-Load Channel C (EDSS-MS), Bus-to-Load Channel D (EDSS-MS), Bus-to-Load	Maintain circuit integrity between termination points.	Loss of conductor continuity	Failed structural support, insulation degradation, physical damage to conductor or connector; misuse; design deficiency; quality defect.	(A, B) Loss of ability of the channel/division to supply power to loads on the affected circuit.	(A, B) Channel/division no longer supplies power to loads on affected circuit. Safety-related functions may be actuated.*	Inspection of conductor; periodic testing.	Acceptable. No conceivable single failures result in loss of interfacing safety-related system functions. All failures are detectable. * Conservatively assumes worst-case condition described in Note 1; else, this failure would not result in potential actuation of safety-related functions.
		Conductor to external ground short circuit				MCR alarm on ground fault detection; periodic testing.	
		Loss of insulation resistance				Periodic testing.	
		Hot short		(A) Continued loading on battery chargers. (B) Continued loading on batteries.	(A, B) None. EDSS isolated from safety system by PSPM, if required.	Inspection of associated plant load; periodic testing.	
Conductor Division I (EDSS-C), Charger-to-Bus Division II (EDSS-C), Charger-to-Bus Channel A (EDSS-MS), Charger-to-Bus Channel B (EDSS-MS), Charger-to-Bus Channel C (EDSS-MS), Charger-to-Bus Channel D (EDSS-MS), Charger-to-Bus	Maintain circuit integrity between termination points.	Loss of conductor continuity	Failed structural support, insulation degradation, physical damage to conductor or connector; misuse; design deficiency; quality defect.	(A) System load supplied by redundant charger of affected channel/division. (B) None.	(A, B) None.	MCR alarm on battery charger low/no DC output; local indication of battery charger output current and voltage.	Acceptable. No conceivable single failures result in safety-related system actuation or loss of interfacing safety-related system functions. All failures are detectable.
		Conductor to external ground short circuit				MCR alarm on ground fault detection; periodic testing.	
		Loss of insulation resistance				Periodic testing.	
		Hot short		(A, B) None.		Local/MCR indication; periodic testing.	

Component Identification	Function	Failure Description (Note 1)		Effects Description (Note 2)		Method of Failure Detection	Remarks
		Failure Mode	Failure Mechanism	Effect on EDSS	Effect on Interfacing Safety-Related Systems		
Conductor Division I (EDSS-C), Battery-to-Bus Division II (EDSS-C), Battery-to-Bus Channel A (EDSS-MS), Battery-to-Bus Channel B (EDSS-MS), Battery-to-Bus Channel C (EDSS-MS), Battery-to-Bus Channel D (EDSS-MS), Battery-to-Bus	Maintain circuit integrity between termination points.	Loss of conductor continuity	Failed structural support, insulation degradation, physical damage to conductor or connector; misuse; design deficiency; quality defect.	(A) Reduced load on battery chargers.	(A, B) None.	Battery monitor alarm; local indication of battery (charge) current; periodic testing.	Acceptable. No conceivable single failures result in safety-related system actuation or loss of interfacing safety-related system functions. All failures are detectable.
		Conductor to external ground short circuit		(B) System load supplied by redundant battery of affected channel/division.		MCR alarm on ground fault detection; periodic testing.	
		Loss of insulation resistance				Periodic testing.	
		Hot short		(A, B) None.		Operator attention to local/MCR indication; periodic testing.	
Conductor Division I (EDSS-C), Charger-to-XSW Division II (EDSS-C), Charger-to-XSW Channel A (EDSS-MS), Charger-to-XSW Channel B (EDSS-MS), Charger-to-XSW Channel C (EDSS-MS), Charger-to-XSW Channel D (EDSS-MS), Charger-to-XSW	Maintain circuit integrity between termination points.	Loss of conductor continuity	Failed structural support, insulation degradation, physical damage to conductor or connector; misuse; design deficiency; quality defect.	(A, B) None.	(A, B) None.	Periodic testing.	Acceptable. No conceivable single failures result in safety-related system actuation or loss of interfacing safety-related system functions. All failures are detectable.
		Conductor to external ground short circuit					
		Loss of insulation resistance					
		Hot short					

NOTES:

1. This FMEA conservatively assumes that each component single failure occurs concurrently with the unavailability of the redundant channel (for EDSS-MS) or division (for EDSS-C) (e.g., for maintenance). Under normal conditions wherein all channels/divisions are available, this FMEA confirms that here is no failure that would result in potential actuation of or adversely affect the performance of safety-related functions.
2. Effects are described for the following plant operating conditions:

A – AC electrical power available to EDSS battery chargers

B – AC electrical power not available to EDSS battery chargers

Appendix D. Example Safety Analysis Results

This appendix contains example safety analysis results that illustrate how for the example small modular reactor passive plant design reflected in Appendix A and Appendix B, neither electrical power nor operator action is necessary to achieve and maintain reactor safety-related functions. The information provided in this appendix is only an example of safety analysis results provided to facilitate: (1) the NRC's review of the conditions of applicability and augmented provisions for which approval is sought; and (2) an understanding of how this topical report would be implemented by future applicants (including NuScale). As part of the scope of this topical report, NuScale is not seeking NRC approval of the information in this appendix, as the safety analyses specific to the final NuScale power plant design are presented in the NuScale design certification application (DCA).

D.1 Introduction

The example safety analysis results described in this appendix include example qualitative event descriptions that identify the various reactor systems and safety actuations credited to mitigate each postulated design basis event. Each event description is presented in Section D.2, and includes a brief text summary and an event diagram. The event diagrams illustrate the credited systems and actuations using a logic sequence that considers system responses both with and without electrical power. The event diagrams show that the systems credited during a design basis event with electrical power available are the same or are a subset of the systems credited for the design basis event coincident with a low or loss of power condition.

To provide additional context and detail on the overall transient event progressions reflected in the Section D.2 example event descriptions, two sample transients are selected where example calculated transient progression results are presented. The sample transient progression results are presented in Section D.3. These sample transient results illustrate the predicted reactor transient response that is qualitatively described in the event diagrams for a loss of normal feedwater event and an inadvertent reactor recirculation valve (RRV) opening event. These two events are selected to illustrate the effect of electrical power unavailability for a case where the initiating event does not result in emergency core cooling system (ECCS) actuation, and for a case where the initiating event results in ECCS actuation.

D.2 Example Qualitative Event Descriptions – System and Safety Actuations Credited for Design Basis Events

This section provides example event descriptions that summarize the reactor safety-related systems and actuation signals credited to respond to and mitigate design basis events. These event descriptions are based on the example electrical and I&C system designs described in Appendix A, and on the example small modular reactor passive plant design and safety system response characteristics described in the example safety classification assessment evaluations in Appendix B.

The credited systems and actuation signals are illustrated using event logic diagrams for each of the design basis events. Each event diagram outlines the event initiator and the various safety-related systems and actuation signals credited for event mitigation. Each diagram includes a logic branch point labeled “DC Power Available?” that divides the diagram between the systems and actuation signals credited for the event with DC power available and those credited with no DC power available.

The logic branch for no DC power available assumes the unavailability of both the example DC electrical systems and AC electrical systems described in Appendix A (i.e., assumes a loss of all electrical power). The systems and actuation signals credited in the logic branch for no DC power available are the same for each analyzed design basis event. Thus, to eliminate unnecessary duplication, the logic branch for no DC power available is presented in Figure D-1 and is not repeated in the individual event diagrams provided for each design basis event description. The system responses indicated in Figure D-1 are consistent with the example safety classification assessment descriptions in Appendix B, Section B.2.1, which summarize how reactor safety-related functions (e.g., core cooling, containment isolation, etc.) are achieved upon a loss of electrical power (both AC and DC). Additional detail of an example passive plant response to select design basis events concurrent with a complete loss of electrical power is provided in Section D.3

The systems and actuation signals credited in the logic branch for events wherein DC power is available are presented in the event diagrams that support the following subsections. These event diagrams support the descriptions in Appendix B, Section B.2.1, which summarize how with electrical power available, the example plant power module safety related functions may be initiated automatically by the module protection system (MPS) as a result of an engineered safety feature actuation (ESFAS) signal, or may be initiated manually by the main control room (MCR) operator. The event diagrams show that the systems credited during a design basis event with power are the same or are a subset of the systems credited for the design basis event coincident with a loss of electrical power condition (shown in Figure D-1).

D.2.1 Cooldown Events

This section presents the event diagrams for postulated overcooling events with the exception of the inadvertent opening of a steam generator (SG) pressure relief valve as discussed in Section D.2.1.4.

D.2.1.1 Decrease in Feedwater Temperature

A decrease in feedwater temperature will cause an overcooling of the reactor coolant system (RCS) and a resultant increase in reactor power due to the moderator temperature reactivity feedback. A sufficient overcooling event will result in a high power (flux) reactor trip, and rapid cooldown events may cause reactor trip due to a signal of high flux rate. The MPS design is such that the high flux and high flux rate trips also actuate the chemical and volume control system (CVCS) containment isolation valves, in order to mitigate a boron dilution event. Without the nonsafety-related makeup capability due to the isolated CVCS, normal cooling will result in RCS level shrinkage requiring the pressurizer (PZR) heater trip to protect the heater sheaths that are part of the reactor coolant pressure boundary (RCPB).

Figure D-2 shows the event diagram for the safety analysis event progression for a decrease in feedwater temperature with electrical power available. Figure D-1 shows the safety-related system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, CVCS isolation (as a subset of containment isolation actuation), and PZR heater trip.

D.2.1.2 Increase in Feedwater Flow

An increase in feedwater flow will cause an overcooling of the RCS and a resultant increase in reactor power due to the moderator temperature reactivity feedback. Sufficient increases in flow will eventually result in a high power (flux) reactor trip. Rapid increases in feedwater flow may also cause the high flux rate trip. The MPS design is such that the high flux and high flux rate trips also actuate the CVCS containment isolation valves, in order to mitigate a boron dilution event. Without the nonsafety-related makeup capability due to the isolated CVCS, normal cooling will result in RCS level shrinkage requiring the PZR heater trip to protect the heater sheaths that are part of the RCPB.

Figure D-3 shows the event diagram for the safety analysis event progression for an increase in feedwater flow with electrical power available. Figure D-1 shows the safety-related system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, CVCS isolation (as a subset of containment isolation actuation), and PZR heater trip.

D.2.1.3 Increase in Steam Flow

Small increases in normal steam flow will result in a slight depressurization of the secondary and a gradual overcooling of the RCS. The moderator temperature reactivity feedback will cause an increase in core power eventually resulting in a high flux reactor trip. Rapid increases in steam flow will result in a faster core power response and a more rapid steam depressurization resulting in either a power (flux) rate trip or low steam pressure signal. The latter will cause a decay heat removal system (DHRS) actuation in order to protect the DHRS/SG inventory from the depressurization transient. The MPS design is such that the high flux and high flux rate trips also actuate the CVCS containment isolation valves, in order to mitigate a boron dilution event. Without the nonsafety-related makeup capability due to the isolated CVCS, normal cooling will result in RCS level shrinkage requiring the PZR heater trip to protect the heater sheaths that are part of the RCPB.

Figure D-4 shows the event diagram for the safety analysis event progression for an increase in steam flow with electrical power available. Figure D-1 shows the safety-related system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, CVCS isolation (as a subset of containment isolation actuation), and PZR heater trip.

D.2.1.4 Inadvertent Opening of a Steam Generator Safety Valve

The example small modular reactor passive plant (see Appendix B) SG design is rated for the same pressure as the reactor pressure vessel (RPV). This design feature bounds the possible secondary pressures that could result from a steam generator tube failure or any of the other secondary overpressurization events. Therefore, a safety relief valve is not required in the example SG design.

D.2.1.5 Steam Line Break

The steam line break (SLB) event phenomena and associated MPS responses are different for a postulated SLB location inside containment and a postulated SLB location outside containment. Therefore, the two break locations are addressed separately as follows.

SLB Inside Containment

The SLB inside containment quickly causes a high containment vessel (CNV) pressure signal resulting in reactor trip, complete CNV isolation, and DHRS actuation. Normal DHRS actuation includes the closure of the feedwater isolation valves (FWIVs) and main steam isolation valves (MSIVs) in order to close the DHRS natural circulation loop. With the FWIV closures, the SLB event is mitigated in terms of mass and energy being released to containment. Without the nonsafety-related makeup capability due to the isolated CVCS as part of CNV isolation, DHRS cooling will result in RCS level shrinkage requiring the PZR heater trip to protect the heater sheaths that are part of the RCPB.

Figure D-5 shows the event diagram for the safety analysis event progression for a SLB inside containment with electrical power available. Figure D-1 shows the safety-related system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, DHRS actuation, and PZR heater trip.

SLB Outside Containment

The SLB outside containment will be quite similar to the increase in steam flow event in that smaller breaks cause the high power (flux) trip and larger breaks cause the low steam pressure trip. In the event of a smaller break, the low steam pressure signal will occur after the reactor trip on high flux or flux rate as the break will continue to depressurize the steam system. Valve alignments that are part of DHRS actuation include closure of the MSIVs and FWIVs, which mitigates the break release. Without the nonsafety-related makeup capability due to the isolated CVCS, DHRS cooling will result in RCS level shrinkage requiring the PZR heater trip to protect the heater sheaths that are part of the RCPB.

Figure D-6 shows the event diagram for the safety analysis event progression for a SLB outside containment with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, DHRS actuation, CVCS isolation (as a subset of containment isolation actuation), and PZR heater trip.

D.2.1.6 Loss of Containment Vessel Vacuum

The loss of CNV vacuum can be caused by a variety of initiators including various CNV flooding events or containment evacuation system (CES) malfunctions. These events generally lead to a mild cooldown of the RPV due to additional heat loss through the CNV. Reactor trip, containment isolation and DHRS are initiated on high CNV pressure ending the event. Without the nonsafety-related makeup capability due to the isolated CVCS, DHRS cooling will result in RCS level shrinkage requiring the PZR heater trip to protect the heater sheaths which are part of the RCPB.

Figure D-7 shows the event diagram for the safety analysis event progression for a loss of CNV vacuum with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, CNV isolation, DHRS actuation, and PZR heater trip.

D.2.2 Heatup Events

This section presents the event diagrams for postulated power module heatup events.

D.2.2.1 Loss of External Load

The loss of load, turbine trip, loss of condenser vacuum, and inadvertent closure of the turbine throttle valve, which controls steam pressure, are all very similar events for the power module. If the condenser is functional, the anticipated plant response to a loss of steam flow to the turbine would be an actuation of the nonsafety-related turbine bypass to continue full power operation of the power module until operators decide to power down the module or put the turbine back online. The conservative analysis assumes failure of the turbine bypass and therefore a loss of steam flow at the turbine causes an increase in pressure in the steam line and a loss of heat removal from the RCS. Depending on the rate of the decrease in steam flow, the high steam pressure, high steam superheat, or high PZR pressure trip will occur. Any of these signals will cause reactor trip and DHRS actuation. If the PZR pressurization is sufficient, the reactor safety valves (RSVs) may lift to ensure RPV pressure limits are not exceeded. The RSV blowdown will likely cause a high CNV pressure signal and a subsequent CNV isolation. Without the nonsafety-related makeup capability from the isolated CVCS, DHRS cooling will result in RCS level shrinkage requiring the PZR heater trip to protect the heater sheaths which are part of the RCBP.

Figure D-8 shows the event diagram for the safety analysis event progression for a loss of external load with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, DHRS actuation, and PZR heater trip.

D.2.2.2 Turbine Trip

Refer to Section D.2.2.1 for a description of this event. Figure D-9 shows the event diagram for the safety analysis event progression with power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, DHRS actuation, and PZR heater trip.

D.2.2.3 Loss of Condenser Vacuum

Refer to Section D.2.2.1 for a description of this event. Figure D-10 shows the event diagram for the safety analysis event progression with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, DHRS actuation, and PZR heater trip.

D.2.2.4 Inadvertent Closure of an Main Steam Isolation Valve

Inadvertent closure of one MSIV will cause a complete loss of heat removal in one SG and a diversion of FW flow to the other SG which will cause a high RCS pressure or temperature signal resulting in reactor trip and DHRS actuation. If the event initiator is the closure of both MSIVs, then a high steam pressure or superheat signal will initiate reactor trip and DHRS actuation. If the PZR pressurization is sufficient, the RSVs may lift to ensure RPV pressure limits are not exceeded. The RSV blowdown will likely cause a high CNV pressure signal and a subsequent CNV isolation. Without the nonsafety-related makeup capability from the isolated CVCS, DHRS cooling will result in RCS level shrinkage requiring the PZR heater trip to protect the heater sheaths that are part of the RCPB.

Figure D-11 shows the event diagram for the safety analysis event progression with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, DHRS actuation and PZR heater trip.

D.2.2.5 Inadvertent Closure of the Turbine Throttle Valve

Refer to Section D.2.2.1 for a description of this event. Figure D-12 shows the event diagram for the safety analysis event progression with power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, DHRS actuation, and PZR heater trip.

D.2.2.6 Loss of Alternating Current (AC) Power

Loss of AC power will result in a combination of a turbine trip and loss of feedwater event. Nominal plant response is expected to immediately trip the reactor through the nonsafety-related plant control system (PCS). MPS will not actuate until the heatup event causes a high PZR or steam pressure or high superheat signal, at which point reactor trip and DHRS will actuate. If the PZR pressurization is sufficient, the RSVs may lift to ensure RPV pressure limits are not exceeded. The RSV blowdown will likely cause a high CNV pressure signal and a subsequent CNV isolation. Without the nonsafety-related makeup capability from the isolated CVCS, DHRS cooling will result in RCS level shrinkage requiring the PZR heater trip to protect the heater sheaths that are part of the RCPB.

Figure D-13 shows the event diagram for the safety analysis event progression with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, DHRS actuation, and PZR heater trip.

D.2.2.7 Loss of Normal Feedwater

Loss of normal feedwater will cause a heatup of the RCS resulting in a high PZR pressure, high hot leg temperature, or high steam superheat signal, which will cause reactor trip and DHRS actuation. If the PZR pressurization is sufficient, the RSVs may lift to ensure RPV pressure limits are not exceeded. The RSV blowdown will likely cause a high CNV pressure signal and a subsequent CNV isolation. Without the nonsafety-related makeup capability from the isolated CVCS, DHRS cooling will result in RCS level shrinkage requiring the PZR heater trip to protect the heater sheaths that are part of the RCPB.

Figure D-14 shows the event diagram for the safety analysis event progression with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, DHRS actuation and PZR heater trip.

D.2.2.8 Inadvertent Actuation of Decay Heat Removal System

Inadvertent opening of a DHRS valve at full power is a minor version of a loss of normal feedwater as the pressure drop across the SG is higher than DRHS causing a FW flow diversion path. The gradual heatup of the RCS will result in a high PZR pressure or high hot leg temperature signal, which will cause a reactor trip. If the PZR pressurization is sufficient, the RSVs may lift to ensure RPV pressure limits are not exceeded. The RSV blowdown will likely cause a high CNV pressure signal and a subsequent CNV isolation. Without the nonsafety-related makeup capability from the isolated CVCS, DHRS cooling will result in RCS level shrinkage requiring the PZR heater trip to protect the heater sheaths that are part of the RCPB.

Figure D-15 shows the event diagram for the safety analysis event progression with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, DHRS actuation and PZR heater trip.

D.2.2.9 Feedwater Line Break

The feedwater line break (FWLB) event phenomena and associated MPS responses are different for a postulated FWLB location inside containment and a postulated FWLB location outside containment. Therefore, the two break locations are addressed separately as follows.

FWLB Inside Containment

The FWLB inside containment quickly causes a high CNV pressure signal resulting in reactor trip, complete CNV isolation, and DHRS actuation. Normal DHRS actuation includes the closure of the FWIVs and MSIVs in order to close the DHRS natural circulation loop. With the FWIV closures, the FWLB release is mitigated. Without the nonsafety-related makeup capability from the isolated CVCS as part of CNV isolation, DHRS cooling will result in RCS level shrinkage requiring the PZR heater trip to protect the heater sheaths that are part of the RCPB.

Figure D-16 shows the event diagram for the safety analysis event progression with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, DHRS actuation, and PZR heater trip.

FWLB Outside Containment

The FWLB outside of containment will be similar to the decrease in feedwater flow event. For smaller breaks, the high PZR pressure or high hot leg temperature is credited and for larger breaks, the low steam pressure trip may also be reached. All three MPS signals will result in reactor trip and DHRS actuation, which includes closure of both FWIVs, mitigating the break release. If the PZR pressurization is sufficient, the RSVs may lift to ensure RPV pressure limits are not exceeded. The RSV blowdown will likely cause a high CNV pressure signal and a subsequent CNV isolation. Without the nonsafety-related makeup capability from the isolated CVCS, DHRS cooling will result in RCS level shrinkage requiring the PZR heater trip to protect the heater sheaths that are part of the RCPB.

Figure D-17 shows the event diagram for the safety analysis event progression with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, DHRS actuation and PZR heater trip.

D.2.2.10 Pressurizer Heater Malfunction

A malfunction of the PZR heater control system that involves both sets of heaters fully energized results in an over-pressurization event. The reactor will trip and DHRS will actuate on high PZR pressure, but the MPS will not isolate the PZR heaters until sufficient mass is vented through the RSVs to sufficiently reduce PZR level to reach the PZR heater trip on low level. The RSV blowdown will cause a high CNV pressure signal and a subsequent CNV isolation.

Figure D-18 shows the event diagram for the safety analysis event progression with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, DHRS actuation and PZR heater trip.

D.2.3 Increase in RCS Inventory

D.2.3.1 Pressurizer Level Control System Malfunction

Inadvertent CVCS makeup is slow but the overall transient response is dependent on whether the nonsafety-related PZR spray system is assumed functional. Since makeup capacity is small, the PZR level will slowly rise, collapsing the PZR vapor space and resulting in a pressure increase. If the spray system is functional, the pressure increase will be mitigated by the PZR spray system, resulting in an eventual high PZR level signal which trips the reactor and isolates the CVCS, ending the event. Without the nonsafety-related makeup capability due to the isolated CVCS, normal or DHRS cooling will result in RCS level shrinkage requiring the PZR heater trip to protect the heater sheaths which are part of the RCPB.

If PZR spray is not assumed functional, the level rise collapses the PZR vapor space, eventually causing a high PZR pressure signal which trips the reactor and actuates DHRS. Reactor trip in combination with DHRS actuation causes a short-term loss of RCS flow and results in a low RCS flow signal. This isolates the CVCS valves, ending the event. Without the nonsafety-related makeup capability due to the isolated CVCS, DHRS cooling will result in RCS level shrinkage requiring the PZR heater trip to protect the heater sheaths that are part of the RCPB.

Figure D-19 shows the event diagram for the safety analysis event progression with PZR spray and electrical power available. Figure D-20 shows the event diagram for the safety analysis event progression with PZR spray not available and electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable for both scenarios. These safety-related system actuations include reactor trip, DHRS actuation, CVCS isolation (as a subset of containment isolation actuation), and PZR heater trip.

D.2.3.2 Pressurizer Spray System Malfunction

The PZR spray system malfunction is a postulated transient where the nonsafety-related PZR pressure control system malfunctions and actuates the PZR spray. The PZR spray system functions by diverting flow from the CVCS injection line to the PZR spray line, which collapses the PZR vapor space causing a drop in RCS pressure. The nominal plant response would be to activate the PZR heaters to maintain pressure. However, if the PZR heaters do not function or are insufficient to maintain pressure, then the PZR pressure will drop until the low PZR pressure MPS signal trips the reactor, closes all CNV isolation valves, and actuates DHRS. As part of CNV isolation, the PZR spray lines would be isolated, ending the event. Without the nonsafety-related makeup capability due to the isolated CVCS, DHRS cooling will result in RCS level shrinkage requiring the PZR heater trip to protect the heater sheaths that are part of the RCPB.

Figure D-21 shows the event diagram for the safety analysis event progression with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, DHRS actuation, CVCS isolation (as a subset of containment isolation actuation), and PZR heater trip.

D.2.4 Reactivity Events

D.2.4.1 Uncontrolled Control Rod Bank Withdrawal – Low Power or Subcritical Conditions

The uncontrolled control rod bank withdrawal at low power or subcritical conditions is a rapid reactivity event that generally relies on low power range detection to mitigate. The MPS design has a log power rate trip and a partial power high flux trip at 25 percent power. These are credited for the rapid power rate increase events. Slower power increases will result in RCS expansion causing a reactor trip and DHRS actuation on high pressure. The MPS design is such that the high flux and high flux rate trips also actuate closure the CVCS containment isolation valves, in order to mitigate a boron dilution event. Without the nonsafety-related makeup capability due to the isolated CVCS, normal or DHRS cooling will result in RCS level shrinkage requiring the PZR heater trip to protect the heater sheaths that are part of the RCPB.

Figure D-22 shows the event diagram for the safety analysis event progression with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, DHRS actuation, CVCS isolation (as a subset of containment isolation actuation), and PZR heater trip.

D.2.4.2 Uncontrolled Control Rod Bank Withdrawal at Power

The uncontrolled control rod bank withdrawal at power is a less rapid reactivity event that generally relies on the high flux or flux rate trip. Slower power increases will cause an increase in RCS temperature, resulting in MPS signals due to high hot leg temperature or high PZR pressure that actuate reactor trip and DHRS operation. The MPS design is such that the high flux and high flux rate trips also actuate the CVCS containment isolation valves, in order to mitigate a boron dilution event. Without the nonsafety-related makeup capability due to the isolated CVCS, normal or DHRS cooling will result in RCS level shrinkage requiring the PZR heater trip to protect the heater sheaths that are part of the RCPB.

Figure D-23 shows the event diagram for the safety analysis event progression with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, DHRS actuation, CVCS isolation (as a subset of containment isolation actuation), and PZR heater trip.

D.2.4.3 Control Rod Misoperation

The control rod misoperation events considered include: (1) withdrawal of a single control rod; (2) drop of a single control rod; and (3) control rod misalignment. These events are addressed as follows.

Single Control Rod Withdrawal

The single rod withdrawal at power is similar to the bank withdrawal and relies on the high flux or flux rate trip. Slower power increases will cause an increase in RCS temperature, resulting in MPS signals due to high hot leg temperature or high PZR pressure that actuate reactor trip and DHRS operation. The MPS design is such that the high flux and high flux rate trips also actuate the CVCS containment isolation valves in order to mitigate a boron dilution event. Without the nonsafety-related makeup capability due to the isolated CVCS, normal or DHRS cooling will result in RCS level shrinkage requiring the PZR heater trip to protect the heater sheaths that are part of the RCPB.

Figure D-24 shows the event diagram for the safety analysis event progression with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, DHRS actuation, CVCS isolation (as a subset of containment isolation actuation), and PZR heater trip.

Control Rod Drop

A single control rod drop results in a reduction in reactor power and a skewed radial flux profile in the core, while a group (4) control rod drop results in a dramatic reduction in reactor power. The MPS response would include reactor trip and CVCS isolation as a result of a negative flux rate signal. Without the nonsafety-related makeup capability due to the isolated CVCS, normal cooling will result in RCS level shrinkage requiring the PZR heater trip to protect the heater sheaths that are part of the RCPB.

Figure D-25 shows the event diagram for the safety analysis event progression with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, CVCS isolation (as a subset of containment isolation actuation), and PZR heater trip.

Control Rod Misalignment

Control rod misalignment is addressed via analysis of the cycle-specific core design and extent of misalignment possibilities to demonstrate acceptable detection of the condition without reliance on a specific MPS response.

D.2.4.4 Inadvertent Cold Water Addition to the Reactor Coolant System

Inadvertent CVCS addition of cold water is a slow overcooling event that would most likely lead to a new steady-state condition; however, it could eventually result in a high flux or flux rate signal which will trip the reactor and isolate CVCS. Without the nonsafety-related makeup capability due to the isolated CVCS, normal cooling will result in RCS level shrinkage requiring the PZR heater trip to protect the heater sheaths that are part of the RCPB.

Figure D-26 shows the event diagram for the safety analysis event progression with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, CVCS isolation (as a subset of containment isolation actuation), and PZR heater trip.

D.2.4.5 Inadvertent Boron Dilution

An inadvertent boron dilution event is a slow reactivity insertion event that will eventually result in a high flux or flux rate signal that will trip the reactor and isolate the CVCS. Without the nonsafety-related makeup capability due to the isolated CVCS, normal cooling will result in RCS level shrinkage, requiring the PZR heater trip to protect the heater sheaths that are part of the RCPB.

Figure D-27 shows the event diagram for the safety analysis event progression with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, CVCS isolation (as a subset of containment isolation actuation), and PZR heater trip.

D.2.4.6 Fuel Assembly Misload

Fuel assembly misload is addressed via analysis of the cycle-specific core design and extent of misload possibilities to demonstrate acceptable detection of the condition without reliance on a specific MPS response.

D.2.4.7 Control Rod Ejection

Control rod ejection is a very fast reactivity insertion event that results in high power levels for a very short period of time. A rod ejection event will cause a reactor trip and CVCS isolation on high reactor flux. If a breach of the RCPB is considered, the high CNV pressure signal will also occur quickly, which results in CNV isolation and DHRS actuation. As the RCS break flow from the RPV to CNV continues, eventually the PZR heaters will trip off on low PZR level and the ECCS will actuate on low RCS level.

Figure D-28 shows the event diagram for the safety analysis event progression with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, CNV isolation, PZR heater trip, and ECCS actuation.

D.2.5 Decrease in Inventory

D.2.5.1 Spurious Opening of Reactor Safety Valve, Reactor Vent Valve, or Reactor Recirculation Valve

An inadvertently opened RSV, reactor vent valve (RVV), or reactor recirculation valve (RRV) results in a rapid high CNV pressure signal, which causes the MPS to trip the reactor, close the CNV isolation valves, and actuate the DHRS. As RCS level continues to decrease, the PZR heaters trip off on low PZR level, and the ECCS eventually actuates on low RCS level.

Figure D-29 shows the event diagram for the safety analysis event progression with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, CNV isolation, PZR heater trip and ECCS actuation.

D.2.5.2 Small Line Break Outside Containment

The event response due to a postulated RCS pipe break outside containment is dependent on break size and location. Double-ended guillotine breaks of the PZR spray system will rapidly cause a low PZR pressure signal which trips the reactor, isolates the CNV, and actuates the DHRS. Smaller CVCS breaks outside of CNV will result in a gradual level reduction causing a low PZR level reactor and PZR heater trip. Continued loss of inventory will result in a low-low PZR level trip or low PZR pressure trip signal, which will isolate the CNV and mitigate the release.

Figure D-30 shows the event diagram for the safety analysis event progression with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, CNV isolation, DHRS actuation, and PZR heater trip.

D.2.5.3 Steam Generator Tube Failure

The response to the SG tube failure event is a slow loss of RCS inventory to the SG, which eventually causes reactor trip and PZR heater trip upon receipt of a low PZR level signal. Continued loss of inventory will result in a low-low PZR level trip or low PZR pressure trip signal, which will isolate the CNV and actuate the DHRS to mitigate the release.

Figure D-31 shows the event diagram for the safety analysis event progression with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, CNV isolation, DHRS actuation, and PZR heater trip.

D.2.5.4 Loss of Coolant Accident

The response to an RCS pipe break is a rapid high CNV pressure signal which causes the MPS to trip the reactor, close the CNV isolation valves, and actuate the DHRS. As level continues to decrease, the PZR heaters trip off on low PZR level, and the ECCS eventually actuates on low RCS level.

Figure D-32 shows the event diagram for the safety analysis event progression with electrical power available. Figure D-1 shows the system actuations if electrical power, including DC power from the EDSS, is unavailable. These safety-related system actuations include reactor trip, CNV isolation, DHRS actuation, PZR heater trip, and ECCS actuation.

D.3 Example Transient Event Progressions With and Without Electrical Power

To provide additional context and detail on the example transient event progressions summarized in Section D.2 (with event diagrams), two sample transients are selected where example transient progressions are further described. Specifically, these descriptions reflect example calculations of the plant transient response that is qualitatively described in the Section D.2 event diagrams for a loss of normal feedwater event and an inadvertent RRV opening event. These scenarios are selected to illustrate the effect of power unavailability for a case where the initiating event does not result in ECCS actuation and for a case where the initiating event results in ECCS actuation, respectively.

The example transient event progressions described in this section consider the following cases:

1. Event with AC and DC power available. This is the normal anticipated response to a transient event.
2. Event with DC power available but loss of AC power. This is the normal anticipated response to a transient, assuming a concurrent loss of normal AC power supply.
3. Event without AC or DC power available. This is the response to a transient event, assuming that all electrical systems (i.e., both AC and DC electrical systems) are lost coincident with the event.

D.3.1 Example Loss of Normal Feedwater Transient

D.3.1.1 Loss of Feedwater Event Description and Sequence

LOFW with AC and DC Electrical Power Available

A loss of normal feedwater (LOFW) flow is an anticipated operational occurrence (AOO) which could be caused by a variety of initiators including valve failures, feedwater pump malfunctions, condensate pump malfunctions, or loss of power. A LOFW flow to the SGs will cause a reduction in SG level and increase in temperature in the RCS downcomer region due to decreased heat removal by the secondary system. The event diagram for a LOFW with electrical power available is provided in Figure D-14.

Based on the example MPS design (see Appendix A, Section A.2, and Appendix B, Section B.2), the primary indicator of a heatup event is increased PZR pressure. As the downcomer temperature increases, the RCS volume swells and causes a PZR liquid in-surge. The PZR in-surge compresses the PZR steam space, increasing PZR pressure. The rate of the pressure increase depends on the magnitude of FW flow reduction and the initial operating conditions. On indication of high PZR pressure, the MPS will actuate both a reactor trip and the DHRS as summarized in Section D.2.2.7 and illustrated in Figure D-14.

Actuation of the DHRS causes the opening of the DHRS valves and closure of the main steam containment isolation and main feedwater containment isolation valves. After the valves reposition, a closed loop is created between the SG secondary side and the DHRS condenser that is submerged in the reactor pool portion of the ultimate heat sink (UHS). Within a few minutes of DHRS actuation, the system pressurizes as vapor is generated in the SG tubes due to heat transfer from the primary RCS, and condenses in the DHRS condenser as heat is transferred to the UHS. As natural circulation flow in the DHRS is established, depending on the rate of RCS pressure increase in response to the initiating event, the RSVs may lift to vent vapor and relieve PZR pressure. The RSVs will automatically reseal once PZR pressure is no longer sufficient to keep the valve open. If the RCS pressure increase is sufficient, the RSVs ensure primary pressure limits are not exceeded, as identified in Figure D-14.

Upon establishing DHRS cooling, RCS pressure will decrease. If the normal control systems are operational, the PZR heaters will be energized to maintain normal RCS pressure. Without operator action, the PZR heaters will continue to function until DHRS cooling results in decreasing RCS temperatures and associated volume shrinkage such that the low PZR level is reached. As indicated in Figure D-14, when the low PZR level is reached, the MPS de-energizes the PZR heaters to maintain integrity of the heater sheaths, which are part of the RCPB. Without operator action to slow the cooldown rate or add inventory, the RCS level will continue to shrink until the low-low PZR level is reached, at which time the MPS will actuate CNV isolation. With power available, there will be no MPS signal to actuate ECCS, so the DHRS will continue to provide core cooling until operator action is taken.

Variations of this LOFW event sequence include decreases in feedwater flow where the PZR level swell and subsequent pressurization increase can be mitigated by the automatic PZR spray system. In this scenario, RCS average temperature would continue to rise until the high hot leg signal caused a reactor trip and DHRS actuation.

The event sequence for the LOFW event is typical of the heatup events except for the specific trip signal generated. For instance, rapid steam flow blockage events will likely generate a high steam pressure signal before the high PZR pressure signal. However, the subsequent event sequence of reactor trip, DHRS actuation, possible pressure relief via the RSVs, and eventual level shrinkage is typical of the heatup events.

The example MPS design specifies the high PZR pressure analytical limit at 2000 psia, the low PZR level analytical limit at 35 percent PZR level for PZR heater isolation, and the low-low PZR level analytical limit at 20 percent PZR level for CNV isolation. The analytical limit is the value credited in the example safety analysis.

LOFW Without AC or DC Electrical Power

In general, transient analyses evaluate a loss of power condition as either coincident with the initiating event or coincident with turbine trip, which is taken as the time of reactor trip for convenience. For the LOFW event, a coincident loss of the main AC electrical system and onsite DC electrical systems at the event initiation will cause automatic actuation of the mitigating safety-related systems. In this scenario, the LOFW heatup event will not develop because the reactor is tripped and DHRS is actuated at the start of the event rather than due to the high PZR pressure condition that is expected to occur in the nominal LOFW case where AC and DC power are available.

Loss of both AC and DC electrical systems coincident with the event actuates the mitigating safety-related systems, as they are designed to “fail safe” on the loss of power condition. As discussed in Appendix B, Section B.2.1, with normal power available, upon receiving the trip limit condition signal from safety sensors (using 2 of 4 logic), the MPS disconnects the EDSS DC power supply from the safety-related system actuators, causing the safety-related systems to actuate via stored potential energy. Therefore, if the loss of AC and DC power occurs at the time of the event, the loss of voltage (rather than the MPS signal) would result in reactor trip, DHRS actuation, and isolation of the PZR heaters at the beginning of the event. This is reflected in the loss of electrical power event diagram that is common to all events provided in Figure D-1.

The loss of electrical power condition will result in the actuation of containment isolation and the ECCS, which are two systems that are normally not expected to actuate for the LOFW event. Containment isolation at event initiation or at the time of reactor trip does not impact the identified safety-related systems that are credited for mitigating the LOFW event. Because the PZR heaters are de-energized at the time of loss of electrical power, the function of PZR level control is not required to protect the PZR heater sheaths that are part of the RCPB.

As indicated above, a LOFW with electrical power available would not result in ECCS actuation; however, the ECCS will actuate upon a loss of all electrical power. The RCS will be at high pressure (>1600 psia) at the time of ECCS actuation. Because of the ECCS actuator design, the passive inadvertent actuation block (IAB) on each ECCS valve would be actuated due to the high RCS pressure conditions. After the RCS pressure is sufficiently reduced by DHRS cooling, the IABs will release and the ECCS valves will open, resulting in a reduced blowdown to the CNV. Shortly after ECCS actuation, DHRS cooling is stopped because the loss of RCS level interrupts the natural circulation path of the RCS. At this point, normal ECCS core cooling is established to allow for decay heat removal from the reactor core.

In summary, Figure D-14 identifies the need for the reactor trip system (RTS), RSVs, DHRS, and PZR heater trip to mitigate the effects of a LOFW. Should a loss of all power occur coincident to the event or at the time of reactor trip, these systems will still actuate and function to bring the reactor to a safe, depressurized and cooled condition as shown in Figure D-1.

LOFW With AC Electrical Power Unavailable and DC Electrical Power Available

The LOFW event coincident with a loss of AC power but where DC electrical power is available results in either a nonsafety-related actuation of reactor trip by the plant control system (PCS) or normal MPS function where reactor trip and DHRS actuation will occur on the high PZR pressure or high temperature signal. If the loss of AC power is coincident with reactor trip then the functionality assumption of the nonsafety-related PCS low AC voltage signal has no impact on the event. The PCS reactor trip case will likely result in slower heatup as the core heat source is only decay heat and not fission power. However, in any case the LOFW without AC electrical power but with DC electrical power available will eventually follow a similar sequence as the power available event sequence (Figure D-14) with the exception that if AC power is not restored within 24 hours, the ECCS would actuate.

In summary, the difference in the LOFW event sequences for no electrical power available and for no AC power but DC electrical power available is the timing of ECCS actuation.

D.3.1.2 Example Loss of Feedwater Calculation Results

The purpose of this section is to summarize example NRELAP5 calculation results that support the LOFW event diagrams presented in Figure D-14 and Figure D-1. Figure D-33 contains a diagram of the event sequences for three event scenarios: (1) the nominal case where AC and DC power is available but no operator interventions are assumed; (2) the loss of AC power case where DC electrical power is available; and (3) the loss of both AC and DC electrical power where all safety-related systems are actuated immediately and ECCS valve opening is delayed for a short period due to the inadvertent actuation block.

In the first case presented in Figure D-33 where AC and DC power are available, DHRS and reactor trip are initiated with the high PZR pressure signal at around 20 seconds into the event. With DC electrical power available to hold the ECCS valves closed, DHRS cooling would continue as long as there was sufficient core decay heat to maintain RCS temperature to ensure level remained above the top of the RCS riser (hence maintaining the natural circulation path). In this particular scenario, the RSVs are assumed to not lift until the high drift point (i.e., setpoint plus 3 percent drift). Thus the calculated PZR peak pressure does not cause the RSVs to lift. The example LOFW transient calculations results extended for approximately 30 minutes past the event initiation at which point level had not sufficient dropped due to RCS shrinkage to reach either the PZR heater trip or CNV isolation point on low and low-low PZR level, respectively.

In Figure D-33, the second case illustrates the results of the event where AC power is lost coincident with the event, but the highly reliable DC power system (EDSS) is available. It was assumed that a nonsafety-related degraded AC electrical voltage signal would actuate DHRS and containment isolation as well as trip the reactor. As demonstrated in the second case presented in Figure D-33, DHRS cooldown is maintained for the 24-hour minimum duration of the EDSS batteries relied upon to hold the ECCS valves shut (see Appendix A, Section A.1.2). After 24 hours, the ECCS is assumed to actuate and the core cooling transitions from the DHRS to the ECCS (see Appendix B, Section B.2.1.3). The PZR heater trip and CNV isolation would have occurred before 24 hours due to the low PZR level signals. Thus the only ESFAS actuation that would result at the expiration of the minimum 24-hour duration of the EDSS batteries would be ECCS per Figure D-1.

The final (third) case presented in Figure D-33 assumes loss of all (both AC and DC) electrical power coincident with the LOFW initiating event. In this case, reactor trip, DHRS actuation, PZR heater de-energization, CNV isolation, and ECCS actuation all occur on the low DC power signal per the event diagram presented in Figure D-1. For this particular case, it is assumed that the IAB for each of the ECCS valves successfully actuates, so that the ECCS valves remain closed while the RCS pressure is high. This allows DHRS to continue normal cooldown until heat loss and level shrinkage reduce the PZR pressure to the IAB release pressure, assumed in the example calculation to be 1100 psia and to occur approximately 2.2 hours after transient initiation. Based on the example IAB design, once actuated, the block of the ECCS valve will not release until the pressure in the RPV is approximately 800 psia. This would result in some additional ECCS actuation delay (as compared to that reflected in Figure D-33), but does not change the event sequence substantially.

Reactor Trip System Actuation

Reactor trip is the first mitigating action for the LOFW event. The calculation results demonstrate that RTS will actuate in the event of functioning AC and DC power via normal MPS reactor trip signals on the indicators of a heatup event. Should AC power not be available but DC electrical power is available, either a nonsafety-related PCS signal will trip the reactor, or normal MPS function will occur due to DC power provided to the MPS from the EDSS. A loss of all (both AC and DC) electrical power, whether coincident with the LOFW initiating event or coincident with reactor trip, would result in a loss of electrical power to the CRDM coils and to the CRDM trip breakers, either of which result in rod insertion. The manner in which the reactor trip safety function is assured upon a loss of various different electrical supply sources is described further in Appendix B, Section B.2.1.1.

Core Cooling

Figure D-1 identifies two example safety-related systems, the DHRS and the ECCS, which are designed to provide core cooling during design basis events. Because the LOFW event is not inherently a decrease in RCS inventory event, ECCS is not required to actuate as part of the normal event mitigation, as illustrated in Figure D-14. Figure D-34 illustrates the effects of core cooling by the DHRS following a LOFW for the three cases being considered. For the power available case (blue), the rapid pressurization due to the heatup event results in a peak RPV lower plenum pressure of approximately 2060 psia, with pressure remaining below the RSV lift point. DHRS heat removal begins to reduce pressure within the first 60 seconds and becomes steady after a few minutes (300 seconds). For the cases with AC power unavailable (red and green), because loss of AC power is assumed coincident to event initiation, the initial pressurization due to the LOFW heat event is avoided because the reactor trips and the DHRS actuates immediately. The normal DHRS cooling trend can be seen in Figure D-34, where the power available LOFW calculation of RPV pressure (blue) is trending in a similar manner as the loss of AC power calculations (red and green) for the early part of the transient core cooling and RPV depressurization. Note that for the loss of AC power cases, DC power availability does not change the first 1800 sec of the event, so the red and green curves overlay.

Figure D-35 and Figure D-36 demonstrate the longer term RPV pressure responses for the three transient scenarios. The primary difference between the three cases can be seen in these figures where the ECCS valve opening occurs at 24 hours for the scenario with no AC electrical power but DC electrical power available, and at approximately 2.2 hours for the case with no electrical power available. The nominal LOFW case where power is assumed available was executed only for the first 1800 seconds of the event. The DHRS cooling can be seen in Figure D-35 for the first 24 hours for the case with only DC power available, and a similar pressure and cooling trend is expected for the power available scenario.

Another metric for demonstrating core cooling in DHRS mode is shown in Figure D-37, where DHRS flowrate demonstrates the passive ability of the system to generate natural circulation flow without the need for electrical power. The short plot of the power available case (blue) shows a slightly higher DHRS flow than the loss of AC power cases, which is due to the heatup event causing a higher RCS temperature and thereby driving more initial heat removal and natural circulation flow. After about seven hours of DHRS operation, the RCS coolant shrinkage and loss of level begin to limit primary coolant flow, thereby limiting the DHRS cooling capability and flowrate as a quasi-steady state condition is reached.

The loss of AC and DC power case also demonstrates that as ECCS actuates and the normal RCS flow loop is interrupted (as a result of the drop in RCS level), the DHRS no longer effectively functions as a heat removal system. A more complete description of ECCS function will be presented in Section D.3.2. However, both cases with ECCS actuation result in long-term core cooling and substantial RCS liquid level above the top of active fuel.

Reactor Coolant Pressure Boundary

The RPV 2100 psia design pressure was not exceeded or challenged for the LOFW event with power available as demonstrated in Figure D-34. Both of the cases where normal power is assumed to be compromised concurrent to the initiating event do not experience a pressurization event because the reactor is tripped and DHRS is actuated at the start of the transient. The other protection action for the RCPB is the PZR heater trip. Both loss of electrical power scenarios assumed that the PZR heaters lose power with the loss of AC power. For the cases where MPS is assumed to function, the DHRS cooling would sufficiently lower the RCS temperature such that coolant shrinkage will cause the PZR heaters to become uncovered. Prior to this occurring, the MPS will open the PZR heater trip breakers to ensure the heater sheaths are protected and the RCPB is preserved.

Containment Isolation

Containment isolation is not required for the nominal LOFW where power is available per the event diagram presented in Figure D-14. As discussed previously, if the MPS is available and no operator intervention is assumed, then normal DHRS cooling is expected to lower RCS temperature sufficiently such that coolant shrinkage is expected to uncover the PZR heaters and eventually reach the low PZR level CNV isolation point. This sequence will occur for both the electrical power available case and the loss of AC power case, while the loss of all electrical power case will result in CNV isolation with the loss of DC power (and associated loss of MPS function) at the event initiation.

Containment Integrity

The loss of AC and DC electrical power event results in an ECCS actuation within the first few hours of the transient. As shown in Figure D-38 (green), the calculated CNV pressure is well below the design pressure of 1000 psia. In the case where DC power is assumed available for 24 hours (red), DHRS cooling well exceeds the energy added to the RCS from decay heat, and there is a much smaller CNV pressurization upon ECCS actuation at 24 hours.

D.3.2 Example Inadvertent Reactor Recirculation Valve Opening Transient

D.3.2.1 Inadvertent Reactor Recirculation Valve Opening Event Description and Sequence

Inadvertent RRV Opening With AC and DC Electrical Power Available

The inadvertent opening of a reactor recirculation valve (RRV) is a design basis event which is caused by a failure within the valve actuator or the highly reliable DC power system (EDSS) that causes the valve actuator to depressurize. Failure of the inadvertent actuation block (IAB) must also be assumed in order for the valve to open as an initiating event while the reactor is at pressure and power. This is a decrease in inventory event which releases superheated liquid to the CNV. The inadvertent opening of a RRV with power available event diagram is shown in Figure D-29.

Based on the example design (see Appendix A, Section A.2, and Appendix B, Section B.2), the primary indicator of a decrease in RCS inventory event, where RCS inventory is being released to the CNV, is increased CNV pressure. As shown in Figure D-29, on indication of high CNV pressure, the MPS will actuate both a reactor trip and the DHRS, and will isolate the CNV.

As the event progresses, the RCS level will continue to drop due to the liquid being released to the CNV from the opened RRV. Initially PZR heaters are expected to energize in response to the RCS depressurization; however, once the low PZR level limit is reached, the heaters will be de-energized to ensure they don't uncover while energized. As level continues to drop, the top of the riser will be uncovered. This effectively ends the DHRS cooling due to loss of the RCS natural circulation loop. The ECCS actuation setpoint on low RCS level will be reached, and when the RCS is sufficiently depressurized the ECCS valves will open.

Upon actuation of ECCS, a rapid depressurization of the RCS and pressurization of the CNV will occur. RCS inventory will blowdown into containment until sufficient level is achieved in the CNV to provide static pressure head that is equal to the pressure difference between the RPV and CNV. At this point, recirculation flow will begin, establishing core cooling from the ECCS.

The example MPS design specifies the high CNV pressure analytical limit of 9.5 psia, the low PZR level analytical limit at 35 percent PZR level for PZR heater isolation, and a low RCS level of 20 ft above the top of active fuel for ECCS actuation. The analytical limit is the value credited in the example safety analysis.

Inadvertent RRV Opening Without AC or DC Electrical Power

Loss of both AC and DC electrical systems coincident with the inadvertent RRV opening event actuates the mitigating safety-related systems, as they are designed to "fail safe" on the loss of power condition. As discussed in Appendix B, Section B.2.1, with normal power available, upon receiving the trip limit condition signal from safety sensors (using 2 of 4 logic), the MPS disconnects the EDSS DC power supply from the safety-related actuators, causing the safety-related systems to actuate via stored potential energy. Therefore, if the loss of AC and DC power occurs at the time of the event, the loss of voltage (rather than the MPS signal) would result in reactor trip, DHRS actuation, isolation of the PZR heaters, and ECCS actuation at the beginning of the event. This is reflected in the loss of electrical power event diagram that is common to all events provided in Figure D-1.

The timing of ECCS actuation is a primary difference between the loss of all power and the power available event sequence for the inadvertently opened RRV event. In the loss of all power scenario coincident to the event initiation, the RCS will be at high pressure (>1600 psia) at the time of ECCS actuation. Because of the ECCS actuator design, the passive inadvertent actuation block (IAB) on each ECCS valve would prevent valve opening due to the high RCS pressure conditions. After the RCS pressure is sufficiently reduced by DHRS cooling and the break flow mass and energy release, the IABs will release and the ECCS valves will open, resulting in blowdown to the CNV.

The timing of the PZR heater trip will also be impacted by the assumption of the loss of electrical power. As discussed previously, if power is available, the PZR heaters would increase in power, due to the normal module control system (MCS) response to a low PZR pressure signal, and would remain powered until the low PZR level signal occurred for two of four PZR level sensors and MPS disconnected power to the PZR heater trip breaker. If electrical power is lost coincident to the event initiation, then the PZR heaters would be de-energized immediately rather than at the low PZR level.

A loss of AC and DC power coincident with the reactor trip rather than coincident to event initiation results in essentially the same event because the high CNV pressure signal is reached in the first few seconds after opening of the RRV.

In summary, Figure D-29 identifies the need for the RTS, DHRS, PZR heater trip, and ECCS to ensure the safety of the reactor in the event of an inadvertently opened RRV. Should a loss of all electrical power occur coincident to the event or at the time of reactor trip, these safety-related systems will still actuate and function to bring the reactor to a safe, depressurized and cooled condition as shown in Figure D-1.

Inadvertent RRV Opening With AC Electrical Power Unavailable and DC Electrical Power Available

The inadvertent opening of an RRV with a loss of AC power at the time of reactor trip and with DC electrical power available will follow a similar progression as the case where AC power is available. The MPS will function normally and actuate ECCS on low RCS level. The PZR heaters will not function due to the loss of AC power, but the heater trip breakers will not be opened until the low PZR level signal is reached per the normal MPS function.

D.3.2.2 Example Inadvertent Opening of RRV Calculation Results

The purpose of this section is to summarize example NRELAP5 calculation results that support the inadvertent RRV opening event diagrams presented in Figure D-29 and Figure D-1. Figure D-39 contains a diagram of the event sequences for three event scenarios: (1) the nominal case where AC and DC power is available but no operator interventions are assumed; (2) the loss of AC power case where DC electrical power is available; and (3) the loss of both AC and DC electrical power where all safety-related systems are actuated immediately and ECCS valve opening is delayed for a short period due to the inadvertent actuation block.

In the first case presented in Figure D-39 where AC and DC power are available, CNV isolation, DHRS actuation, and reactor trip are initiated with the high CNV pressure signal at around 7 seconds into the event. With DC electrical power available to hold the ECCS valves closed, DHRS cooling would continue until the natural circulation path was interrupted due to RCS cooling and loss of liquid inventory due to the opened RRV. Although not expressly indicated in Figure D-39, the PZR heaters will trip off on low PZR level well before ECCS actuation occurs approximately 4 minutes into the event. The IAB release pressure is assumed in the example calculation to be 1200 psia, which would be reached a few minutes after the transient initiation (allowing ECCS valves to open). Based on the example IAB design, once actuated, the block of the ECCS valves will not release until the pressure in the RPV is approximately 800 psia. This would result in some additional ECCS valve opening delay (as compared to that reflected in Figure D-39), but does not change the event sequence substantially.

The example inadvertent RRV opening calculation assumed that ECCS actuation would occur on high CNV level, where the example event progression descriptions described herein are based on the low RCS level signal as an actuation signal for ECCS. For the inadvertent RRV opening event, the timing of the high CNV level signal compared with the low RCS level signal is not expected to be significantly different. As indicated in Figure D-39, ECCS is expected to actuate within the first few minutes of the transient.

In Figure D-39, the second case illustrates the results of the event where AC power is lost but the highly reliable DC power system (EDSS) is available resulting in nearly the identical event sequence as if both AC and DC power were available. The MPS will trip the PZR heaters and actuate ECCS on the normal ESFASs.

The final (third) case presented in Figure D-39 assumes loss of all (both AC and DC) electrical power coincident with the inadvertent RRV opening initiating event. In this case, reactor trip, DHRS actuation, PZR heater de-energization, CNV isolation, and ECCS actuation all occur on the low DC power signal per the event diagram presented in Figure D-1. For this particular case, it is assumed that an IAB for each ECCS valve successfully prevents the ECCS valves from opening while the RCS pressure is high. This allows DHRS to continue normal cooldown until energy loss and level shrinkage, due to the open RRV, reduce the PZR pressure to the IAB release pressure within a few minutes after transient initiation.

Reactor Trip System Actuation

Reactor trip is the first mitigating action for the inadvertent RRV opening event. The calculation results demonstrate that RTS will actuate in the event of functioning AC and DC power via normal MPS reactor trip signals on the high CNV pressure. Should AC power not be available but DC electrical power is available, either a nonsafety-related plant control system (PCS) signal will trip the core, or normal MPS function will occur due to DC power provided to the MSP from the EDSS. A loss of all (both AC and DC) electrical power, whether coincident with the inadvertent RRV opening initiating event or coincident with reactor trip, would result in a loss of electrical power to the CRDM coils and to the CRDM trip breakers, either of which result in rod insertion. The manner in which the reactor trip safety function is assured upon a loss of various different electrical supply sources is described further in Appendix B, Section B.2.1.1.

Core Cooling

Figure D-1 identifies two example safety-related systems, the DHRS and the ECCS, which are designed to provide core cooling during design basis events. Figure D-40 presents the calculated results for outer surface cladding temperature. With respect to power availability, because of the similarity of the event progression as shown in Figure D-39, only the calculation results for the AC and DC power available case are presented.

The initial reactor trip can be immediately seen in Figure D-40 with the initial drop in temperature followed by a short reheating due to the increased core inlet temperature that is caused by the loss of SG heat removal while DHRS is actuating. The shorter decrease in temperature is due to DHRS cooling which is followed by a rapid drop in temperature due to the depressurization of the RCS from ECCS actuation. At around 500°F, the temperature follows the depressurization until finally stabilizing with sustained ECCS cooling.

Another metric for demonstrating core cooling in ECCS mode is shown in Figure D-41 where RCS collapsed level is shown relative to the top of the core. Because of the location of the RRV in the RCS downcomer region, the RCS liquid level drops rapidly until approximately 28 ft above the core, at which point the ECCS actuates on high CNV level. ECCS actuation results in a much more rapid level drop until CNV pressure begins to build, slowing the loss of RCS inventory at around 18 ft above the core. Collapsed level reaches the minimum point, just below 10 ft above the core, and slowly begins to increase due to the equalization of pressure between the RPV and CNV in the later stages of the event. At all times during the inadvertent RRV opening event, liquid level in the RPV is sufficient to keep the core covered, allowing for normal nucleate boiling to keep the core cooled.

Reactor Coolant Pressure Boundary

This event causes a release of mass and energy from the RCS to the CNV and therefore does not result in a challenge to the RPV design pressure as illustrated in Figure D-42.

The other protection action for the RCPB is the PZR heater trip. Both loss of power scenarios assumed that the PZR heaters lose power with the loss of AC power. For the cases where MPS is assumed to function, the DHRS cooling and RCS inventory decrease through the open RRV would sufficiently lower the RCS temperature such that coolant shrinkage will cause the PZR heaters to become uncovered. Prior to this occurring, the MPS will open the PZR heater trip breakers to ensure the heater sheaths are protected and the RCPB is preserved.

Containment Isolation

The inadvertent RRV opening event causes a rapid pressurization within the CNV. As indicated in Figure D-39, this results in a high CNV pressure signal and an isolation of containment within a few seconds. Figure D-39 illustrates that the availability of AC or DC power will have little impact on the timing of CNV isolation. In addition, as described in Appendix B, Section B.2.1.4, electrical power is not necessary during and following a design basis event to ensure performance of the containment isolation function.

Containment Integrity

Figure D-43 presents example calculation results for containment pressure for the inadvertent RRV opening event with electrical power available. Upon ECCS actuation, CNV pressure reaches approximately 700 psia, which is well below the example CNV design pressure of 1000 psia. In this case, the ECCS valves were assumed to open when actuated, when the RCS pressure reached approximately 1200 psia as shown in Figure D-42. Based on the example IAB design, once the ECCS valves receive an actuation signal, the IABs will prevent the ECCS valves from opening until the pressure in the RPV is approximately 800 psia. This would result in some additional ECCS actuation delay (as compared to that reflected in Figure D-42 and Figure D-43), but does not change the event sequence substantially.

D.4 Example Summary Conclusions

The example safety analysis results described in Section D.2 and Section D.3 illustrate how for the example small modular reactor passive plant design reflected in Appendix A and Appendix B, neither electrical power nor operator action is necessary to achieve and maintain reactor safety-related functions.

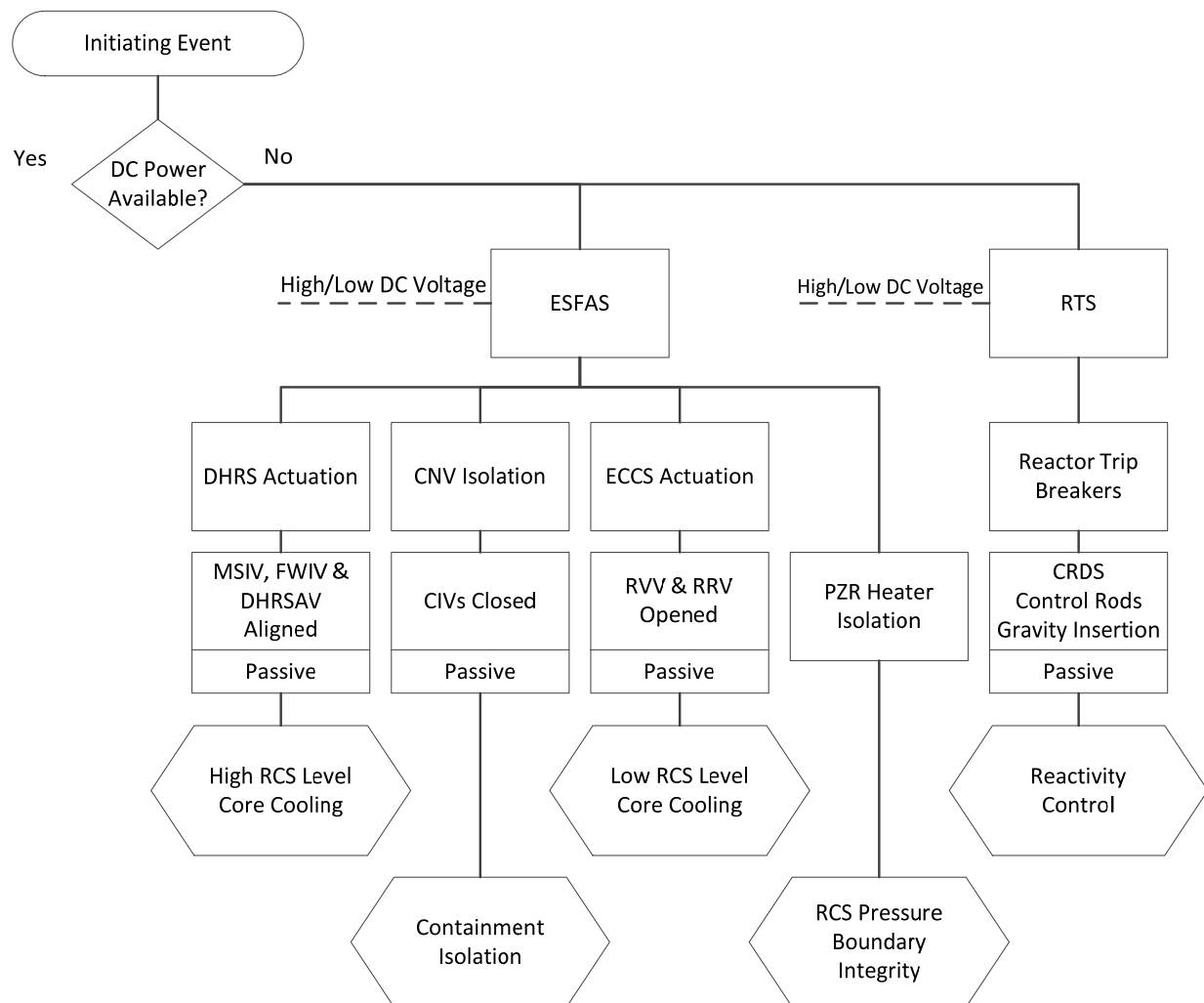


Figure D-1. Loss of DC electrical power event diagram – common to all design basis events

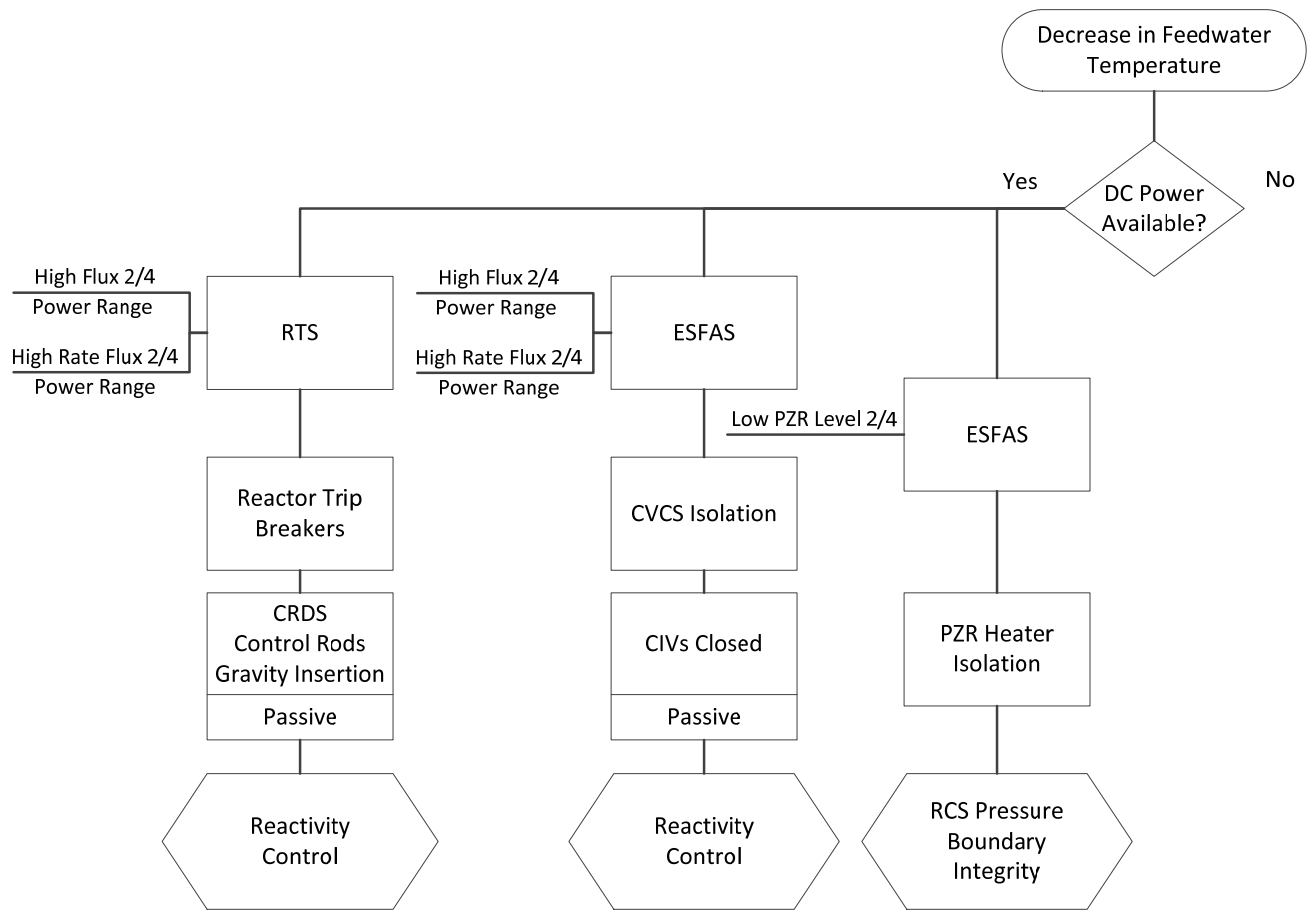


Figure D-2. Decrease in feedwater temperature event diagram

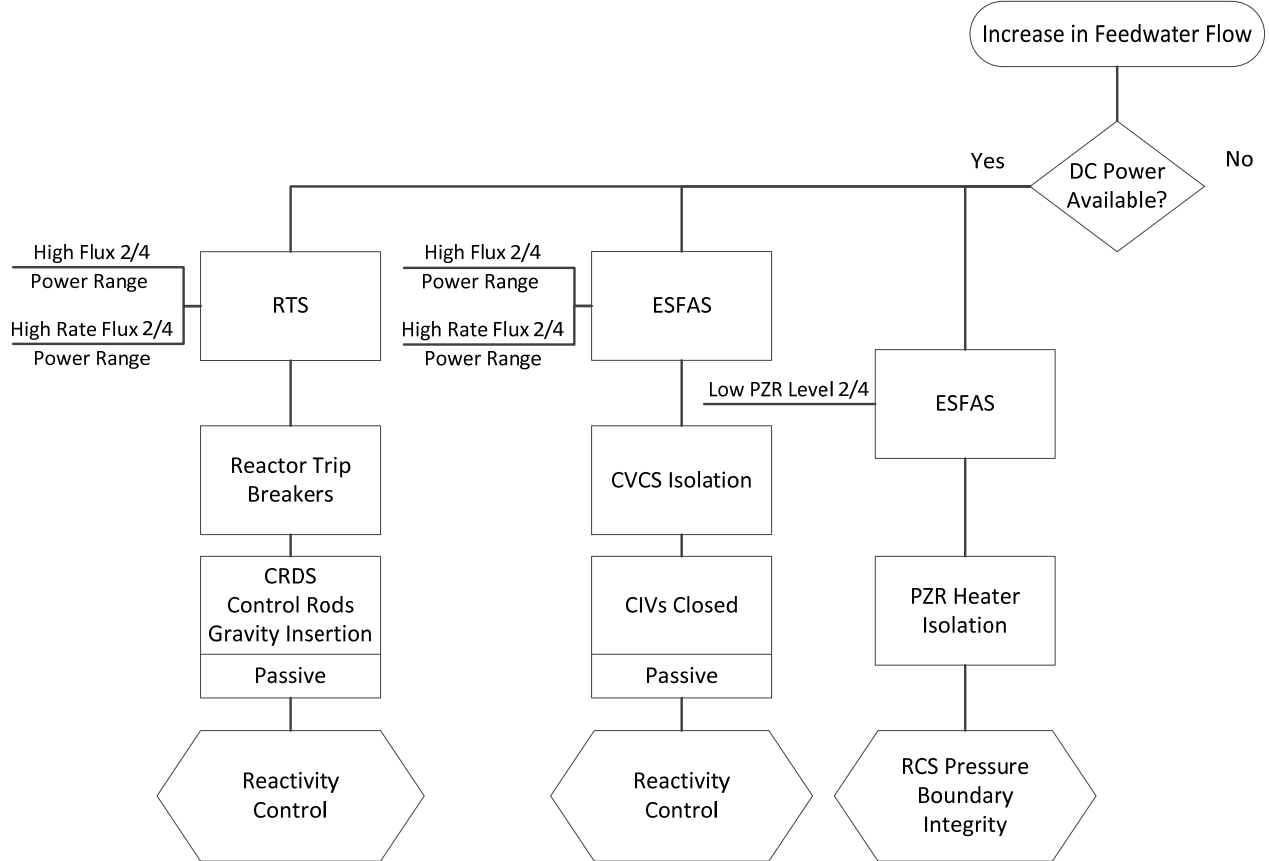


Figure D-3. Increase in feedwater flow event diagram

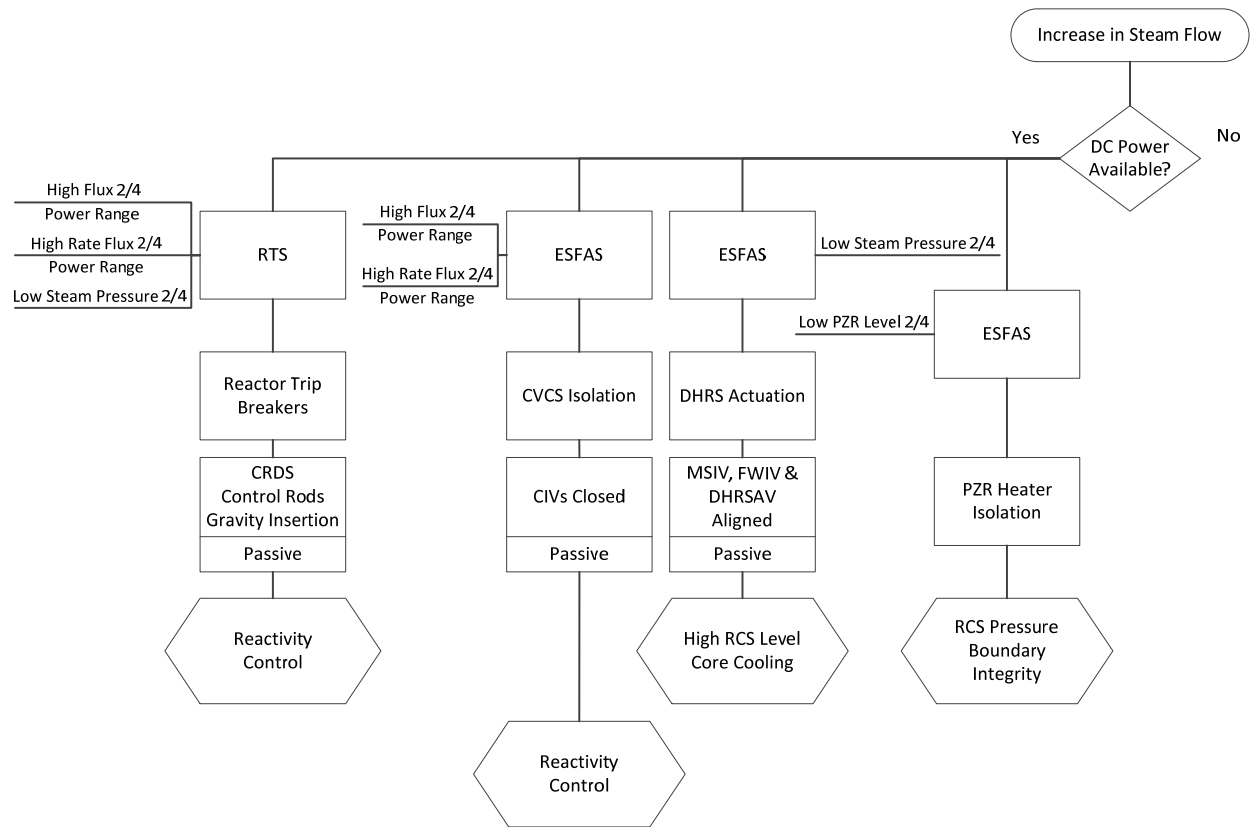


Figure D-4. Increase in steam flow event diagram

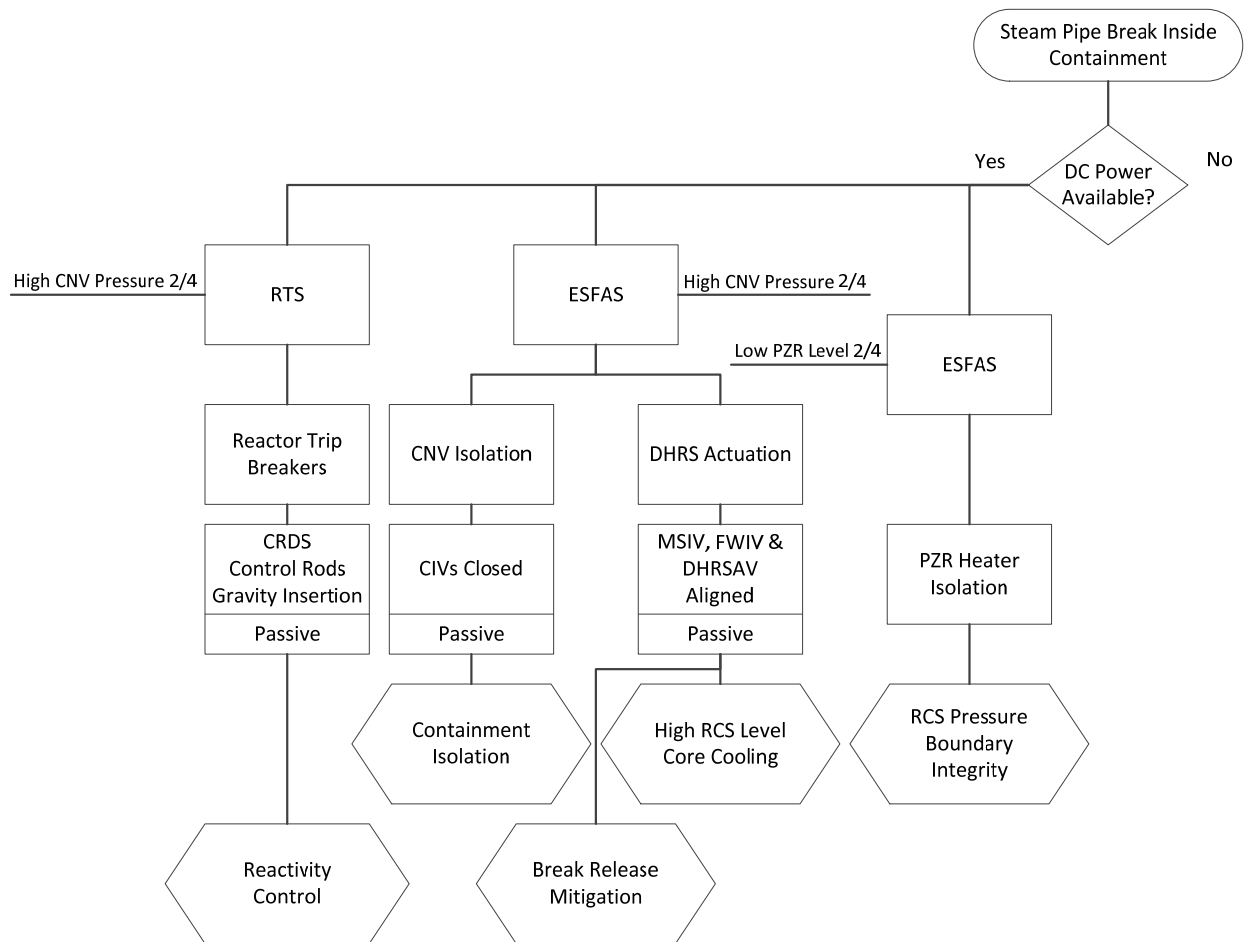


Figure D-5. Steam line break inside containment event diagram

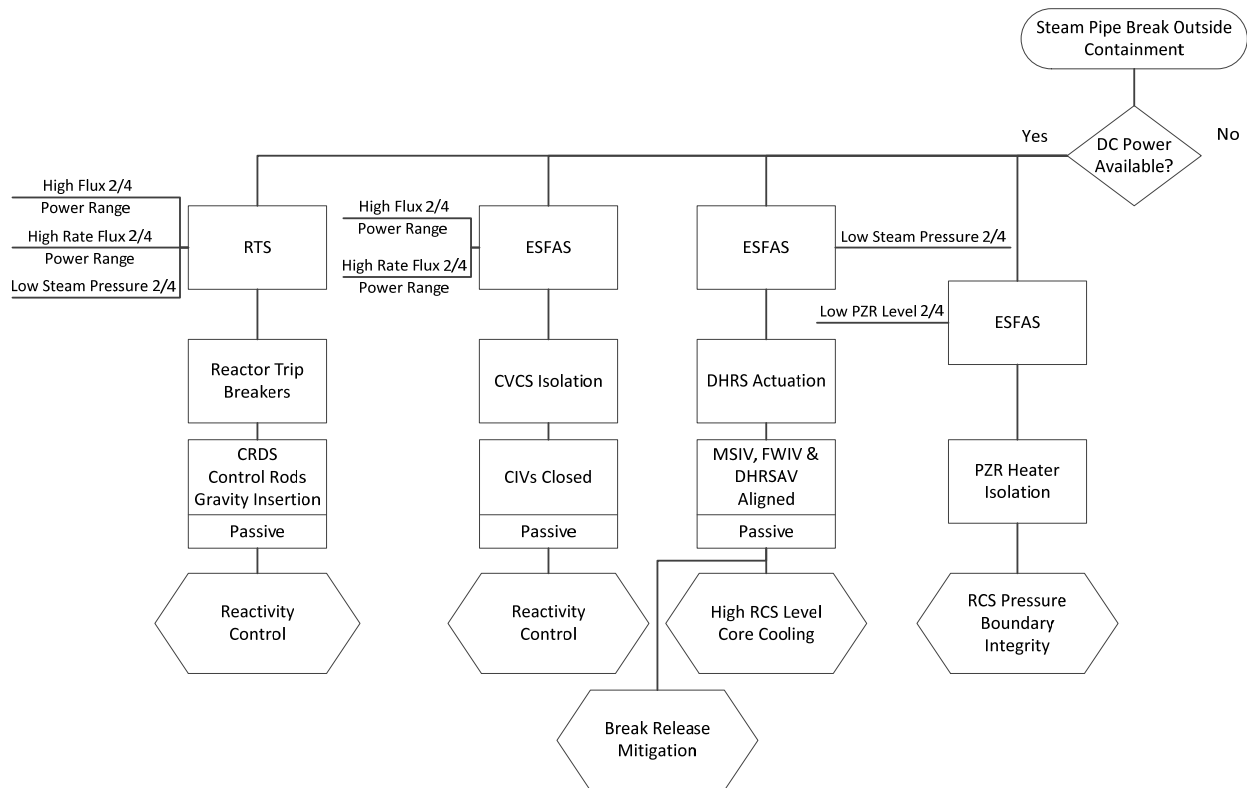


Figure D-6. Steam line break outside containment event diagram

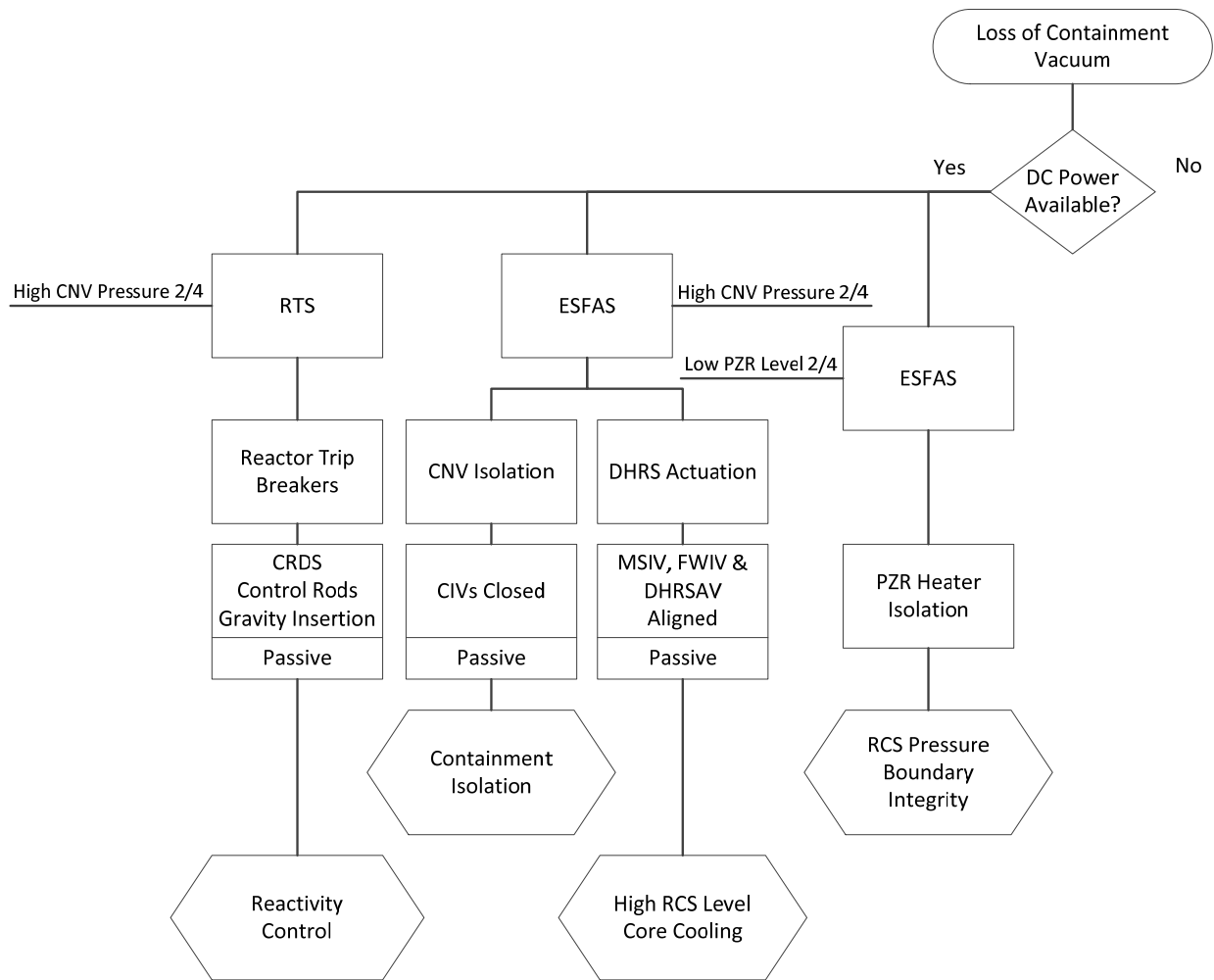


Figure D-7. Loss of containment vacuum event diagram

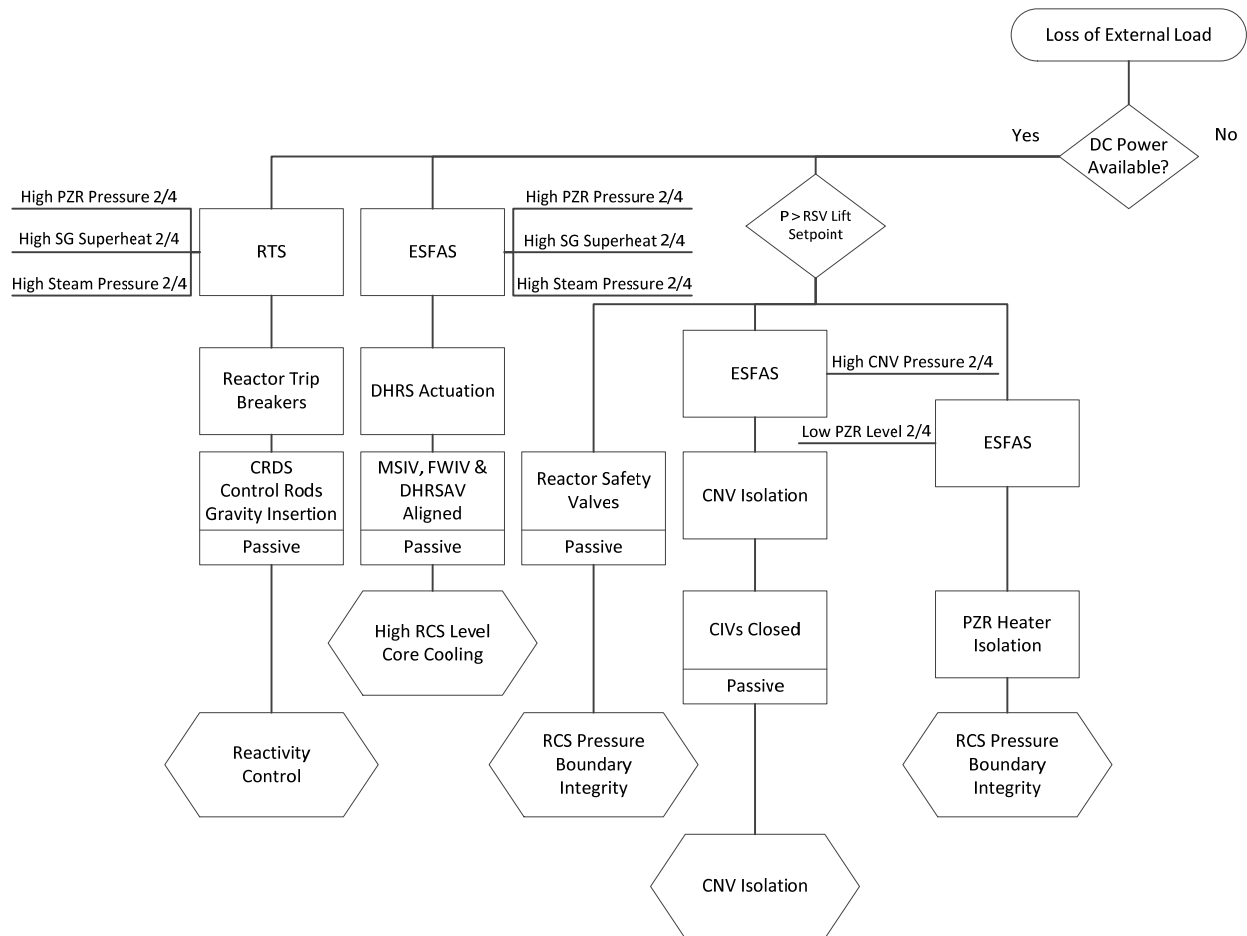


Figure D-8. Loss of external load event diagram

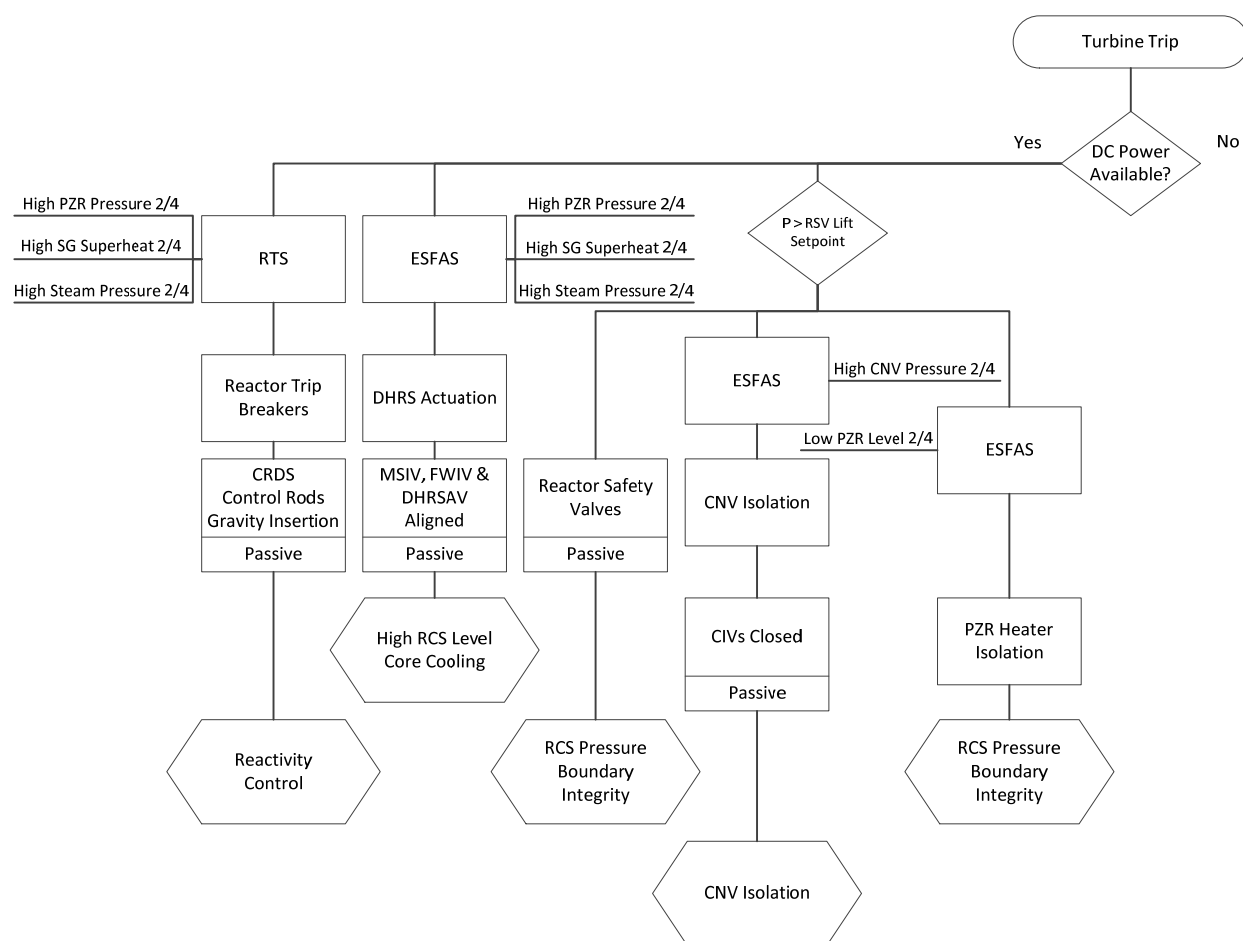


Figure D-9. Turbine trip event diagram

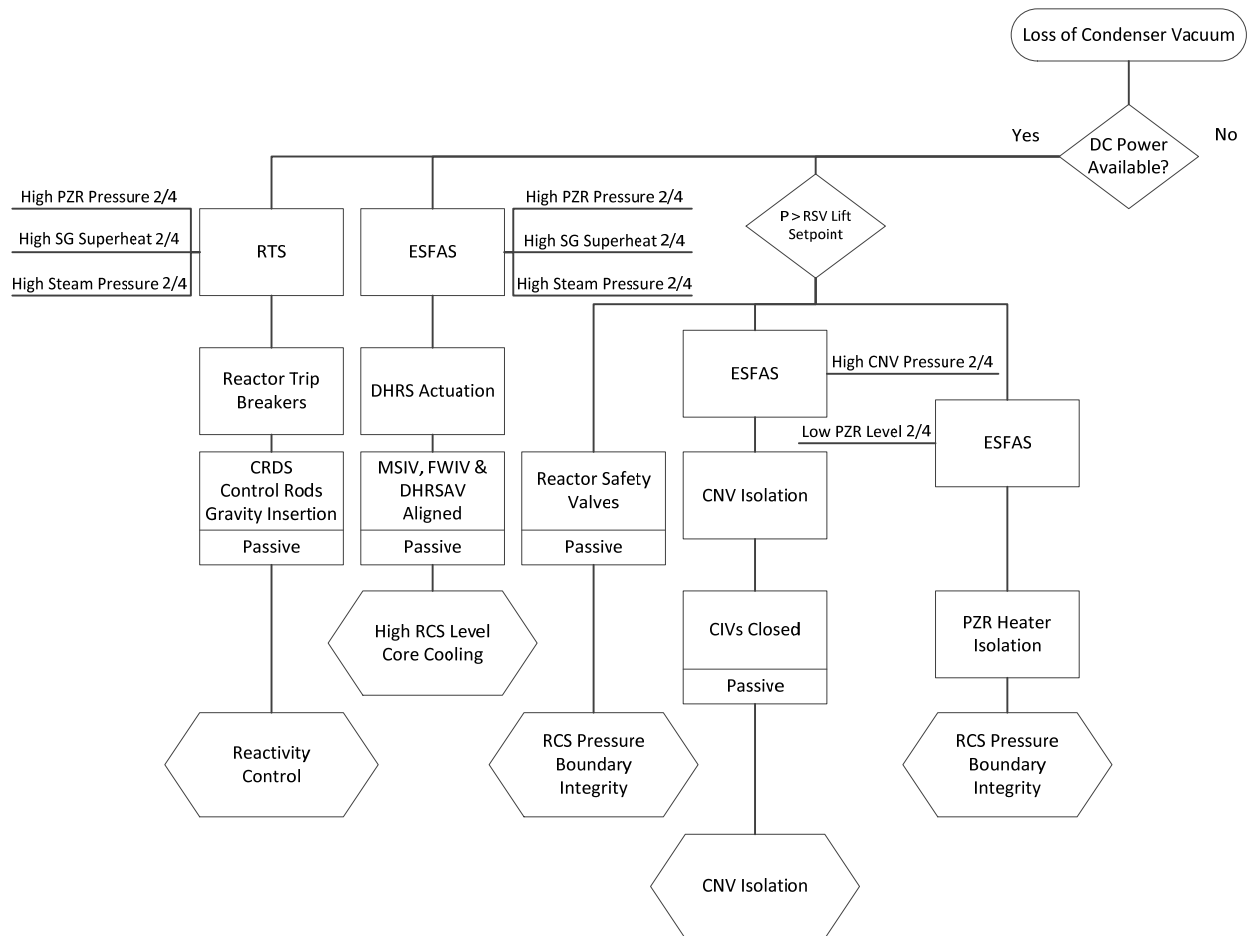


Figure D-10. Loss of condenser vacuum event diagram

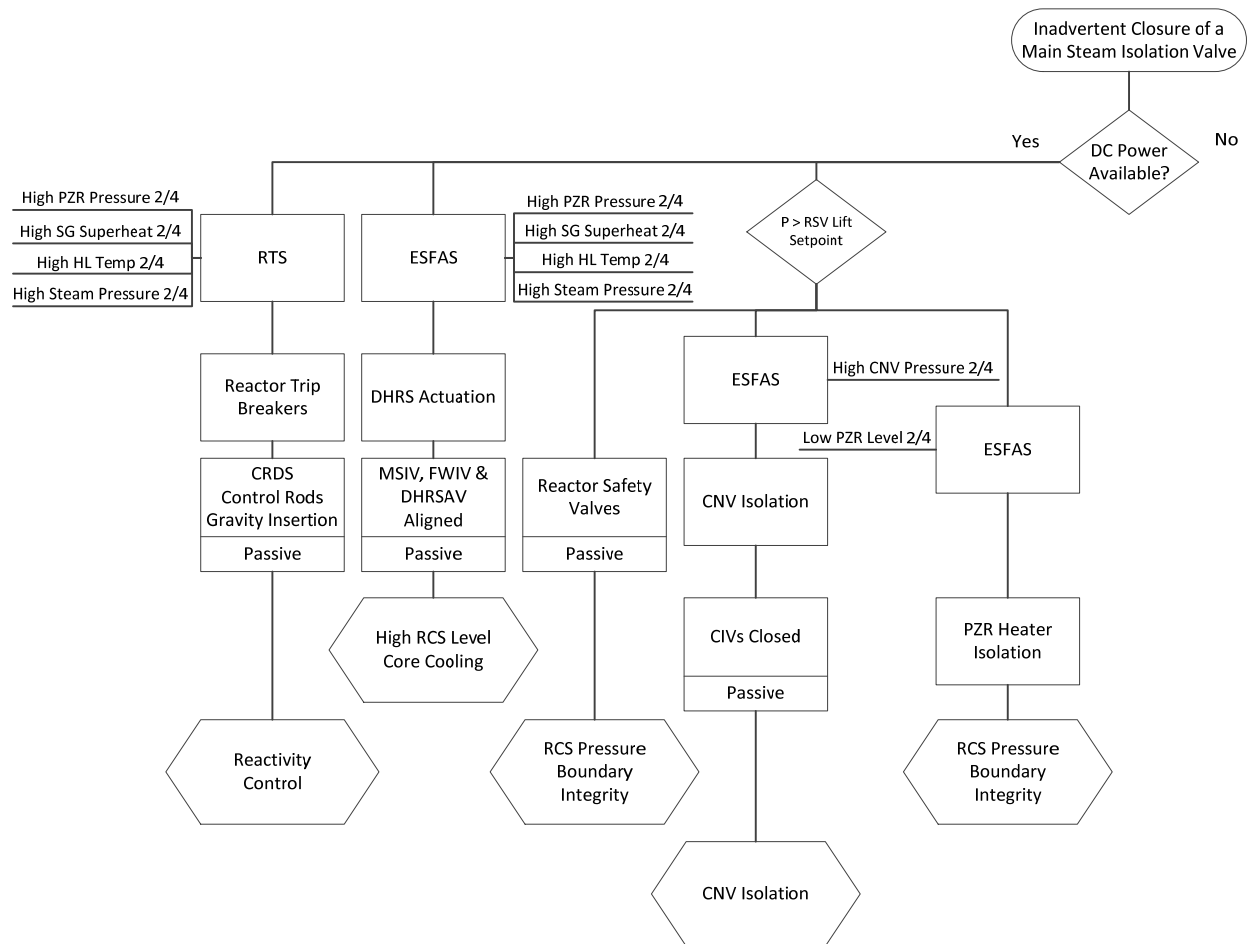


Figure D-11. Inadvertent closure of an MSIV event diagram

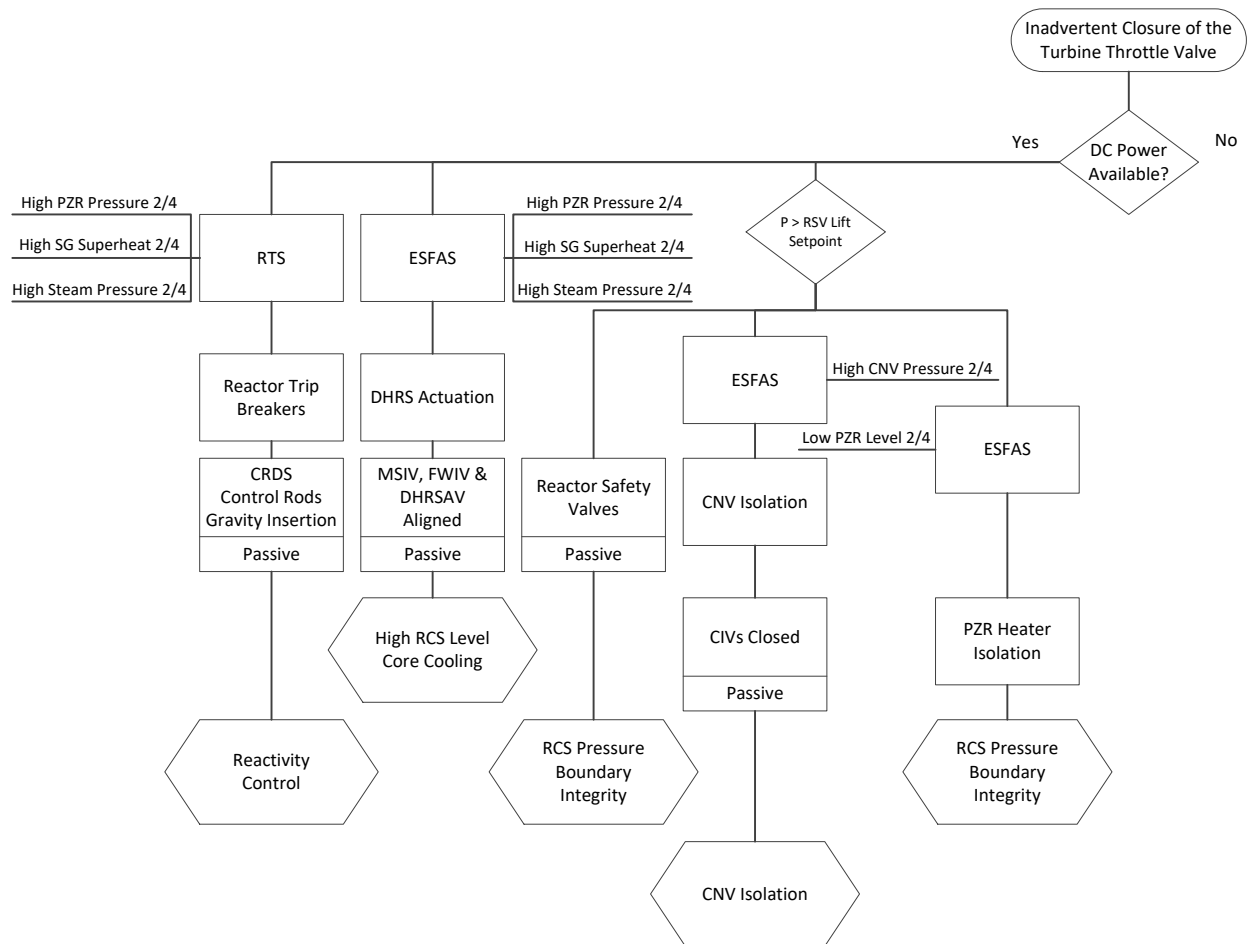


Figure D-12. Inadvertent closure of the turbine throttle valve event diagram

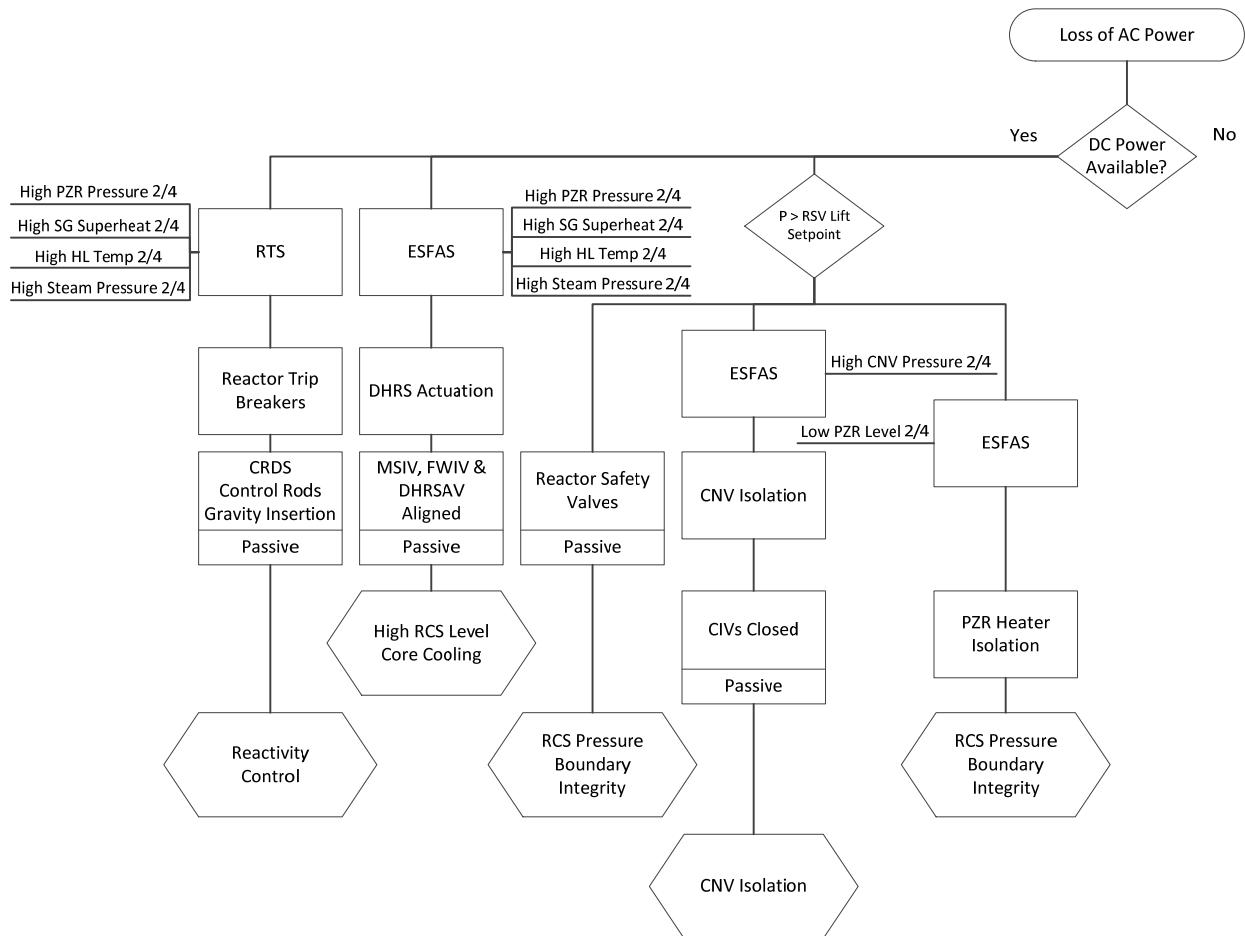


Figure D-13. Loss of AC power event diagram

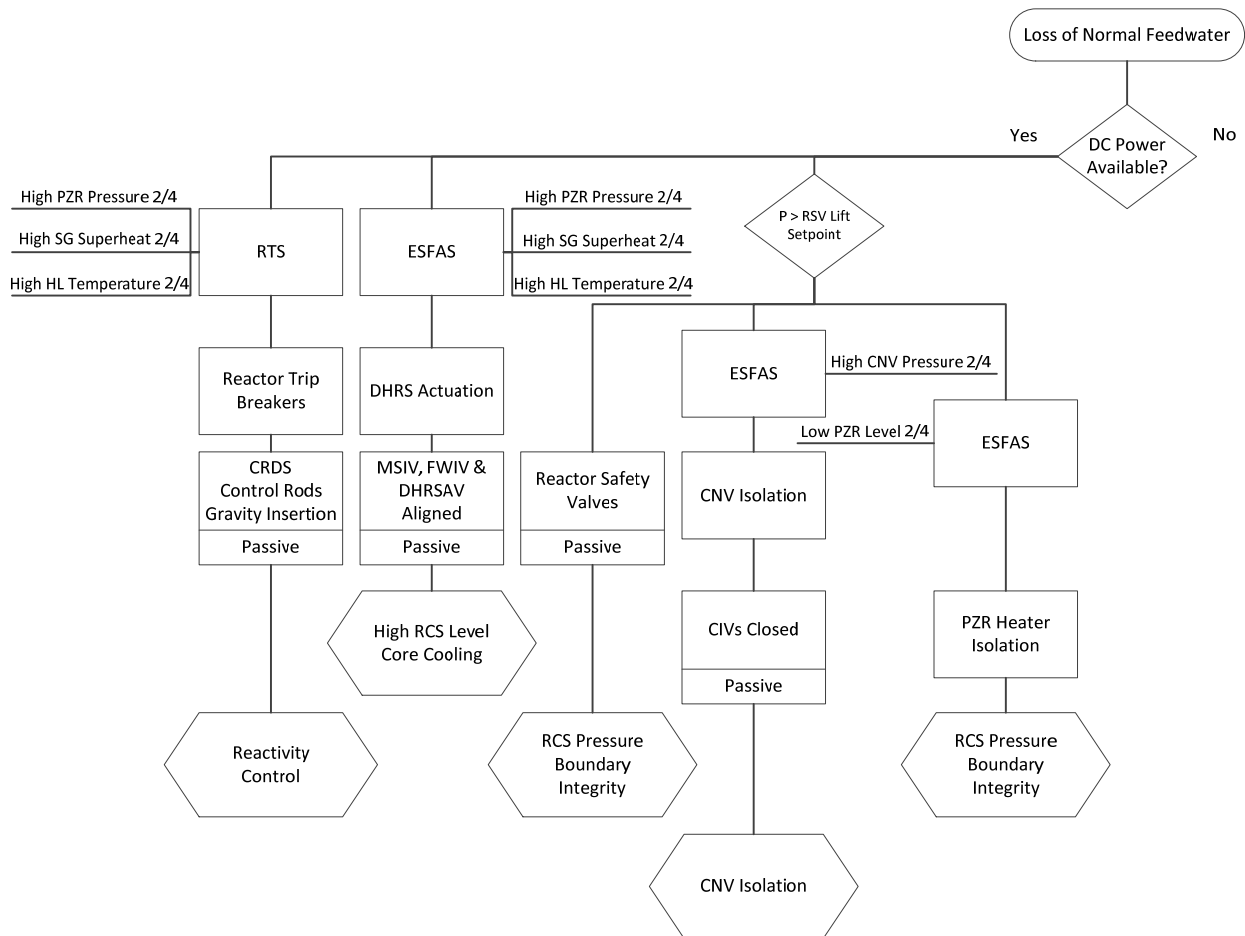


Figure D-14. Loss of normal feedwater flow event diagram

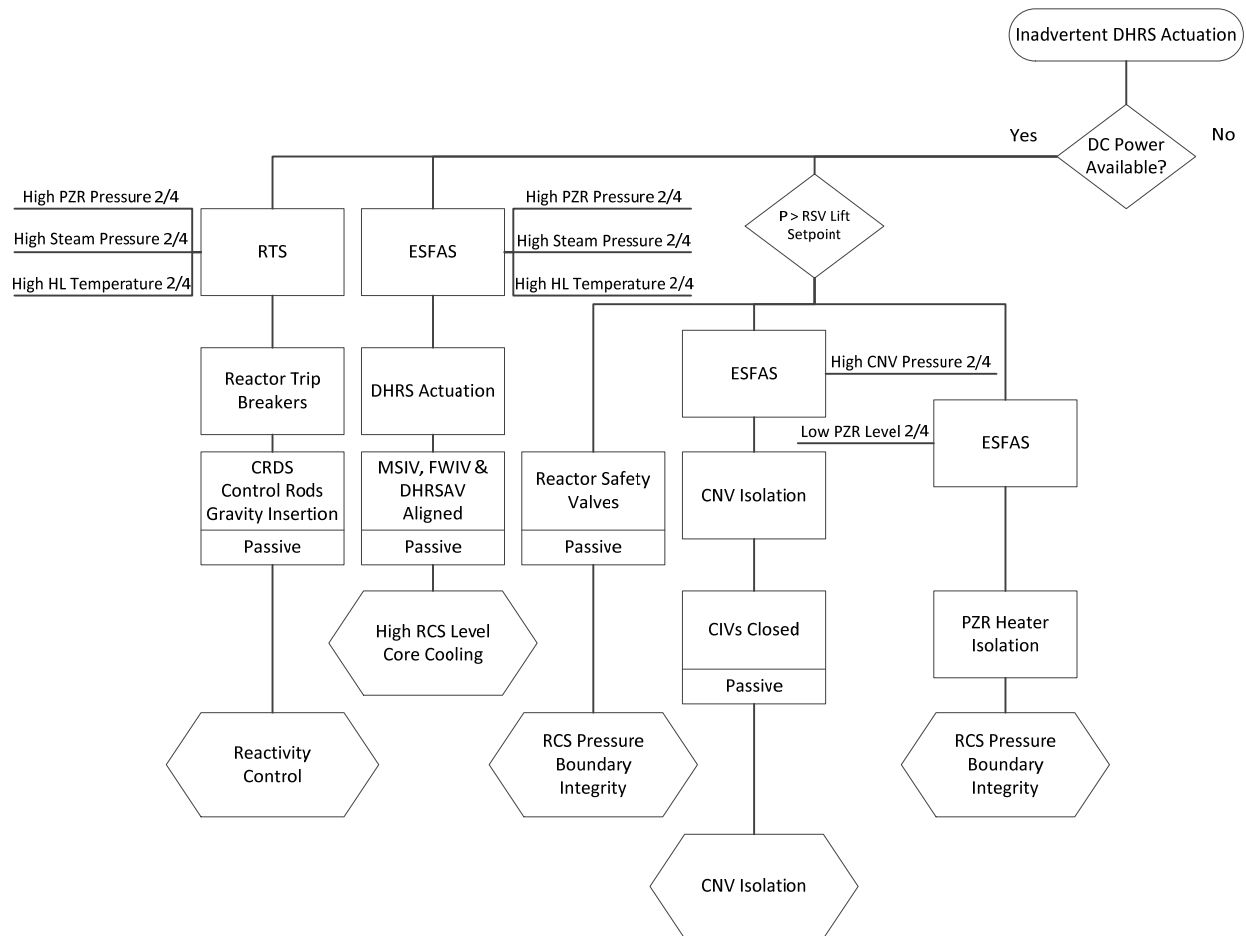


Figure D-15. Inadvertent actuation of DHRS event diagram

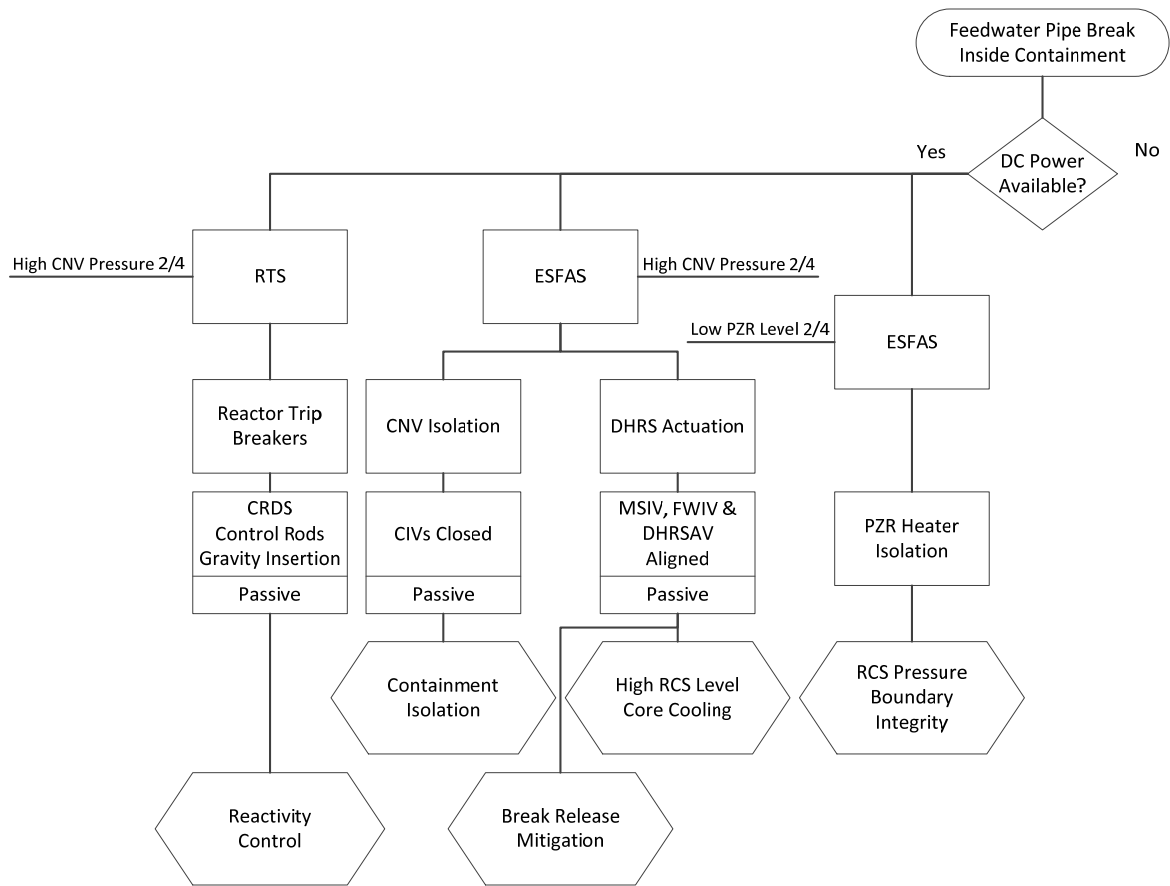


Figure D-16. Feedwater line break inside containment event diagram

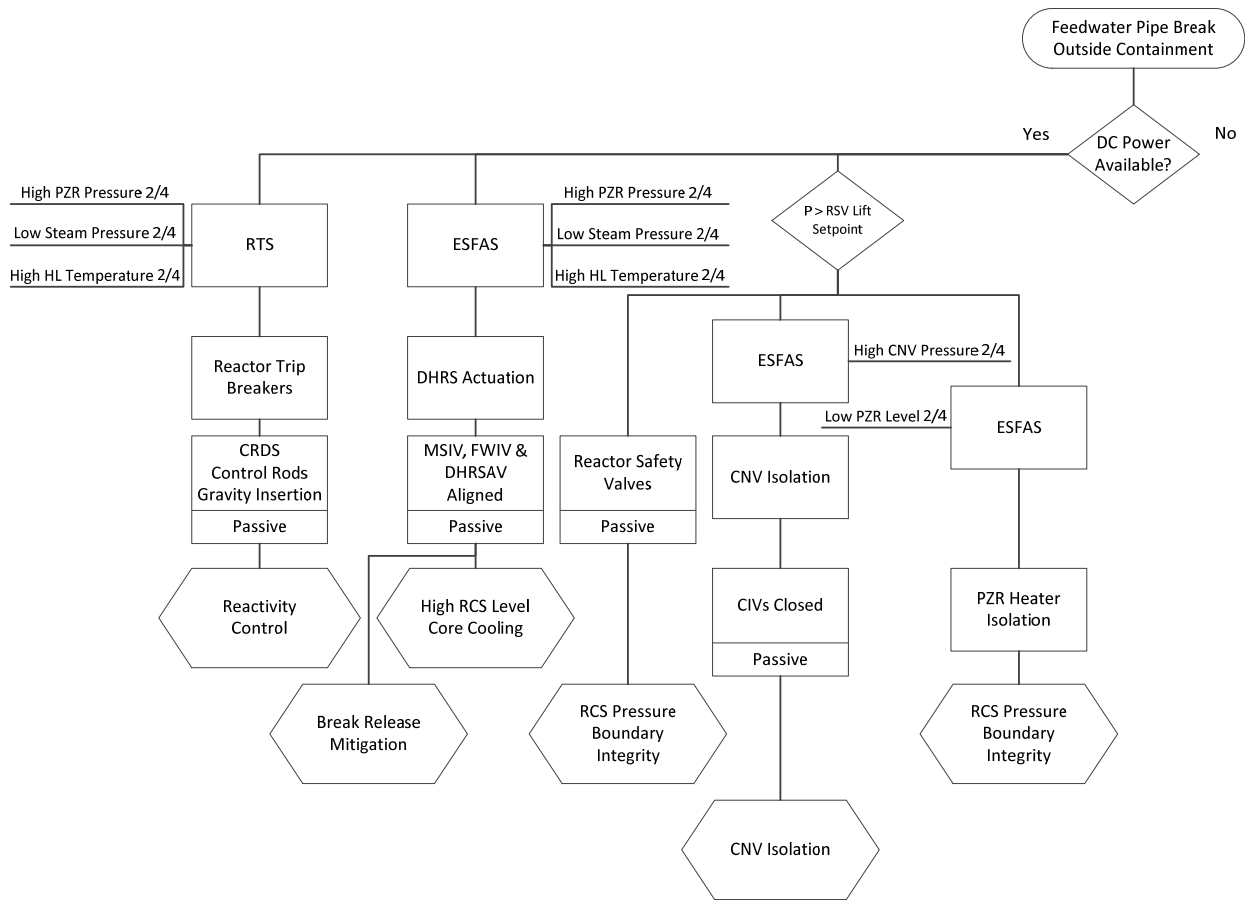


Figure D-17. Feedwater line break outside containment event diagram

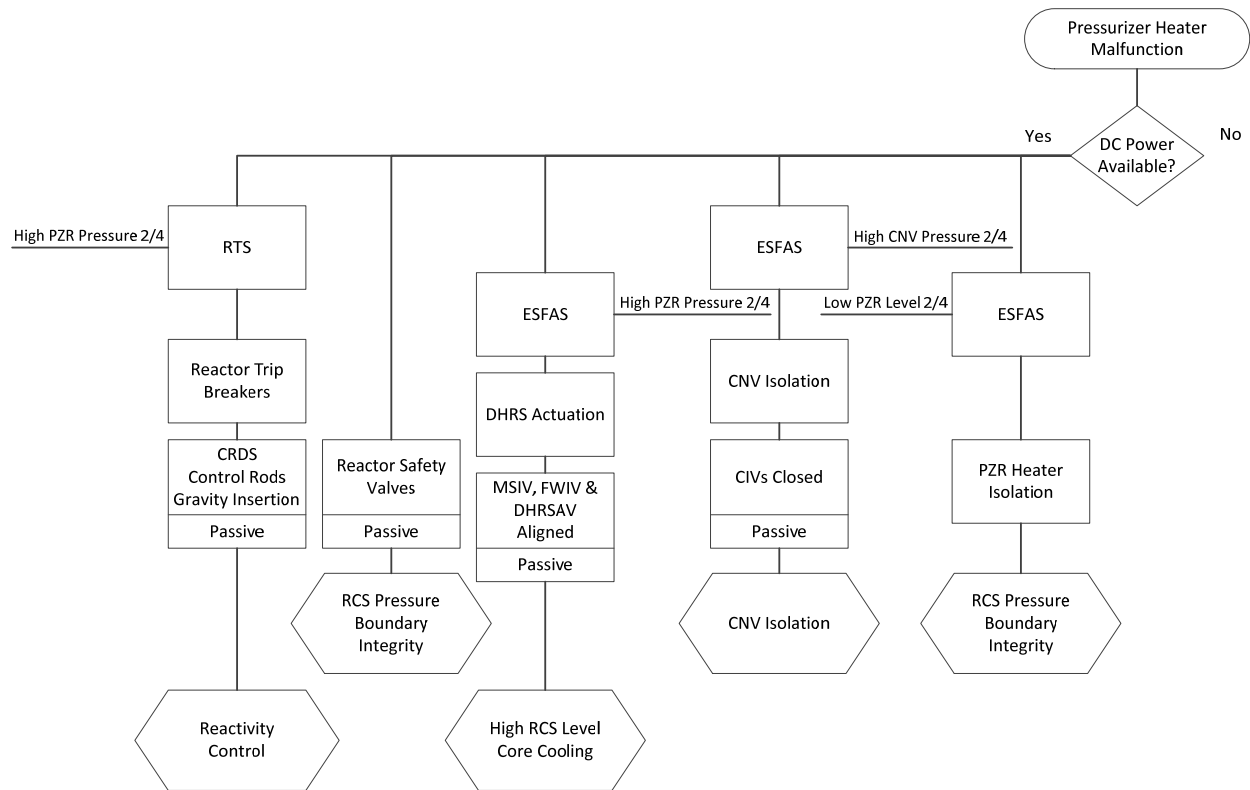


Figure D-18.PZR heater malfunction event diagram

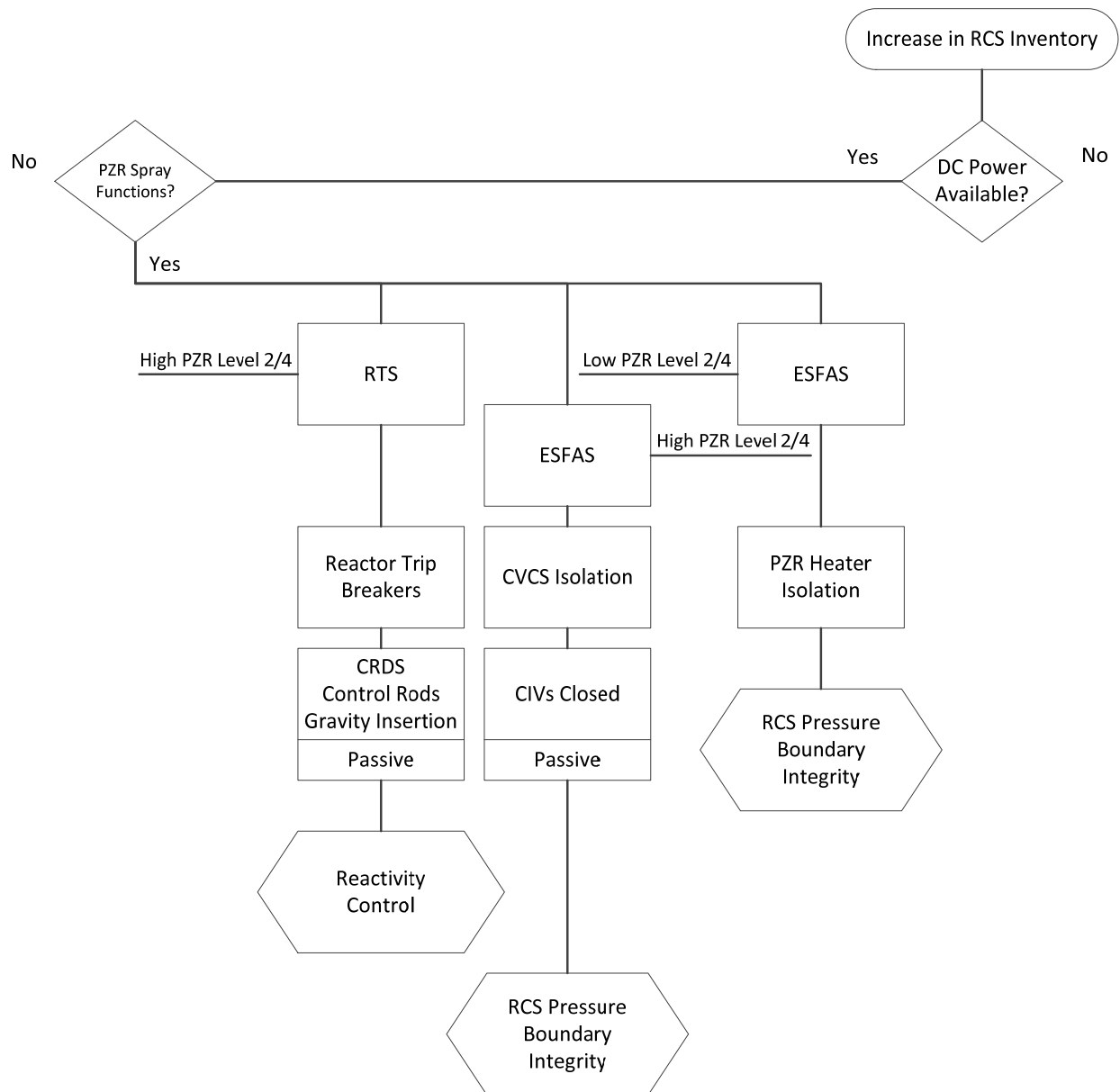


Figure D-19.PZR level control malfunction (PZR spray available) event diagram

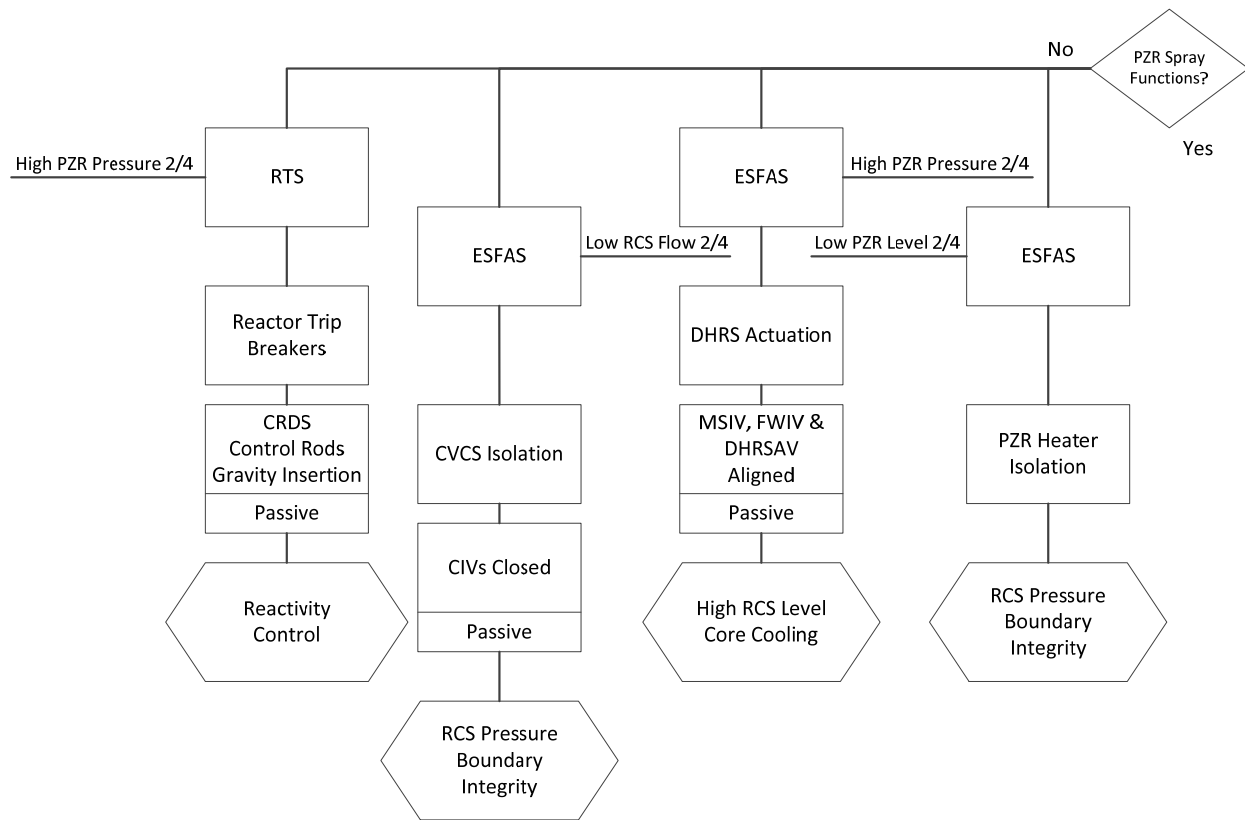


Figure D-20.PZR level control malfunction (PZR spray not available) event diagram

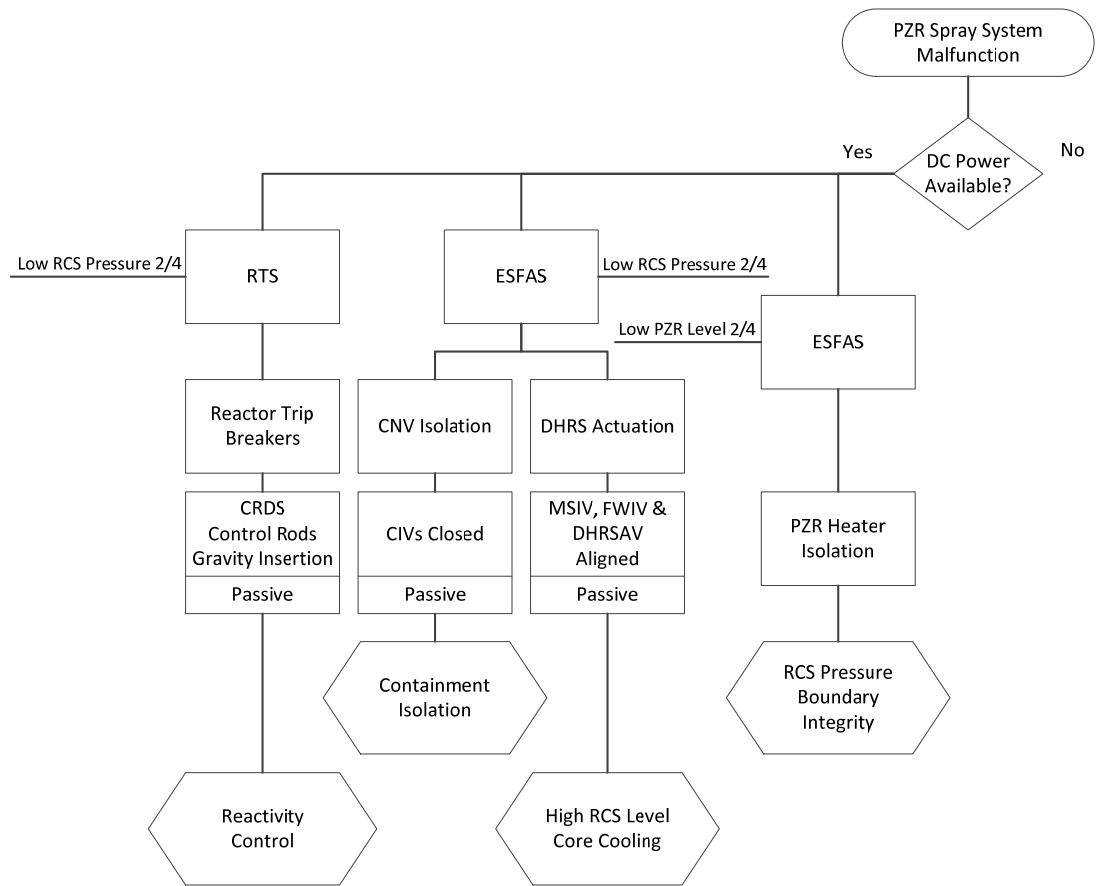


Figure D-21.PZR spray control malfunction event diagram

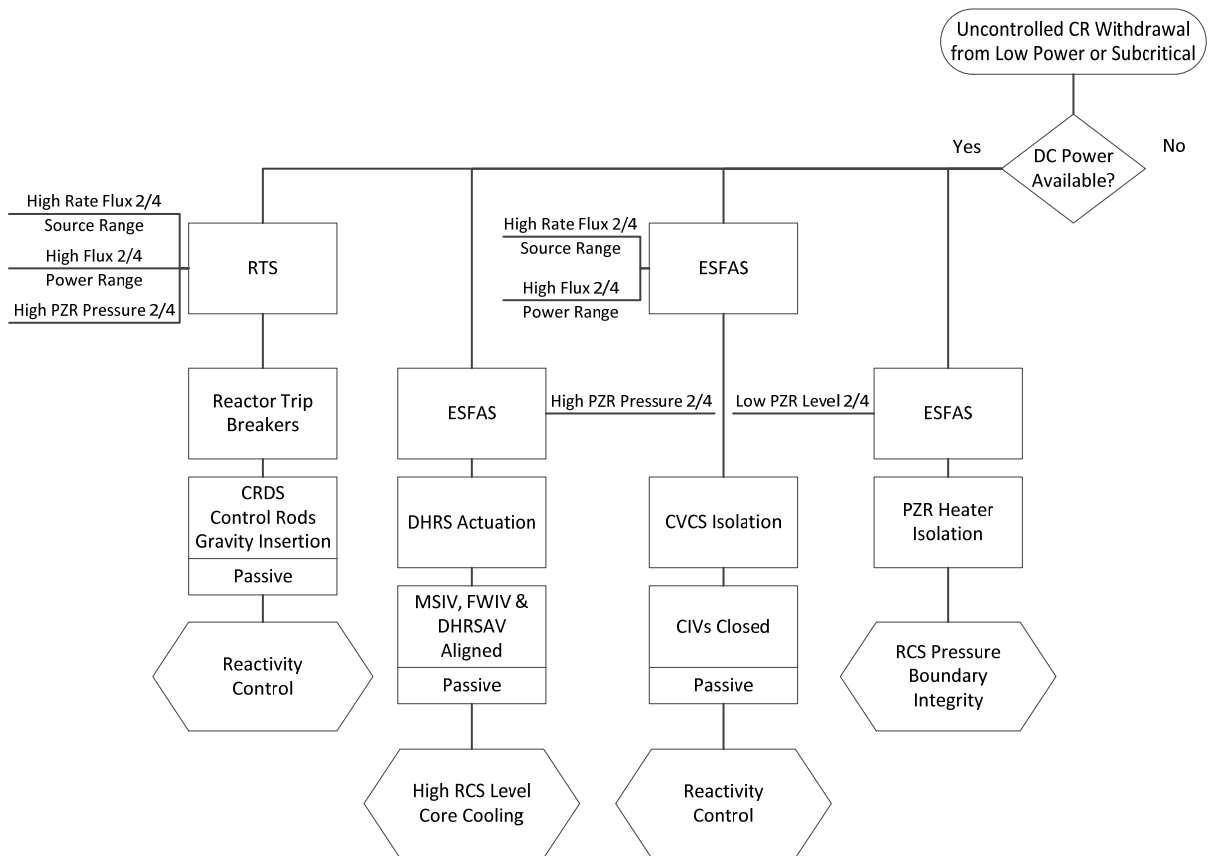


Figure D-22. Uncontrolled control rod bank withdrawal in low power or subcritical conditions event diagram

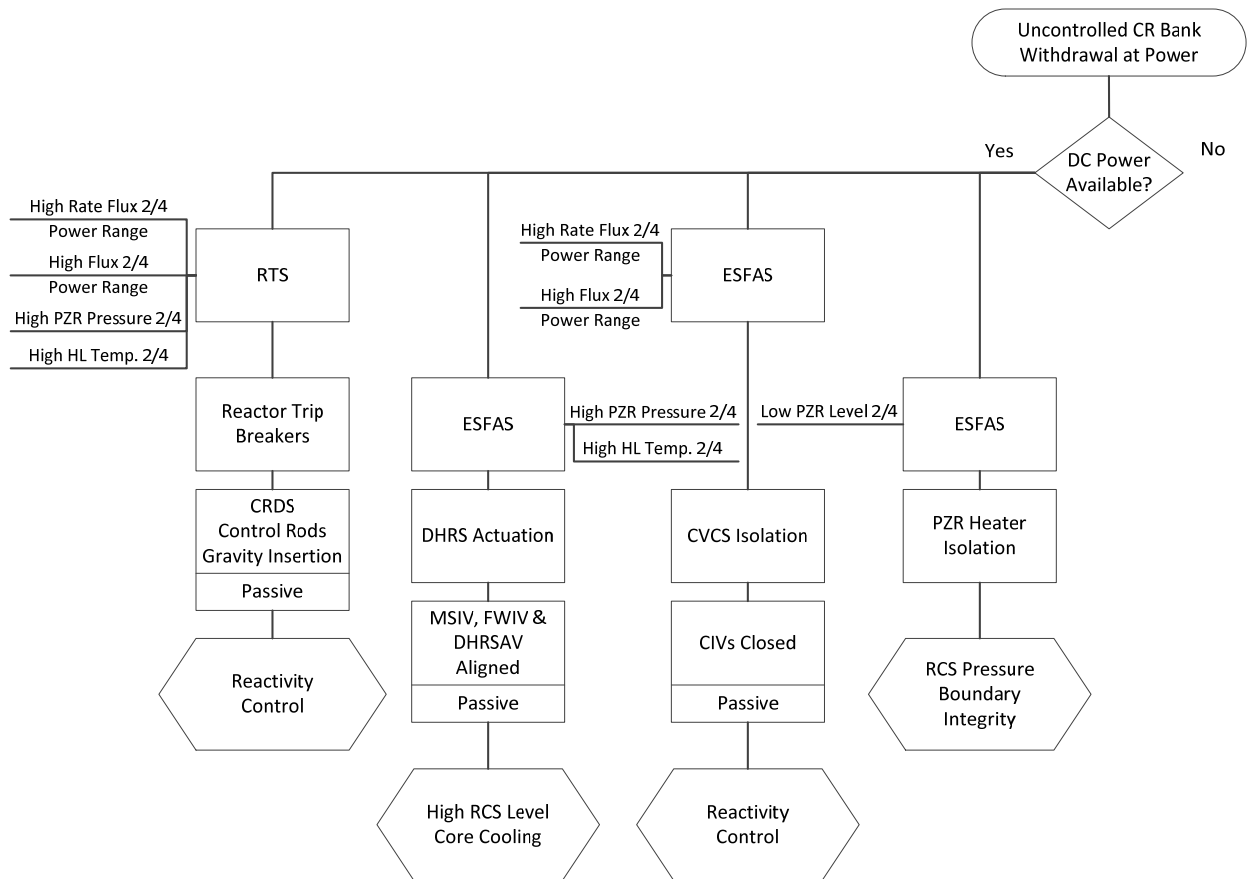


Figure D-23. Uncontrolled control rod bank withdrawal at power event diagram

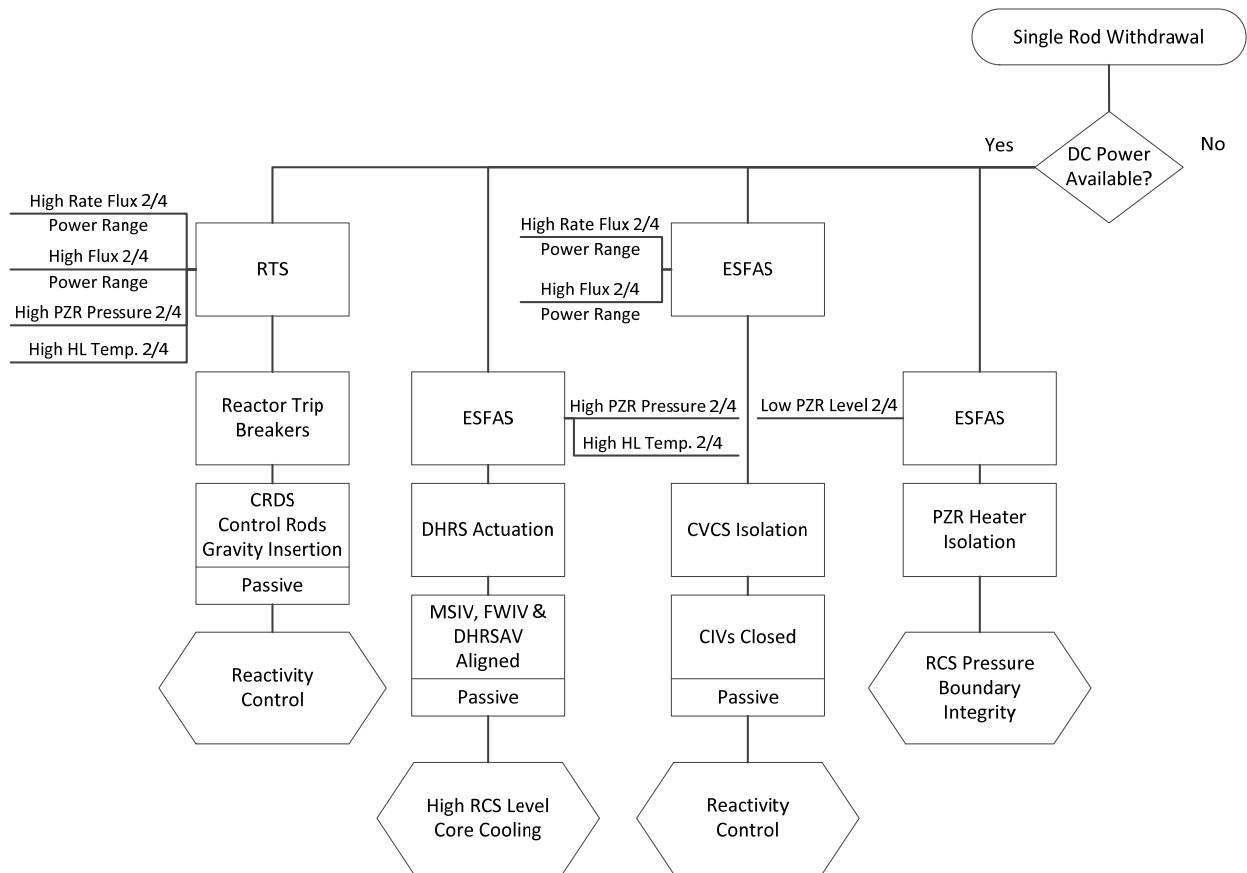


Figure D-24. Single control rod withdrawal event diagram

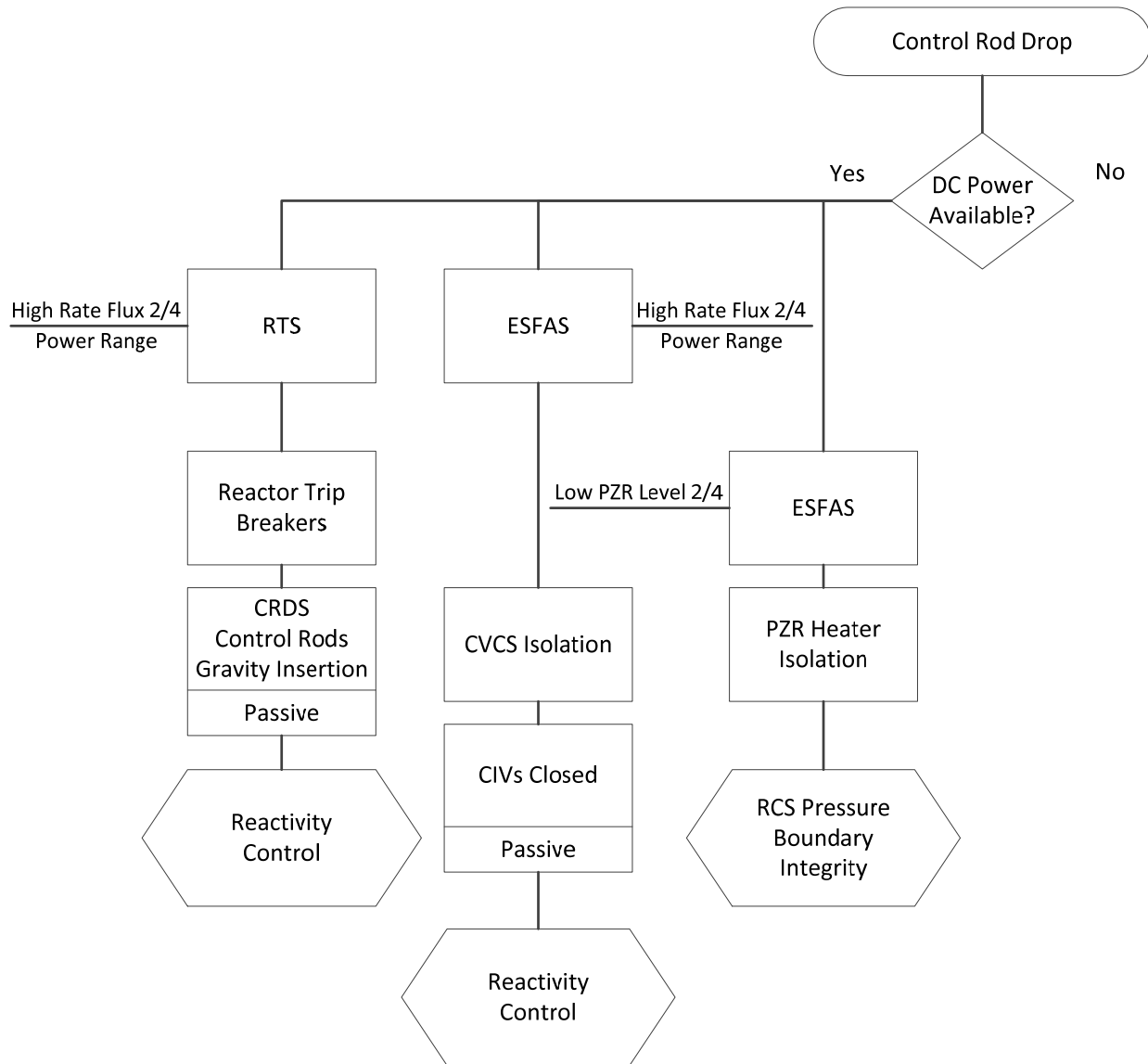


Figure D-25. Control rod drop event diagram

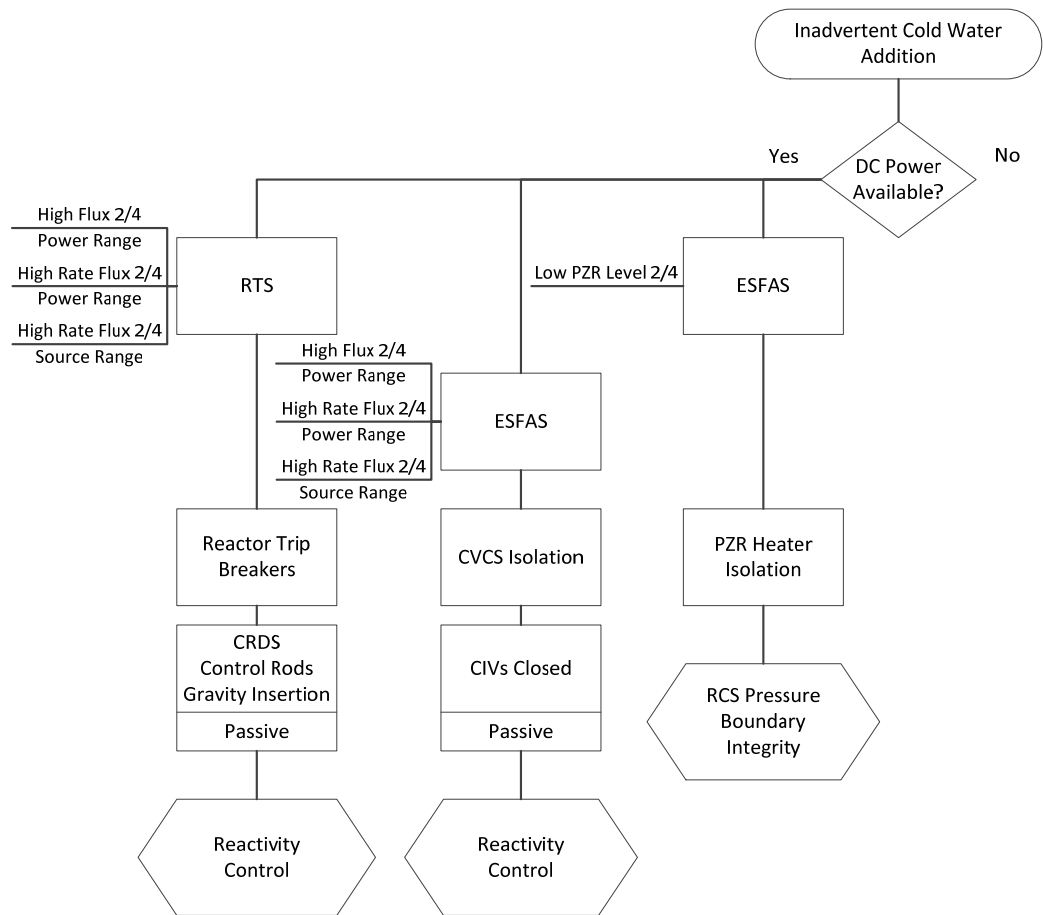


Figure D-26. Inadvertent cold water addition to the RCS event diagram

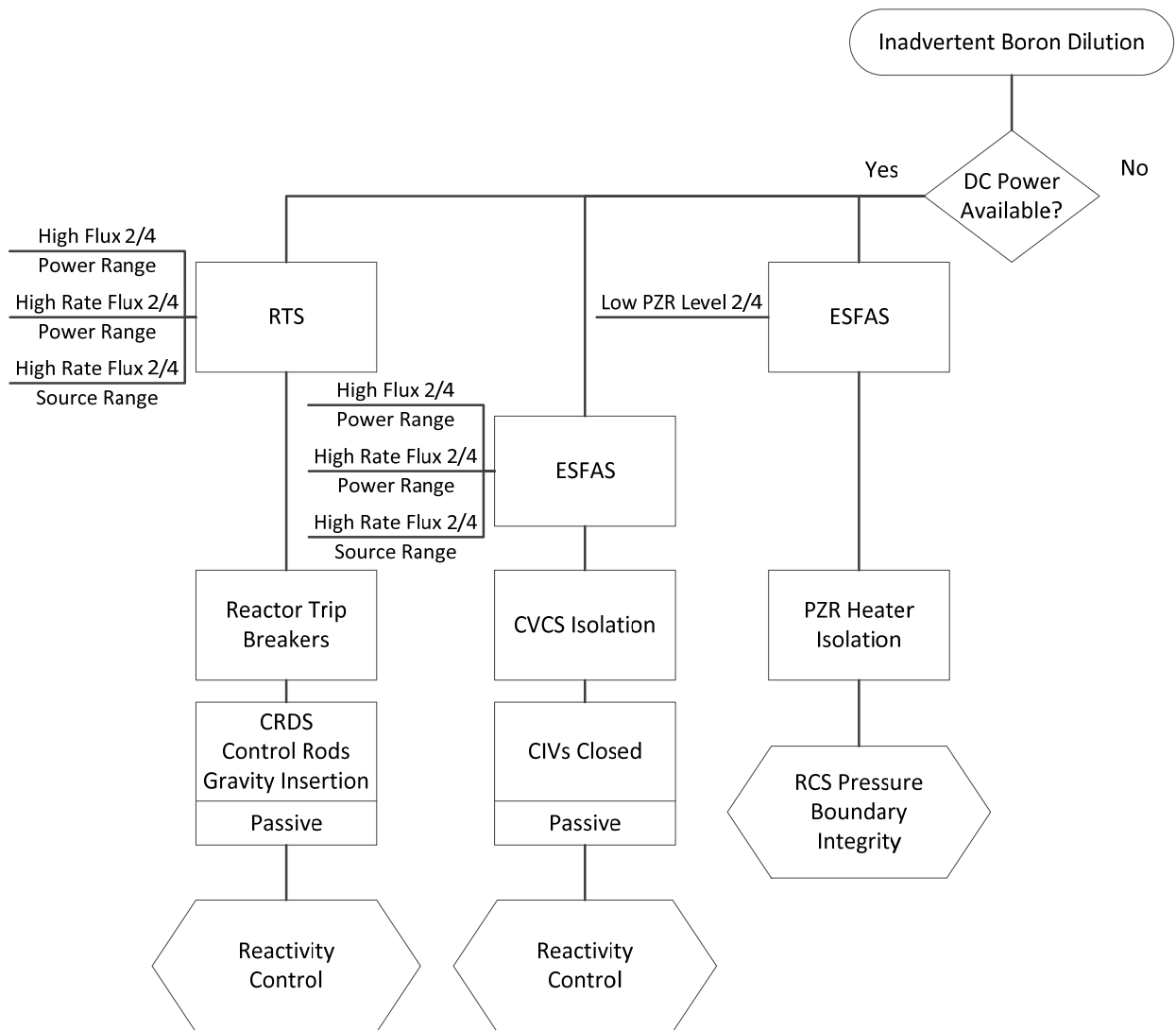


Figure D-27. Inadvertent boron dilution event diagram

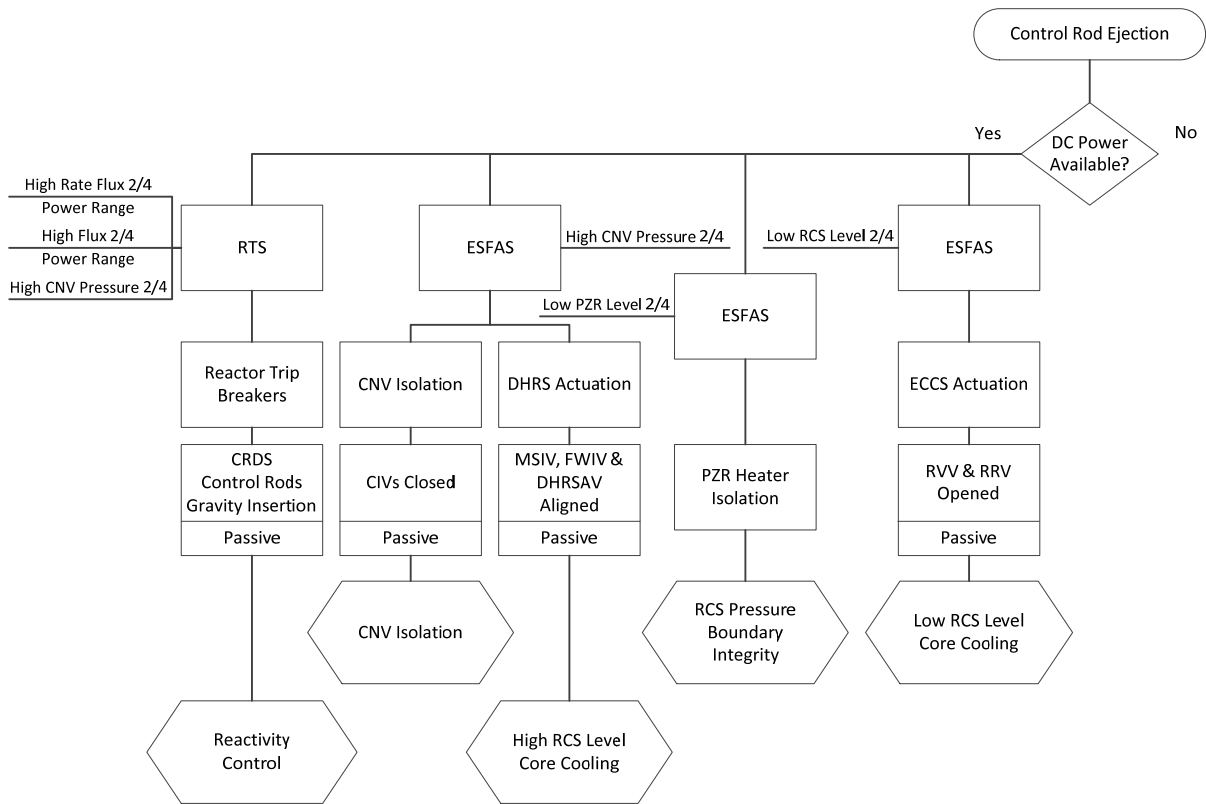


Figure D-28. Control rod ejection event diagram



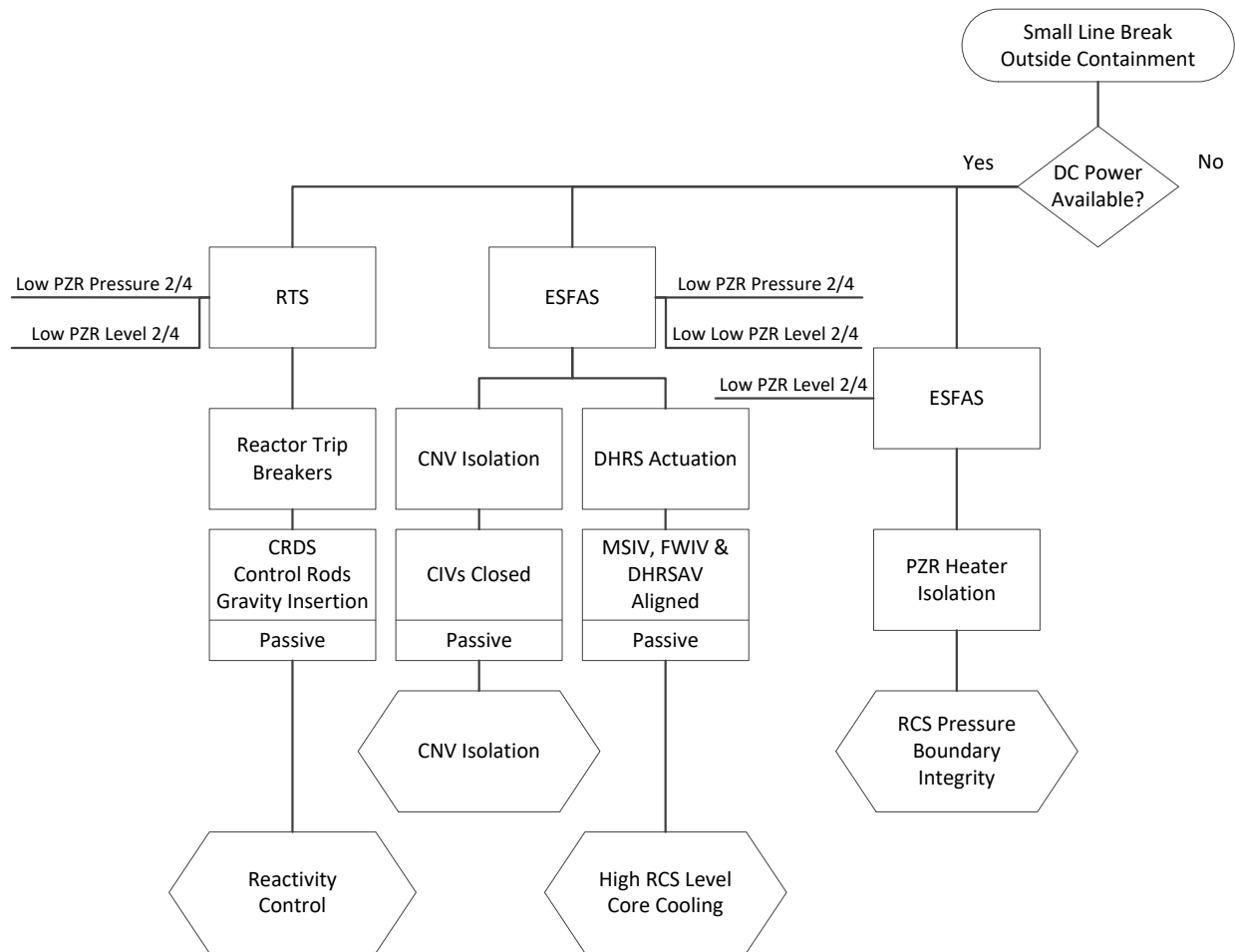


Figure D-30.Small line break outside containment event diagram

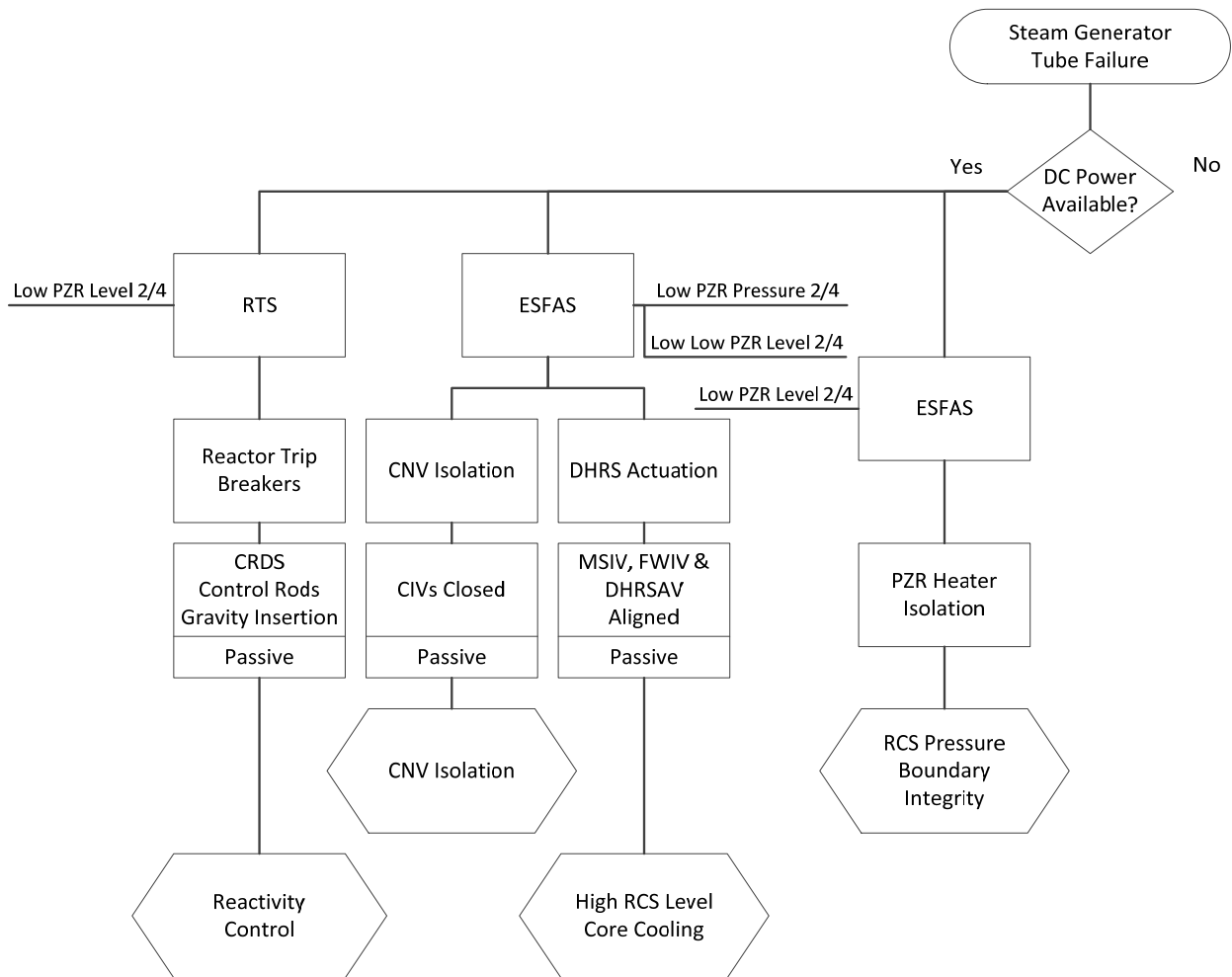


Figure D-31.Steam generator tube failure event diagram

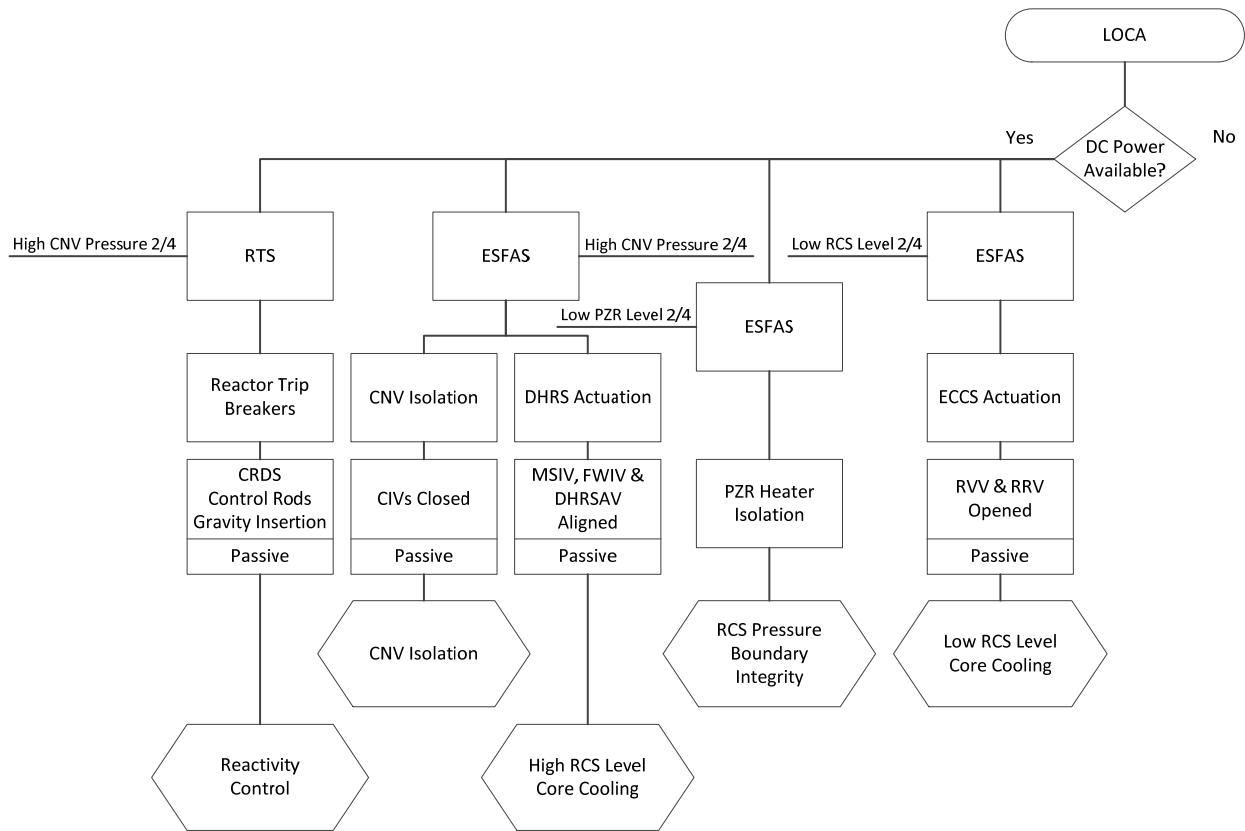


Figure D-32. Loss of coolant accident event diagram

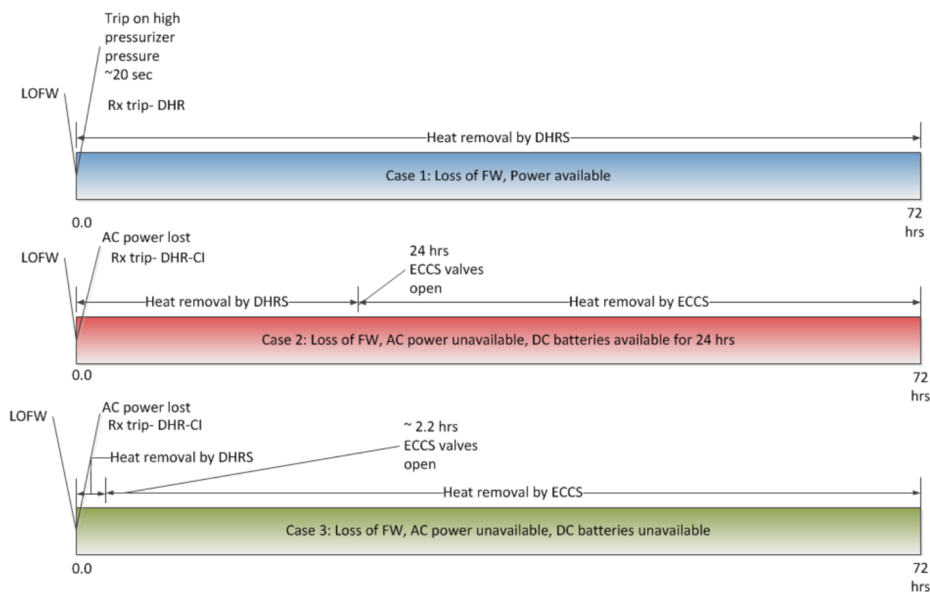


Figure D-33.LOFW event sequence diagram

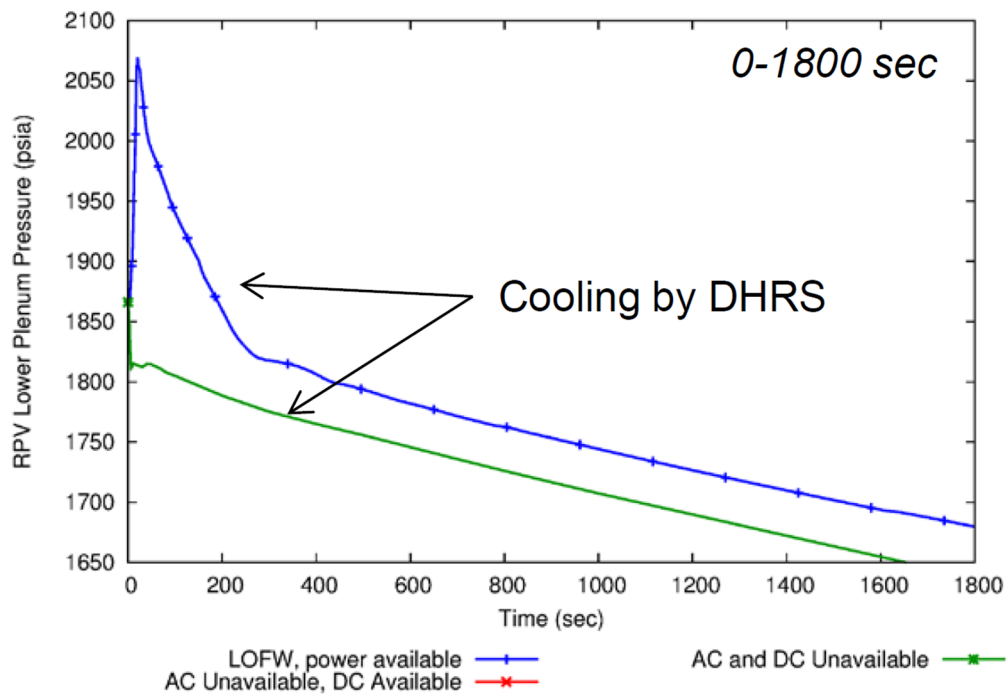


Figure D-34.RPV pressure for LOFW (30 minutes)

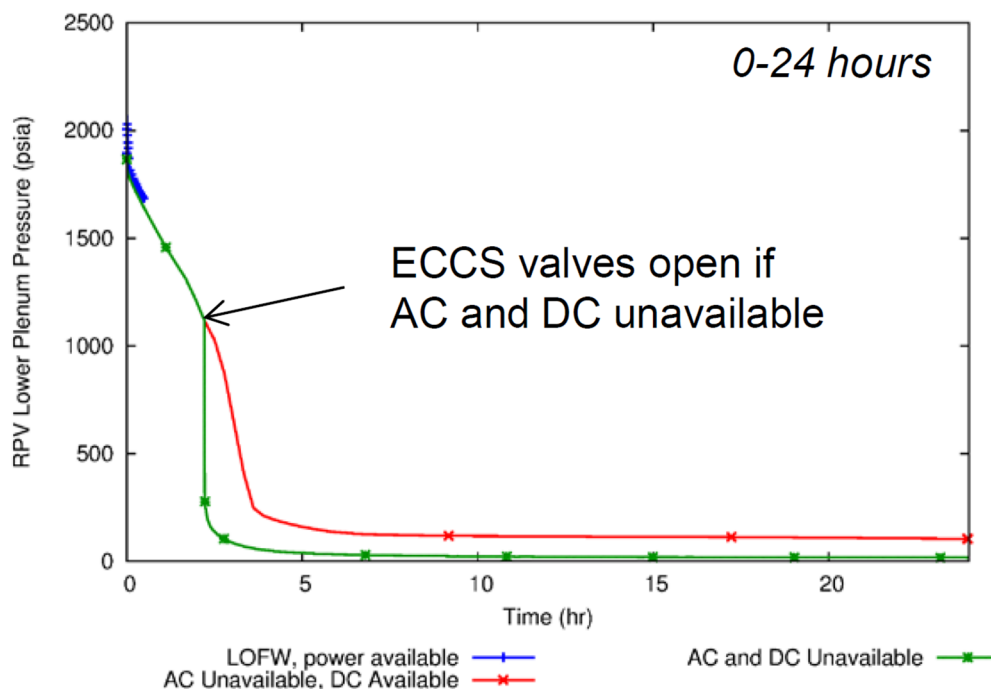


Figure D-35.RPV pressure for LOFW (24 hours)

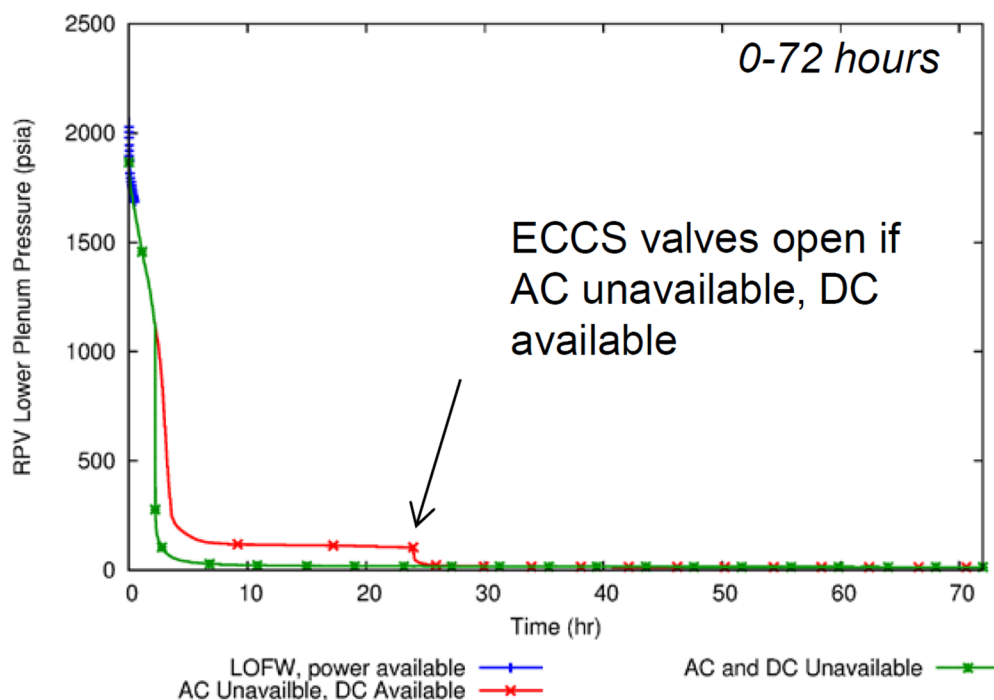


Figure D-36.RPV pressure for LOFW (72 hours)

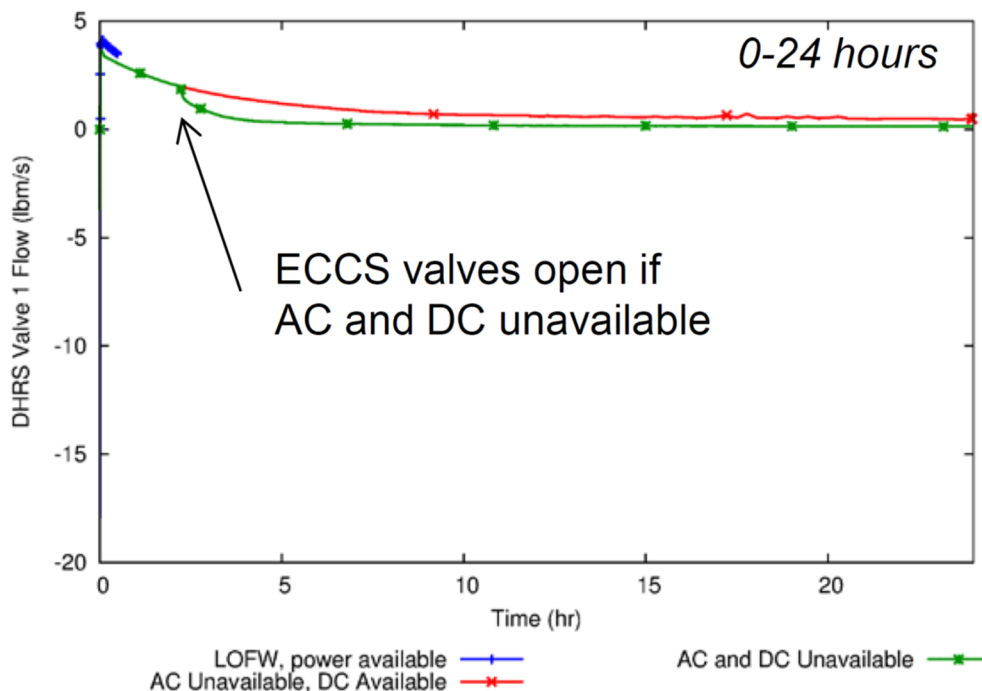


Figure D-37.DHRS flowrate for LOFW (24 hours)

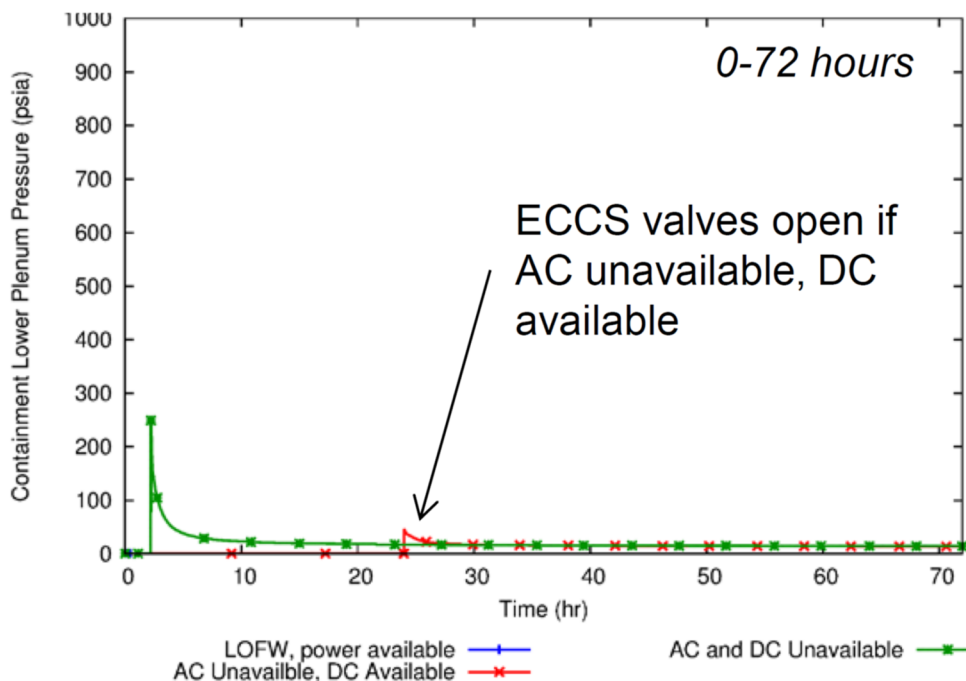


Figure D-38.CNV pressure for LOFW (24 hours)

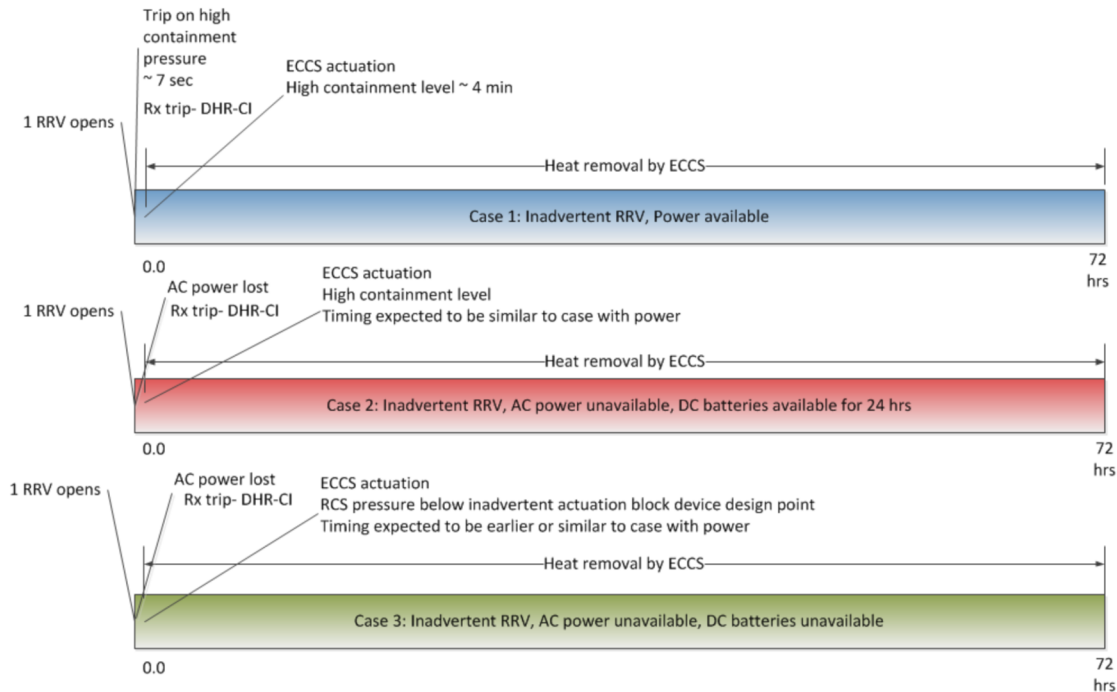


Figure D-39. Inadvertent RRV opening event sequence diagram

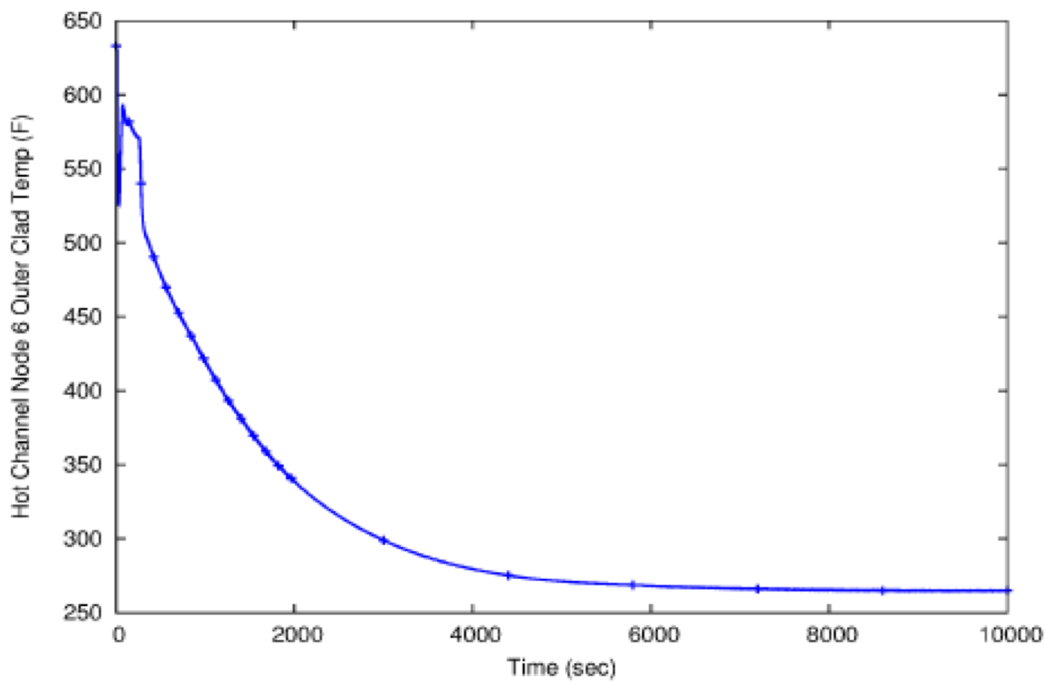


Figure D-40. Peak cladding temperature for inadvertent RRV opening event

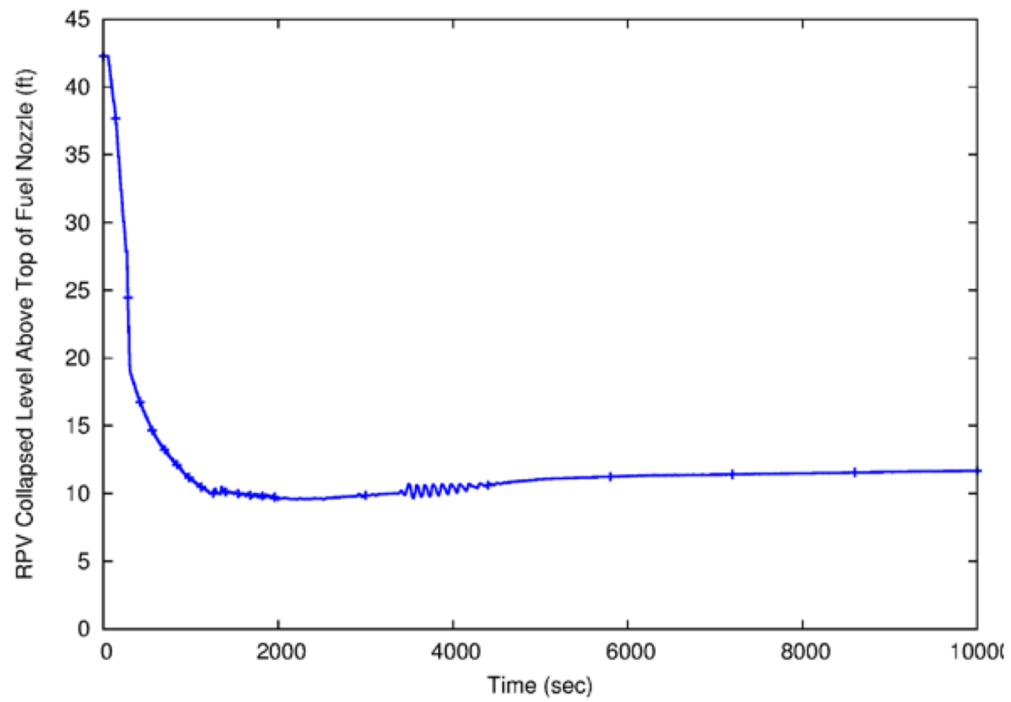


Figure D-41.RPV liquid level for inadvertent RRV opening event

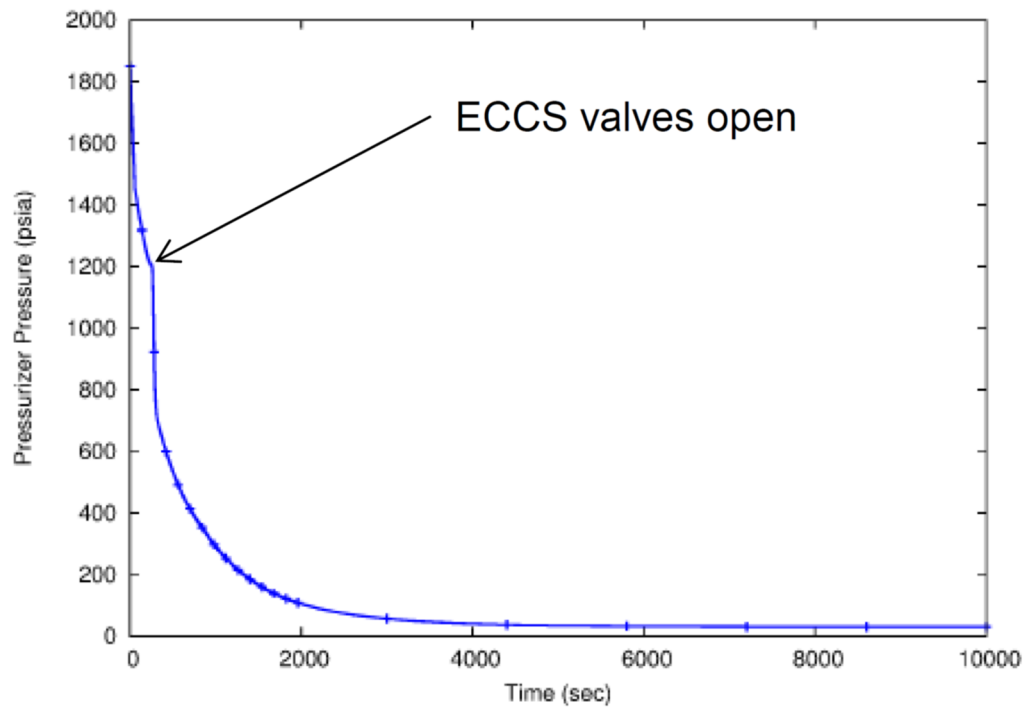


Figure D-42.RPV pressure for inadvertent RRV opening event

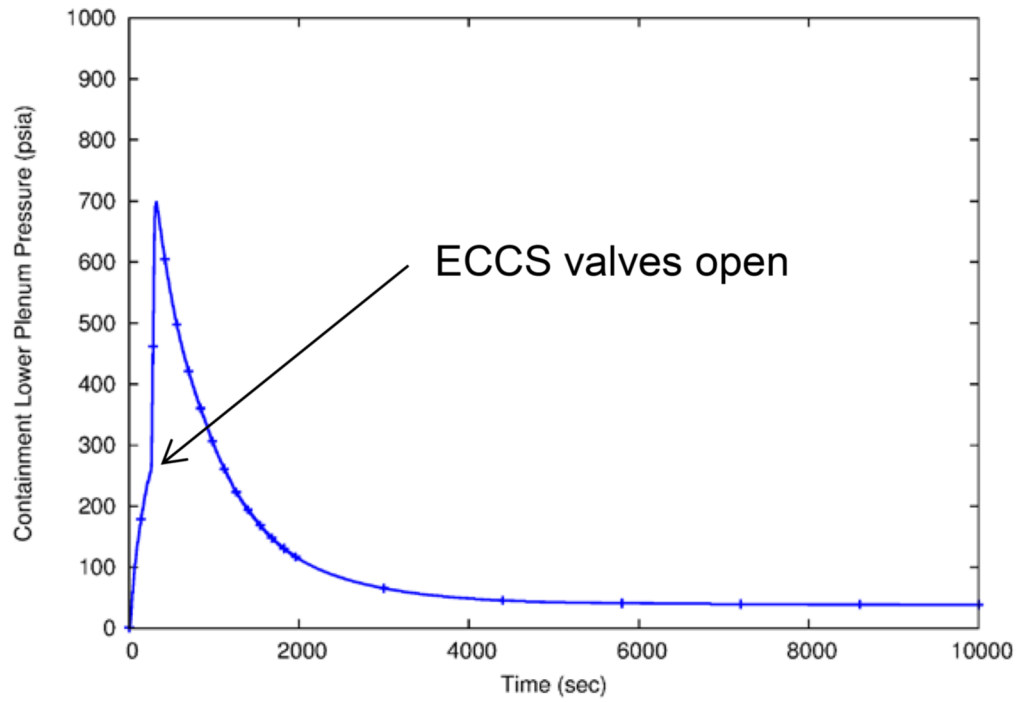


Figure D-43.CNV pressure for inadvertent RRV opening event

Section C

December 5, 2016

Docket: PROJ0769

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
One White Flint North
11555 Rockville Pike
Rockville, MD 20852-2738

SUBJECT: NuScale Power, LLC Submittal of Response to Request for Additional Information Letter No. 8 for the review of Topical Report 0815-16497, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 0.(CAC NO. RQ6002) dated October 7, 2016 (NRC Project No. 0769).

REFERENCES:

1. Letter from NuScale Power, LLC to U.S. Nuclear Regulatory Commission, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 0, TR-0815-16497, dated October 29, 2015 (ML 15306A126).
2. NuScale Topical Report, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 0, TR-0815-16497, dated October 29, 2015 (ML 15306A126).
3. Letter from U.S. Nuclear Regulatory Commission to NuScale Power, LLC, "Request for Additional Information Letter No. 8 for the Review of Topical Report 0815-16497, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 0.(CAC NO. RQ6002) dated October 7, 2016 (NRC Project No. 0769, ML16281A103).

In a letter dated October 29, 2015 (Reference 1), NuScale Power, LLC (NuScale) submitted the topical report entitled "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 0 (Reference 2). In a letter dated October 6, 2016 (Reference 3), the NRC Staff submitted Requests for Additional Information (RAI) regarding the subject topical report.

The purpose of this letter is to provide NuScale's response to the NRC RAIs. Enclosure 1 is the NuScale Response to Request for Additional Information Letter No. 8 for the review of Topical Report 0815-16497, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 0.

This letter makes no regulatory commitments and no revisions to any existing regulatory commitments. Please feel free to contact Steven Unikewicz at 240-833-3015 or at sunikewicz@nuscalepower.com if you have any questions.

Sincerely,



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

Distribution: Frank Akstulewicz, NRC, TWFN-6C20
Greg Cranston, NRC, TWFN-6E55
Omid Tabatabai, NRC, TWFN-6E55
Mark Tonacci, NRC, TWFN-6E55
Samuel Lee, NRC TWFN-6E55

Enclosure 1: Response to NRC Letter "Request for Additional Information Letter No. 8 for the review of Topical Report 0815-16497, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 0

NRC RAI Number: 8

NRC RAI Date: October 29, 2016

NRC Review of: Safety Classification of Passive Nuclear Power Plant Electrical Systems, TR-0815-16497, Revision 0.

The electrical power system presented in the Licensing Topical Report (LTR) depicts a design with no Class 1E power sources as the proposed reactor design does not require any safety-related electrical loads to support the safety analyses. However, 10 CFR 50.34(f)(2)(xx) calls for vital-bus-powered post- accident monitoring instrumentation with backup power from emergency power supplies. In order for the staff to be able to conclude that an electrical design such as the one presented in the TR provides equivalent protection to that prescribed in the regulation, the staff must be able to conclude that the proposed design is of similar (high) reliability. To that end, the staff requires the following additional information:

NRC RAI Question Number: 08.03.02-01

NRC RAI Question:

Table 3-2 of the TR states that Valve Regulated Lead Acid (VRLA) batteries will be used for the direct current (DC) power system. Based on various industry publications, including Institute of Electrical and Electronics Engineers (IEEE) Std. 1187, "Recommended Practice for Installation Design and Installation of Valve-Regulated Lead- Acid (VRLA) Batteries for Stationary Applications," the life of a VRLA battery can be seriously and suddenly reduced due to factors such as: 1) prolonged high ambient temperatures, 2) magnitude and frequency of discharge cycles, and 3) overcharging.

Please describe how these factors will be addressed in the design and operation of a passive reactor nuclear power plant that relies on VLRA battery systems to ensure high reliability DC power system.

NuScale RAI Question Response:

NuScale agrees that the life of a VRLA battery can be seriously and suddenly reduced due to prolonged high ambient temperatures. These effects are mitigated through the implementation of IEEE Std. 1187 and IEEE Std. 1188, "IEEE Recommended Practice for Maintenance, Testing, and Replacement of Valve-Regulated Lead- Acid (VRLA) Batteries for Stationary Applications" as noted in Table 3-2. Additionally, IEEE Std. 1187 refers to IEEE Std. 1491, "IEEE Guide for Selection and Use of Battery Monitoring Equipment in Stationary Applications," and IEEE Std. 1635, "IEEE/ASHRAE Guide for the Ventilation and Thermal Management of Batteries for Stationary Applications."

The use of IEEE Std. 1187 and 1188 as supplemented by IEEE Std. 1491 and 1635 provide reasonable assurance that the VLRA batteries will function as intended following exposure to prolonged periods of high ambient temperature. Further, the heating, ventilation, and air conditioning systems serving the battery and associated charger rooms are provided back-up

power from the backup power supply system to avoid prolonged periods of high ambient temperature.

NuScale agrees that the life of a VRLA battery can be seriously and suddenly reduced due to the magnitude and frequency of discharge cycles. Magnitude and frequency of discharge cycles are design considerations addressed in IEEE Std. 1187 and IEEE Std. 1188, "IEEE Recommended Practice for Maintenance, Testing, and Replacement of Valve-Regulated Lead-Acid (VRLA) Batteries for Stationary Applications" as noted in Table 3-2. Additionally, IEEE Std. 1187 refers to IEEE Std. 1491, "IEEE Guide for Selection and Use of Battery Monitoring Equipment in Stationary Applications." IEEE Std. 1491 provides monitoring criteria that may be used to detect and monitor a battery for degradation.

The use of IEEE Std. 1187 and 1188 as supplemented by IEEE Std. 1491 provide reasonable assurance that the VRLA batteries are designed, constructed, and monitored considering the potential for magnitude and frequency of discharge cycles to degrade battery performance.

NuScale agrees that the life of a VRLA battery can be seriously and suddenly reduced due to overcharging. These effects are mitigated through the implementation of IEEE Std. 1187. IEEE Std. 1187 refers to IEEE Std. 1491, "IEEE Guide for Selection and Use of Battery Monitoring Equipment in Stationary Applications."

The use of IEEE Std. 1187 as supplemented by IEEE Std. 1491 provides reasonable assurance that the VRLA batteries will not be overcharged and that instances of potential overcharging will be detected prior to degrading a battery to a point where it is not able to perform its intended function.

Impact of NRC RAI Question Response on Topical Report 0815-16497, "Safety Classification of Passive Nuclear Power Plant Electrical Systems":

This RAI Response does not require Licensing Document revisions.

Attachments:

None

NRC RAI Question Number: 08.03.02-02

NRC RAI Question:

Table 3-2 of the TR provides a comparison of the “Class 1E DC Electrical system” to the “Non Safety-Related DC Electrical System(s) Relied upon to Power Type B and Type C Accident Monitoring Instrumentation.” Under the provision “Quality Assurance” in the Table 3-2, it stated that a Graded QA Program will be applied to the DC Electrical System, which will meet or exceed the augmented QA provisions specified in RG 1.155, Appendix A, “Quality Assurance Guidance for Non-Safety Systems and Equipment”. RG 1.155, Appendix A provides QA guidance for meeting the requirements of 10 CFR 50.63 and not already explicitly covered by existing QA requirements in 10 CFR Part 50 in Appendix B or R.

Please describe the proposed quality assurance program in sufficient detail that will allow the staff to verify it meets or exceeds the provisions of RG 1.155.

NuScale RAI Question Response:

A COL applicant that references Topical Report 0815-16497 will be required to incorporate the guidance contained in RG 1.155 Appendix A, “Quality Assurance Guidance for Non-Safety Systems and Equipment as part of their Quality Assurance Program.” It is not the intention of this LTR to provide an example quality assurance program as that is COL applicant specific. Verification of sufficient detail is considered a potential NRC COL review topic.

Impact of NRC RAI Question Response on Topical Report 0815-16497, “Safety Classification of Passive Nuclear Power Plant Electrical Systems”:

This RAI Response does not require Licensing Document revisions.

Attachments:

None

NRC RAI Question Number: 08.03.02-03

NRC RAI Question:

Table 3-2 of the TR, under the provision “Batteries,” states that the VRLA batteries have augmented design, QA, and qualification provisions.

Please describe the methods and processes that will be used by a passive reactor nuclear power plant to verify that VRLA batteries will perform their intended function(s) during normal operation, operational occurrences and postulated design basis events.

NuScale RAI Question Response:

The VRLA batteries used in a passive reactor nuclear power plant design are not credited for use in mitigating the consequences of postulated design basis events.

To provide reasonable assurance that VRLA batteries will perform their intended function(s) when called upon, an applicant utilizing this TR shall implement a testing and monitoring program as described in IEEE Std. 1188, “Recommended Practice for Maintenance, Testing, and Replacement of Valve-Regulated Lead- Acid (VRLA) Batteries for Stationary Applications” and in IEEE Std. 1491, “IEEE Guide for Selection and Use of Battery Monitoring Equipment in Stationary Applications.” These Standards provide for a wide variety of operating parameters to be monitored on a continuous basis including cell specific parameters.

Additionally, Table 3-2 of the TR notes that applicants are required to environmentally qualify their VRLA batteries in accordance with IEEE Std. 323, “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations,” and seismically qualify their batteries in accordance with IEEE Std. 344, “IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations.” Such qualification provides further assurance that the batteries will perform their intended functions.

NRC RAI Question (Continued):

Please also provide the industry standards or applicable references that will be used for verification purposes.

NuScale Response (Continued):

The industry standards that will be used for verification purposes include:

1. IEEE Std. 323, “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations” as endorsed by RG 1.89
2. IEEE Std. 344, “IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations” as endorsed by RG 1.100
3. IEEE Std. 1188, “Recommended Practice for Maintenance, Testing, and Replacement of Valve-Regulated Lead- Acid (VRLA) Batteries for Stationary Applications”
4. IEEE Std. 1491, “IEEE Guide for Selection and Use of Battery Monitoring Equipment in Stationary Applications”

Impact of NRC RAI Question Response on Topical Report 0815-16497, "Safety Classification of Passive Nuclear Power Plant Electrical Systems":

This RAI Response does not require Licensing Document revisions.

Attachments:

None

NRC RAI Question Number: 08.03.02-04

NRC RAI Question:

The TR describes the presented dc power system as “highly reliable” and substantially equal in reliability to that of an analogous Class 1E dc power system. These statements have not been described adequately in the TR. In order for the staff to be able to fully evaluate the design and ultimately conclude on its acceptability as a highly reliable power system, the staff requests that NuScale provide a description of the methodology that will be used to compare the highly reliable DC system to be described in its design certification application to a Class 1E dc power system to show that the highly reliable DC system is substantially equal in reliability to a typical Class 1E dc power system.

NuScale RAI Question Response:

The LTR seeks NRC approval of the conditions of applicability, and the methodology and bases used in their development. The LTR further seeks NRC approval of the acceptability of a set of augmented design, qualification, and QA provisions to be applied by the conditions of applicability. The augmented provisions are intended to ensure suitable reliability for a direct current (DC) power system performing the nonsafety-related functions described in the LTR, analogous to a traditional licensee’s application of the augmented provisions for a 1E power system, which has been judged acceptable without a quantitative reliability acceptance criterion.

The LTR terms the subject DC power system(s) as the “highly reliable DC electrical system(s).” The LTR further states that a comparison of specified augmented design, qualification, and QA provisions to a typical Class 1E DC electrical system “supports a determination that the augmented provisions result in an electrical system reliability substantially similar to that of a Class 1E DC power system.” In using these descriptive phrases, NuScale intended to reflect, qualitatively, the attributes of a DC power system meeting the specified augmented design, qualification, and QA provisions. However, these descriptive phrases were not intended to define additional conditions for use of the LTR, distinct from the specified augmented provisions that a user of the report must implement.

However, while NuScale does not intend that a user of the LTR must, as a condition of its use, explicitly and quantitatively demonstrate “substantially similar” reliability to a typical Class 1E DC power system, NuScale intends to make available such a demonstration as one method of determining the system performs at a suitable reliability to perform the important functions addressed by the LTR. The NuScale example calculation shows that the highly reliable DC electrical system has a reliability that is approximately a factor of 5 better than that of a class 1E power system. In comparing reliability to a typical design, a user of the report should consider the specific nonsafety-related functions performed by their DC system, and the safety characteristics and risk profile of the overall plant design.

The method a Design Certification Applicant may use to compare the reliability of the highly reliable DC system to that of a typical Class 1E DC power system is as follows:

- First, define the required mission(s) the power system is required to support.

- Second, define the design and system boundaries that are needed to accomplish the required mission.
- Third, establish a measure of comparable reliability (i.e., how reliable should the system be) by reviewing a “typical” design. This typical system will be a Class 1E DC power system that supports a similar mission for a licensed facility. NuScale will build a reliability model for the typical design and assess that reliability.
- Fourth, build a reliability model for its highly reliable DC system design and assess the reliability in fulfilling the required mission.
- Finally, compare the reliability of the highly DC system to that of the typical Class 1E design. A determination that the reliability of the highly reliable DC system has reliability equal to or greater than the typical design is sufficient¹ to conclude that the reliability is acceptable for the required missions.

Impact of NRC RAI Question Response on Topical Report 0815-16497, "Safety Classification of Passive Nuclear Power Plant Electrical Systems":

This RAI Response does not require Licensing Document revisions.

Attachments:

None

¹ Reliability less than, but similar to, that of the typical system is not expected, but would require further evaluation to determine if it is adequate to support the required missions.

NRC RAI Question Number: 08.03.02-05

NRC RAI Question:

The regulation set forth in 10 CFR 50.55a(h)(3) requires that design certification applications under part 52 meet the requirements of IEEE Std. 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations." IEEE Std. 603-1991 provides a definition of "safety system" and states that the electrical portion of the safety systems, that perform safety functions, is classified as Class 1E. Included in the definition of safety system is a system that is relied upon to remain functional during and following a design basis event to ensure the capability to shut down the reactor and maintain it in a safe shutdown condition.

Condition of Applicability Item I.1.b, contained in Table 3-1 of the TR, states that sufficient reactor coolant inventory and negative reactivity are assured during and following a design basis event to achieve and maintain safe shutdown. Additionally, the TR provides a clarifying example assessment to illustrate how the Conditions of Applicability would be demonstrated. This example assessment did not include a quantitative safety analysis to demonstrate the ability to insert sufficient negative reactivity during and following a design basis event to achieve and maintain safe shutdown.

SECY-94-084, "Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems in Passive Plant Designs," clarifies the conditions that constitute a safe shutdown as reactor sub-criticality, decay heat removal, and radioactive material containment. Additionally, SECY 94-084 states that an appropriate safety analysis can be used to demonstrate passive system capabilities to bring the plant to a safe stable condition and to maintain this condition. NRC staff is seeking to clarify whether Condition of Applicability Item I.1.b is consistent with the description of safe shutdown provided in SECY-94-084. Additionally, NRC staff is seeking to clarify the requirements for demonstrating how Condition of Applicability Item I.1.b is satisfied. NRC staff requests the following additional information:

1. Specify the criteria that constitute a safe-shutdown as applied to Condition of Applicability Item I.1.b

NuScale RAI Question Response:

The criteria that constitute a safe shutdown are sub-criticality and decay heat removal in order to maintain fuel clad integrity (radioactive material containment).

These criteria are based on guidance for attaining safe shutdown in current generation reactors and for certified advanced reactors. NRC regulations that address safe shutdown do not include criteria for a safe shutdown condition or for the reliability of systems necessary to attain safe shutdown. What constitutes safe shutdown is addressed in SECY-94-084 for advanced reactors and in guidance such as RG 1.139 and BTP 5-4 for current generation reactors.

For current generation reactors that address RG 1.139 and BTP 5-4, safety analyses of design basis events are not typically relied on to demonstrate design capability to attain safe shutdown conditions. Rather, safety analyses of DBEs (as presented in Chapter 15 of a facility's final safety analysis report) is focused on the short term reactor response to ensure that fuel integrity

is maintained for anticipated operational occurrences (AOO) and a coolable core geometry is maintained for accidents. The safety analyses thereby evaluate the capability of the reactivity control systems to perform their protection function, rather than their shutdown function.

The safety issue that underpins these NRC guidance documents (SECY-94-084, RG 1.139, and BTP 5-4) and their specification of a safe shutdown condition and the systems' capability to attain safe shutdown is relevant to GDC 34, in that systems or equipment failures resulting in insufficient heat removal capability can lead to core damage. Per RG 1.139, a risk evaluation of the heat removal capability of a typical pressurized-water reactor (PWR) and boiling water reactor (BWR) plant following a plant trip showed that

...systems or equipment failures that led to the inability to remove decay heat resulted in a higher probability of a core melt than that predicted for a large LOCA for both PWRs and BWRs. Consequently, a significant safety benefit will be gained by upgrading those systems and equipment needed to maintain the RCS at the hot-standby condition for extended periods or those needed to cool and depressurize the RCS so that the RHR system can be operated.

To address the safety issue of system limitations or equipment failures resulting in insufficient heat removal capability for advanced designs, NRC staff proposed in SECY-94-084 that passive system capabilities can be demonstrated by:

- 1. A safety analysis to demonstrate that the passive systems can bring the plant to a safe stable condition and maintain this condition, that no transients will result in the SAFDLs and pressure boundary design limit being violated, and that no high-energy piping failure being initiated from this condition will result in violation of 10 CFR 50.46 criteria.*
- 2. A probabilistic reliability analysis, including events initiated from the safe shutdown conditions, to ensure conformance with the safety goal guidelines. The PRA would also determine the R/A missions of risk significant systems and components as a part of the effort for regulatory treatment of non-safety systems.*

Conservative assumptions are applied to Chapter 15 safety analysis of DBEs appropriate for the intended purpose of ensuring appropriate margins to protect fuel integrity or core coolability. Although these safety analyses can be used to demonstrate adequate shutdown capability per SECY-94-084, application of the same conservative assumptions may lead to excessive margin with respect to shutdown capability. Shutdown with additional margin due to conservative safety analysis assumptions may not be appropriate, considering a specific design's heat removal and shutdown capability and reliability.

NRC RAI Question (Continued):

2. Describe how a future passive plant applicant will demonstrate that electrical power is not necessary to achieve and maintain a safe shutdown for a minimum of 72 hours.

NuScale Response (Continued):

Electrical power is not necessary to achieve and maintain a safe shutdown condition for a minimum of 72 hours if the design includes safety-related capability to maintain a safe shutdown condition that does not depend on electrical power.

To demonstrate that capability, an applicant will evaluate the reactivity control systems to ensure sufficient shutdown function capability and evaluate the decay heat removal system to ensure sufficient heat removal capability. To ensure that safe shutdown capability is sufficient to address the safety issue of heat removal reliability, a probabilistic risk assessment is used to ensure that the reliability of systems used to achieve and maintain safe shutdown supports conformance to the commission's safety goal guidelines.

The response to RAIs 08.03.02-05, Question 1 and 2, describes an approach to meet the Conditions of Applicability. The design capability along with the approach to meet Conditions of Applicability is design specific and should be evaluated as part of an applicant's design certification or combined license application, rather than evaluating it within the scope of Topical Report 0815-16497, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," which is intended to be design independent. Requiring a specific approach to meet Conditions of Applicability may be suitable for some designs but overly prescriptive for other designs.

Impact of NRC RAI Question Response on Topical Report 0815-16497, "Safety Classification of Passive Nuclear Power Plant Electrical Systems":

This RAI Response does not require Licensing Document revisions.

Attachments:

None

NRC RAI Question Number: 08.03-02-06

NRC RAI Question:

GDC 15 requires the reactor coolant system and associated auxiliary, control, and protection systems be designed with sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, including anticipated operational occurrences.

Condition No. I.1 of the Conditions of Applicability, contained in Table 3-1 of TR-0815- 16497, states that for a design basis event, electrical power is not necessary to maintain the reactor coolant pressure boundary (RCPB) integrity for a minimum of 72 hours. Additionally, TR-0815-16497 provides a clarifying example assessment to illustrate how the Conditions of Applicability would be demonstrated. This example assessment includes a safety analysis showing an example passive plant response to an anticipated operational occurrence. The safety analysis shows that the example passive plant response to the anticipated operational occurrence includes establishing a direct coolant flow path between the reactor core and the containment, thereby removing a fission product barrier. This caused NRC staff to question if the items under Conditions of Applicability I.1 are sufficient to demonstrate RCPB integrity. Additionally, RIS 2005-29, discusses the design criteria for event non-escalation. NRC staff is questioning why the removal of a fission product barrier is not considered an event escalation.

NRC staff requests the following information:

1. Specify the criteria that constitute RCPB integrity as applied to Condition No. I.1 of the Conditions of Applicability.

NuScale RAI Question Response:

RCPB integrity refers to the structural integrity of RCPB components designed to retain pressure and contain reactor coolant. A loss of RCPB integrity or loss of structural integrity involves a mechanical failure in an RCPB component, for example a pipe. For an AOO, the RCPB integrity acceptance criterion is that pressure in the reactor coolant and main steam systems should be maintained below 110 percent of the design values. For a postulated accident, the criteria for RCPB integrity is that pressure in the RCS is maintained below acceptable design limits, considering potential brittle as well as ductile failures.

Opening of a valve(s) that allows reactor coolant to pass into or out of the RCPB does not involve a mechanical failure in an RCPB component and does not constitute a loss of RCPB integrity. An interpretation that RCPB integrity is lost when opening a valve to allow fluid to pass through the RCPB is problematic in the following respects:

- It would preclude advanced designs that offer improvements in safety by relying on valves to depressurize the RCS for safe shutdown. As described in RG 1.139 and BTP 5-4, depressurization is one of the processes that support safe shutdown. The safety benefit of RCS depressurization through valves include: providing highly reliable means for depressurization; reducing the driving force for coolant out of the RCS; and reducing the driving force for fission products out of containment in the event of a loss in clad

integrity. Further, the ability to depressurize and provide long term heat removal using valves is consistent with the NRC's position to minimize the potential for an intersystem Loss of Coolant Accident (LOCA) outside of containment in advanced or evolutionary light-water reactors in SECY-90-016 and SECY-93-087 and their associated staff requirements memoranda. Lastly, the capability of advanced designs, such as NuScale, to safely depressurize the RCS reduces the importance of RCPB integrity to safety.

- It is not consistent with the licensing basis for PWRs and BWRs; it would imply that these designs do not comply with GDC 15. GDC 15 is relevant to Standard Review Plan (SRP) Section 15.0 "as it relates to the RCS and its associated auxiliaries being designed with appropriate margin to ensure that the pressure boundary will not be breached during normal operations, including AOOs." Interpreting that opening of a valve to allow fluid to pass into or out of the RCPB constitutes a breach of the RCPB would imply that licensed facilities do not meet GDC 15 in the following instances.
 - PWRs and BWRs rely on safety relief valves to prevent exceeding RCPB design limits for select AOOs.
 - PWRs and BWRs evaluate inadvertent opening of a pressure relief valve as an AOO in accordance with SRP 15.0 and SRP 15.6.1.
 - BWRs open valves (safety relief valve, reactor core isolation cooling) to route reactor coolant out of the RCPB to containment for the purpose of heat removal and RCS depressurization prior to transitioning to heat removal using the residual heat removal (RHR) system at low pressures.
 - The RHR systems for PWRs and BWRs are not part of the RCPB. Valves are opened upon RHR system actuation to cycle reactor coolant into and out of the RCPB and through the RHR system for the purpose of heat removal.
- It is not consistent with Appendix A to 10 CFR 50 which address maintaining structural integrity of RCPB components rather than preventing the opening of valves to allow fluid to pass into or out of the RCPB. Under Appendix A, GDC 14, "Protection by Multiple Fission Product Barriers," addresses RCPB integrity: "The reactor coolant pressure boundary shall be designed, fabricated, erected, and tested so as to have an extremely low probability of abnormal leakage, of rapidly propagating failure, and of gross rupture." Further, GDCs 15, 17, 28, 30, 31, 32, 33 and 34 include provisions to design, operate, and maintain the RCPB in order to prevent loss of structural integrity.

The opening of RCPB valves is addressed by 10 CFR 50.34(f)(1)(iv). The safety concern addressed by 10 CFR 50.34(f)(1)(iv), however, is the adverse impact on core damage frequency (CDF) due to frequent valve actuation, rather than a loss of RCPB integrity. 10 CFR 50.34(f)(1)(iv) was added after the TMI-2 accident when it was recognized that a loss of coolant from a stuck open PORV and other small-break LOCA contributors was more likely to lead to core damage than a large pipe break. The rule requires evaluation of the potential benefit from automatic PORV isolation for current generation PWR's in order to reduce CDF by reducing the demand on ECCS system. For advanced designs with a low CDF, a reduction in CDF by limiting deliberate or inadvertent RCPB valve actuation to reduce the CDF may not be warranted.

NRC RAI Question (Continued):

2. Explain why the removal of a fission product barrier during an anticipated operational occurrence is not considered an event escalation.

NuScale RAI Question Response (Continued):

Opening a valve to depressurize the RCS and establish long term cooling is not considered a removal of a fission product barrier, and thus not an event escalation, because the functions of the RCS barrier are not lost. The RCS barrier continues to provide a confined volume for reactor coolant which allows a flow path for cooling the core and thus, confining fission products to the fuel. The basis for this response is as follows.

As part of the analysis acceptance criteria for AOOs (p15.0-5, SRP 15.0),

The reviewer applies a third criterion, based on the American Nuclear Safety (ANS) standards to ensure that there is no possibility of initiating a postulated accident with the frequency of occurrence of an AOO.

This review is performed under Acceptance Criterion 2.A.iii, based on the ANS standards referenced in SRP 15.0, which states:

An AOO should not generate a postulated accident without other faults occurring independently or result in a consequential loss of function of the RCS or reactor containment barriers.

Based on SRP 15.0, the intent of the non-escalation criterion is to ensure that the consequences associated with accidents do not occur at the frequency of an AOO. Such a condition would lead to an unacceptable risk to the public, due to frequent events with more significant consequences. The two parts of the non-escalation criterion, preventing accidents generated by an AOO and protecting the functions of barriers, are intended to prevent such an increase in risk. Thus, events that do not result in unacceptable consequences or significantly increase the risk for radiological release do not challenge the intent of the non-escalation criterion.

With respect to whether opening of a valve to depressurize the RCS involves a “consequential loss of function of the RCS barrier,” it is helpful to review the regulatory history of this acceptance criterion. Acceptance Criterion 2.A.iii and the definition of event categories were first introduced in Rev. 0 of the SRP and were derived from the PWR and BWR ANS standards for nuclear safety. The PWR standard referred to in Rev. 0 of the SRP, ANSI N18.2, was reviewed to clarify what was meant with this acceptance criterion.

The SRP cites this acceptance criterion for ANSI N18.2 Condition II (“Incidents of Moderate Frequency”) and Condition III (“Infrequent Incidents”) events. ANSI N18.2 presents the following events as examples of Condition II and III events:

- Condition II example: “depressurization by spurious operation of an active element, for example, relief valve, pressurizer spray valve.”

- Condition III example: “loss of reactor coolant, such as from a small ruptured pipe or from a crack in a large pipe, which would prevent orderly reactor shutdown and cooldown assuming makeup is provided by normal makeup systems only” (i.e., small-break loss of coolant accident (LOCA)).

These ANSI N18.2 examples are also included in examples of AOOs in SRP 15.0. The ANSI N18.2 design requirement that is the basis for Acceptance Criterion 2.A.iii (3) in SRP 15.0 is:

A Condition III incident shall not, by itself, generate a Condition IV fault or result in a consequential loss of function of the reactor coolant system or reactor containment barriers.

Thus, Condition II and III events do not in themselves involve a consequential (significant)² loss of function of the RCS barrier. Of particular interest, the two examples given above that result in continuously blowing down reactor coolant from the RCS, either through a valve (Condition II) or through a small-break LOCA (Condition III), do not result in a consequential loss of function of the RCS barrier.

A consequential loss of function of the RCS barrier is associated with only Condition IV (“Limiting Fault” or “Postulated Accident”) events. Based on the Condition IV example provided in ANSI N18.2 and repeated in SRP 15.0, a loss of function of the RCS barrier is associated with a major pipe rupture. This interpretation is consistent with Appendix A to 10 CFR Part 50 Section II, “Protection by Multiple Fission Product Barriers” which includes general design criteria for the fission product barriers. GDCs 14 and 15 state the design criteria for the RCPB and the RCS, which are intended to have “an extremely low probability of abnormal leakage, of rapidly propagating failure and of gross rupture.”

That is, the function of the RCS, as implemented by these GDCs, is not to form a leak-tight radionuclide barrier to the environment; in contrast the function of the containment as stated in GDC 16 is to “...establish an essentially leak-tight barrier against the uncontrolled release of radioactivity to the environment”

Rather, the RCPB functions, which are equivalent to that of the RCS barrier, are stated in SRP 5.2.3 under the technical rationale for GDC 14:

The RCPB provides a fission product barrier, a confined volume for the inventory of reactor coolant, and flow paths to facilitate core cooling.

A loss of these functions is also described in SRP Section 5.2.3 as a “gross failure of the RCPB resulting in substantial reduction in capability to contain reactor coolant inventory, reduction in capability to confine fission products, or interference with core cooling.”

² The word “consequential” can mean resultant or significant. “Significant” makes more sense in the context of Acceptance Criterion 2.A.iii. Under “Barrier Integrity Criteria” for the RCPB, ANSI N18.2 (3rd criterion, p8, Reference 9) states that the RCPB “shall withstand Conditions I, II, III and IV, including thermal transients associated with the operation of the emergency core cooling system, without significant consequential rupture (that is, if consequential rupture occurs, it shall not appreciably worsen the safety consequences).” The terms “result in a consequential loss of function” (Acceptance Criterion 2.A.iii) and “significant consequential rupture” (ANSI N18.2) are equivalent and are interpreted to mean “result in a significant loss of function due to RCPB rupture.” In comparison, the design criterion for the “Containment Barrier” is: “The design pressure, temperature, and leakage rate of the reactor containment shall not be exceeded as a result of Conditions I, II, III, or IV.”

Thus, gross failure is a necessary condition for such a substantial loss of function. Further, gross failure resulting in a substantial reduction of any one of the three functions of the RCPB constitutes a substantial or consequential loss in function of the RCS barrier. This is because the function of fission product confinement is integrated with the functions of inventory control and heat removal; i.e., the function of fission product confinement is maintained if the functions of inventory control and heat removal are maintained. “Fission product barrier” does not mean that leakage from fuel defects or activation products in RCS coolant must be confined in the RCS after all design basis events. It refers to maintaining integrity of the cladding. Absent the potential for fuel cladding failure, there are no significant radiological consequences associated with the event, and therefore no “consequential loss of function” of the RCS barrier.

Thus, opening a valve to depressurize the RCS and establish long term cooling does not result in a consequential loss of function of the RCS barrier, i.e. a substantial reduction in capability to contain reactor coolant inventory, reduction in capability to confine fission products, or interference with core cooling. Accordingly, opening such valve during an anticipated operational occurrence is not considered an event escalation.

Impact of NRC RAI Question Response on Topical Report 0815-16497, "Safety Classification of Passive Nuclear Power Plant Electrical Systems":

This RAI Response does not require Licensing Document revisions.

Attachments:

None

Section D

February 17, 2017

Docket: PROJ0769

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
One White Flint North
11555 Rockville Pike
Rockville, MD 20852-2738

SUBJECT: NuScale Power, LLC Submittal of Topical Report TR-0815-16497, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 1 (CAC No. RQ6002)

REFERENCES:

1. Letter from NuScale Power, LLC to U.S. Nuclear Regulatory Commission, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 0 TR-0815-16497, dated October 29, 2015 (ML 15306A126)
2. NuScale Topical Report, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 0, TR-0815-16497, dated October 29, 2015 (ML 15306A126)
3. Letter from U.S. Nuclear Regulatory Commission to NuScale Power, LLC, "Request for Additional Information Letter No. 8 for the Review of NuScale Topical Report (TR) 0815-17497, 'Safety Classification of Passive Nuclear Power Plant Electrical Systems,' Revision 0 (CAC No. RQ6002)," dated October 7, 2016 (ML16281A103).
4. Letter from NuScale Power, LLC to U.S. Nuclear Regulatory Commission, "Submittal of Response to Request for Additional Information Letter No. 8 for the review of Topical Report 0815-16497, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 0, dated December 5, 2016 (ML 16340D339)

In a letter dated October 29, 2015 (Reference 1), NuScale Power, LLC (NuScale) submitted the topical report titled "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 0 (Reference 2). In a letter dated October 7, 2016 (Reference 3), the NRC Staff provided Request for Additional Information (RAI) No. 8 regarding the subject topical report. NuScale submitted responses to the NRC RAI in a letter dated December 5, 2016 (Reference 4).

The purpose of this letter is to provide Revision 1 of the Topical Report TR-0815-16497 incorporating changes that resulted from the RAI responses in Reference 4. Changes are summarized with revision bars in the margin. Additional edits have also been made to the proprietary markings of the report, assuring consistency with the recently submitted NuScale Final Safety Analysis Report and other industry guidance. These proprietary marking revisions were not highlighted with revision bars.

Enclosure 1 is the proprietary version of the report titled "Safety Classification of Passive Nuclear Power Plant Electrical Systems" Revision 1. Enclosure 2 is the nonproprietary version of the report titled "Safety Classification of Passive Nuclear Power Plant Electrical Systems" Revision 1.

NuScale requests that the proprietary Enclosure 1 be withheld from public disclosure in accordance with the requirements of 10 CFR § 2.390. The enclosed affidavit (Enclosure 3) supports this request.

This letter and its enclosures make no regulatory commitments and no revisions to any existing regulatory commitments.

Please feel free to contact Jennie Wike at (541) 360-0539 or at jwike@nuscalepower.com if you have any questions.

Sincerely,



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

Distribution: Frank Akstulewicz, NRC, TWFN-6C20
Greg Cranston, NRC, TWFN-6E55
Omid Tabatabai, NRC, TWFN-6E55
Samuel Lee, NRC, TWFN-6C20

- Enclosure 1: TR-0815-16497-P, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 1, proprietary version
- Enclosure 2: TR-0815-16497-NP, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 1, nonproprietary version
- Enclosure 3: Affidavit of Thomas A. Bergman, AF-0217-52964

Enclosure 2:

TR-0815-16497-NP, "Safety Classification of Passive Nuclear Power Plant Electrical Systems," Revision 1, nonproprietary version

Note: This enclosure to NuScale's February 17, 2017 letter to the NRC was the non-redlined version of Revision 1 of the Safety Classification of Passive Nuclear Power Plant Electrical Systems Topical Report, and is the same as Revision 1 included in Section B, with the exception that the Section B version includes "-A" in the document identification number. Therefore, this enclosure is not included in the current package.

Enclosure 3:

Affidavit of Thomas A. Bergman, AF-0118-58310

NuScale Power, LLC

AFFIDAVIT of Thomas A. Bergman

I, Thomas A. Bergman, state as follows:

- (1) I am the Vice President of Regulatory Affairs of NuScale Power, LLC (NuScale), and as such, I have been specifically delegated the function of reviewing the information described in this Affidavit that NuScale seeks to have withheld from public disclosure, and am authorized to apply for its withholding on behalf of NuScale.
- (2) I am knowledgeable of the criteria and procedures used by NuScale in designating information as a trade secret, privileged, or as confidential commercial or financial information. This request to withhold information from public disclosure is driven by one or more of the following:
 - (a) The information requested to be withheld reveals distinguishing aspects of a process (or component, structure, tool, method, etc.) whose use by NuScale competitors, without a license from NuScale, would constitute a competitive economic disadvantage to NuScale.
 - (b) The information requested to be withheld consists of supporting data, including test data, relative to a process (or component, structure, tool, method, etc.), and the application of the data secures a competitive economic advantage, as described more fully in paragraph 3 of this Affidavit.
 - (c) Use by a competitor of the information requested to be withheld would reduce the competitor's expenditure of resources, or improve its competitive position, in the design, manufacture, shipment, installation, assurance of quality, or licensing of a similar product.
 - (d) The information requested to be withheld reveals cost or price information, production capabilities, budget levels, or commercial strategies of NuScale.
 - (e) The information requested to be withheld consists of patentable ideas.
- (3) Public disclosure of the information sought to be withheld is likely to cause substantial harm to NuScale's competitive position and foreclose or reduce the availability of profit-making opportunities. The accompanying Approved Version of Topical Report TR-0815-16497 Revision 1 reveals distinguishing aspects about the process and method by which NuScale develops its Safety Classification of Passive Nuclear Power Plant Electrical Systems Methodology.

NuScale has performed significant research and evaluation to develop a basis for this methodology and has invested significant resources, including the expenditure of a considerable sum of money.

The precise financial value of the information is difficult to quantify, but it is a key element of the design basis for a NuScale plant and, therefore, has substantial value to NuScale.

If the information were disclosed to the public, NuScale's competitors would have access to the information without purchasing the right to use it or having been required to undertake a similar expenditure of resources. Such disclosure would constitute a misappropriation of NuScale's intellectual property, and would deprive NuScale of the opportunity to exercise its competitive advantage to seek an adequate return on its investment.

- (4) The information sought to be withheld is in Section B of Enclosure 1 to NuScale letter titled "Submittal of Approved Version of Topical Report TR-0815-16497, "Safety Classification of Passive Nuclear Power Plant Electrical Systems, Revision 1." Enclosure 1 contains the designation "Proprietary" at the top of each page containing proprietary information. The information considered by NuScale to be proprietary is identified within double braces, "{{ }}" in the document.

- (5) The basis for proposing that the information be withheld is that NuScale treats the information as a trade secret, privileged, or as confidential commercial or financial information. NuScale relies upon the exemption from disclosure set forth in the Freedom of Information Act ("FOIA"), 5 USC § 552(b)(4), as well as exemptions applicable to the NRC under 10 CFR §§ 2.390(a)(4) and 9.17(a)(4).
- (6) Pursuant to the provisions set forth in 10 CFR § 2.390(b)(4), the following is provided for consideration by the Commission in determining whether the information sought to be withheld from public disclosure should be withheld:
- (a) The information sought to be withheld is owned and has been held in confidence by NuScale.
 - (b) The information is of a sort customarily held in confidence by NuScale and, to the best of my knowledge and belief, consistently has been held in confidence by NuScale. The procedure for approval of external release of such information typically requires review by the staff manager, project manager, chief technology officer or other equivalent authority, or the manager of the cognizant marketing function (or his delegate), for technical content, competitive effect, and determination of the accuracy of the proprietary designation. Disclosures outside NuScale are limited to regulatory bodies, customers and potential customers and their agents, suppliers, licensees, and others with a legitimate need for the information, and then only in accordance with appropriate regulatory provisions or contractual agreements to maintain confidentiality.
 - (c) The information is being transmitted to and received by the NRC in confidence.
 - (d) No public disclosure of the information has been made, and it is not available in public sources. All disclosures to third parties, including any required transmittals to NRC, have been made, or must be made, pursuant to regulatory provisions or contractual agreements that provide for maintenance of the information in confidence.
 - (e) Public disclosure of the information is likely to cause substantial harm to the competitive position of NuScale, taking into account the value of the information to NuScale, the amount of effort and money expended by NuScale in developing the information, and the difficulty others would have in acquiring or duplicating the information. The information sought to be withheld is part of NuScale's technology that provides NuScale with a competitive advantage over other firms in the industry. NuScale has invested significant human and financial capital in developing this technology and NuScale believes it would be difficult for others to duplicate the technology without access to the information sought to be withheld.

I declare under penalty of perjury that the foregoing is true and correct. Executed on February 23, 2018.



Thomas A. Bergman