Licensing Technical Report

Treatment of DC Power in Safety Analyses

August 2023

Revision 1

Docket: 52-050

NuScale Power, LLC
1100 NE Circle Blvd., Suite 200
Corvallis, Oregon 97330
www.nuscalepower.com
© Copyright 2023 by NuScale Power, LLC

© Copyright 2023 by NuScale Power, LLC

Licensing Technical Report

COPYRIGHT NOTICE

This report has been prepared by NuScale Power, LLC and bears a NuScale Power, LLC, copyright notice. No right to disclose, use, or copy any of the information in this report, 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 this report that is necessary 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 copies necessary 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 and contain the proprietary marking if the original was identified as proprietary.

© Copyright 2023 by NuScale Power, LLC

Licensing Technical Report

Department of Energy Acknowledgement and Disclaimer

This material is based upon work supported by the Department of Energy under Award Number DE-NE0008928.

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.

© Copyright 2023 by NuScale Power, LLC

Table of Contents

© Copyright 2023 by NuScale Power, LLC

Table of Contents

© Copyright 2023 by NuScale Power, LLC

List of Tables

© Copyright 2023 by NuScale Power, LLC

List of Figures

© Copyright 2023 by NuScale Power, LLC

Abstract

This technical report provides a single-source document of the technical and regulatory bases for the safety analysis treatment of the augmented DC power system for the NuScale Power Module in the US460 Standard Design. The document provides a high-level overview of the following:

- The US460 design, including the NuScale Power Module, the emergency core-cooling systems, the decay heat removal system, and the DC electrical power systems.
- The NuScale design process to determine the safety and risk classification of systems, structures, and components, including the application of this process to the DC power electrical systems.
- Event identification and classification for safety analyses
- Identification and quantification of initiating events for safety analysis
- Deterministic technical basis for the loss of power considerations in safety analysis
- An evaluation of the inadvertent operation of the emergency core cooling system with the loss of augmented DC power
- A summary of the probabilistic risk assessment for the US460

© Copyright 2023 by NuScale Power, LLC

Executive Summary

The US460 NuScale Power Module is a unique integral PWR design that relies on natural circulation and a limited number of safety-related systems to mitigate the consequences of postulated accidents.

NuScale's methodology for classifying and categorizing SSCs is a risk-informed, performance-based design process consistent with guidance in ANSI/ANS 30.3 and ANSI/ANS 58.14. The NRC approved NuScale's risk significance determination methodology to determine system-level categorizations in TR-0515-13952-NP-A, Revision 0. Design system functions are assigned to plant-level safety functions and categorization of those system functions based on risk-significance and defense-in-depth. A systematic method is applied to ensure that specific plant SSC are designed, manufactured, procured, installed, and operated with established processes to ensure that their quality and reliability are commensurate with their influence on safety.

SSC are classified based on the functions provided in the licensing basis. These classifications are (1) safety-related, (2) non-safety-related, and (3) nonsafety-related with augmented requirements (i.e., special treatment). Safety-related SSCs are relied upon to remain functional during and following design-basis events to meet the requirements of 10 CFR 50.2. SSCs not classified as safety-related are classified as nonsafety-related (with or without augmented requirements).

Nonsafety-related system functions are screened against a set of generic functions needed to meet the General Design Criteria or other regulatory requirements to determine if the nonsafety-related functions are supplemented with augmented requirements. When this NRC-approved process is applied to the augmented DC power system (EDAS), the EDAS is classified as not risk-significant, non-safety related with augmented design requirements.

The design of the EDAS prevents the failure of any single power channel from causing a loss of DC power to the module. An initiating event analysis has determined that probability of a random failure (at any time) of the EDAS is 2.6E-04 mcyr (per module critical year), and the probability of an EDAS "smart failure" during a separate initiating event is on the order of 1.5E-8 mcyr.

In the unlikely event of an EDAS "smart failure" during a separate initiating incident, analyses show that the CHFR remains above the MCHFR limit for the majority of state-point conditions. {{

}}[2(a),(c)] well below the peak clad temperature limit of 2200°F for 10 CFR 50.46, preserving a coolable geometry.

© Copyright 2023 by NuScale Power, LLC

Finally, the NuScale probabilistic risk assessment quantifies the risk impact of all identified and credible design-basis and beyond design-basis events. The risk metrics that NuScale quantifies are core damage frequency and large release frequency, which the NRC have identified as surrogates for cancer fatality risk and early fatality risk, respectively. The results of the PRA show that the risk metrics satisfy the NRC safety goals by multiple orders of magnitude, thereby preserving public health and safety. Additionally, when compared to the PRA results from the US600, approved by the NRC in the US600 DCA, the large release frequency is reduced by two orders of magnitude.

Probabilistic risk assessment results for NuScale designs

Design - Model	**CDF**	**LRF**
US460 - Base model	5.4E-09	3.4E-13
US600 - Base model	2.7E-10	1.7E-11
NRC Safety Goal	**1.0E-04**	**1.0E-06**

© Copyright 2023 by NuScale Power, LLC

1.0 Introduction

1.1 Purpose

The purpose of this report is to provide a technical and regulatory justification regarding the availability of the nonsafety-related augmented direct current (DC) electrical system (EDAS) during design-basis events considered in the safety analysis. This report demonstrates that the approach used in the Final Safety Analysis Report (FSAR) Chapter 15 safety analysis is consistent with regulatory requirements for safety analysis and consistent with the deterministically evaluated mechanistic, causal system/component failures of the electrical system design for the NuScale Power Plant US460 standard design.

1.2 Scope

Section 2.0 provides a description of the NuScale Power Module and its operation. Section 3.0 provides an overview of the NuScale safety and risk classification for systems, structures, and components (SSC). Section 4.0 discusses the event initiation frequencies for the safety analysis. Section 5.0 summarizes the event classification process for the safety analyses based on the event frequencies and design and operation of the NPM. Section 6.0 provides the application of the NuScale design process to the EDAS. Section 7.0 provides analysis of the inadvertent operation of a release valve (IORV) event assuming the coincident loss of AC and DC power in conjunction with the worst stuck control rod. Finally, Section 8.0 shows that the probabilistic risk analysis results for the US460 are more favorable than the NRC-approved results from the US600 and exceed NRC minimums by more than an order of magnitude.

Additional details are in the appendices. Appendix A provides a listing of the applicable regulatory requirements. Appendix B provides further detail of the US460 design and operation, including the ECCS, DHRS and DC power system. Appendix C provides the technical and regulatory basis for the loss of power considerations for safety analyses

© Copyright 2023 by NuScale Power, LLC

1.3 Abbreviations

Table 1-1 Abbreviations

Term	Definition
AC	alternating current
ANS	American Nuclear Society
ANSI	American National Standards Institute
AOO	anticipated operational occurrence
ASME	American Society of Mechanical Engineers
BWR	boiling water reactor
CCF	common cause failure
CDF	core damage frequency
CES	containment evacuation system
CFR	Code of Federal Regulations
CHF	critical heat flux
CHFR	critical heat flux ratio
CHW	chilled water
CNV	containment vessel
CNTS	containment system
CRDS	control rod drive system
CRHS	control room habitability system
CVCS	containment volume control system
DBE	design basis event
DC	direct current
DHRHX	decay heat removal heat exchanger
DHRS	decay heat removal system
DID	Defense-in-depth
D-RAP	design reliability assurance program
DSRS	design specific review standard
ECCS	emergency core cooling system
EDAS	augmented direct current power system
EDNS	normal direct current power system
EHVS	high voltage AC electrical system
ELVS	low voltage AC electrical system
EMVS	medium voltage AC electrical system
EPRI	Electric Power Research Institute
ESF	engineered safety feature
FMEA	failure modes and effects analysis
FSAR	final safety analysis report
GDC	general design criteria
GQA	graded quality assurance
IAB	inadvertent actuation block
IEEE	Institute of Electrical and Electronics Engineers
INL	Idaho National Laboratory
IORV	inadvertent operation of a relief valve
LBE	licensing basis events
LOCA	loss of coolant accident
LRF	large release frequency

© Copyright 2023 by NuScale Power, LLC

Table 1-1 Abbreviations (Continued)

Term	Definition
LWR	light water reactor
MCHFR	minimum critical heat flux ratio
MCR	main control room
MCS	module control system
mcyr	module critical year
MFIV	main feed isolation valve
MLD	master logic diagram
MOV	Motor operated valve
MPS	module protection system
MSIV	main steam isolation valve
NPM	NuScale power module
NSSS	nuclear steam supply system
PA	postulated accident
PAM	post-accident monitoring
PCS	plant control system
PCT	peak cladding temperature
PRA	probabilistic risk assessment
PWR	pressurized water reactor
QA	quality assurance
QAPD	quality assurance program description
RCPB	reactor coolant pressure boundary
RCS	reactor coolant system
RG	regulatory guide
RPV	reactor pressure vessel
RRV	reactor recirculation valve
RSV	reactor safety valve
RVV	reactor vent valve
RTNSS	regulatory treatment of nonsafety systems
SBO	station blackout
SE	special event
SFP	spent fuel pool
SG	steam generator
SRP	standard review plan
SSC	structures, systems, and components
UHS	ultimate heat sink
VRLA	valve-regulated lead acid

© Copyright 2023 by NuScale Power, LLC

2.0 NuScale Power Module Description and Operation

2.1 General Plant Design

The US460 design consists of up to six NPMs, each is a small, integral PWR with passive safety systems. The NPM consists of the nuclear steam supply system (NSSS), which includes the nuclear core, the helical coil SGs and the pressurizer, within a single pressure vessel and the compact steel containment vessel (CNV) that houses the NSSS.

Unique features of the plant design include the following:

- reduced core size
- natural circulation reactor coolant flow (i.e., no reactor coolant pumps)
- integrated SG and a pressurizer inside the reactor pressure vessel (RPV)
- simplified passive safety-related systems
- high-pressure steel containment
- containment partially immersed in a water-filled pool providing an effective passive heat sink for emergency cooling

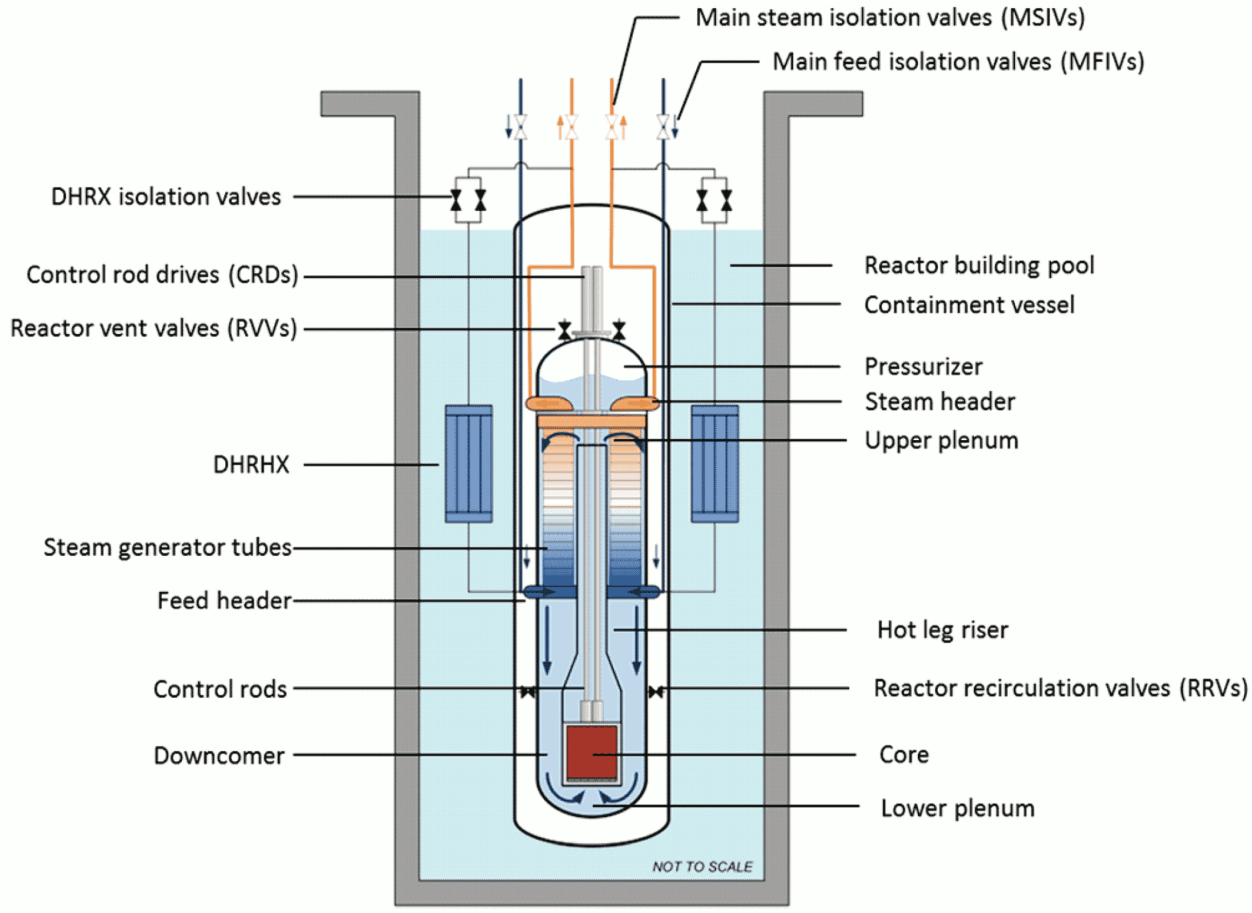
The NPM is designed to operate efficiently at full-power conditions using natural circulation as the means of providing core coolant flow, eliminating the need for reactor coolant pumps. As shown in Figure 2-1, the reactor core is located inside a shroud connected to the hot leg riser. The reactor core heats reactor coolant, decreasing its density, causing the coolant to flow upward through the riser. When the heated reactor coolant exits the riser, it passes across the tubes of the helical coil SG, which acts as a heat sink. As the reactor coolant passes over the SG tubes, it cools, increases in density, and naturally circulates through the downcomer to the reactor core.

The NPMs are partially immersed in a reactor pool and protected by passive safety-related systems. Each NPM has a dedicated emergency core-cooling system (ECCS), chemical and volume control system (CVCS), and decay heat removal system (DHRS).

In the US460 design, primary components are integral to the RPV, eliminating external coolant loops and pressurizer piping, which significantly reduces the size and number of possible LOCA scenarios.

© Copyright 2023 by NuScale Power, LLC

Figure 2-1 A Single NuScale Power Module During Normal Operation (Representative)

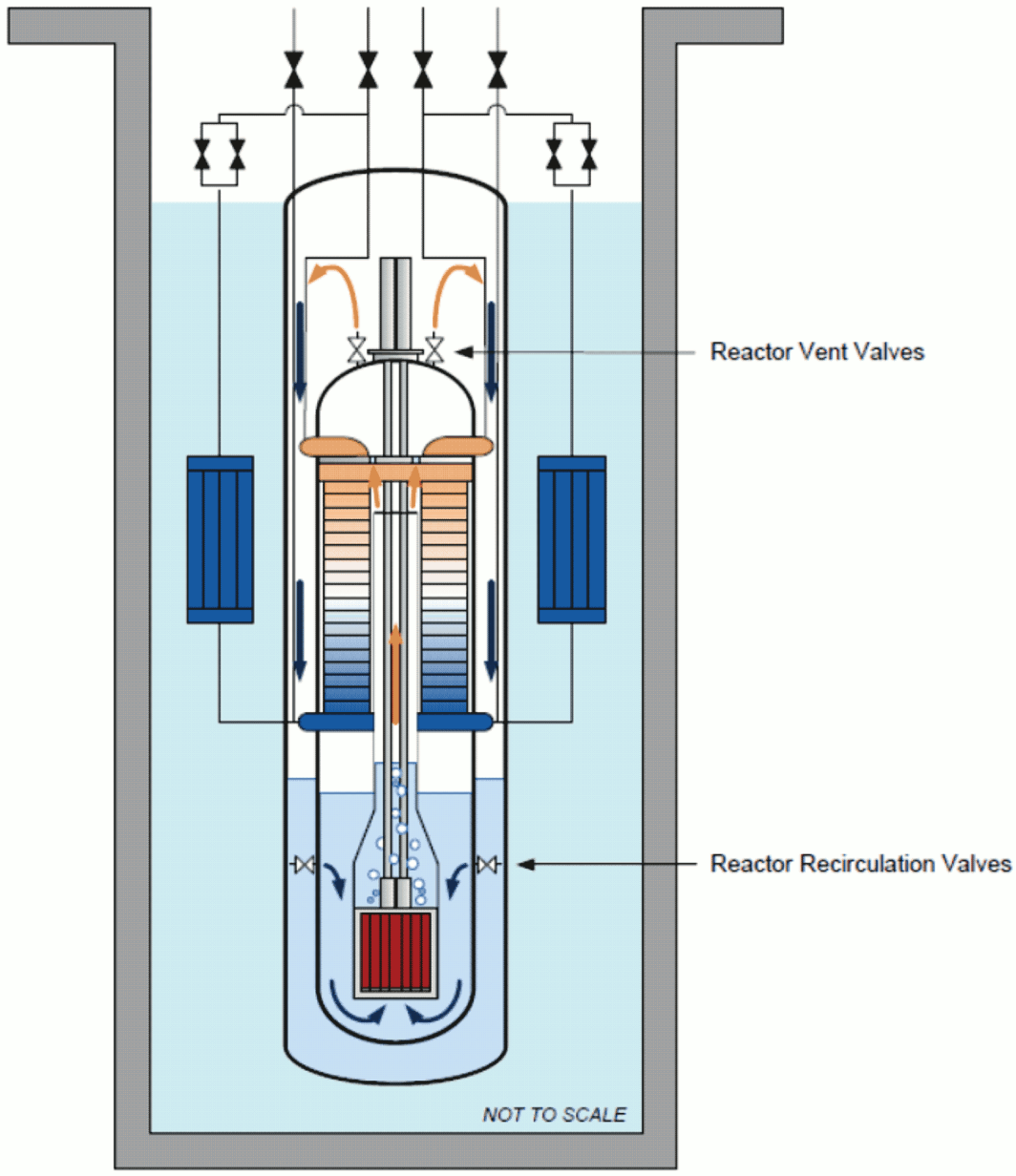


The NPM is designed with the intent of reducing the impact of a LOCA event. Both the DHRS and the ECCS are designed to actuate in response to a LOCA event. As shown in Figure 2-2, the ECCS consists of two independent reactor vent valves (RVV) and two independent reactor recirculation valves (RRV).

The ECCS is initiated by opening the RVVs exiting the top of the RPV and the RRVs entering the RPV in the downcomer region (above the core elevation). Opening the valves allows the RPV and the CNV pressure to equalize, creating a natural circulation path to remove decay heat from the core. Water that is vaporized in the core leaves as steam through the RVVs, is condensed and collected in the CNV, and is then returned to the downcomer region inside the RPV through the RRVs by natural circulation.

© Copyright 2023 by NuScale Power, LLC

Figure 2-2 Schematic of NuScale Power Module with Decay Heat Removal System and Emergency Core Cooling System in Operation



© Copyright 2023 by NuScale Power, LLC

2.2 Plant Operation

Pressurizer heaters and a pressurizer spray system are used to maintain nominal operating pressure. At full-power conditions, the flow rate is dependent on the fluid density differences through the loop, the losses incurred along the loop, and the elevation difference between the core and the SG.

During nominal full-power conditions, the control rods are retracted up to or above their insertion limits. Borated water is used as the primary coolant and the CVCS regulates the boron concentration to maintain criticality. The CVCS provides reactor inventory make-up through the RCS injection line in the riser and inventory let-down through a separate RCS discharge line in the downcomer region.

The secondary side is operated such that the SGs remove the heat generated by the reactor core. The DHRS heat exchangers are isolated from the steam line and do not remove heat during normal operation.

The containment is evacuated during normal operation to provide an insulated barrier between the reactor and containment.

2.3 Engineered Safety Features Operation

The Module Protection System (MPS) is composed primarily of the reactor trip system and the engineered safety features actuation system. The MPS protection functions are limited to automated safety responses to off-normal conditions. The MPS functional response to an initiating event is a reactor trip; isolation of main feedwater, main steam, CVCS, demineralized water system, and containment; followed by an integrated safety actuation of one or more of the passive safety-related systems (DHRS and ECCS). Containment isolation is achieved by closing the containment isolation valves, which also fail closed on a loss of power.

The reactor trip system consists of four independent separation groups with independent measurement channels to monitor plant parameters that can generate a reactor trip. Each measurement channel trips when the parameter exceeds a predetermined setpoint.

The engineered safety features actuation system also consists of four independent separation groups with independent measurement channels that monitor plant parameters that activate the operation of the engineered safety features.

ECCS is actuated by the MPS on appropriate signals indicating a LOCA event. Interlocks are designed to prevent ECCS actuations for expected operational conditions or non-LOCA transients.

© Copyright 2023 by NuScale Power, LLC

2.3.1 Emergency Core Cooling System

The ECCS is a two-phase natural circulation system that maintains a liquid water supply to the core during its operation in a LOCA scenario, which results in a collapsed liquid level in the RPV that is above the top of the core.

The ECCS consists of two independent RVVs and two independent RRVs. The ECCS is initiated by simultaneously actuating the RVVs on the top of the RPV in the pressurizer region and the RRVs on the side of the RPV in the downcomer region. The RRVs are designed to provide a low-resistance flow path for coolant to flow from the CNV into the RPV. The RVVs are designed to equalize pressure between the two vessels allowing steam from the reactor to vent to the containment and to provide hydrostatic equalization that allows coolant flow through the RRVs back into the reactor downcomer region.

During ECCS actuation, the RPV depressurizes due to liquid and steam exiting the RPV through the RVVs. Steam entering containment is condensed on the containment wall, which in turn is cooled by the reactor pool. Initially, the containment pressure increases to a peak, and then decrease as flow from the RPV decreases and heat is transferred from the CNV to the reactor pool. The RPV water inventory decreases while the containment level increases due to inventory transferred from the RPV.

As the pressure between the two vessels reach a near-equilibrium condition, the collapsed liquid level in the containment rises to a level higher than the RRV elevation, creating enough static head to overcome the pressure difference between the RPV and CNV. At this point, the condensed liquid in containment enters the RPV through the RRVs while steam continues to exit the RPV through the RVVs. This boiling/condensing circulation process continues, maintaining a collapsed water level above the top of the active fuel.

The RRVs are equipped with an inadvertent actuation block (IAB) feature that prevents their opening at full operating pressure. The IAB allows the RRV main valve to open only after the differential pressure between the RPV and CNV has decreased below the IAB release pressure setpoint. Meanwhile, the RVV main valves open immediately after actuation, resulting in rapid depressurization of the RPV into containment that allows ECCS recirculation cooling to be established after the RRVs open.

The ECCS valves open on low differential pressure between the RPV and CNV, independent of an ECCS actuation signal. This action is a function of the mechanical design of the valves, where the valve spring causes the valves to open if the pressure difference across the main chamber drops below approximately 15 psid. The ECCS valves open by this function during some rapid depressurization events as the RPV and CNV pressures equalize. This function opens the ECCS valves earlier in some depressurization scenarios but does not significantly impact accident progression or results.

© Copyright 2023 by NuScale Power, LLC

2.3.2 Decay Heat Removal System

The DHRS is a passive safety-related system that relies on natural circulation to remove heat from the RCS through the SG and reject heat to the reactor pool through the DHRS condenser. The DHRS is composed of two DHRS trains; one train is associated with each of the two NPM SGs. Each DHRS train is capable of independently removing 100 percent of decay heat. The DHRS piping connects to the main steam and feedwater lines specific to the associated SG. During normal operation, the DHRS condenser and piping are isolated by valves on the steam side of the SG. The condensate side of the DHRS is open to the feedwater piping supplying the associated SG.

Upon actuation of the DHRS, the SG feedwater and steam isolation valves, as well as their nonsafety-related backup valves, close and the DHRS isolation valves open, creating a closed loop between the SG and DHRS condenser. Both liquid and vapor are contained in the SG/DHRS loop on system actuation. Because the DHRS is a closed system, the total water mass remains constant during the system operation.

For successful operation, liquid water enters the SG through the feedwater line and is boiled by heat from the RCS. The vapor exits the SG through the steam line and is directed to the DHRS condenser where it condenses back to liquid before return to the SG. Thus, the loop transfers heat from the RCS to the DHRS fluid and then from the DHRS to the reactor pool water.

The bottom of the DHRS condenser is located above the bottom of the SG providing the static head to drive natural circulation.

2.4 Augmented DC Power System

The EDAS consists of two DC subsystems: the module-specific subsystem (EDAS-MS) and the common plant subsystem (EDAS-C).

2.4.1 Module Specific Subsystem

The EDAS-MS contains four power channels for each module. Power channels A and C are a part of EDAS Division I. Power channels B and D are a part of EDAS Division II. Each power channel contains one battery, one battery charger, and one DC distribution panel assembly. Each distribution panel assembly consists of a bus, fused disconnect switch, tie breaker, breakers, relays, metering, associated interconnections, and supporting structure.

Each EDAS-MS power channel charger is sized to carry 100 percent of the divisional DC bus loading during normal plant operation. In the event of a loss of a charger for maintenance or equipment failure, the divisional power channels can be connected together with the functional battery charger providing power to the divisional loads while maintaining connected batteries on float charge.

© Copyright 2023 by NuScale Power, LLC

Each EDAS-MS battery is sized with sufficient capacity to provide power to ECCS Hold Mode loads for 24 hours. The EDAS-MS channel B and channel C are designed with additional capacity to provide battery power to PAM Only Mode loads for 72 hours.

2.4.2 Common Plant Subsystem

The EDAS-C contains two divisions, EDAS Division I and EDAS Division II. Each common plant subsystem division contains one battery, two identical battery chargers, and one DC distribution panel assembly. Each distribution panel assembly consists of a bus, disconnect switch, breakers, relays, metering, associated interconnections, and supporting structure.

Each EDAS-C charger is sized to carry 100 percent of the respective divisional DC bus loading during normal plant operation while maintaining connected batteries on float charge.

Each EDAS-C battery is sized with sufficient capacity to provide power to required loads for 72 hours.

2.4.3 Functions

EDAS functions operationally to:

- Provide electrical power for the prevention of unintended ECCS actuation.
- Provide backup electrical power for Post-Accident Monitoring (PAM) instrumentation for type B, C, D, and F variables.
- Provide module-specific and common DC electrical power with adequate voltage and current to EDAS loads when AC power is either available or not available to EDAS.

  Module-specific loads include:

  - Module protection system
  - Neutron monitoring system
  - Radiation monitoring system

  Common loads include:

  - Safety display indication
  - Plant protection system

© Copyright 2023 by NuScale Power, LLC

- Provide module-specific and common DC electrical power with adequate voltage, current, and capacity to specified EDAS module-specific and common loads when AC power is either available or not available to EDAS.

  Loads include:

  - EDAS battery monitoring system (module-specific, common)
  - Main control room lighting (common)
- Provide EDAS instrumentation and control, capability for EDAS battery testing, and EDAS battery monitoring.

2.5 Normal DC Power System

The normal DC power system (EDNS) is an electrical DC and AC distribution system consisting of batteries, battery chargers, direct current (DC) switchboards, inverters, voltage regulating transformers, maintenance bypass switches, alternating current (AC) panel boards, fused transfer switch boxes, battery monitors, associated electrical protective devices, and instrumentation, and interconnecting system cabling.

2.5.1 Functions

The functions supported by the EDNS include:

- Provide AC and/or DC electrical power with adequate voltage and current to EDNS loads.

  Loads include:

  - The EDNS provides DC control power to the normal high voltage, medium voltage, and low voltage distribution systems (EHVS, EMVS, and ELVS, respectively).
  - The EDNS provides electrical power to the module control system (MCS) and plant control system (PCS).
- Provide battery backup AC and/or DC electrical power with adequate voltage and current to EDNS loads when AC power is not available.
  - The EDNS backup battery capacity is 40 minutes.

© Copyright 2023 by NuScale Power, LLC

3.0 Overview of the Risk-Informed Performance-Based Design Process

The NuScale risk-informed, performance-based design process is shown in Figure 3-1 and is consistent with guidance in ANSI/ANS 30.3 (Reference 10.1) and ANSI/ANS 58.14 (Reference 10.2).

The first step in this process is to define plant safety functions and requirements. These need to take into consideration fundamental safety functions and high-level safety goals from the regulator and the designer. Design requirements are the set of functional, nonfunctional, and performance requirements that bound plant design and help ensure a satisfactory final design. The design requirements are dependent on a range of site, technology, and stakeholder-specific needs. These external inputs are formally documented, reviewed, and evaluated together to ensure that a wide variety of design constraints can be appropriately translated into a multilevel design requirements document. The requirements analysis process is the process for examining, evaluating, and translating applicable inputs into design requirements that can be objectively evaluated and verified in later phases of design. Performance-based safety objectives are used to support decision-making related to design and evaluation of plant systems and components.

In supporting the safety requirements definition, the plant response to postulated initiating events including coincident equipment failures and malfunctions that could challenge plant safety are analyzed. The licensing basis events (LBEs) include the collection of design-basis events (DBEs) and special events (SEs) for the plant design. At a minimum, DBEs consist of anticipated operational occurrences (AOOs) and postulated accidents (PAs). Initiating events for DBEs are identified by developing a list of functional transient and accident types that could challenge plant-level safety functions and associated mitigating systems depending on the operating mode of the plant at the time of the challenge. Initiating event selection begins with the listing of potential DBE scenarios using both traditional deterministic processes and the design-specific PRA. Initiating events are categorized according to expected frequency of occurrence and by functional event type. Categorization by frequency of occurrence provides a basis for selection of the applicable analysis acceptance criteria for each initiating event. Categorization of initiating events by functional event type provides a basis for comparison between initiating events, which makes it possible to identify and evaluate the limiting cases. Both traditional deterministic processes and the design-specific PRA should use hazard analysis methods (e.g., failure modes and effects analysis, hazard and operability analysis, and fault tree analysis), combined with malfunctions of individual plant systems and historical experience, as available, for defining an initial list of individual initiators leading to different DBE types.

DBEs are those AOOs and PAs that form the basis for the design of the plant including SSC relied upon to protect design-specific fission product barriers during those transients and accidents. Using the DBEs as input to formal design of the plant results in a robust plant that, using conservative analyses of plant response, can be shown to meet limits established in applicable codes, standards, and regulations with design safety margin, thereby demonstrating adequate protection of the health and safety of the public.

© Copyright 2023 by NuScale Power, LLC

Once the conceptual design has progressed to a high enough level of maturity or detail, additional quantitative evaluations of risk and margins are conducted. From a safety perspective, these evaluations are risk-informed such that they consider both probabilistic and deterministic information. At this early stage in the design process, margins may be small or exceeded in limited cases depending on the state of the design. Design iterations may continue to occur within the conceptual design phase to address these issues, but the design may also progress to the next phase of design if the exceedances are known and plans to address them are agreed upon. In other words, as long as the design is feasible, it may progress to the next phase of design even with some potential exceedance of safety limits or limited margins.

The conceptual design, identification of LBEs, PRA, and design-basis safety analysis activities in practice occur in parallel versus the idealized sequential order shown in Figure 3-1.

Binning of the initiating events into functional event types, the deterministic approach considers the potential for additional malfunctions or plant operating conditions that may occur coincident with the initiating events under evaluation. The design-specific PRA is then reviewed to identify other failures that may be worth consideration as a part of the selected DBEs or accidents beyond those identified deterministically. This review focuses on the consequences of the event or event sequence with a consideration of the probability of the event.

In deterministic safety analyses, potential for single active failures are evaluated following a postulated transient or accident initiating event. These single active failures are postulated within the collection of plant systems relied upon in response to the transient and accident initiating event.

A review of the accident sequences of the PRA is performed to identify any risk-significant mitigating system equipment malfunctions that should be included in the design-basis analyses. Potential equipment malfunctions for inclusion in the design-basis analyses include those single failures and common-cause failure that, when combined with a given initiating event, can challenge regulatory requirements.

To establish whether there are common-cause or multiple random failures that may be risk-significant with respect to the plant design, a review of fault tree analyses for the mitigating systems relied upon during a DBE is performed. Selected dominant contributors to mitigating system failure probability in the form of common-cause or multiple random failures are reviewed and an engineering rationale developed as to whether or not these common-cause or multiple random failures should be included as a part of the DBEs. Such a rationale considers whether the initiating event for the DBE, combined with the common-cause or multiple random failures, would result in challenges to the fission product barriers that exceeded those for existing DBEs or if the probability of the common cause failure is significantly less than that for single failures or coincident occurrences identified

© Copyright 2023 by NuScale Power, LLC

At the end of the conceptual design phase, design system functions are assigned to plant-level safety functions and categorization of those system functions based on risk-significance and defense-in-depth is conducted. As the safety of a nuclear plant is dependent on the reliability and integrity of its individual SSC, a systematic method is necessary to ensure that specific plant SSC are designed, manufactured, procured, installed, and operated with established processes to ensure that their quality and reliability are commensurate with their influence on safety. Selection of these specific SSC is achieved through a classification and categorization process. NuScale utilizes an NRC-approved risk significance determination methodology in TR-0515-13952-NP-A, Revision 0 (Reference 10.3) and the SSC classification process to first determine system-level categorizations. Once this classification is achieved, the preliminary design phase can begin.

The system functions that are relied upon in the safety analyses of DBEs to provide or support the plant-level safety-related functions are determined. These systems and their corresponding safety-related plant-level functions are classified as safety-related. Only those systems necessary and sufficient to accomplish any of the basic safety-related functions need to be classified as safety-related. Not all systems capable of performing a given plant-level safety function may need to be classified as safety-related and that for some DBEs, not all plant-level safety-related functions are required.

Nonsafety-related system functions are screened against a set of generic functions needed to meet the General Design Criteria or regulatory requirements to determine if the nonsafety-related functions are supplemented with augmented requirements. For each system function that is classified as nonsafety-related with augmented requirements functionality, the basis is documented and the associated augmented design requirements are identified. Multiple nonsafety-related with augmented requirements functions may be applied to a single system function.

The system function categorizations are reviewed by the design reliability assurance program (D-RAP) expert panel. The expert panel is a select team of experts with collective experience in safety analysis, licensing, PRA, design engineering, and operations and maintenance processes. The expert panel reviews the recommendation for categorization of system functions by the presenting subject matter expert. The licensing representative is responsible for ensuring licensing commitments are verified as part of panel deliberations. The expert panel reviews and provides input on the creation of and modification to the nonsafety-related with augmented requirements functions.

In the preliminary design phase, system design is progressed to component design or selection. Failure modes and effects analysis (FMEAs) are conducted on select systems to evaluate system reliability and search for failure modes not previously considered in the conceptual design phase. Similar to the conceptual design phase, preliminary design is iterative, recursive, and many design activities progress in parallel that are not shown in Figure 3-1.

© Copyright 2023 by NuScale Power, LLC

At the end of the preliminary design phase, SSC are classified regarding the functions provided in the licensing basis. These classifications are (1) safety-related, (2) non-safety-related, and (3) nonsafety-related with augmented requirements (i.e., special treatment).

As defined in 10 CFR 50.2, safety-related SSC are those that are relied upon to remain functional during and following design-basis events to assure:

1. The integrity of the reactor coolant pressure boundary
2. The capability to shut down the reactor and maintain it in a safe shutdown condition; or
3. The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the applicable guideline exposures set forth in 10 CFR 50.34(a)(1) or 10 CFR 100.11, as applicable.

Safety classification of SSC is based on the functions that the items are credited to perform in the safety analyses of design-basis events and not on design criteria or operations requirements. Some items providing only nonsafety-related functions might be subject to operations requirements such as technical specifications, emergency operating procedures, or surveillance procedures. Operations requirements, however, may not be the basis for functionally classifying an item as safety-related.

The components (including component-level structures) and parts (including consumables) are classified by considering the function of the components or parts in the safety-related systems and the safety-related functions that have been identified in the systems.

General criteria for the classification of components and parts are listed below:

- The classification of a component or part shall be based upon its function. If the component or part is relied upon for the satisfactory performance of a safety-related function, the component or part shall be classified as safety-related.
- A component or part that is relied upon in an analysis of a design-basis event to provide a safety-related function shall be classified as safety-related.
- A component or part that is relied upon to satisfy a safety-related interface requirement shall be classified as safety-related.
- A component or part that is relied upon to initiate, control, or maintain a safety-related function shall be classified as safety-related.
- A component or part that is relied upon during or following a design-basis event to maintain an environment to ensure that a safety-related item can perform its safety-related function shall be classified as safety-related.

© Copyright 2023 by NuScale Power, LLC

- A component or part that is relied upon to prevent the release of radioactive material that could result in potential off-site exposures comparable to 10 CFR 100, Subparts A and B guideline exposures, during or following a design-basis event, shall be classified as safety-related.
- If the function of a component or part is not safety-related, and its failure could not prevent the satisfactory performance of a safety-related function, the component or part shall be classified as nonsafety-related.

The above classification criteria applies to all plant components and parts.

Items that are not classified as safety-related per the criteria above are classified as nonsafety-related.

When evaluating failures of a component or part that does not perform or support a safety-related function, any potential failure of the component or part is deemed credible unless justified otherwise in accordance with an established basis (Reference 10.3). Such justification may be based upon the following:

1. The failure is not physically possible for the functional or environmental conditions that would exist during or following a DBE;
2. The component or part is qualified to resist the failure. For example, for a component or part that is Seismic Category I or II, failures due to a safe shutdown earthquake do not need to be assessed. For a component or part that is environmentally qualified, failures due to environmental conditions that it is qualified for do not need to be assessed;
3. A probability evaluation shows that the frequency of occurrence for the DBE sequence including the failure is less than 10-7/year or less than 10-6/year if when combined with reasonable qualitative arguments, the realistic frequency can be shown to be lower.; A documented basis exists for declaring the failure incredible (e.g., catastrophic reactor vessel failure).

The expert panel reviews the list of SSC that are risk-significant, nonsafety-related with augmented requirements, or require regulatory treatment of non-safety systems (RTNSS), once the equipment lists are compiled into the D-RAP summary report and D-RAP list. The chair of the expert panel is responsible for the complete and accurate documentation of the expert panel findings, with support from the D-RAP coordinator. The chair approves the D-RAP summary report that documents the expert panel results.

During the review of the D-RAP summary report, defense-in-depth (DID) adequacy is evaluated. The DID approach contributes specific requirements to reactor design and operations, as determined by the subject matter expert and reviewed by the D-RAP expert panel. These requirements are established based on considerations including PRA information, selection of LBEs, SSC safety classifications, and special treatments for SSC. The SSC are identified, documented, and classified into appropriate levels (or bins), and DID attributes assigned accordingly.

© Copyright 2023 by NuScale Power, LLC

For each of the SSC presented to the expert panel in the D-RAP list, the functional and performance criteria are clearly identified.

The expert panel performs a DID adequacy evaluation towards the end of the SSC classification process that is documented in the D-RAP summary report. This evaluation ensures the D-RAP list reflects the concept that multiple layers of DID have been evaluated in response to internal and external initiating events; and, that the reliability and capability of SSC to perform their safety functions for the life of the plant for the specific events that an SSC participates in is assured through specific programmatic actions that result in application of conservative safety margins against performance targets and limits.

The expert panel considers the following DID fundamental objectives when conducting DID adequacy evaluations:

- prevent accidents or lessen the effects of damage if an accident or malfunction occurs
- provide multiple barriers (including functional layers of defense) against fission product releases
- provide redundancy in safety function performance
- ensure that safety is not wholly dependent on any single feature of the design or operation
- select engineered features preferentially over administrative controls
- ensure that the public is adequately protected on the intended site and that well-conceived, workable emergency plans surround the nuclear facility
- use risk analysis to improve engineering and operational decisions by identifying and taking advantage of opportunities to reduce risk or reduce unnecessary burdens in cost beneficial ways.

In meeting its objectives, the D-RAP expert panel:

- confirms that a balance between event prevention and mitigation is reflected in the layers of defense for risk-significant LBEs.
- confirms whether any single feature is excessively relied on to achieve public safety objectives, and, if so, identify options to reduce or eliminate such dependency.
- confirms that adequate technical bases for classifying SSC exist and their capabilities to execute the safety functions are defined.
- confirms that the effectiveness of physical and functional barriers to retain radionuclides in preventing or limiting release is established.
- evaluates sources of uncertainty that need to be addressed via programmatic and plant capability DID measures have been adequately addressed.

The results of the expert panel DID adequacy evaluation are documented in the D-RAP summary report.

© Copyright 2023 by NuScale Power, LLC

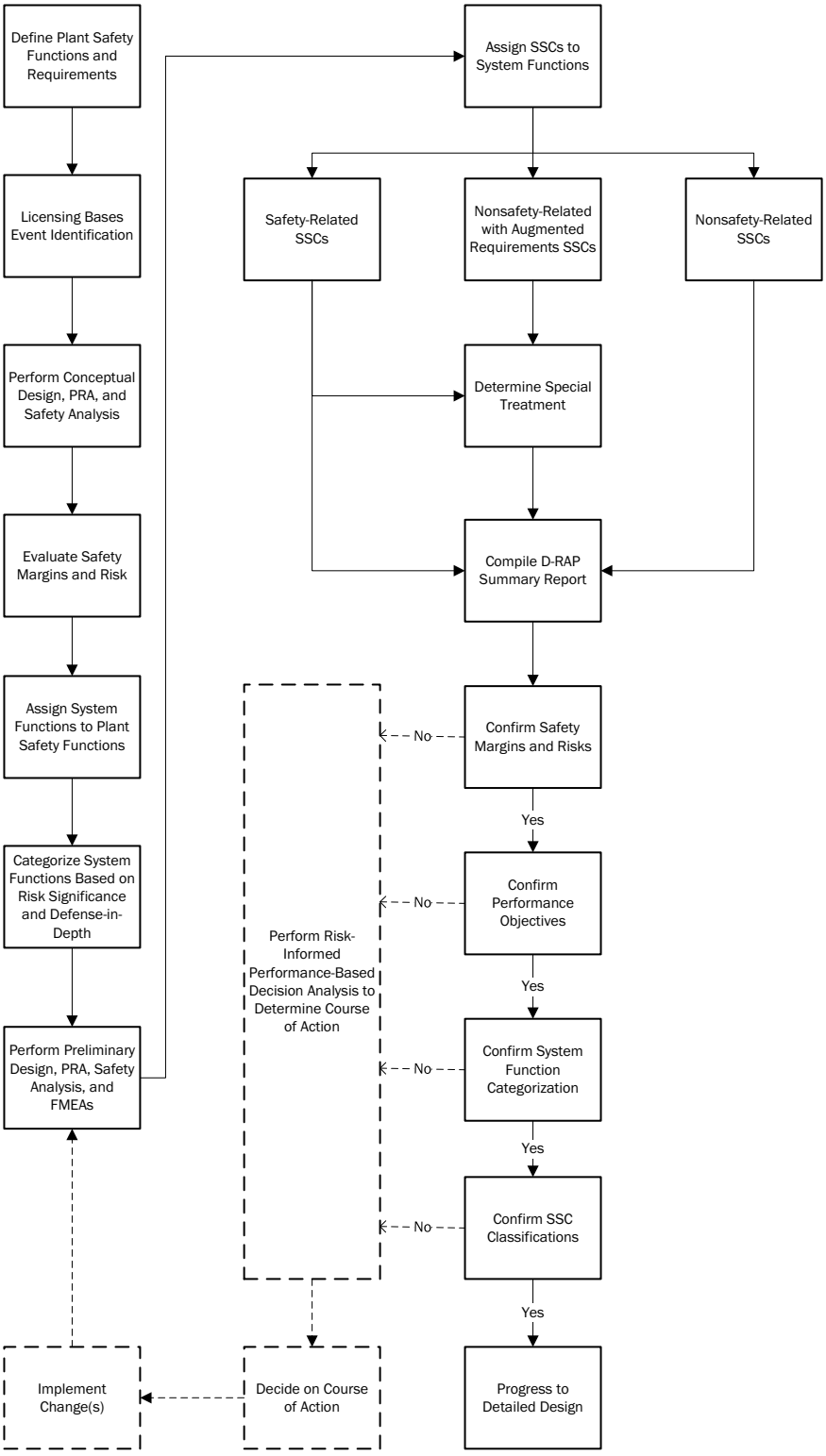
In some cases, DID adequacy may be challenged (e.g., limited margin) and as such, a decision analysis is conducted to evaluate the best course of action.

Decision making during expert panel deliberations is based on criteria specified at the highest level that is feasible to meet functional objectives. This process enables flexibility for realizing successful system performance.

Expert panel recommendations are provided to the NuScale engineering change control board to support effective and timely decisions that may include design, analysis, and/or methodology changes. If necessary, the design process is repeated until DID adequacy objectives are met.

© Copyright 2023 by NuScale Power, LLC

Figure 3-1 System Design and SSC Classification Process



© Copyright 2023 by NuScale Power, LLC

4.0 Event Identification and Classification for Safety Analyses

A review of NPM systems that could cause a reactor trip is used to determine the subset of possible events is within the scope of Chapter 15 design basis analyses based on regulatory guidance from the SRP, NuScale DSRS, and the specifics of the NuScale US460 standard design.

This evaluation leverages the experience gained from the NuScale US600 and changes to the NuScale design for US460 to document the scope of events relevant to the safety design-basis.

4.1 Basis for Event Classification

The SRP and DSRS discuss categorization of events according to frequency of occurrence.

For new applications, the SRP endorses two distinct categories:

- Anticipated Operational Occurrences (AOOs) are events that are expected to occur one or more times during the design life of the nuclear power plant. As identified in the SRP, among other acceptance criteria, fuel cladding integrity shall be maintained by ensuring that the minimum departure from nucleate boiling ratio (DNBR) remains above the 95/95 limit for PWRs.
- Postulated accidents are events that are not expected to occur during the design life of the plant as defined in the DSRS. As identified in the SRP, among other acceptance criteria for accidents, fuel is assumed to have failed if the minimum DNBR limit is not met but the release of radioactive material shall not result in offsite doses in excess of the guidelines of 10 CFR Part 100.

The DSRS Section 15.0 discusses AOOs and postulated accidents, and also recognizes ‘infrequent events’ as a subcategory of postulated accidents with more restrictive radiological acceptance criteria.

The SRP discussion of postulated accidents points to 10 CFR Part 100, but dose criteria used for new reactors are from 10 CFR 52.137.

Considering this evolution of the design-basis event categorization and consequential acceptance criteria, and the DSRS Section 15.0, the NPM design-basis events are categorized into one of three categories:

- AOOs - These are events that are expected to occur one or more times in the design life of the plant. For a 60-year plant design life, events with a frequency greater than 1/60 or 1.67×10^{-2} per module-year could be considered AOOs. For conservatism, events that are expected to occur more than once every 100 years, 1×10^{-2} per module year, are considered AOOs.

© Copyright 2023 by NuScale Power, LLC

- Infrequent Events - Infrequent events include events that are not expected to occur within the lifetime of a plant but have stricter radiological acceptance criteria than postulated accidents. Due to aspects of the NPM design, the expected frequency of occurrence is less than $1x10^{-2}$ per module year, and therefore these events are not expected to occur during the design life of the NPM operation. However, considering the historical treatment of these events as potentially occurring during plant operation, it is not considered appropriate to apply the radiological acceptance criteria appropriate for accidents.' Therefore, for infrequent events, some fuel damage may occur but the radiological acceptance criteria imposed are stricter than those imposed for accidents. Classification of these types of events as infrequent events would require specific evaluation of the event frequency for the NPM design.

  Infrequent events also include some of the typical LWR events for which the NPM design is similar, and the specified radiological acceptance are stricter than imposed for accidents.

- Accidents - These are design-basis events with a probability of occurrence lower than $1x10^{-2}$ per module-year. For an event that is not expected to occur, classification as an AOO or an infrequent event is conservative because more restrictive acceptance criteria are applied.

Defining a lower bound frequency for accidents is considered. For defining the scope of design-basis events, historically, engineering judgment was used to determine what was insufficiently credible to be considered within the design-basis and was approved through the regulatory process. Therefore, events such as large secondary side system breaks, that may have a low probability of occurrence, generally remain part of operating plant design-bases. Considering that the NuScale plant systems are similar to operating PWR systems in many ways, NuScale has not attempted to define a lower bound frequency for accidents to define the limit between design-basis events and beyond-design-basis events. The Chapter 15 safety analysis is intended to identify a sufficiently broad spectrum of transients and accidents, or initiating events.

With respect to analyses presented in Chapter 15 of the FSAR, there are two additional categories of analysis presented in the US460 safety analysis, that are classified as 'special events':

- Some events such as Anticipated Transients without Scram (ATWS) are beyond-design-basis events but are required to be addressed per NRC regulations (i.e., assessment of a specific condition is required by the code of federal regulations).
- Typically, Chapter 15 events are analyzed from a starting point of steady-state hot conditions at the power that minimizes margin to the acceptance criterion of interest for the particular transient. With limited exceptions (for example, analysis of fuel handling accidents), the plant response to required operational occurrences such as startup and shutdown, power changes for load follow, or events that occur during the process of refueling are not typically presented in Chapter 15 of the FSAR. However, given the nature of the NuScale design as a natural circulation reactor and the refueling process, there are some design-specific aspects of normal operation such as reactor stability that is presented in the FSAR.

© Copyright 2023 by NuScale Power, LLC

By exclusion, events that are not anticipated to occur during the course of normal operation bounded by identified design-basis events, are beyond-design-basis events.

4.2 Basis for Event Frequency

For classification of DBEs as AOOs, infrequent events, or accidents, the following approach is used:

- For events that are initiated by abnormal system conditions where the NPM system design is similar to that of operating plants, the event classification as AOO, infrequent event, or accident for the NPM is specified consistent with historical precedent. Radiological acceptance implicitly apply to infrequent events, which is supported by DSRS.
- For events that are specific to the NPM design, or where the NPM design is such that the event frequency is expected to be different than those of operating plants or other design certification applications, then the PRA event frequency for the NPM is considered. If it is available, the PRA event frequency is considered in classifying the event as an AOO, infrequent event or accident. If the event is conservatively classified as an AOO, the specific event frequency may not be determined.

This approach simplifies the event classification by using historical precedent where appropriate, and using NuScale PRA data to inform event classification where the NPM design is unique.

4.3 Event Identification by Chapter 15 Subsection

Table 4-1 provides a summary of the Chapter 15 DBEs and event classification applicable to the NPM.

Table 4-1 Listing of Design Basis Events by FSAR Chapter 15 Section

Event Class(1)	Event(1)	FSAR Section(1)	Classification
Increase in heat removal by secondary system	Decrease in feedwater temperature	15.1.1	AOO
	Increase in feedwater flow	15.1.2	AOO
	Increase in steam flow	15.1.3	AOO
	Inadvertent opening of steam generator relief or safety valve	15.1.4	AOO
	Steam system piping failures	15.1.5	Accident
	Containment flooding/loss of containment vacuum	15.1.6	AOO
Decrease in heat removal by secondary system	Loss of external load	15.2.1	AOO
	Turbine trip	15.2.2	AOO
	Loss of condenser vacuum	15.2.3	AOO
	Main steam isolation valve closure	15.2.4	AOO
	Loss of non-emergency AC power to station auxiliaries	15.2.6	AOO

© Copyright 2023 by NuScale Power, LLC

Table 4-1 Listing of Design Basis Events by FSAR Chapter 15 Section (Continued)

Event Class(1)	Event(1)	FSAR Section(1)	Classification
Decrease in heat removal by secondary system (continued)	Loss of normal feedwater flow (partial or complete)	15.2.7	AOO
	Feedwater system pipe breaks	15.2.8	Accident
	Inadvertent DHRS Operation	15.2.9	AOO
Reactivity and power distribution anomalies	Uncontrolled control rod assembly bank withdrawal from a subcritical or low power startup condition	15.4.1	AOO
	Uncontrolled control rod assembly bank withdrawal at power	15.4.2	AOO
	Control rod misoperation (system malfunction or operator error)	15.4.3	AOO
	Addition of cooler water to the reactor system	15.4.4 - 15.4.5	n/a
	Inadvertent decrease in boron concentration in the reactor coolant	15.4.6	AOO
	Inadvertent loading and operation of a fuel assembly in an improper position	15.4.7	Infrequent Event
	Spectrum of rod ejection accidents	15.4.8	Accident
Increase in RCS Inventory	Chemical and volume control system malfunction that increase RCS inventory	15.5.1	AOO
Decrease in RCS Inventory(8)	Inadvertent opening of a reactor safety valve	15.6.1	AOO
	Failure of small lines carrying primary coolant outside containment	15.6.2	Infrequent Event
	Steam generator tube failure	15.6.3	Accident
	Loss of coolant accident resulting from spectrum of postulated piping breaks within reactor coolant pressure boundary	15.6.5	Accident
	Inadvertent operation of Emergency Core Cooling System	15.6.6	AOO
Other	Radiological consequences of fuel handling accidents	15.7.4	Accident
Other	Spent fuel cask and NPM drop accidents	15.7.5	Accident
Other - BDB	ATWS	15.8	Special event
Other	Demonstration of Stability	15.9	Special event

Notes:

(1) The event class, event, and FSAR section are outlined based on NUREG-0800 and RG 1.206 Section C.I.15, and the NuScale US600 design certification application. Some event classes/events from the SRP are not listed because they are BWR-specific (do not apply to NuScale), or do not apply by nature of the NuScale design (for example, Section 15.3 loss of flow transients). Sections 15.0.3, 15.4.8A, and 15.6.5A are specific to addressing radiological acceptance criteria and are not listed above because these do not represent different initiating events.

© Copyright 2023 by NuScale Power, LLC

4.3.1 Special Consideration for Decrease in RCS Inventory Events

For consideration of LOCA events, the NuScale US460 design differs significantly from operating PWRs in three areas:

1. There are no large pipes connected to the reactor pressure vessel and therefore the traditional large break LOCA is precluded by the design.
2. There are no safety-related systems to add coolant to the reactor vessel. The only means of adding additional water to the RPV is through nonsafety-related CVCS normal makeup.
3. ECCS actuation for the NuScale design results in rapid release of coolant from the primary side, creating a response similar to a pipe break LOCA inside of containment.

Given these significant design differences, the treatment of decrease of RCS inventory events are discussed in Table 4-2.

Table 4-2 Events Involving Decrease of RCS Inventory

Event	Event Category	Basis/Discussion
RCS Leakage outside of containment within the capacity of normal (non-safety) makeup system	n/a	These leakage events are not LOCAs by the definition from 10 CFR 50.46 and 10 CFR 50 Appendix A. 10 CFR Appendix A includes GDC for emergency cooling separate from those regarding makeup for anticipated leakage. In the NuScale design, normal makeup is provided by CVCS; however normal makeup is not automatically initiated and must be authorized by operators. Since makeup is not automatic, various event progressions are considered. For leakage from a pipe outside of containment, whether or not makeup is authorized by the operator affects the volume of primary system fluid that leaks from the RCS prior to containment isolation, which terminates the leakage. This scenario is addressed by the radiological assessment of small pipe breaks outside of containment. If makeup is not authorized and no other action is taken to shut down the module, eventually a low or low-low pressurizer level signal is expected, that isolates containment.

© Copyright 2023 by NuScale Power, LLC

Table 4-2 Events Involving Decrease of RCS Inventory (Continued)

Event	Event Category	Basis/Discussion
RCS Leakage inside of containment within the capacity of normal (non-safety) makeup system	Special Event	These leakage events are not LOCAs by the definition from 10 CFR 50 Appendix A. In the NuScale design, normal makeup is provided by CVCS; however normal makeup is not automatically initiated and must be authorized by operators. Since makeup is not automatic, various event progressions are considered. For leakage inside of containment, if the leakage is within the capacity of the containment evacuation system or the leakage condenses quick enough, the containment pressure does not increase. Then, similar to a leak outside of containment, if makeup is not authorized and no other action is taken to shut down the module, eventually a low or low-low pressurizer level signal is expected, which terminates the leakage. A low pressurizer level signal actuates DHRS. If the leakage exceeds the capacity of the containment evacuation system, then a high containment pressure signal is expected that terminates the leakage and actuate DHRS, consistent with the progression expected in other initiating events resulting in a decrease in inventory from the RCS into containment.
Spurious ECCS signal	AOO	A spurious ECCS signal could signal for opening of all four ECCS valves, or one division of ECCS (1 RRV and 1 RVV). The RRV design includes an inadvertent actuation block feature to prevent opening until the RCS is depressurized to below a set pressure. The RVV does not include an IAB in the US460 design. An inadvertent ECCS signal for 1 ECCS division would result in the full opening of 1 RVV, while a failure causing a signal for all valves would result in simultaneous opening of both RVVs. The IABs on the RRVs would initially block the RRV opening, delaying the RRV opening until after the threshold differential pressure is reached due to RPV discharge into containment through the opened vent valve(s). Although a spurious ECCS signal leading to ECCS valve opening while the module is at power operation is not expected to occur in the life of the plant, the event is conservatively categorized as an AOO and analyzed against AOO acceptance criteria.

© Copyright 2023 by NuScale Power, LLC

Table 4-2 Events Involving Decrease of RCS Inventory (Continued)

Event	Event Category	Basis/Discussion
Spurious opening of single ECCS valve	AOO	A mechanical failure or failure of both solenoids on one valve could result in the opening of a single ECCS valve. The valve opening is considered the initiating event (i.e. the valve opening is not the result of an initiating event plus a coincident single failure). Although an ECCS valve is not expected to spuriously open during the life of a module, the event is conservatively categorized as an AOO and analyzed against the AOO acceptance criteria.
Spurious opening of multiple ECCS valves due to mechanical failure	Beyond Design Basis	Simultaneous mechanical failures on multiple ECCS valves is beyond-design-basis with respect to identifying initiating events. A spurious ECCS signal that could result in the opening of multiple RVVs is categorized as a separate event, per discussion of spurious ECCS signal.
Spurious opening of one reactor safety valve	AOO	The reactor safety valves provide over-pressure protection of the reactor pressure vessel. Mechanical failure associated with the valve internals could result in spurious opening of a reactor safety valve. Consistent with the categorization of the spurious opening of one ECCS valve, this event is conservatively categorized as an AOO and analyzed against AOO acceptance criteria.
Break of small pipes connected to reactor vessel inside containment	Accident	A pipe break is a mechanical failure that is not expected to occur during the design life of a reactor module. This event is classified as an accident.
Break of small pipes connected to reactor vessel outside containment (isolatable)	Accident	A pipe break is a mechanical failure that is not expected to occur during the design life of a reactor module. Consistent with the classification of the break of small pipes connected to the reactor vessel inside of containment, this event is categorized as an accident. It is noted that the radiological consequences for breaks of small pipes outside of containment are of particular relevance and the rate of inventory loss relative to any supplied makeup is important with respect to when, or if, reactor trip and containment isolation are actuated.

© Copyright 2023 by NuScale Power, LLC

Table 4-2 Events Involving Decrease of RCS Inventory (Continued)

Event	Event Category	Basis/Discussion
Break of small pipes connected to reactor vessel outside containment (unisolable)	N/A	Consistent with current plant designs, in the NuScale design this event is mitigated by isolating the break via redundant isolation valves in series for piping connected to the RCS. Therefore, any unisolable break of RCS piping outside of containment is beyond-design-basis (because multiple failures of safety-related isolation valves are necessary following the initiating event). With respect to small pipes or lines connected to the reactor vessel and running outside containment, the following are specifically considered: • In the current design there are no RCS fluid-sensing instrument lines that carry RCS fluid outside of containment pressure boundary • The ECCS valve design includes a hydraulic line inside containment from the main valve on the reactor coolant pressure boundary to a trip valve and reset valve. The trip valve and reset valve are mounted on the exterior of the CNV and are part of the containment pressure boundary. As part of the containment pressure boundary, a gross failure of the trip valve or reset valve that results in an unisolable bypass of RCS fluid to outside the containment pressure boundary is beyond design basis.
Steam generator tube failure	Accident	A steam generator tube failure is classified as an accident. Steam generator tube ruptures are not typically considered AOOs in operating plants (it is noted that the NuScale DSRS identifies that steam generator tube leaks are an example of an AOO, but steam generator tube ruptures are not listed as an example postulated accident). NuScale DSRS Section 15.0.3 lists steam generator tube failure in Table 1 “SMR Accident Dose Criteria”. Therefore, it is appropriate to classify the event as an accident, although it is recognized that the radiological analysis of this event considers various assumptions and different acceptance criteria are applicable depending on those assumptions.

© Copyright 2023 by NuScale Power, LLC

Table 4-2 Events Involving Decrease of RCS Inventory (Continued)

Event	Event Category	Basis/Discussion
Potential LOCA resulting from control rod ejection	N/A	A rod ejection accident (REA) has historically been postulated as the failure of a control rod drive mechanism pressure housing that causes the ejection of a control rod from the reactor. Some plant safety analysis reports identify that the loss of coolant effects for a control rod ejection accident are bounded by the spectrum of LOCA break locations. For the NuScale design the control rod ejection accident is analyzed as a limiting reactivity insertion event. The inventory decrease and associated RCS pressure decrease from a postulated control rod housing failure are insignificant with respect to: • demonstrating that acceptance criteria are met (for the fuel enthalpy increase criterion), • conservatively bounded with respect to demonstrating that acceptance criteria are met (for the radiological acceptance criterion), or • it is conservative to neglect the depressurization effect (for determining maximum RCS pressure and assessing the maximum power response). It is noted that there is precedent in design certification applications that the REA is a rapid positive reactivity insertion analyzed independent of determining a specific failure mechanism.
Gross rupture of reactor vessel	Beyond design basis	Consistent with operating plants, gross rupture of the reactor pressure vessel is beyond design basis.

© Copyright 2023 by NuScale Power, LLC

5.0 Identification and Quantification of Initiating Events

5.1 Introduction

The initiating event analysis identifies plant upsets originating within the plant boundary that disrupt the at-power operations of an NPM. These initiators include random equipment malfunctions and operator errors that either cause an automatic reactor trip or demand a manual trip. Hazards such as floods, fires, earthquakes, and high winds are addressed in separate analyses; upsets unique to low power and shutdown operations are also assessed separately. Accidents arising from acts of sabotage or security threats are beyond the scope of this evaluation.

The quantification of initiating event frequencies typically makes use of Bayesian estimation methods. This statistical inference methodology employs generic prior data and plant-specific data to produce a posterior distribution of an event frequency using Bayes' Theorem. However, since NuScale does not have plant-specific operating experience to draw from, initiating event frequencies are estimated based solely on the generic prior data collected by the NRC through licensee event reports from the U.S. nuclear industry.

In accordance with the ASME/ANS PRA Standard (Reference 10.4) and Regulatory Guide 1.200, the technical characteristics of the initiating event analysis include:

- sufficiently detailed identification and characterization of initiating events
- grouping of events according to plant response and mitigating requirements
- proper screening of individual or grouped initiating events

5.2 Methodology

The key steps in the initiating event analysis are:

1. Identification of Plant Faults

   A listing of plant faults that have the potential for interrupting normal NPM operation is populated through a variety of sources including a literature search of industry data, a master logic diagram (MLD), and failure modes and effects analyses (FMEAs) of plant systems.

2. Screening and Categorization of Plant Faults

   The plant faults are evaluated for their applicability to the NuScale design. The basis for screening out plant faults is described in Section 6.2.2. The remaining plant faults are categorized and grouped.

3. Grouping and Quantification of Initiating Events

   The categorized plant faults are grouped into initiating events according to plant response. An initiating event frequency is estimated by applying industry data or performing NuScale-specific analyses.

© Copyright 2023 by NuScale Power, LLC

5.2.1 Identification of Plant Faults

The initial identification of plant faults for the at-power, internal events PRA includes application of FMEAs and development of an MLD.

Additional data are also reviewed in order to develop a comprehensive list of initiating events for the NuScale PRA:

- NuScale design-basis events
- industry (generic) data
- PRA studies from operating plants
- advanced reactor designs

5.2.2 Screening and Categorization of Plant Faults

The plant faults identified and tabulated are reviewed for applicability to the NuScale design and screened out from further consideration as appropriate. The plant faults that have been screened out use the following criteria:

- Fires and floods as potential initiators are not within the scope of the at-power, internal events PRA because they are addressed in separate analyses.
- Certain plant faults that are relevant to traditional LWR designs that are not applicable to the NuScale design. For example, reactor coolant pump seal loss of coolant accidents (LOCAs) are not applicable to a design without reactor coolant pumps. Similarly, pressurizer power operated relief valve (PORV) opening is excluded because the NuScale design does not include pressurizer PORVs. In addition, interfacing systems loss of coolant accident (ISLOCAs) is screened, as the NuScale design is not susceptible to traditional ISLOCAs.

The plant faults that remain following the screening process are categorized based on plant response, success criteria, timing, potential for radionuclide release, and the effects on the operability and performance of mitigating systems and plant operators. The categories defined for the initiating events are:

- pipe breaks and LOCAs
- steam generator tube failures
- secondary side line breaks
- losses of electric power
- transients

© Copyright 2023 by NuScale Power, LLC

5.2.3 Grouping and Quantification of Initiating Events

Each initiating event category is represented by one or more initiating events. The initiating events themselves are groupings of events that demand a reactor trip or controlled shutdown and lead to a common plant response. The events comprising an initiating event are grouped in order to facilitate the delineation of accident sequences in the PRA event trees. For example, the secondary side line break initiating event is a grouping of pipe breaks/leaks in the main steam, feedwater, and decay heat removal lines because the response of the plant to these occurrences can be assessed similarly in the accident sequence analysis. The events comprising an initiating event are also bounded by the worst case impact within the group. For example, the general reactor trip includes several initiators and the accident progression considers a reactor safety valve (RSV) demand because some initiators result in immediate isolation of the feedwater system.

Quantification of the initiating events is performed by a combination of the following techniques:

- applying relevant operating experience from U.S. nuclear power plants
- use of NuScale-specific studies

Typical practice for PRAs across the nuclear industry uses Bayesian analysis methods to estimate occurrence frequencies. The Bayesian methodology consists of using industry-wide generic data and subjective experience to assign a prior distribution to a parameter, such as failure rate. The second part of Bayesian estimation is in applying plant-specific data to transform the prior distribution into a posterior distribution according to Bayes' Theorem. Bayes' Theorem provides a statistical framework for processing new information as it becomes available over time. In the NuScale design, plant-specific data do not currently exist. Therefore, Bayes' Theorem, in its entirety, cannot be used. The initiating event frequencies have been quantified based solely on generic prior information.

Initiating event frequencies in the NuScale PRA are defined in terms of occurrences per module critical year (mcyr). As described in supporting requirement IE-C5 and note 1 to Table 2-2.1.4(c) in ASME/ANS RA-Sa-2009 (Reference 10.5), initiating event frequencies are to be calculated on a reactor year basis. Included in the initiating event analysis is the plant availability, which is assumed to be 100 percent.

The calculated initiating event frequencies for the NuScale power module are summarized in Table 5-1.

© Copyright 2023 by NuScale Power, LLC

Table 5-1 Initiating Event Frequencies

Category	Initiator	Mean (per mcyr)
Pipe breaks and loss of coolant accidents	CVCS injection line pipe break outside containment	1.7E-05
	CVCS discharge line pipe break outside containment	2.5E-06
	CVCS injection line LOCA inside containment	4.1E-04
	LOCA inside containment	1.3E-03
	Spurious opening of an ECCS valve	7.2E-04
Steam generator tube failures	Steam generator tube failure	4.6E-05
Secondary side line breaks	Secondary side line break	4.4E-05
Loss of electric power	Loss of offsite power - EHVS	2.5E-02
	Loss of DC power - EDAS	2.6E-04
Transients	General reactor trip	5.8E-01
	Loss of support system	5.2E-03

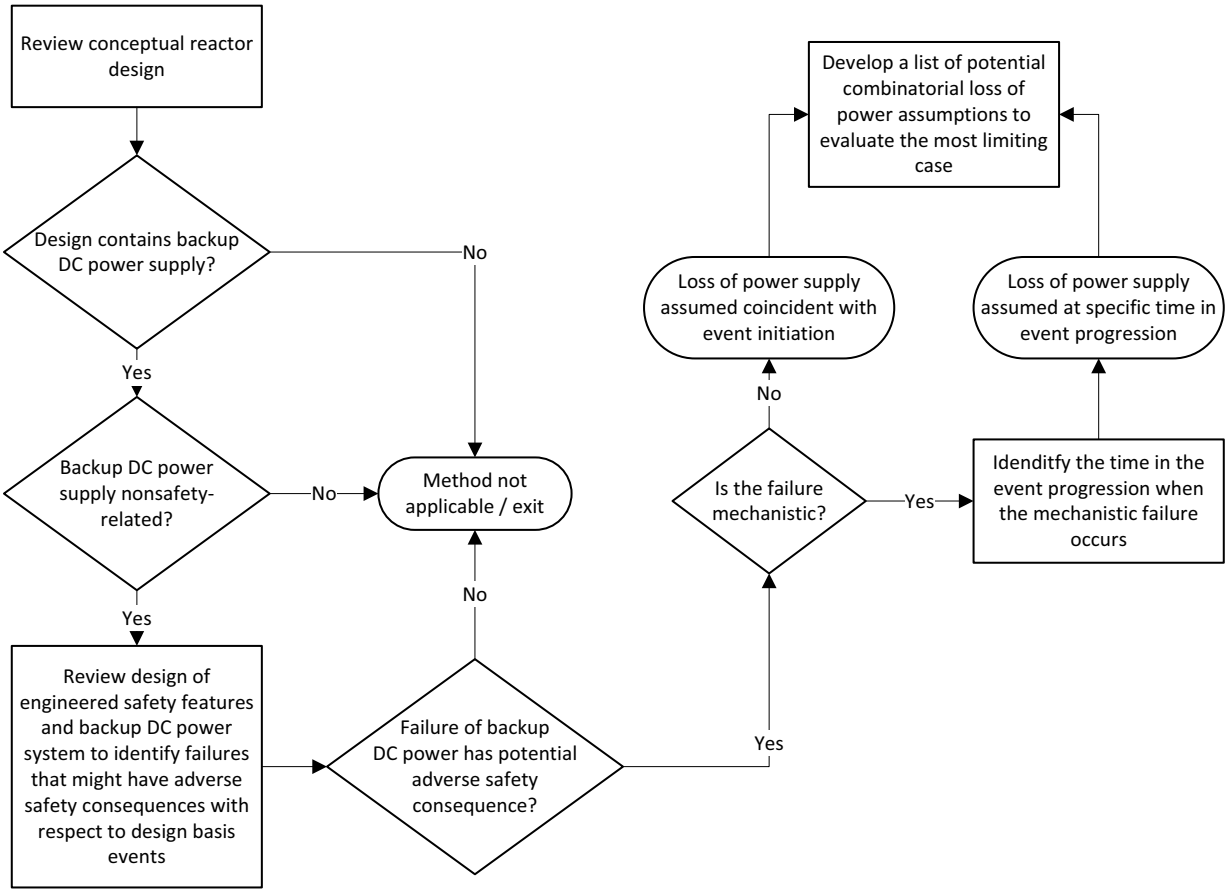
© Copyright 2023 by NuScale Power, LLC

6.0 Implementation of the NuScale Design Process for DC Power Systems

The purpose of this section is to provide the application of the design evaluation process described in Section 3.0. The evaluation is provided for the NuScale Power Module (NPM) US460 as described in Section 2.0. Additional system design details are described as needed to provide context for the evaluation and conclusion.

The DC power systems are first classified based on their functional design purpose to provide nonsafety-related back-up power and then evaluated against the failure credibility criteria and safety-related classification guidance listed in Section 3.0.

Figure 6-1 Treatment of Nonsafety-Related DC Power System Failure Methodology



© Copyright 2023 by NuScale Power, LLC

6.1 Identification of Nonsafety-Related DC Power Systems

As described in Section 2.4 and Section 2.5, the NPM design has two nonsafety-related DC power supply systems, the EDAS with augmented requirements and the EDNS. Each of these systems is considered in the design evaluation.

6.2 Review of Nonsafety-Related DC Power System Functions and Loads

The focus of the review is to identify system functions and loads in order to characterize the interface of each system with the range of design-basis event progressions. The interface is characterized in terms of failures of the system functions and impact on the reactor module thermal-hydraulic response.

6.2.1 Normal DC Power System (EDNS)

As described in Section 2.5, a principal EDNS system function is to supply power to required loads. Therefore, during a design-basis event, if the EDNS is operating as designed and performing this function, this supports:

- AC power systems operating as designed
- Module control system operating as designed
- Plant control system operating as designed

Failures of the EDNS to perform the function of supplying power to each of these loads is evaluated to characterize the interface with the design-basis event progression.

6.2.1.1 Failure to Provide DC Control Power to AC Power Distribution Systems

The principal function of each AC power distribution system is to provide electrical power at the required voltage or current to its specified loads. Therefore, should the EDNS fail to provide control power to AC power distribution systems, the AC power distribution systems may not provide power at the required voltage or current to their specified loads. Ultimately, this failure affects power supply to components that directly affect normal reactor module operation, such as the feedwater pumps, chemical volume control pumps, and pressurizer heaters.

Failure of the normal AC power supply is a safety analysis design-basis initiating event; loss of normal AC power supply is considered in conjunction with design-basis initiating events and due to postulated mechanistic failures during the event progression. Therefore, failure of the EDNS to provide control power to AC power distribution systems is encompassed within the scope of existing design-basis safety analyses.

© Copyright 2023 by NuScale Power, LLC

6.2.1.2 Failure to Provide Power to Module Control System

In the NPM design, the module control system (MCS) provides module-specific normal control functions during power operation, including:

- Pressurizer pressure control, by combination of pressurizer spray and heater control
- Pressurizer water level control, by operation of CVCS makeup pumps and letdown control valve
- Core average coolant temperature control, by combination of secondary side steam demand and control rod movement
- Secondary steam pressure control, by combination of turbine throttle and bypass valves
- Turbine load control, by combination of steam pressure control and feedwater flow rate
- Containment pressure control, by operation of the containment evacuation system

Should the EDNS fail to provide power to the MCS, the module control system does not perform as designed during the design-basis event progression. For example, if pressurizer pressure increases, the MCS would be unable to increase the pressurizer spray flow to attempt to control pressure; the pressurizer heater power could remain constant rather than decreasing, or the pressurizer heater power could cease due to loss of control signal and/or power supply.

Normal plant control system response is evaluated as part of the design-basis safety analyses. If as-designed operation of the normal, nonsafety-related plant control system(s) improves the design-basis event progression, then normal operation is not credited, by assuming that the MCS does not respond to changes in the sensed parameter control input (e.g., pressure, temperature, flow rate, control rod position). Therefore, this type of failure is encompassed within the scope of existing design-basis safety analyses.

Failure of the EDNS to supply power to the MCS could also result in failure of the controlled component output (e.g., pressurizer heaters cease to emit energy, or containment evacuation pumps cease to operate). This type of failure could also be caused by failure of AC power supply. As discussed in Section 6.2.1.1, failure of normal AC power supply is a safety analysis design-basis initiating event and loss of normal AC power supply is considered in conjunction with design-basis initiating events. Therefore, this type of failure is encompassed within the scope of existing design-basis safety analyses.

Based on this evaluation, failure of the EDNS to provide power to the module control system is encompassed within the scope of existing design-basis safety analyses.

© Copyright 2023 by NuScale Power, LLC

6.2.1.3 Failure to Provide Power to Plant Control System

In the NPM design, the plant control system (PCS) provides monitoring and control function for systems with equipment and instrumentation common to all modules, such as:

- Auxiliary boiler system
- Air cooled condenser systems
- Backup power supply system
- Reactor component cooling water system
- Fixed area radiation monitoring systems
- Safety display and indication system
- Neutron monitoring system for refueling
- Module assembly equipment bolting
- Remote recovery platform
- Reactor building crane, turbine building crane
- Boron addition system
- Containment flood and drain system
- Module heatup system
- Integrated control system (for refueling and remote handling)
- Control room habitability system
- Normal control room, reactor building, turbine building, radioactive waste building HVAC systems
- Gaseous, liquid, solid radioactive waste systems
- Radioactive waste drain system, balance of plant drains system
- Demineralized water system
- Chilled water, utility water, site cooling water, potable water systems
- Nitrogen distribution system
- Process sampling system
- Ultimate heat sink
- Turbine lube oil storage
- Instrument and control / service air system
- Seismic monitoring system
- Plant-wide video monitoring system
- Pool cooling and cleanup system

© Copyright 2023 by NuScale Power, LLC

- Meteorological environmental monitoring system
- Fire protection system
- Diesel fuel transfer system
- Reactor building components
- Grounding and lighting protection system
- Equipment that is common to all modules, although it belongs to a system whose components and equipment are predominantly module-specific, such as:
  - Chemical volume control system isolation valves at the interface with the module heatup system
  - Equipment and instrumentation for the condensate polishing resin regeneration in the condensate and feedwater system
  - Common equipment in augmented DC power system, normal DC power system
  - Common equipment in low, medium, high voltage AC electrical distribution systems

Should the EDNS fail to provide power to the PCS, the plant control system, does not perform as designed during the design-basis event progression.

The PCS provides monitoring and control functions of many shared plant systems that do not affect the ability to control reactivity, reactor coolant inventory, reactor coolant pressure or temperature during normal power operation. For example, the radioactive waste systems, seismic monitoring system, or equipment associated with refueling operations do not affect design-basis event progressions.

The PCS provides monitoring and control functions of the reactor building HVAC system, which supports a range of initial conditions for component environments that are integrated with appropriate equipment qualification programs. The safety analyses rely on the equipment qualification program to demonstrate that the equipment within the program is capable of performing its required functions in the specified environmental conditions for the required post-accident durations. Therefore, failures associated with the power supply to the PCS are not evaluated in further detail with respect to the equipment environmental conditions.

The PCS provides monitoring and control functions of shared systems which are used to establish a range of plant initial conditions that are assumed in the design-basis safety analyses. For example, the pool cooling and cleanup system maintains the ultimate heat sink temperature initial condition within bounds analyzed in the safety analyses. The safety analyses subsequently address a range of ultimate heat sink temperatures appropriate to the design-basis event duration, where PCS may be operating and maintaining the ultimate heat sink

© Copyright 2023 by NuScale Power, LLC

temperature within normal bounds or PCS may not be operating due to loss of power supply and the pool temperature may riser over the long-term event progression.

Failures of PCS control of other systems are encompassed in the design-basis safety analyses as initiating events. For example, failures affecting the boron addition system or the demineralized water system could result in an inadvertent boron dilution event and reactivity insertion.

Based on this evaluation, failure of the EDNS to provide power to the plant control system is encompassed within the scope of existing design-basis safety analyses in terms of the initiating events, and the range of initial and boundary conditions analyzed.

6.2.1.4 Summary - EDNS

The system-level functions of the EDNS and the loads associated with the functions are reviewed. The failure of the EDNS to perform these functions, essentially failure to provide power to the identified loads, is considered. Failure of the EDNS to perform the identified functions is encompassed within the scope of the existing design-basis safety analyses, considering the range of initiating events and event progressions (i.e., AC power availability and normal control system operation). Therefore, failures of the EDNS do not introduce a new or different challenge to be addressed in the scope of the design-basis safety analyses.

6.2.2 Augmented DC Power System (EDAS)

As described in Section 2.4, EDAS functions operationally to:

- Provide electrical power for the prevention of unintended ECCS actuation.
- Provide backup electrical power for Post-Accident Monitoring (PAM) instrumentation for type B, C, D, and F variables.
- Provide module-specific and common DC electrical power with adequate voltage and current to EDAS loads when AC power is available to EDAS.
- Provide module-specific and common DC electrical power with adequate voltage, current, and capacity to specified EDAS module-specific and common loads not requiring augmented requirements DC power when AC power is not available to EDAS.

Failures of the EDAS to perform the function of supplying power to required loads is evaluated to characterize the interface with the design-basis event progression. These functions are evaluated separately, which is appropriate for evaluation at the function level and does not require knowledge of whether components and equipment serve different or multiple functions (e.g., equipment with augmented requirements for required loads vs. equipment without augmented requirements for other loads). EDAS

© Copyright 2023 by NuScale Power, LLC

is not relied upon in the safety analyses of DBEs to provide or support plant-level safety-related functions.

6.2.2.1 Failure to Provide Power to Maintain ECCS Valves Closed

The EDAS provides electrical power through the module protection system (MPS) DC-DC converter Class 1E isolation device to prevent unintended ECCS actuation. Power is then routed through the MPS to the ECCS solenoid trip valves.

Failure of the EDAS power supply to the MPS results in reactor trip, containment isolation, DHRS actuation, and ECCS actuation. As described in Section 2.3.1, ECCS actuation results in the RVVs opening and rapid depressurization of the RPV into containment. If the RPV and CNV are initially at normal pressure conditions, opening of the RRVs is initially blocked by the IABs; the RRVs subsequently open after the IAB releases.

ECCS actuation results in a rapid depressurization of the RPV, pressurization of the containment, and redistribution of reactor coolant between the RPV and the containment vessels. The design-basis safety analyses address inadvertent ECCS operation as an initiating event:

- One ECCS valve inadvertently opens (postulated due to mechanical failure)
- Inadvertent ECCS actuation signal, resulting in both vent valves opening simultaneously

The effect of loss of EDAS power to the MPS and resulting ECCS actuation must also be considered in the context of other design-basis initiating events. For example, a postulated pipe break LOCA concurrent with loss of EDAS power supply would result in break flow rates from the RPV to CNV in excess of flow rates resulting from either the LOCA or inadvertent ECCS actuation alone. A design-basis event that causes reactivity insertion can bring the RPV power, pressure, and temperature near the limits for MPS actuations, outside the range of initial conditions assumed for the design-basis event analyses. Therefore, failure of the EDAS function to provide power to maintain the ECCS valves closed is considered in more detail to define the appropriate treatment in the safety analysis scope.

The frequency of ECCS actuation following an AOO is determined by first identifying those AOOs that require ECCS actuation for mitigation and summing their frequencies.

The AOOs that require ECCS are those that result in the relocation of reactor coolant from the reactor pressure vessel to the containment vessel, or otherwise actuate ECCS as part of the mitigation strategy. Of the events classified as AOOs, only the inadvertent opening of an RSV or an ECCS valve relocates coolant to containment.

© Copyright 2023 by NuScale Power, LLC

Then, other causes of ECCS actuation are evaluated. Of the ECCS actuation causes considered, the loss of DC power probabilistic risk assessment (PRA) initiating event is included in this frequency analysis. This initiating event involves the common cause failure of two or more DC buses and is therefore not an AOO. However, it is included as it would be a direct cause of ECCS actuation. Considering this frequency is analogous to safety analyses of AOOs that deterministically assume DC power is not available.

The inadvertent RSV opening is a contributor to the loss of coolant accident (LOCA) inside containment, and only that portion of the frequency from the PRA initiating event is used; the spurious ECCS valve opening and loss of DC power are stand-alone initiating events and their frequencies are used directly.

The total frequency of ECCS actuation following an AOO is shown in Table 6-1.

Table 6-1 AOOs resulting in ECCS actuations

Event	Frequency (mcyr)
Spurious RSV opening	1.1E-03
Spurious ECCS valve opening	7.2E-04
Loss of DC power	2.6E-04
Total	**2.1E-03**

The results in Table 6-1 show that the frequency of ECCS actuation following such events is approximately 2.1E-03/mcyr (module critical year), or once in 476 years. It can therefore be reasonably concluded that ECCS actuation following an AOO is not expected in the 60-year design lifetime of an NPM.

6.2.2.2 Failure to Provide Power for Post-Accident Monitoring

The EDAS provides electrical power for post-accident monitoring (PAM) by providing electrical power through the module protection system (MPS) DC-DC converter Class 1E isolation device. Power is then routed through the MPS to other equipment and components to provide information for PAM variables to the safety display and indication system displays in the main control room. After a design-basis event, the NPM provides automated actuations that place and maintain the NPM passively cooled and subcritical for at least 72 hours. There are no Type A PAM variables in the NPM design. No operators actions, based on PAM indications for Type A variables, are required in response to a design-basis event to accomplish safety-related functions.

Therefore, postulated EDAS failure to provide electrical power for PAM does not affect the ability to control reactivity, reactor coolant inventory, reactor coolant pressure, or temperature during normal power operation.

© Copyright 2023 by NuScale Power, LLC

6.2.2.3 Failure to Provide Power for Other Loads not Requiring Augmented DC Power Supply

The EDAS provides power for other module-specific and common loads that do not require augmented DC power supply. Loads powered from the EDAS differ depending on whether AC power supply is available or not available to the EDAS.

When AC power supply is available to the EDAS, module-specific loads include:

- Module protection system
- Neutron monitoring system
- Radiation monitoring systems

When AC power supply is available to the EDAS, common loads include:

- Safety display indication system
- Plant protection system
- Plant lighting system for control room normal and emergency lighting

When AC power supply is not available to the EDAS, module-specific and common loads include:

- EDAS battery monitoring system
- Main control room lighting

The neutron monitoring system provides analog neutron flux data to the MPS and the MPS continuously monitors for fault signals from the NMS. If EDAS power supply for the neutron monitoring system fails, a high voltage power supply fault is generated, detected by MPS, and then reactor trip is actuated. This scenario is encompassed within the safety analysis.

The radiation monitoring does not affect the control of reactivity, reactor coolant inventory, reactor coolant pressure or temperature. Therefore failures of EDAS to perform this function are not considered further.

The EDAS supplies power to common loads including the safety display indication system and plant lighting system for control room normal and emergency lighting. These systems do not affect the control of reactivity, reactor coolant inventory, reactor coolant pressure or temperature. Therefore, failures of EDAS to perform these functions are not considered further.

The EDAS supplies power to the plant protection system (PPS). The PPS does not perform safety-related functions. Plant protection system functions include providing control room habitability actuation signals; providing plant information for PAM variables, providing data to operators for control and indication as part of power generation; providing plant information for spent fuel pool level; providing power to sensors as required. These functions do not affect the reactor module.

© Copyright 2023 by NuScale Power, LLC

Therefore, EDAS failure to provide power to the PPS does not affect the control of reactivity, reactor coolant inventory, reactor coolant pressure or temperature. Therefore failures of EDAS to perform this function are not considered further.

When AC power supply is not available to EDAS, EDAS loads that do not require augmented DC power supply include power for the EDAS battery monitoring system and main control room lighting. The EDAS failure to provide power to these loads does not affect the control of reactivity, reactor coolant inventory, reactor coolant pressure or temperature.

6.2.2.4 Summary - EDAS

The system-level functions of the EDAS and the loads associated with the functions are reviewed. The failure of the EDAS to perform these functions, essentially failure to provide power to the identified loads, is considered. In some cases, such as failure to provide power for PAM, the control of reactivity, reactor coolant inventory, reactor coolant pressure or temperature are unaffected. Failure of the EDAS to provide power to the neutron monitoring system is encompassed within the scope of the design-basis safety analyses. Failure of the EDAS to provide power to the MPS results in reactor trip, DHRS actuation, containment isolation, and ECCS actuation. Spurious reactor trip, DHRS actuation, containment isolation are encompassed within the scope of design-basis safety analysis.

Failure of the EDAS function to provide power through MPS to maintain the ECCS valves closed is considered in more detail in Section 6.3 to define the appropriate treatment in the safety analysis scope.

6.3 Review of EDAS Design to Identify Mechanistic Failures

The EDAS system design description and system failure modes and effects analysis (FMEA) are the next layers of design detail considered to identify failures that could result in failure to supply power through MPS to maintain ECCS valves closed when not actuated during a design-basis event progression.

The EDAS system design description clarifies that there are different equipment and components for module-specific loads compared to common loads. The failure of the EDAS to supply power to a module is the appropriate failure mode to consider for the design-basis safety analyses. In other words, failure to supply power to maintain the ECCS valves closed is considered as part of failure to supply power to the MPS rather than considering these separately.

© Copyright 2023 by NuScale Power, LLC

Key observations from review of the EDAS FMEA:

- There are no single failures that could cause loss of power supply from EDAS
  - Loss of a single module-specific power channel does not result in loss of power supply, reactor trip, inadvertent ECCS actuation, or loss of PAM monitoring capacity.
  - Failure of any two module-specific power channels results in reactor trip and ECCS actuation.
- EDAS is designed with independent and diverse monitoring devices such that no single monitoring device failure goes undetected and prevents detection of the failure mechanisms evaluated in the FMEA.
- Failures that could affect power supply from EDAS:
  - Fire in the battery rooms is assumed to result in an EDAS module-specific subsystem failure that results in reactor trip and ECCS valve opening.

The observations from the EDAS FMEA are considered in the context of design-basis events. Fire is outside the scope of, and therefore is not postulated to occur, as part of the design-basis safety analyses. As described in the EDAS system design description, the EDAS battery room post-accident conditions and conditions during a 72-hour loss of AC power event are limited to a mild environment by design. The safety analyses rely on the equipment qualification program to demonstrate that the equipment within the program is capable of performing its required functions in the specified environmental conditions for the required post-accident durations. Therefore, it is concluded that design-basis event progressions does not result in a mechanistic or consequential failure of the EDAS to provide power to maintain the ECCS valves closed.

6.4 Summary of EDAS Failures Addressed in Design-Basis Safety Analysis

Based on the reviews performed in Section 6.3, the following EDAS scenarios to supply power are defined for the safety analysis.

- A non-mechanistic failure is assumed where EDAS fails to provide power to the MPS, coincident with the design-basis event initiation. Analysis of this failure demonstrates that the EDAS is not relied upon to perform its functions during the design-basis event, consistent with a classification of the system and its functions as nonsafety-related.
- No mechanistic failures are identified to occur over the course of any design-basis event progression.

The EDAS failure to supply power results in reactor trip, containment isolation, DHRS actuation and ECCS actuation, design-basis events that require operation of the normal feedwater system, main steam system, chemical volume control system, or the control rod drive system to initiate the event essentially collapse to a single initiating event. The reactor trip and containment isolation prevent evolution of those unique initiating events coincident with the EDAS failure. However, other initiating events such as primary or

© Copyright 2023 by NuScale Power, LLC

secondary side break events, inadvertent ECCS actuation, or inadvertent reactor valve opening events would have a different progression when EDAS failure is assumed coincident with the event initiation.

No mechanistic failures of the EDAS due to the progression of a design-basis event are identified to be addressed in the safety analyses. This conclusion is logically consistent with the EDAS system functions and design. A key function of the EDAS system is to provide backup power supply to specified loads when AC power supply is not available. In particular, EDAS provides power for post-accident monitoring, and provides power to prevent inadvertent actuation of the ECCS valves when they are not required to provide cooling. Through the design reliability assurance program (D-RAP), augmented requirements have been applied to the design to support performance of these functions. For design-basis event progressions where EDAS is initially available to supply power, EDAS continues to perform its functions to supply power as designed. Therefore, for event progression analyses where EDAS is assumed to be initially available to supply power, EDAS is assumed to continue to supply power as designed.

6.5 Results

The evaluation concludes:

- Failure of the EDAS to supply power to the MPS results in opening of ECCS valves, which is addressed in the design-basis safety analyses.
- No mechanistic failures of the EDAS are identified to occur over the course of any design-basis event progression.
- Failure of the EDAS is appropriately addressed in the design-basis safety analyses by assuming a non-mechanistic failure where EDAS fails to provide power to the MPS, coincident with the design-basis event initiation. Analysis of this failure demonstrates that the safety analyses do not rely on the EDAS to perform its functions during a design-basis event.

Based on the conclusions of the evaluation, design-basis safety analyses is performed assuming either:

- EDAS performs as designed and power is available throughout the event progression, or
- EDAS power fails coincident with the event initiation.

© Copyright 2023 by NuScale Power, LLC

Because of the extremely low probability[1] of a failure of the EDAS during an event (also known as a "smart failure"), a "smart failure" of EDAS is, at most, a beyond design basis event. This analytical method is consistent with:

- ANS-30.2-2022 (Reference 10.1), Section 5.2.1.1 (frequency below 10^{-7}/plant-yr is beyond design basis event) citing NUREG 75/087, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" (reissued as NUREG-0800) and WASH-1270, "Anticipated Transients Without Scram for Water-Cooled Power Reactors," (1973).
- ANS-58.14-2022, (Reference 10.2), Section 4.5.2 ("low probability events [such as "smart failure" of EDAS] considered not credible"); ANS 58.14 is cited extensively in DG-1371 (ML20168A883).
- ANS-51.1-1973 (Reference 10.6), Section 2.1 ("the full spectra of plant conditions in accordance with their anticipated frequency of occurrence and consequences").
- ANS-51.1-1983 (Reference 10.8), Section 3.2.3 ("If the frequency of occurrence of an event is shown to be < 10^{-6}/reactor year on a best estimate basis, this event shall not be considered for design").
- NEI 18-04, "Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development,"[2] at the safety classification flowchart on page 32 (results in "smart failure" of EDAS being, at most, a beyond design basis event (BDBE)).
- Memorandum to the Commissioners, "Alternative Risk Metrics for New Light-Water Reactor Risk-Informed Applications," and enclosed "White Paper on Options for Risk Metrics for New Reactors," (ML090150636, ML090160004) (Feb. 12, 2009) (1E-6 threshhold)

For the US460 design, because the EDAS failure to supply power results in reactor trip, containment isolation, DHRS actuation and ECCS actuation, design-basis events that require operation of the normal feedwater system, main steam system, chemical volume control system, or the control rod drive system to initiate the event essentially collapse to a single initiating event. The reactor trip and containment isolation prevent evolution of those unique initiating events coincident with the EDAS failure. However, other initiating events such as primary or secondary side break events, inadvertent ECCS actuation, or inadvertent reactor valve opening events would have a different progression when EDAS failure is assumed coincident with the event initiation.

1. That extremely low probability is 1.5E-8/yr. An AOO, by definition, is expected to occur one or more times during the life of a plant. The frequency of a PWR general transient is conservatively used (frequency = 5E-1/yr, INL/EXT-21-65055, November 2021, C-2.1.2). Based on system design and redundancy, the subsequent loss of DC power considered failure of 2 DC buses. Using the Loss of DC power initiating event frequency in Table 5-1 and an exposure time of 1 hour, the probability of a subsequent loss of DC power was calculated to be ~3.0E-8 (2.6E-4/mcyr / 8760 hr/yr * 1 hr= 2.97E-8). Therefore, an AOO followed by a loss of DC power is approximately 1.5E-8/yr (0.5/yr * 3E-8).
2. The NRC approved NEI 18-04 in RG 1.233 at 13 (ML20091L698) (June 2020), with clarifications not affecting this analysis. NEI 18-04 is technology-neutral, and while the title says "non-LWR," nothing in the body of NEI 18-04 nor its endorsing document, RG 1.233, forbid its use with LWRs. Technology-neutral, by its own definition, must include LWRs.

© Copyright 2023 by NuScale Power, LLC

7.0 Evaluation of Plant Defense-in-Depth with Loss of DC Power

This section evaluates the ECCS blowdown consequences following a loss of EDAS power during a design-basis event progression with specific consideration of MCHFR margin. This is not considered to be a credible failure and is conducted to evaluate plant defense-in-depth. A loss of EDAS is evaluated beginning from a spectrum of initial conditions with parameters, which range from normal operating conditions to the analytical trip limits for cooldown, heatup, reactivity, and loss of inventory transient events. Additionally, an evaluation of post-CHF heat transfer and clad heatup is performed. This spectrum of calculation results is performed to quantify conditions that could challenge MCHFR margin if EDAS power supply is randomly lost during a design-basis event progression up to the time of reactor trip.

7.1 Range of Evaluated Conditions

The evaluated reactor power ranges from nominal 100 percent to the high power limit of 115 percent, pressurizer pressure ranges from the low pressure limit of 1850 psia to the high pressure limit of 2100 psia, and the hot leg temperature ranges from an approximate nominal value of 600°F to the high hot leg temperature limit of 620°F. These ranges are representative of the limiting module conditions during design-basis events before reactor trip occurs and provide an evaluation of the limiting MCHFR following a loss of EDAS after event initiation, which is not credible but conducted to evaluate plant defense-in-depth.

7.2 MCHFR State-Point Spectrum

It is expected that the conditions that result in the most limiting MCHFR occurs just prior to reactor trip. Evaluation of the MCHFR in loss-of-coolant accident (LOCA) and inadvertent ECCS actuation events show a rapid increase in CHFR margin once the control rods are inserted. Therefore, a loss of EDAS transient is evaluated beginning from a spectrum of initial conditions with parameters that align with the analytical trip limits for cooldown, heatup, reactivity, and loss of inventory events. These state-points represent the expected worst possible conditions before reactor trip occurs. The spectrum of initial power levels, hot leg temperatures, and pressures are shown in Table 7-1. Except for these parameters, other model inputs and biases are conservatively implemented to reduce MCHFR, consistent with the methodology for Phase 0 (early blowdown) analysis of LOCA or inadvertent ECCS actuation events (Reference 10.6).

- Case 1 - Transients that increase power, pressure, and hot leg temperature (reactivity events, cooldown events).
- Case 2 - Transients that increase power and hot leg temperature (reactivity events, cooldown events).
- Case 3 - Transients that increase pressure and temperature (heatup events).
- Case 4 - Transients that increase power (reactivity events).
- Case 5 - Transients that increase temperature (heatup events).
- Case 6 - Transients that decrease pressure (loss of inventory events).

© Copyright 2023 by NuScale Power, LLC

{{

}}2(a),(c)

The MCHFR spectrum results are shown in Table 7-1 and can be compared to the Phase 0 event analysis limit of 1.20. {{

}}2(a),(c)

Table 7-1 Minimum Critical Heat Flux Ratio Initial Condition Spectrum Cases and Results

{{

}}2(a),(c)

© Copyright 2023 by NuScale Power, LLC

7.3 Estimate of Post-CHF Clad Temperature

The MCHFR spectrum results in Table 7-1 show that {{ }}[2(a),(c)] To gauge the potential cladding temperature response should CHF be reached, post-CHF fuel cladding temperatures are estimated using boundary conditions from points 7, 8, and 9 of cases 1 and 2. Conditions from these cases are applied since these yield the most limiting MCHFRs.

In general, the methodology to evaluate post-CHF cladding temperature is an extension of the NuScale LOCA evaluation model, which itself conforms with 10 CFR Part 50, Appendix K. This method defines model inputs and biases that are conservative for core temperatures and already maximizes peak cladding temperature. However, because loss of inventory events and other design-basis accidents do not violate MCHFR margin limits, NuScale has not developed an NRC approved methodology for evaluating post-CHF heat transfer. NuScale is not seeking NRC approval of a method to evaluate post-CHF heat transfer. These results are provided to illustrate the magnitude of cladding temperature increase during a postulated event with random loss of EDAS after event initiation but up to the time of reactor trip. This evaluation applies the default post-CHF heat transfer correlations and transition logic built into NRELAP5.

A case-dependent multiplier is applied to the CHF to ensure NRELAP5 transitions to post-CHF heat transfer.

Table 7-2 provides the peak clad temperature results for the analyzed cases. Figure 7-1 presents peak clad temperature as a function of time for case 1-9 (i.e., the case with the most limiting PCT). Results from case 1-9 with post-CHF transition disabled are also plotted to compare the core response when CHF is not reached. {{

}}[2(a),(c)] The increase in flow allows the clad surface to re-wet and transition back to the nucleate boiling heat transfer regime. The clad temperature excursion lasts for less than 10 seconds before returning to temperatures less than the initial value. After this excursion, the transient behaves similarly to the longer-term transient. Decreased core power and continuous liquid coverage ensure margin to CHF is maintained over the long-term. Additionally, no loss of coolable geometry is anticipated due to low PCT compared to the 2200°F limit of 10 CFR 50.46(b)(1).

© Copyright 2023 by NuScale Power, LLC

Table 7-2 Peak Clad Temperature for Limiting Cases

{{

}}2(a),(c)

Figure 7-1 Peak Clad Temperature

{{

}}2(a),(c)

© Copyright 2023 by NuScale Power, LLC

8.0 Probabilistic Risk Assessment Insights

NuScale probabilistic risk assessment (PRA) evaluates the risk of beyond-design-basis events. The risk metrics that NuScale quantifies are core damage frequency (CDF) and large release frequency (LRF), which the NRC has identified as surrogates for cancer fatality risk and early fatality risk, respectively. Although the NRC has established safety goals for the CDF and LRF risk metrics, NuScale has shown that the design is far safer than that required by these safety goals by multiple orders of magnitude.

As part of the assessment performed for determining SSC required to be included in the regulatory treatment of nonsafety-related systems (RTNSS), a "focused" PRA is quantified that only takes credit for safety-related SSC (i.e., all nonsafety-related SSC fail). The objective of this assessment is to identify those nonsafety-related SSC that need to be added to the quantification in order to meet the NRC's safety goals. Those nonsafety-related SSC that need to be added into the focused PRA in order to meet the safety goals are then classified as RTNSS. For the NuScale design, no nonsafety-related SSC (including EDAS) need to be credited; the NuScale design satisfies the NRC safety goals crediting only safety-related SSC.

In the context of assessing the NuScale plant response to various upset conditions, the primary function of EDAS is to maintain the ECCS in a standby configuration; that is, EDAS prevents the opening of the ECCS valves when they do not need to open. (Note that as with all safety-related actuations, a loss of EDAS results in the actuation of ECCS.)

In the analysis performed to support the PRA, the ECCS functions to preserve RCS inventory: a single train is sufficient to allow core cooling without RCS makeup from external source. ECCS reliability is high because there is no dependence on any support system (i.e., AC or DC power, or service water) or operator action, no reliance on external sources of inventory addition, redundancy in the design, and because of the fail-safe nature of ECCS operation.

The only other post-accident function of DC power is post-accident monitoring (PAM). However, in the context of mitigating severe accidents, there are no plant responses or operator actions that require or depend on PAM. Therefore, the absence of PAM (due to the potential unavailability of EDAS) does not affect the public health and safety in any quantifiable manner.

Table 8-1 provides the point estimate results for both the CDF and LRF per module critical year (mcyr) for the US460 design. The results from the US600 design are also provided for comparison purposes.

Table 8-1 Probabilistic risk assessment results for NuScale designs

Design - Model	CDF	LRF
US460 - Base model	5.4E-09	3.4E-13
US600 - Base model	2.7E-10	1.7E-11
NRC Safety Goal	**1.0E-04**	**1.0E-06**

© Copyright 2023 by NuScale Power, LLC

9.0 Summary and Conclusions

The US460 NuScale Power Module is a unique integral PWR design that relies on natural circulation, and a limited number of safety-related systems to mitigate the consequences of postulated accidents. NuScale applies a risk-informed, performance-based design process, consistent with ANSI/ANS 30.3, ANSI/ANS 58.14, and other guidance and policy to determine the risk and safety classification of individual system functions. SSCs are classified as (1) safety-related, (2) nonsafety-related, or (3) nonsafety-related with augmented requirements (i.e., special treatment). This design process is applied to the DC power systems to conclude that the EDAS is appropriately classified as not risk-significant, non-safety related with augmented design requirements.

The design of the EDAS prevents the failure of any single power channel from causing a loss of DC power to the module. An initiating event analysis has determined that probability of a random failure (at any time) of the EDAS is 2.6E-04 mcyr (per module critical year), and the probability of an EDAS "smart failure" during a separate initiating event is on the order of 1.5E-8 mcyr.

In addition to being highly unlikely, a "smart failure" of EDAS during a separate initiating event has low to no safety consequences. The CHFR remains above the LOCA/IORV MCHFR limit for the majority of state-point conditions. The CHFR decreases below the analysis limit for cases that combine high power with high hot leg temperature. The cladding temperature response as a function of time is determined from the most limiting conditions to determine the significance of this result. {{

}}2(a),(c)

well below the peak clad temperature limit of 2200°F for 10 CFR 50.46, preserving a coolable geometry.

Finally, the NuScale probabilistic risk assessment (PRA) quantifies the risk impact of all identified and credible design-basis and beyond design-basis events. The risk metrics that NuScale quantifies are core damage frequency (CDF) and large release frequency (LRF), which the NRC have identified as surrogates for cancer fatality risk and early fatality risk, respectively. The results of the PRA show that the risk metrics satisfy the NRC safety goals by multiple orders of magnitude, thereby preserving public health and safety. Additionally, when compared to the PRA results from the US600, approved by the NRC in the US600 DCA, the LRF is reduced by an order of magnitude.

© Copyright 2023 by NuScale Power, LLC

10.0 References

10.1 American National Standards Institute, “Light Water Reactor Risk-Informed, Performance Based Design,” ANSI/ANS-30.3-2022, La Grange Park, IL.

10.2 American National Standards Institute, “Safety and Pressure Integrity Classification Criteria for Light Water Reactors,” ANSI/ANS-58.14-2022, La Grange Park, IL.

10.3 NuScale Power, LLC, “Risk Significance Determination,” TR-0515-13952-NP-A, Revision 0.

10.4 American Society of Mechanical Engineers/American Nuclear Society, “Addenda to ASME/ANS RA-S-2008 Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications,” ASME/ANS RA-Sa-2009, ASME/ANS, New York, NY, February 2009.

10.5 NuScale Power, LLC, “Non-Loss-of-Coolant Accident Methodology.” TR-0516-49416-P, Revision 4.

10.6 NuScale Power, LLC, “Loss-of-Coolant Accident Methodology.” TR-0516-49422-P, Revision 3.

10.7 American National Standards Institute, "Nuclear Safety Criteria for the Design of Stationary Pressurized Water Water Reactor Plants." ANSI/ANS 51.1-1973, La Grange Park, IL.

10.8 American National Standards Institute, "Nuclear Safety Criteria for the Design of Stationary Pressurized Water Water Reactor Plants." ANSI/ANS 51.1-1983, La Grange Park, IL.

© Copyright 2023 by NuScale Power, LLC

Appendix A Background

The NPM design is unique as a passive, natural circulation reactor, with reliance on a limited number of safety-related SSC.

A.1 Regulatory Framework

This section identifies the regulatory requirements relevant to safety classification of EDAS and the treatment of EDAS in safety analysis for the NPM. Several of the GDCs are subject to exemptions for the US460 standard design; they are listed here because the rules inform NuScale's approach to safety analysis and demonstration that the design meets the underlying purpose of the GDCs.

10 CFR 50.2

Safety-related structures, systems and components means those structures, systems and components that are relied upon to remain functional during and following design-basis events to assure:

(1) The integrity of the reactor coolant pressure boundary

(2) The capability to shut down the reactor and maintain it in a safe shutdown condition; or

(3) The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the applicable guideline exposures set forth in 50.34(a)(1) or 100.11 of this chapter, as applicable.

10 CFR 50 Appendix A GDCs

GDC 10 - Reactor design.

The reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences.

GDC 15 - Reactor coolant system design.

The reactor coolant system and associated auxiliary, control, and protection systems shall 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.

© Copyright 2023 by NuScale Power, LLC

GDC 17 - *Electric power systems*.

An onsite electric power system and an offsite electric power system shall be provided to permit functioning of structures, systems, and components important to safety. The safety function for each system (assuming the other system is not functioning) shall be to provide sufficient capacity and capability to assure that (1) specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded as a result of anticipated operational occurrences and (2) the core is cooled and containment integrity and other vital functions are maintained in the event of postulated accidents.

The onsite electric power supplies, including the batteries, and the onsite electric distribution system, shall have sufficient independence, redundancy, and testability to perform their safety functions assuming a single failure.

Electric power from the transmission network to the onsite electric distribution system shall be supplied by two physically independent circuits (not necessarily on separate rights of way) designed and located so as to minimize to the extent practical the likelihood of their simultaneous failure under operating and postulated accident and environmental conditions. A switchyard common to both circuits is acceptable. Each of these circuits shall be designed to be available in sufficient time following a loss of all onsite alternating current power supplies and the other offsite electric power circuit, to assure that specified acceptable fuel design limits and design conditions of the reactor coolant pressure boundary are not exceeded. One of these circuits shall be designed to be available within a few seconds following a loss-of-coolant accident to assure that core cooling, containment integrity, and other vital safety functions are maintained.

Provisions shall be included to minimize the probability of losing electric power from any of the remaining supplies as a result of, or coincident with, the loss of power generated by the nuclear power unit, the loss of power from the transmission network, or the loss of power from the onsite electric power supplies.

GDC 18 - Inspection and testing of electric power systems.

Electric power systems important to safety shall be designed to permit appropriate periodic inspection and testing of important areas and features, such as wiring, insulation, connections, and switchboards, to assess the continuity of the systems and the condition of their components. The systems shall be designed with a capability to test periodically (1) the operability and functional performance of the components of the systems, such as onsite power sources, relays, switches, and buses, and (2) the operability of the systems as a whole and, under conditions as close to design as practical, the full operation sequence that brings the systems into operation, including operation of applicable portions of the protection system, and the transfer of power among the nuclear power unit, the offsite power system, and the onsite power system.

© Copyright 2023 by NuScale Power, LLC

GDC 20 - Protection system functions.

The protection system shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety.

GDC 26 - Reactivity control system redundancy and capability.

Two independent reactivity control systems of different design principles shall be provided. One of the systems shall use control rods, preferably including a positive means for inserting the rods, and shall be capable of reliably controlling reactivity changes to assure that under conditions of normal operation, including anticipated operational occurrences, and with appropriate margin for malfunctions such as stuck rods, specified acceptable fuel design limits are not exceeded. The second reactivity control system shall be capable of reliably controlling the rate of reactivity changes resulting from planned, normal power changes (including xenon burnout) to assure acceptable fuel design limits are not exceeded. One of the systems shall be capable of holding the reactor core subcritical under cold conditions.

GDC 29 - Protection against anticipated operational occurrences.

The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.

GDC 33 - *Reactor coolant makeup*.

A system to supply reactor coolant makeup for protection against small breaks in the reactor coolant pressure boundary shall be provided. The system safety function shall be to assure that specified acceptable fuel design limits are not exceeded as a result of reactor coolant loss due to leakage from the reactor coolant pressure boundary and rupture of small piping or other small components which are part of the boundary. The system shall be designed to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished using the piping, pumps, and valves used to maintain coolant inventory during normal reactor operation.

GDC 34 - *Residual heat removal*.

A system to remove residual heat shall 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 specified acceptable fuel design limits and the design conditions of the reactor coolant pressure boundary are not exceeded.

© Copyright 2023 by NuScale Power, LLC

Suitable redundancy in components and features, and suitable interconnections, leak detection, and isolation capabilities shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure.

GDC 35 - *Emergency core cooling*.

A system to provide abundant emergency core cooling shall be provided. The system safety function shall be to transfer heat from the reactor core following any loss of reactor coolant at a rate such that (1) fuel and clad damage that could interfere with continued effective core cooling is prevented and (2) clad metal-water reaction is limited to negligible amounts.

Suitable redundancy in components and features, and suitable interconnections, leak detection, isolation, and containment capabilities shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure.

GDC 38 - *Containment heat removal*.

A system to remove heat from the reactor containment shall be provided. The system safety function shall be to reduce rapidly, consistent with the functioning of other associated systems, the containment pressure and temperature following any loss-of-coolant accident and maintain them at acceptably low levels.

Suitable redundancy in components and features, and suitable interconnections, leak detection, isolation, and containment capabilities shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure.

GDC 44 - *Cooling water*.

A system to transfer heat from structures, systems, and components important to safety, to an ultimate heat sink shall be provided. The system safety function shall be to transfer the combined heat load of these structures, systems, and components under normal operating and accident conditions.

Suitable redundancy in components and features, and suitable interconnections, leak detection, and isolation capabilities shall be provided to assure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) the system safety function can be accomplished, assuming a single failure.

© Copyright 2023 by NuScale Power, LLC

Appendix B Design Attributes

Table B-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. These attributes include augmented design, qualification, and quality assurance (QA) requirements 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. Table B-1 also specifies a reliability comparison between the nonsafety-related DC electrical system(s) and typical Class 1E DC electrical system(s). The augmented requirements to be applied to such electrical system(s) are detailed in Table B-2.

The process NuScale used to develop the attributes of Table B-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. Specifically, the application of augmented requirements is consistent with the process established in the NRC regulatory framework for "special treatment" of nonsafety-related SSC that are determined to have risk-significance. This well-established framework includes previous Commission policy statements in SECY-94-084 and SECY-95-132 and their associated Staff Requirements Memorandums as implemented further in NUREG-0800, Section 19.3, "Regulatory Treatment of Nonsafety Systems for Passive Advanced Light Water Reactors." The application of the augmented requirements described in Table B-2 via Table B-1 is consistent with the approach of these regulatory policy and guidance documents.

© Copyright 2023 by NuScale Power, LLC

Table B-1 EDAS Safety Classification Basis

Condition No.	Design Attributes and Conditions Satisfied	Justification
1.	For a design-basis event, electrical power is not necessary to achieve safe shutdown, core cooling, containment isolation and integrity, and RCPB integrity, and to maintain them for a minimum of 72 hours.	Design-basis Event Assumptions • 72 hour stabilized condition DBE end state without operator actions required • DBE analysis includes loss of electrical power • SBO Loss of AC and DC power for 72 hour duration
a.	Reactor trip is assured.	• CRDS does not rely on electrical power • SBO reactor trip
b.	Sufficient reactor coolant inventory and negative reactivity are assured during and following a design-basis event to achieve and maintain safe shutdown.	• Shutdown capability does not rely on electrical power • Decrease in inventory event analyses do not rely on electrical power or credit active injection sources • SBO does not rely on electrical power for shutdown or inventory control
c.	Core cooling systems achieve and maintain their safety-related functions.	• DHRS function does not rely on electrical power • ECCS function does not rely on electrical power • DBE analysis does not credit electrical power for DHRS or ECCS functions • Fuel and core acceptance criteria confirm core cooling • SBO core cooling relies on DHRS and ECCS
d.	Containment isolation is achieved and maintained.	• CNV isolation function does not rely on electrical power • SBO containment integrity does not rely on electrical power
e.	Containment integrity is achieved and maintained with no reliance on active ESF heat removal and combustible gas control systems.	• Passive CNTS and UHS design does not include active ESF heat removal and combustible gas control systems • DBE thermal hydraulic acceptance criteria confirm containment peak pressure margin • No credit for active ESF heat removal for containment integrity in SBO analysis

© Copyright 2023 by NuScale Power, LLC

Table B-1 EDAS Safety Classification Basis (Continued)

Condition No.	Design Attributes and Conditions Satisfied	Justification
f.	Active fission product control and removal systems (e.g., ESF atmospheric clean-up systems, containment spray systems, etc.) are not needed to maintain doses less than the applicable guideline exposures set forth in 10 CFR 100.21, 10 CFR 50.34(a)(1)(ii)(D), and 10 CFR 52.137(a)(2)(iv)	• Active fission product removal systems are not required • DBE radiological consequences show guidelines maintained
g.	RCPB overpressure protection is achieved and maintained.	• Overpressure protection system does not rely on electrical power • SBO RPV pressure margin • DBE thermal hydraulic analyses confirm margin to RCS pressure acceptance criteria
2.	Post-accident monitoring instrumentation is not necessary to fulfill the functions contemplated in the IEEE Std. 603 and IEEE Std. 308 definition of Class1E in response to a design-basis event.	
a.	Operator action is not required to achieve safe shutdown, core cooling, containment isolation and integrity, and RCPB integrity, and to maintain them for a minimum of 72 hours.	• PAM design • No credit for manual actions in SBO analysis
b.	The design does not include Type A variables as defined in IEEE Std. 497-2002 as modified in Position C.4 of Regulatory Guide 1.97, Revision 4.	• PAM design
c.	The design does not include Type B and Type C variables that are necessary for the performance of operator actions in response to a design-basis event.	• PAM design
3.	Adequate cooling and shielding of spent fuel assemblies (i.e., water level greater than 10 feet above the top of spent fuel assemblies in the spent fuel pool [SFP]) is assured for a minimum of 72 hours with no reliance on electrical power or operator action.	• UHS and SFP integrated passive cooling function does not rely on electrical power • SFP design maintains 10 feet in SFP above racks without active systems

© Copyright 2023 by NuScale Power, LLC

Table B-1 EDAS Safety Classification Basis (Continued)

Condition No.	Design Attributes and Conditions Satisfied	Justification
4.	Adequate cooling and shielding of reactor fuel assemblies in the process of core unloading and loading, including movement between the spent fuel pool and the reactor core, is assured for a minimum of 72 hours with no reliance on active systems that require electrical power or operator action.	• UHS and SFP integrated passive cooling function does not rely on electrical power • SFP design maintains 10 feet in SFP above racks without active systems • UHS provides a minimum of 10 feet for shielding available during fuel handling
5.	Electrical power is not necessary to actuate control room habitability system (CRHS) functions and to maintain them for a minimum of 72 hours.	• CRHS does not rely on electrical power • Main control room habitable during SBO without relying on electrical power
6.	Temperatures in building areas housing equipment relied upon to operate during station blackout (SBO) conditions are maintained within required equipment qualification limits for a minimum of 72 hours, with no reliance on electrical power and assuming the worst-case heat loads for the areas of concern.	• PAM environmental qualification • 72 hour loss of ventilation • EDAS environment • SBO mitigation equipment for 10 CFR 50.63 (DHRS and ECCS) is operable in SBO environment
7.	Active ventilation or fission product removal systems are not necessary in response to a postulated design-basis event - including a fuel handling accident - to maintain doses less than the applicable guideline exposures set forth in 10 CFR 100.21, 10 CFR 50.34(a)(1)(ii)(D), and 10 CFR 52.137(a)(2)(iv).	Active fission product removal systems • Active fission product removal systems are not required to meet regulatory requirements Active ventilation systems not required to mitigate the consequences of design-basis events • Reactor building ventilation system • No engineered safety function ventilation in design Dose analyses • No active ventilation systems are required to maintain offsite doses within applicable guidelines
8.	The reliability of the EDAS is comparable to that of a typical Class 1E DC power system	• EDAS reliability evaluation
9.	The plant emergency lighting capability satisfies the guidance of SRP/DSRS Section 9.5.3; Regulatory Guide1.189; and NUREG-0700, with appropriate portions powered from EDAS.	• SBO emergency lighting • Fire protection • Emergency lighting design
10.	Compliance with 10 CFR 50.63	• SBO

© Copyright 2023 by NuScale Power, LLC

Table B-1 EDAS Safety Classification Basis (Continued)

Condition No.	Design Attributes and Conditions Satisfied	Justification
11.	EDAS SSC that provide backup power are seismic category I	• EDAS seismic design
12.	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)	• PAM design does not include type A variables • Operator actions not needed to support DBE analysis
13.	The frequency for which a combination of an AOO and an actuation of the NuScale ECCS is not expected to occur during the lifetime of the module	• Section B.1
14.	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.	• Shutdown capability • CVCS safety evaluation • No return to power

© Copyright 2023 by NuScale Power, LLC

Table B-2 US460 Augmented Design, Qualification and Quality Assurance Requirements to Support EDAS Safety Classification

Topic	Provision
Quality Assurance (QA)	Graded QA (GQA) Program • GQA as described in QA Program Description (QAPD) meets or exceeds augmented QA provisions specified in RG 1.155, Appendix A
Environmental Qualification (EQ)	Batteries providing backup DC power are environmentally qualified per IEEE 323-2003 and located in a mild environment
Batteries	Commercial grade valve-regulated lead acid (VRLA) batteries • Design and installation per IEEE Std. 1187-2013 • Maintenance and testing shall be performed in accordance with IEEE Std.1188-2005(R2010) with 2014 amendment • Sizing per IEEE Std. 485-2020 • Instrumentation, indication, and alarms per IEEE Std. 946-2020, IEEE Std. 1491-2012, IEEE Std. 1187-2013, and IEEE 1188-2005
Onsite Standby Power Sources	Nonsafety-related backup generators • Per SRP Section 19.3 • Per EPRI Utility Requirements Document, Rev. 13 • Per SECY-94-084, SECY-95-132, and associated SRMs
Identification	Per IEEE Std.384-1992 as endorsed with modification by RG 1.75
Independence	Independence via physical separation and electrical isolation per IEEE Std. 384-1992 as endorsed with modification by RG 1.75
Single Failure Criterion	The single-failure criterion is applied to EDAS SSC that provide electrical power to prevent unintended ECCS valve actuation per IEEE 379-2020 as endorsed by RG 1.53.
Common-Cause Failure (CCF)	CCF probability minimized to the extent practicable • redundant divisions and channels • protection from environmental and dynamic effects of internal equipment failures via augmented seismic • design/qualification, environmental qualification, and quality assurance provisions, and protection from natural phenomena via augmented seismic design/qualification and quality assurance provisions and location of the EDAS within Seismic Category I structures • Each battery supply shall be immediately available during both normal operations and following the loss of power from the AC system. • EDAS batteries are connected to the DC distribution panel and maintained on a float charge. Upon a loss of AC power the batteries immediately supply all required EDAS loads without interruption.

© Copyright 2023 by NuScale Power, LLC

Table B-2 US460 Augmented Design, Qualification and Quality Assurance Requirements to Support EDAS Safety Classification (Continued)

Topic	Provision
Protection	Equipment protection and coordination studies are performed in accordance with IEEE 242, IEEE 946, and IEEE 1375.
Power Quality	Safety systems protected from variations in voltage, frequency, and waveform Class 1E isolation equipment at each interface between the non-Class 1E electrical system and downstream Class 1E circuits.
Location of Indicators and Controls	Controls and indication provided inside and outside the MCR: • EDAS instrumentation, indication, and alarming features are consistent with guidance contained in the IEEE 946, IEEE 1491, IEEE 1187, and IEEE 1188
Surveillance and Testing	Surveillance and testing: • Periodic inspection and testing is performed on the EDAS for operational, commercial, and plant investment protection purposes.
Multi-Module Considerations	No sharing of DC power between modules that results in potential adverse interactions.

© Copyright 2023 by NuScale Power, LLC

B.1 Frequency of ECCS Actuation after AOOs

The frequency of ECCS actuation following an AOO is determined by first identifying those AOOs that require ECCS actuation for mitigation and summing their frequencies.

The AOOs that require ECCS are those that result in the relocation of reactor coolant from the reactor pressure vessel to the containment vessel, or otherwise actuate ECCS as part of the mitigation strategy. Of the events classified as AOOs, only the inadvertent opening of an RSV or the ECCS relocates coolant to containment.

Then, other causes of ECCS actuation are evaluated. Of the ECCS actuation causes considered, the loss of DC power (i.e., EDAS) probabilistic risk assessment (PRA) initiating event is included in this frequency analysis. This initiating event involves the common cause failure of two or more DC buses and is therefore not an AOO. However, it is included as it would be a direct cause of ECCS actuation. Considering this frequency is analogous to safety analyses of AOOs that deterministically assume DC power is not available.

The inadvertent RSV opening is a contributor to the loss of coolant accident (LOCA) inside containment, and only that portion of the frequency from the PRA initiating event is used; the spurious ECCS valve opening and loss of DC power are stand-alone initiating events and their frequencies are used directly.

The total frequency of ECCS actuation following an AOO is shown in Table B-3.

Table B-3 AOOs resulting in ECCS actuations

Event	Frequency (mcyr)
Spurious RSV opening	1.1E-03
Spurious ECCS valve opening	7.2E-04
Loss of DC power	2.6E-04
Total	**2.1E-03**

The results in Table B-3 show that the frequency of ECCS actuation following such events is approximately 2.1E-03/mcyr (module critical year), or once in 476 years. It can therefore be reasonably concluded that ECCS actuation following an AOO is not expected in the 60-year design lifetime of an NPM.

© Copyright 2023 by NuScale Power, LLC

Appendix C Loss of Power Considerations

In typical LWR safety analyses, ‘loss of offsite power’ is considered for many transients coincident with the initiating event and the limiting single failure of systems relied on to mitigate the transient. However, the role of ‘offsite power’ is not required for NuScale plants. The reliance on natural circulation for normal operation and safety system performance reduces the impact to the core from a loss of electric power relative to a design with forced circulation. The US460 product has no safety-related electrical power supply. The EDAS employs multiple channels with battery backups to provide DC power for module protection system (MPS) operation for at least 72 hours, and maintaining ECCS valves closed for at least 24 hours following a loss of AC power. With a loss of AC power to the EDAS battery charger, the EDAS batteries supply DC power to keep the ECCS valves closed. After 24 hours, the ECCS valves open.

From a non-LOCA transient perspective, details of the power systems are used to define what constitutes a loss of power. Specifically, affected systems and equipment are identified to help categorize the system responses.

The following areas are discussed:

- Whether to consider a loss of power for an event.
- Which electrical systems to consider.
  - Systems and components lost.
- Time that a source of power is lost.
  - Loss of power scenarios and associated system responses.
  - EDAS failure is not a unique initiating event.
  - Generic evaluations of selected loss of power scenarios.
- Summary of loss of power scenarios for FSAR Chapter 15.

The effect of a specific power availability scenario should be assessed as part of the transient simulation. This assessment may be qualitative, quantitative, or a combination of both. An example is any combination of:

- Reference to a higher-level methodology that documents why a specific power availability scenario is not limiting for that transient.
- Qualitative engineering assessment to document the limiting or non-limiting nature of a specific power availability scenario for that transient.
- Quantitative assessment to document sensitivity results for that specific power availability scenario.

Assessments are needed for each applicable acceptance criterion because the power availability scenarios generally differ. The applicable acceptance criteria are those defined in the SRP and the NuScale DSRS. For non-LOCA transients, the time that the ECCS valves open depends on EDAS availability (Section C.2). If EDAS is lost, ECCS actuates and the event is no longer addressed under the non-LOCA methodology. ECCS actuation is addressed in FSAR Sections 15.6.5 and 15.6.6 using LOCA methodology or IORV methodology.

© Copyright 2023 by NuScale Power, LLC

C.1 Basis for Considering Loss of Power for Non-LOCA Transients

The events from Table C-1 are reviewed to identify events that explicitly consider loss of power. This review is specific to the relevant SRP or NuScale DSRS subsection. The list of events is then reduced to those events that employ the non-LOCA methodology (Reference 10.6). The non-LOCA transients that explicitly consider loss of power are listed in Table C-1. The comments provide a summary of regulator expectations.

Review Procedure 7 to SRP 15.4.1 and Review Procedure 5 to SRP 15.4.2 direct that a loss of offsite power in conjunction with the limiting single active failure must be considered when evaluating the results of these anticipated operational occurrences for new applications. This position is based on interpretation of GDC 17, as documented in the Final Safety Evaluation Report for the ABB-CE System 80+ design certification.

A review of the event classifications from Table 4-1 indicates that the non-LOCA transients of Table C-1 correspond to AOOs and accidents. Those non-LOCA transients classified as accidents are shown with *red italics* in Table C-1. For non-LOCA transients not identified in Table C-1, power must generally be available for the system or component to malfunction.

Each non-LOCA transient considers the effect of loss of power when evaluating the acceptance criterion of interest.

© Copyright 2023 by NuScale Power, LLC

Table C-1 Loss of Power for non-LOCA Transients

FSAR Section	Event	Comment
15.1.5	*Steam system piping failures*	*Note 1.*
15.2.1	Loss of external load	Note 2.
15.2.2	Turbine trip	Note 2.
15.2.3	Loss of condenser vacuum	Note 2.
15.2.4	Main steam isolation valve closure	Note 2.
15.2.7	Loss of normal feedwater flow	Note 3.
15.2.8	*Feedwater system pipe breaks*	*Note 4.*
15.4.1	Uncontrolled control rod assembly bank withdrawal from a subcritical or low power startup condition	Note 5.
15.4.2	Uncontrolled control rod assembly bank withdrawal at power	Note 6.

1. Assumption 2 to DSRS 15.1.5: Assumptions as to the loss of offsite power and the time of loss should be made to study their effects on the consequences of the accident. A loss of offsite power could occur simultaneously with the pipe break or during the accident, or offsite power might not be lost.
2. Technical Rationale 4 of DSRS 15.2.1 - 15.2.5: GDC 17 requirements provide assurance that SAFDLs and reactor coolant pressure boundary design conditions are not exceeded in initiating events that decrease heat removal by the secondary system, concurrent with a loss of offsite power.
3. Item 2 of Review Procedures to DSRS 15.2.7: Loss of feedwater should be analyzed with and without a loss of offsite power in combination with a single active failure.
4. Assumption 5B to DSRS Acceptance Criteria for DSRS 15.2.8: Assumptions as to the loss of offsite power and the time of loss should be conservative. Offsite power may be lost simultaneously with the pipe break, the loss may occur during the accident, or offsite power may not be lost.
5. Technical Rationale 3 of DSRS 15.4.1: Meeting GDC 17 ensures that fuel cladding integrity is not challenged during an uncontrolled control rod assembly withdrawal in conjunction with a loss of onsite or of offsite power.
6. Technical Rationale 3 of DSRS 15.4.2: Meeting the requirements of GDC 17 provides reasonable assurance that an uncontrolled control rod assembly withdrawal at power, in combination with loss of offsite power, does not result in a reactor transient that could cause the reactor coolant pressure boundary design conditions or the fuel design limits to be exceeded.

© Copyright 2023 by NuScale Power, LLC

C.2 NuScale Electrical Systems and Loss of Normal Power for Safety Analyses

The following electrical systems are considered to identify the loads they supply that have a direct impact on the safety analysis:

- EHVS - High voltage (13.8kV) AC electrical system and switchyard
- EMVS - Medium voltage (4.16 kV) AC electrical distribution system
- ELVS - Low voltage (480V and 120V) AC electrical distribution system
- EDAS - Augmented DC power system
- EDNS - Normal DC power system

Safety analysis does not credit the backup power supply system to provide power following a loss of normal AC power and therefore this system is not considered further.

The plant lighting, grounding and lightning protection system and the security power system are not relevant to the design basis safety analyses and are not considered further.

Table C-2 summarizes the electrical system loads and whether they are of direct impact to the safety analysis calculations.

© Copyright 2023 by NuScale Power, LLC

Table C-2 Review of Electrical Systems for Loads Important to Safety Analysis

System	Relevant Loads	Impact
EHVS	AC power supply to EMVS	Direct (1)
EMVS	Site cooling water pumps (2)	Other (1)
	Chiller packages (2)	Other
	AC power supply to ELVS	Direct
ELVS	EDAS Battery Chargers (module-specific)	Direct
	Feedwater pump motors	Direct
	Condensate pump motors	Direct
	Pressurizer heaters	Direct
	Containment evacuation system vacuum pumps	Direct
	CRDS power and control power	Direct
	Motor control center in RXB (3)	Direct
	Motor control center in TGB (3)	Direct
	EDNS Battery Chargers	Direct
	Air cooled condenser fans, vacuum pumps, & recirculation pump motors (2)	Other
	EDAS Battery Chargers (common loads)	Other
EDNS	MCS modules, cabinets	Direct
EDAS	MPS (via Class 1E isolation devices)	Direct
	NMS (via Class 1E isolation devices)	Other

Table C-2 Notes:

(1) A ‘direct’ impact to safety analysis is one that, if lost, has direct impact on the reactor module primary or secondary side conditions. An ‘other’ impact is one that may affect a system that connects to systems directly impacting the module, or may affect the ability to monitor the system.

(2) Safety analysis does not directly model these systems. Loss of power to these loads might trigger a reactor shutdown or downstream effect on systems modeled by safety analysis (such as increase in feedwater temperature due to loss of condenser cooling).

(3) The loads relevant to safety analysis include:

- Chemical and volume control RCS injection pump motors
- Chemical and volume control recirculation pump motors
- Containment evacuation system vacuum pump motors
- Turbine stop valve control oil pump motor

Motor operated valves (MOVs) are identified as part of the electrical loads because these valves use an electric motor to adjust position. Since a loss of power may affect their operation, which systems utilize MOVs is important. MOVs are used in the chemical and volume control (CVCS), chilled water, containment evacuation (CES), nitrogen distribution, pool cooling and cleanup, reactor component cooling water, and site cooling water. The MOVs in CVCS, containment evacuation system, and main steam directly impact the primary or secondary side of the reactor module, therefore, an assessment for each system is provided.

If ELVS is not available, the motors for the CVCS RCS injection pumps and recirculation pumps do not have power. CVCS flow stops regardless of the impact of the loss of power

© Copyright 2023 by NuScale Power, LLC

on any MOVs in the flow path. Therefore, the specific impact of loss of ELVS on MOVs in the CVCS is not further investigated.

If ELVS is not available, the motors for the CES vacuum pumps do not have power. Flow from the vacuum pumps stops regardless of the impact of the loss of power on MOVs in the flow path. Therefore, the specific impact of loss of ELVS on MOVs in the CES is not further investigated. If ELVS is not available, the motor for the turbine generator system control oil pump does not have power. Consequently, 1) the hydraulically operated turbine stop valve uses the high pressure fire-resistant hydraulic fluid from the control oil system for control and protection; and, 2) the vendor supplied main turbine control system monitors and controls all turbine and generator subsystems, including the turbine control oil. If the main turbine control system determines there is a problem that warrants immediate action, the controller initiates a turbine trip to close the turbine stop valve and turbine control valve. The module control system would act to maintain secondary pressure by opening the turbine bypass valve. However, with ELVS not available, turbine bypass is not operable because the motors for the feedwater and condensate pumps do not have power. Impacts to the main steam system valves due to loss of control signal are bounded by the turbine stop valve closure without turbine bypass. Therefore, the main steam system is not further investigated.

Based on Table C-2, the electrical systems and main loads important to safety analysis are summarized below and are illustrated in Figure C-1:

- EHVS - 13.8 kV high voltage electrical system (AC power) No main loads important to safety analysis
  - Powers EMVS, and from there to ELVS, EDNS chargers, EDAS chargers. No specific loads to components or other systems that are relevant to safety analysis.
- EMVS - 4.16 kV medium voltage electrical system (AC power) No main loads important to safety analysis
  - Powers ELVS, and from there to EDNS chargers, EDAS chargers. No specific loads to components or other systems that are relevant to safety analysis.
- ELVS - 480 V, 120 V low voltage electrical system (AC power) Loads relevant to safety analysis include:
  - Feedwater pump motors, condensate pump motors, pressurizer heaters
  - Control rod drive mechanisms
  - Power to the motor control center in the reactor building and turbine generator building. The loads relevant to safety analysis are:
    - Chemical and volume control RCS injection pump motors
    - Chemical and volume control recirculation pump motors
    - Containment evacuation system vacuum pump motors
    - Turbine stop valve control oil pump motor
  - Power to EDNS battery chargers, EDAS battery chargers

© Copyright 2023 by NuScale Power, LLC

- EDNS - 250 V DC, 120/208 V AC - Normal DC power system Loads relevant to safety analysis include:
  - Module control system
    - Only the EDNS provides power to the MCS.
    - The turbine generator automatically trips on several set points, including reactor scram. Therefore, the turbine generator is expected to trip as a result of reactor scram.
- EDAS - 125V DC - Augmented DC power system - Loads relevant to safety analysis include:
  - Module protection system
    - Only the EDAS provides power to the MPS safety-related loads.

Both the EDNS and the EDAS are designed with battery backup for continued DC power in the event that normal AC power supply to the chargers is not available. The EDNS batteries are sized to supply loads for 40 minutes.

If normal AC power to the EDAS chargers is lost, the MPS initiates reactor trip, actuate DHRS, and close containment isolation valves. If the EDAS battery backup is available and the operators prevent ECCS actuation 8 hours after reactor trip, the EDAS continues to provide power to the MPS and to hold the ECCS valves closed for 24 hours, after that point the ECCS valves are actuated by the MPS. Upon loss of EDAS, ECCS actuates. The RVVs open immediately and the RRVs open when RCS pressure drops to below the IAB release pressure.

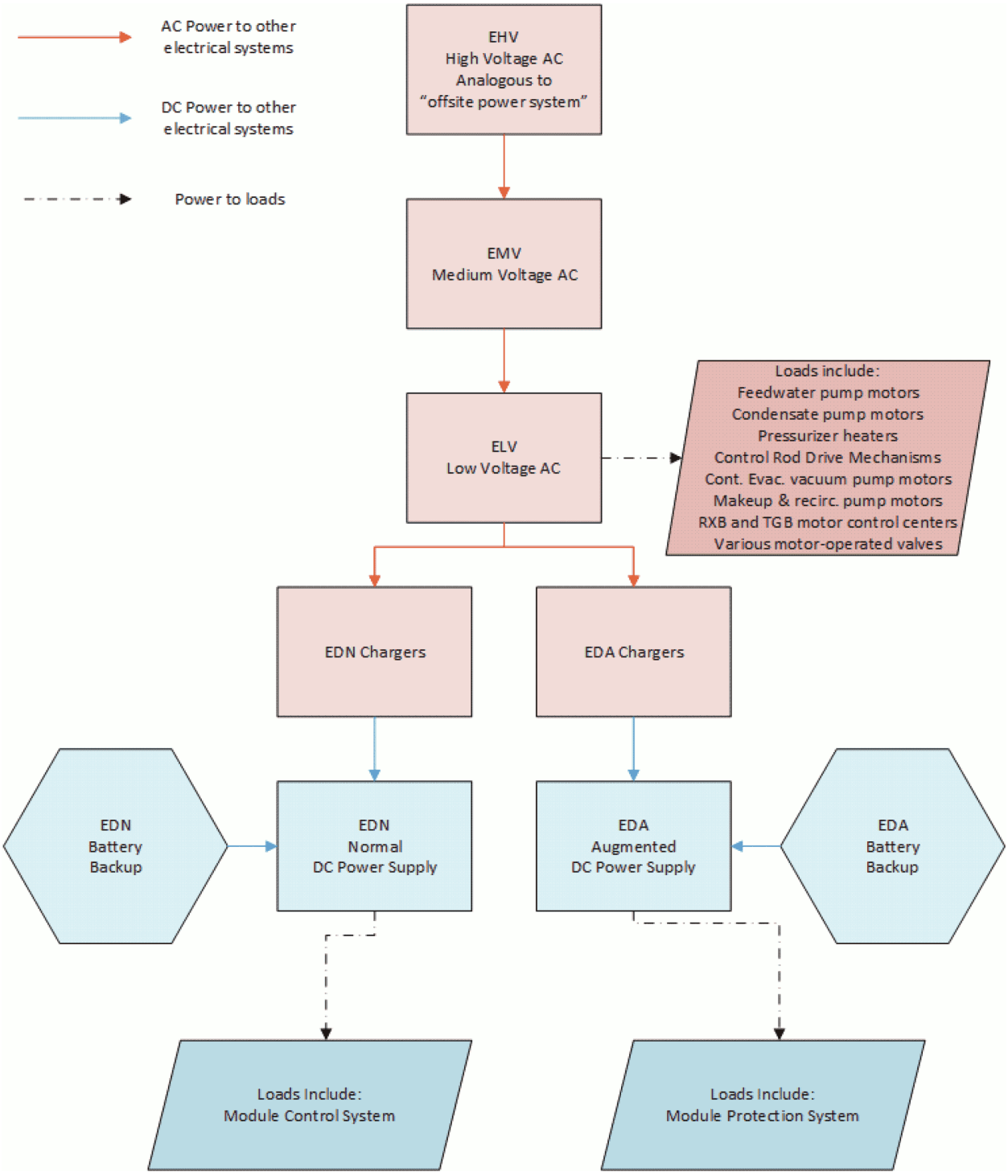
Based on this review of the electrical system design, for FSAR Chapter 15 safety analyses, ‘loss of normal AC power’ means loss of the ELVS, either due to failures within the ELVS or due to loss of power provided through EMVS and EHVS. Failures of EMVS or EHVS are not separately considered.

Since EDNS and EDAS are not safety-related systems, and have battery backup, the availability or unavailability of these DC power supply systems is also be considered.

The timing for considering the loss of power supply is discussed in Section C.3.

© Copyright 2023 by NuScale Power, LLC

Figure C-1 Simplified Schematic of Electrical Systems and Loads Important to Safety Analysis



© Copyright 2023 by NuScale Power, LLC

C.3 Loss of Power Timing and NuScale Event Progression

C.3.1 Timing for Assumption of Loss of Power

SRP Section 15 and associated sub-sections and DSRS Section 15 and associated sub-sections are not prescriptive regarding when to consider a loss of power. For example, DSRS Section 15.1.5 states:

> *A loss of offsite power may occur simultaneously with the pipe break or during the accident, or offsite power may not be lost.*

For non-LOCA transients, loss of normal AC power is considered at two different points in the event progression:

- Coincident with the event.
- Coincident with turbine trip.

The basis for considering loss of power coincident with the event is that an external event could cause the initiating event as well as cause a loss of normal AC power. For example, a seismic event that might cause a pipe rupture could result in loss of normal AC power supply to the plant.

During an event progression, nonsafety-related controls are expected to trip the turbine following reactor trip. The basis for considering loss of normal AC power coincident with turbine trip during the event progression is that typically, large nuclear plants consider loss of offsite AC power a consequence of the event due to a disruption of the electrical grid following a turbine trip and loss of the ~1000 MWe power supply from the nuclear plant. The NuScale design is much smaller and loss of power from a single NPM is not expected to significantly disrupt the grid power supply, however this event progression is assessed as part of the safety analyses. Delays between reactor trip and turbine trip are conservatively treated in the safety analysis.

Considering loss of power coincident with the event and coincident with turbine trip is consistent with other advanced reactor designs and SRP Section 8.3.1. Specifically, Technical Rationale 4 of SRP Section 8.3.1 states:

> The trip of a nuclear power unit … can result in reduced switchyard voltage, potentially actuating the plant's degraded voltage protection and separating the plant's safety buses from offsite power. It can also result in grid instability, potential grid collapse, inadequate switchyard voltages, and a subsequent [loss of offsite power] due to loss of the real and/or reactive power support supplied to the grid from the nuclear unit.

With respect to EDNS and EDAS availability, these nonsafety-related systems could be deterministically postulated to randomly fail during the event. However, it is not typical or generally required to consider the random loss of a non-safety system part-way through an event. In particular, the redundancy and augmented

© Copyright 2023 by NuScale Power, LLC

requirements of the EDAS, supports not assuming a loss of EDAS after event initiation, if it is initially available.

Facts supporting this conclusion are discussed below:

The EDAS battery backup has an independent connection to the DC bus that provides power to MPS, therefore, a loss of AC power does not have a direct causal link to failure of the DC bus supported by the EDAS batteries. Failure of the battery charger due to an electrical fault is electrically separated from the DC bus. Although the EDAS is not safety-related, many of the augmented requirements of a safety-related system are part of the design.

The Failure Modes and Effects Analysis (FMEA) for the EDAS shows that there are no single failures that could cause loss of power supply from EDAS. Consequently, loss of a single module-specific power channel does not result in loss of power supply, reactor trip, inadvertent ECCS actuation, or loss of post-accident monitoring capacity. Failures to multiple module-specific power channels must occur to initiate reactor trip or ECCS actuation.

The EDAS is designed with independent and diverse monitoring devices such that no single monitoring device failure goes undetected and prevent detection of the failure mechanisms evaluated in the FMEA. The EDAS batteries are designed to Seismic Category I requirements.

The EDAS FMEA conclusions are further summarized below:

Transition from normal EDAS and/or BPSS AC power supply available (Condition A) to loss of all AC (Condition B)

There is no adverse causal relationship during the transition from EDAS operation with AC power available (condition A) and AC power unavailable (condition B). There are no failure modes while EDAS is operating in condition A that causes EDAS operating in condition B to be unable to meet the required functions and duty cycle.

DC System Monitoring

The use of DC system condition monitoring equipment (battery, charger/ switchgear) combined with periodic testing provides assurance that undetectable VRLA cell failures and associated EDAS subsystem failure does not occur. Proper consideration of monitoring system and test data allows for proactive corrective maintenance prior to an unacceptable VRLA battery cell condition.

All Equipment Available

When considering all EDAS equipment available, the functional EDAS is not susceptible to subsystem failure consequences, following the failure of any single component.

© Copyright 2023 by NuScale Power, LLC

Fire Considerations

Fire is considered for EDAS due to the arrangement of the power channel components in the reactor building and the consequences on interfacing systems. The following circumstances could cause an EDAS subsystem to fail:

1. With AC power available: fire in a switchgear room causes reactor trip and ECCS actuation.
2. With AC power unavailable: fire in a battery string or switchgear room causes ECCS actuation.

In both instances, EDAS power is maintained by the other power channel components and no safety functions are impacted.

Digital Common Cause Failure

1. With AC power available: digital common cause failures of the battery chargers during normal plant operation do not prevent the batteries from fulfilling the EDAS mission. Should a digital control issue result in the battery chargers supplying abnormal or erratic voltage, the DC-DC converters function to ensure safety systems are either powered within a specific input voltage span or isolated to preclude degradation of the safety system(s).
2. With AC power unavailable: all battery chargers are not working. Therefore, digital common-cause failures need not be considered.
3. With AC power available or unavailable: common cause failures of equipment and monitoring during normal plant operation or following a loss of AC power does not affect the ability of EDAS to fulfill its mission. Because the battery monitoring devices only provide indication, the batteries supplying backup power are not susceptible to this failure mechanism.

The EDNS serves different functions than EDAS and accordingly does not require augmented design requirements. Non-mechanistic failure of the EDNS power supply is postulated, but has limited effects on transient event progression as summarized in Section C.3.2.

Considering the regulatory guidance and EDAS design features, the following scenarios are considered:

- EDNS and/or EDAS power is available.
- EDNS and/or EDAS power is lost coincident with the event either due to the conditions that result in loss of normal AC coincident with the event or as a non-mechanistic assumption.
- EDNS power is lost coincident with the turbine trip when the EDNS battery backup to the buses fail to provide power after normal AC power is lost.

© Copyright 2023 by NuScale Power, LLC

C.3.2 Loss of Power Scenarios for Chapter 15 Design Basis Event Analysis and Transient Progression

Based on the NuScale electrical power system design and the timing of when AC or DC power is assumed to be available or lost, the loss of power scenarios for FSAR Chapter 15 design basis event analysis are defined. First, for completeness, the scenarios are identified in a parametric manner:

1. AC power is available
    a. EDNS available, EDAS available
    b. EDNS fails (at event initiation), EDAS available
    c. EDNS available, EDAS fails (at event initiation)
    d. EDNS fails (at event initiation), EDAS fails (at event initiation)
2. AC power is lost coincident with the event
    a. EDNS available, EDAS available
    b. EDNS fails (at event initiation), EDAS available
    c. EDNS available, EDAS fails (at event initiation)
    d. EDNS fails (at event initiation), EDAS fails (at event initiation)
3. AC power is lost at turbine trip
    a. EDNS available, EDAS available
    b. EDNS fails (at turbine trip), EDAS available

The plant response in each of these loss of power scenarios is described in Table C-3. As shown in Table C-3, the plant response to several of the loss of power scenarios is equivalent.

Some of the power scenarios need to be considered individually for each initiating event. However, other power scenarios are considered generically to demonstrate why they are non-limiting or are not considered specific initiating events. Two scenarios are considered generically in the following subsections:

- Loss of EDAS but AC power and EDNS batteries available.
- Loss of all AC and DC power at event initiation.

© Copyright 2023 by NuScale Power, LLC

Table C-3 NuScale Plant Response in Various Power Scenarios

Scenario	AC Power	EDNS	EDAS	Description of Plant Response	Equivalent Scenario
1a	Available	Available	Available	All power sources available	n/a
1b	Available	Not available through transient	Available	Loss of EDNS causes MCS to lose power. Therefore: • Turbine trip at event initiation due to loss of control power. • Feedwater pumps stop at event initiation due to loss of control power. • CVCS pumps stop at event initiation due to loss of control power. • Pressurizer heaters turn off at event initiation due to loss of control power.	n/a
1c	Available	Available	Not available through transient	Loss of EDAS removes power from the MPS. Therefore, power to the reactor trip breakers is removed and all safety-related valves are actuated to go to their respective safety positions on loss of power to the valve actuators: • Reactor trip at event initiation due to loss of EDAS. • DHRS actuation valves open due to loss of EDAS. • Containment isolation valves and secondary side backup isolation valves close due to loss of EDAS. • ECCS valves are actuated; both RVVs open immediately, the inadvertent actuation block holds the RRVs closed until the RCS pressure decreases below the IAB release pressure. • Feedwater and CVCS pumps have power but the isolation valves close and block the flow path.	discussion in Section C.3.3.
1d	Available	Not available through transient	Not available through transient	Loss of EDNS causes the MCS to lose power. Loss of EDAS removes power from the MPS. The plant response is equivalent to scenario 2d (loss of AC, EDNS and EDAS at event initiation) because although AC power is available, the loss of control signal stops the feedwater pumps and CVCS pumps, and power to the pressurizer heaters is removed.	2d

© Copyright 2023 by NuScale Power, LLC

Table C-3 NuScale Plant Response in Various Power Scenarios (Continued)

Scenario	AC Power	EDNS	EDAS	Description of Plant Response	Equivalent Scenario
2a	Lost at event initiation	Available	Available	AC power is lost at the event initiation. Therefore: • Control rods begin to fall after loss of power to the CRDMs (before MPS actuation). • The MPS actuates DHRS and containment isolation after 60seconds due to low AC voltage to the EDAS battery chargers, if another signal is not generated. • Turbine trip at event initiation due to loss of AC power. • The feedwater pumps and CVCS pumps stop at event initiation due to loss of AC power to the pump motors. • Pressurizer heaters turn off at event initiation because power to the heaters is lost. The EDNS and EDAS battery backups are available (40 min for EDNS and 24/72 hours for EDAS). At 40 min, the battery backup to EDNS is depleted, which removes power from the MCS. Since the plant already tripped, there are no additional changes to the plant status or equipment. 8 hours after reactor trip: If the operators do not bypass the ECCS actuation signal, ECCS actuates. All ECCS valves are expected to open if RCS pressure is below the IAB threshold; otherwise the RVVs open immediately and the RRVs open at the IAB release pressure. If the operators bypassed ECCS actuation at 8 hours, then at 24 hours, the MPS reduces the load on the EDAS batteries by removing power to the ECCS valves. The RCS is depressurized by the DHRS by this time and all ECCS valves are expected to open. If RCS pressure remains above the IAB threshold, the RVVs still open due to removal of EDAS power. This transition occurs well beyond the short-term transient progression and is addressed in long term cooing analysis.	n/a
2b	Lost at event initiation	Lost at event initiation	Available	AC power is lost at event initiation and the EDNS battery backups do not pick up. The plant response is equivalent to scenario 2a because the effects of the loss of the EDNS batteries (removes power to the MCS) are already caused by the loss of AC power.	2a

© Copyright 2023 by NuScale Power, LLC

Table C-3 NuScale Plant Response in Various Power Scenarios (Continued)

Scenario	AC Power	EDNS	EDAS	Description of Plant Response	Equivalent Scenario
2c	Lost at event initiation	Available	Lost at event initiation	AC power is lost at event initiation and the EDAS battery backups do not pickup. The plant response is equivalent to scenario 2d (loss of AC, EDNS and EDAS at event initiation). The loss of AC power and EDAS causes reactor trip, DHRS actuation, containment isolation, ECCS valve actuation (RVVs open immediately, RRVs open at IAB release pressure), turbine trip, loss of power to the feedwater pumps, loss of power to the CVCS pumps, loss of power to the pressurizer heaters. The availability of the EDNS battery backup to the MCS does not affect the plant response.	2d
2d	Lost at event initiation	Lost at event initiation	Lost at event initiation	AC power is lost at event initiation. The EDNS and EDAS batteries fail to provide power. All AC and DC power is lost. Therefore: • Reactor trip at event initiation due to loss of AC power or EDAS. • DHRS actuation at event initiation due to loss of EDAS. • Containment isolation valves and secondary side backup isolation valves close at event initiation due to loss of EDAS. • Turbine trip at event initiation due to loss of AC power. • The feedwater pumps and CVCS pumps stop due to loss of AC power to the pump motors. • Pressurizer heaters turn off because power to the heaters is lost. • The ECCS valves are actuated due to loss of power from the EDAS to the valve actuators. The RVVs open immediately and the RRVs open when RCS pressure drops below the IAB release pressure.	n/a

© Copyright 2023 by NuScale Power, LLC

Table C-3 NuScale Plant Response in Various Power Scenarios (Continued)

Scenario	AC Power	EDNS	EDAS	Description of Plant Response	Equivalent Scenario
3a	Lost at turbine trip	Available	Available	The initiating event progresses until the MPS actuates reactor trip to protect the module. Turbine trip is initiated due to reactor trip. Due to grid disruption from the turbine trip, AC power is lost. EDNS and EDAS batteries are available. The loss of AC power at the turbine trip results in: • The MPS actuates DHRS and containment isolation at the turbine trip after 60 seconds due to loss of AC power to the EDAS battery chargers (if not already actuated by the MPS; reactor trip is already initiated by the MPS due to module conditions). • The feedwater pumps and CVCS pumps stop due to loss of AC power to the pump motors. • Pressurizer heaters turn off because power to the heaters is lost. The EDNS and EDAS battery backups are available (40 min for EDNS and 24/72 hours for EDAS). At 40 min, the battery backup to EDNS is depleted, which removes power from the MCS. Since the plant already tripped, there are no additional changes to the plant status or equipment. 8 hours after reactor trip: If the operators do not bypass the ECCS actuation signal, ECCS actuates. All ECCS valves are expected to open if RCS pressure is below the IAB threshold; otherwise the RVVs open immediately and the RRVs open at the IAB release pressure. If the operators bypassed ECCS actuation at 8 hours, then at 24 hours, the MPS reduces the load on the EDAS batteries by removing power to the ECCS valves. The RCS is depressurized by the DHRS by this time and all ECCS valves are expected to open. If RCS pressure remains above the IAB threshold, the RVVs still opens due to removal of EDAS power. This transition occurs well beyond the short-term transient progression and is addressed in long term cooling analysis.	n/a

© Copyright 2023 by NuScale Power, LLC

Table C-3 NuScale Plant Response in Various Power Scenarios (Continued)

Scenario	AC Power	EDNS	EDAS	Description of Plant Response	Equivalent Scenario
3b	Lost at turbine trip	Lost at turbine trip	Available	The initiating event progresses until the MPS actuates reactor trip to protect the module. Turbine trip is initiated due to reactor trip. Due to grid disruption from the turbine trip, AC power is lost. EDNS batteries fail to provide power. EDAS batteries are available. The plant response is equivalent to scenario 3a because the effects of the loss of the EDNS batteries (removes power to the MCS) are already caused by the loss of AC power.	3a

© Copyright 2023 by NuScale Power, LLC

C.3.3 Generic Evaluation of Loss of EDAS

The EDAS is an non-safety related system with augmented requirements. Typically in safety analysis, non-safety systems are assumed to function or to not function in order to determine if the condition is conservative with respect to the transient results (CVCS function for pressurizer heaters or spray, for example). Loss of a non-safety system or malfunction in a non-safety system can also be an event initiator (for example, malfunctions in the condensate and feedwater system, which result in a loss of feedwater). First, the basis for not considering loss of EDAS as a unique initiating event is discussed.

Loss of EDAS is not considered as a unique event initiator because a complete loss of EDAS is unlikely due to the level of redundancy in the design and the augmented requirements imposed; and, because loss of EDAS is considered in conjunction with each of the other design-basis events. Although the effects of a loss of EDAS are considered as part of the power availability scenarios, the plant response is not evaluated with non-LOCA methodology. Instead, the loss of EDAS is evaluated with the inadvertent opening of reactor valve(s) methodology.

The EDAS provides power to the MPS. If the EDAS is lost, but normal AC power is available (Table C-3, Scenario 1c), the following response is expected:

- Reactor trips at event initiation due to loss of EDAS;
- DHRS actuates due to loss of EDAS, to open DHRS actuation valves and close feedwater and main steam isolation valves, feedwater regulating valves, and secondary main steam isolation valves;
- Containment isolation valves actuate (to close) due to loss of EDAS; and,
- ECCS valves actuate - RVVs open immediately.
    - The inadvertent actuation block delays opening of the RRVs until the RCS pressure decreases below the IAB release pressure.

Although a loss of EDAS coincident with the event actuates the safety systems, the overall plant response and transient analysis acceptance criteria for non-LOCA transients are expected to be bounded by other events evaluated using the inadvertent opening of reactor valve(s) methodology.

Variations in the system response for effects of scram time, valve closure times, etc. are bounded by other events. For example, if loss of EDAS is postulated as an initiating event as part of DHRS actuation, the feedwater and main steam valves close while the feedwater pumps are assumed to continue running. If the main steam isolation valves close quickly while the main feedwater isolation valves close slowly or experience a single failure; this could result in higher pressure in the steam generator secondary side. However, this scenario is bounded by considering the same combination of valve closure times and single failure in the loss of load event.

© Copyright 2023 by NuScale Power, LLC

Considering the redundancy and augmented requirements imposed on the EDAS, loss of the EDAS independent of any other type of initiating event is not expected to occur in the life of the module (demonstrated quantitatively in Section 5.0). Since loss of the EDAS actuates the safety systems, loss of EDAS as an event initiator does not introduce a different or more limiting plant transient progression relative to other scenarios that are analyzed. Therefore, as a nonsafety-related system, the EDAS available/not available is considered as part of the power availability scenarios for all design basis events. Loss of EDAS is not treated as a unique initiating event.

Although the loss of EDAS is bounded by other events, the power availability Scenario 1c is generically evaluated to assist with understanding the expected response.

In Table C-3, Scenario 1c postulates loss of EDAS while AC power and EDNS are available.

The main analysis acceptance criteria of concern are maximum RCS pressure, maximum secondary side pressure, minimum critical heat flux ratio, maximum fuel centerline temperature, and maximum containment pressure. Each of these acceptance criteria are considered below. Loss of EDAS causes both RVVs to open immediately and RRVs to open when RCS pressure drops below the IAB release pressure.

- RCS pressure: Actuation of reactor trip coincident with the event reduces core power to decay heat levels, and DHRS is actuated coincident with the event to provide cooling. Therefore the RCS pressure response is non-limiting compared to scenarios where the safety system response is delayed until MPS analytical limits are reached, or compared to normal operating conditions. Different event types are considered below.
  - Heatup events - RCS pressure expected to increase, so earlier MPS actuation is a benefit.
  - Cooldown events - RCS pressure tends to decrease; this acceptance criterion is not challenged.
  - Reactivity events - Events driven by rod movement are mitigated by immediate reactor trip and containment isolation, except control rod ejection. Control rod ejection response is mitigated by the fuel design, followed by reactor trip. Opening the RVVs limits the pressure increase. Boron dilution is mitigated by immediate reactor trip and demineralized water system isolation.
  - Increase inventory event - Halted by containment isolation valve closures, so non-limiting.

© Copyright 2023 by NuScale Power, LLC

- Secondary side pressure: The secondary side inventory and the primary side conditions at the time of DHRS actuation affect the peak secondary side pressure. Higher secondary side inventory and lower loop volume are expected to result in increased peak pressure. Therefore, actuation of reactor trip and DHRS coincident with the event is bounded by considering the range of conditions that increase secondary side inventory prior to DHRS actuation or containment isolation, and by considering the effects of single failures of the main steam isolation valve and feedwater isolation valve on the secondary loop volume. Different event types are considered below:
  - Heatup events - The turbine trip event or the main steam isolation valve closure stops steam flow out of the steam generator; as the feedwater pumps continue to operate, the secondary side inventory increases until a DHRS actuation signal is generated. This event bounds considering a DHRS actuation signal generated coincident with the event, and other heatup events where feedwater flow is not available.
  - Cooldown events - Some cooldown events, such as increase in feedwater flow, increase the steam generator inventory until a DHRS actuation signal is generated. This event bounds considering a DHRS actuation signal generated coincident with the event.
  - Reactivity events - Events driven by rod movement are mitigated by an immediate reactor trip and containment isolation, except for control rod ejection. Control rod ejection response is mitigated by the fuel design, followed by reactor trip. Boron dilution is mitigated by immediate reactor trip and demineralized water system isolation. Secondary side pressure is not expected to be challenged for these events, compared to heatup or cooldown events.
  - Increased inventory event - Mitigated by containment isolation and therefore containment isolation coincident with the event is non-limiting.
- Minimum critical heat flux ratio and maximum fuel centerline temperature: The immediate reactor trip coincident with the event reduces core power and heat fluxes. Actuation of reactor trip coincident with the event generally increases the margin compared to scenarios where the safety system response is delayed until MPS analytical limits are reached. For rod ejection, loss of EDAS causes an immediate scram that reduces the total reactivity inserted and the resulting peak power, which increases margin regardless of the RCS pressure response.
- Maximum containment pressure: For the non-LOCA events that do not have initial mass and energy release into the containment, opening the ECCS valves later in the event progression (on the 8 hour or 24 hour timer) is bounded by the inadvertent opening of a valve in conjunction with the immediate opening of both RVVs from full power conditions (inadvertent ECCS actuation is analyzed as an AOO). For secondary side high energy line breaks inside containment, the secondary side mass and energy release followed by ECCS valve opening with an assumed loss of EDAS could challenge containment pressure. These scenarios and the impacts of single failures are considered in the bounding containment pressure analysis for FSAR Chapter 6.

© Copyright 2023 by NuScale Power, LLC

With respect to radiological dose consequences for infrequent events and accidents, loss of EDAS results in immediate containment isolation, and ECCS RVV valve opening. Similar to an inadvertent ECCS actuation, containment isolation reduces the potential release paths to containment leakage. Fuel failures are not expected to occur for the main steam line break, main feedwater line break, small line break outside containment, or the steam generator tube failure events. For these events, loss of EDAS and opening of the ECCS RVVs results in a higher containment pressure response compared to the event-specific scenario evaluations for loss of AC power at event initiation (where the ECCS valves remain closed until 8 hours after reactor trip or 24 hours after event initiation). In the radiological dose analyses, the containment leak rate is determined assuming that the containment leaks at the design basis leak rate for 24 hours and at half the design basis leak rate thereafter. Since the design basis leak rate is not a function of the peak pressure, this scenario is non-limiting with respect to releases prior to containment isolation and does not need to be specifically considered for these events to provide separate containment pressure input for the radiological dose analyses.

Fuel failure in the control rod ejection accident is determined by the physics of the design, such as the core design peaking and control rod worth. Similar to the other infrequent events and accidents, the radiological dose analysis bounds the plant response using conservative assumptions for transport of radionuclides into containment and containment leak rate. The power scenario 1c is not specifically considered for the control rod ejection accident to provide input for the radiological dose analyses. Since a loss of EDAS would open the RVVs concurrent with ejecting the rod, this event scenario is evaluated to demonstrate that fuel failure for the rod ejection accident is comparable to the inadvertent ECCS actuation.

As discussed above, scenario 1c (loss of EDAS) does not produce limiting consequences for maximum RCS pressure, maximum secondary side pressure, minimum critical heat flux rate, maximum fuel centerline temperature, or radiological dose criteria. Further consideration of loss of EDAS is not required for these acceptance criteria. The bounding containment pressure analysis for FSAR Chapter 6 considers the response to a secondary side break followed by ECCS valve opening due to loss of EDAS.

Loss of EDAS is not considered a separate, unique initiating event because of the redundancy and augmented requirements imposed on the design. Therefore, for the design basis events, if AC power is available, EDAS is assumed to be available.

© Copyright 2023 by NuScale Power, LLC

C.3.4 Generic Evaluation of Loss of all Power at Event Initiation

In Table C-3, power scenario 2d is loss of AC power, loss of EDNS batteries, and loss of EDAS batteries at event initiation. All AC and DC power is lost. Therefore, the following plant response is expected:

- Reactor trip at event initiation due to loss of power;
- DHRS actuation due to loss of power, to open DHRS valves and close main feedwater and main steam isolation valves and backup isolation valves;
- Containment isolation valves actuate (to close) due to loss of power;
- Turbine trip at event initiation due to loss of power;
- Feedwater pumps and CVCS pumps stop due to loss of AC power to the pump motors;
- Pressurizer heaters turn off due to loss of power; and,
- ECCS valves actuate due to loss of EDAS - RVVs open immediately.
    - The inadvertent actuation block delays opening of the RRVs until the RCS pressure decreases to below the IAB release pressure.

The plant response to this loss of power scenario is the same as that in scenario 2a (loss of AC power) except that the ECCS valves actuate and the turbine trips at event initiation. Although the ECCS design changes produce a significantly different system response, the turbine trip has little impact on the margin for secondary pressure because the isolation valves close on loss of EDAS. With respect to ECCS actuation, the RVVs open immediately while the RRVs are closed until RCS pressure decreases to below the IAB release pressure. The availability of AC power does not change the timing for safety system actuation, ECCS operation, or margin for secondary pressure, so the system response is the same as scenario 1c (loss of EDAS at time zero). Therefore, the discussion in Section C.3.3 is applicable.

© Copyright 2023 by NuScale Power, LLC

C.4 Summary of Loss of Power Cases for FSAR Chapter 15 Design Basis Events

Based on Table C-3 and the generic evaluations in Section C.3.3 and Section C.3.4, the following loss of power scenarios are considered for the FSAR Chapter 15 design basis events.

Scenarios considered on an event-specific basis:

1. AC power, EDNS and EDAS available - in this scenario all normal power sources are available.
   a. Table C-3 Scenario 1a
2. AC power and EDAS available, EDNS not available during the transient.
   a. Table C-3 Scenario 1b
3. Loss of AC power at event initiation, EDAS available; EDNS available
   a. Table C-3 Scenario 2a
4. Loss of AC power at turbine trip, EDAS available; EDNS available
   a. Table C-3 Scenario 3a

© Copyright 2023 by NuScale Power, LLC