NuScale Power™

LO-0617-54688

June 29, 2017

Docket No. 52-048

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

SUBJECT: NuScale Power, LLC Submittal of Changes to "NuScale Instrument Setpoint Methodology Technical Report" TR-0616-49121 and Final Safety Analysis Report Tier 1 Section 2.5 and Tier 2 Chapter 1 and Chapter 7

REFERENCE:

1. Memorandum from Omid Tabatabai to Samuel Lee, "Summary of April 18 and 20, 2017, Public Meetings with NuScale Power, LLC, to discuss the U.S. Nuclear Regulatory Commission Staff's questions related to chapter 7, 'Instrumentation and Controls,' of the NuScale Design Certification Application (Docket No. 52-048)," dated May 12, 2017 (ML17130A991)

2. Memorandum from Omid Tabatabai to Samuel Lee, "Summary of May 17-18, 2017 Public Meetings with NuScale Power, LLC, to discuss various topics related to Chapter 7, 'Instrumentation and Controls,' of the NuScale Design Certification Application (Docket No. 52-048)," dated June 15, 2017 (ML17159A750)

3. Letter from NuScale Power, LLC to Nuclear Regulatory Commission, "NuScale Power, LLC Submittal of the NuScale Standard Plant Design Certification Application," dated December 31, 2016 (ML17013A229)

During the dates of April 18 and 20, 2017 and May 17-18, 2017, representatives of the U.S. Nuclear Regulatory Commission (NRC) and NuScale Power, LLC (NuScale) held public and closed meetings to discuss NRC Staff questions on Chapter 7 related topics and NuScale responses. As a result of these discussions, NuScale revised Tier 1 Section 2.5 and Tier 2 Chapter 1 and Chapter 7 of the Final Safety Analysis Report (FSAR) and the "NuScale Instrument Setpoint Methodology Technical Report," TR-0616-49121.

Enclosure 1 is proprietary version of the "NuScale Instrument Setpoint Methodology Technical Report," TR-0616-49121-P draft Revision 1. NuScale requests that the proprietary version be withheld from public disclosure in accordance with the requirements of 10 CFR § 2.390. The enclosed affidavit (Enclosure 3) supports this request. Enclosure 2 is the nonproprietary version of the "NuScale Instrument Setpoint Methodology Technical Report," TR-0616-49121-NP draft Revision 1. Enclosure 4 is the mark-up of the FSAR pages incorporating revisions to FSAR Tier 1 Section 2.5 and Tier 2 Chapter 1 and Chapter 7, in redline/strikeout format. NuScale will include these changes as part of a future revision to the NuScale Design Certification Application. Enclosure 5 to this letter contains a modified list of the "Summary of NRC Staff Questions and NuScale Responses", taken from Reference 1 and Reference 2, which provides references to pertinent portions of the markups of Enclosures 1, 2, and 4 that address NRC Staff questions.

Note that the page numbers in the excerpts of draft revisions to NuScale documents shown in Enclosures 1, 2, and 4 may not necessarily be representative of the page numbers of the final submittal of these revised documents. Section numbers may be used to identify the location of content within the draft and final revisions of the documents.

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

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

Sincerely,

Zackary W. Rad
Director, Regulatory Affairs
NuScale Power, LLC

Distribution: Samuel Lee, NRC, TWFN-6C20
Gregory Cranston, NRC, TWFN-6E55
Omid Tabatabai, NRC, NRO

Enclosure 1: Changes to "NuScale Instrument Setpoint Methodology Technical Report," TR-0616-49121-P
Enclosure 2: Changes to "NuScale Instrument Setpoint Methodology Technical Report," TR-0616-49121-NP
Enclosure 3: Affidavit of Zackary W. Rad, AF-0617-54702
Enclosure 4: Changes to Final Safety Analysis Report Tier 1 Section 2.5 and Tier 2 Chapter 1 and Chapter 7
Enclosure 5: Summary of NRC Staff Questions and NuScale Responses with references to applicable changes

Enclosure 1:

Changes to “NuScale Instrument Setpoint Methodology Technical Report,” TR-0616-49121-P

NuScale Power, LLC
1100 NE Circle Blvd., Suite 200 Corvallis, Oregon 97330 Office 541.360-0500 Fax 541.207.3928
www.nuscalepower.com

Enclosure 2:

Changes to “NuScale Instrument Setpoint Methodology Technical Report,” TR-0616-49121-NP

NuScale Instrument Setpoint Methodology

Technical Report

December 2016

Draft Revision ~~0~~1

Docket: ~~PROJ0769~~52-048

NuScale Power, LLC

1100 NE Circle Blvd., Suite 200

Corvallis, Oregon 97330

www.nuscalepower.com

Executive Summary

This technical report describes the instrument setpoint determination methodology applied to the safety-related instrumentation and control (I&C) functions. The methodology described in this report has been established to ensure that the Reactor Trip System (RTS) and Engineered Safety Features Actuation System (ESFAS) setpoints are consistent with the assumptions made in the safety analysis and conform to the setpoint-related requirements of industry standard, ANSI/ISA-S67.04-2006, U.S. Nuclear Regulatory Commission (NRC) Regulatory Guide (RG) 1.105 Revision 3, and addresses the regulatory issues identified in Regulatory Issue Summary (RIS) 2006-17.

Setpoints for the RTS and ESFAS must be selected to provide sufficient allowance between the trip setpoint and the safety limit to account for instrument channel uncertainties. The methodology for establishing safety-related trip setpoints and their associated uncertainties ensures that the analytical limit applied to safety-related MPS protective actions is satisfied in accordance with the plant~~Chapter 15~~ safety analysis. The instrument setpoint methodology is used to establish module protection system (MPS) setpoints for the safety-related instrumentation. The instrument setpoint methodology determines calibration uncertainty allowances, including as-found and as-left tolerances, used in plant surveillance tests to verify that setpoints for safety-related protective functions are within Technical Specification limits. The methodology also establishes performance and test acceptance criteria to evaluate setpoints during surveillance testing and calibration for setpoint drift.

The sources of error and uncertainty associated with instrumentation channels (i.e., process measurement and miscellaneous effects errors, sensor errors, and digital system processing errors) are described in Section 3.0.

The relationships between trip setpoints, analytical limits, and the plant safety limits that are used to properly account for the total instrument channel uncertainty in the establishment of the setpoints are described in Section 4.0.

The assumptions applicable to the NuScale Instrument Setpoint Methodology are described in Section 5.0.

Sample uncertainty and setpoint calculations based on the methodology described in this document are provided in Section 6.0, to demonstrate the application of the methodologies presented in this document and are not to be used in plant calibration procedures or for development of Technical Specifications. The detailed setpoint calculation processes for the module protection system are described in this report and may change according to the plant-specific data. This methodology does not included provisions for using a graded approach for less important instrumentation.

The analytical limits, uncertainties, and setpoints for each RTS and ESFAS function are summarized in Section 7.0.

1.0 Introduction

1.1 Purpose

This document describes the methodology for determining setpoints for the safety-related instrumentation and control (I&C) functions. Setpoints for the Reactor Trip System (RTS) and Engineered Safety Features Actuation System (ESFAS) must be selected to provide sufficient allowance between the trip setpoint and the safety limit to account for instrument channel uncertainties. The methodology for determining NuScale safety-related instrument channel uncertainties described in this document is based on U.S. Nuclear Regulatory Commission (NRC) Regulatory Guide (RG) 1.105, Revision 3 (Reference 9.4). RG 1.105 endorses conformance with ANSI/ISA–S67.04, Part I–1994 (with certain exceptions and clarifications) as an acceptable method for satisfying the NRC's regulations for ensuring that setpoint for safety-related instrumentation are established and maintained within the Technical Specification limits. To address updated industry guidance and account for the regulatory issues raised in Regulatory Issue Summary (RIS) 2006-17 (Reference 9.6), the NuScale Instrument Setpoint Methodology is based on the updated International Society of Automation (ISA) standard ISA-67.04.01-2006 (Reference 9.11), and ISA-RP67.04.02-2000 (Reference 9.12). These standards provide updated guidance which is equivalent to the regulatory guidance contained in RG 1.105.

The NRC released Draft RG (DG) 1141 in June 2014, as a proposed Revision 4 to RG 1.105 (Reference 9.5). DG 1141 endorses Reference 9.11 and includes criteria, guidance, and concepts that have not been addressed in previous revisions of RG 1.105. The NuScale Instrument Setpoint Methodology addresses established regulatory guidance and the additional concepts proposed by NRC in the DG 1141.

Channel uncertainty calculations include instrument setpoint drift allowances. Periodic surveillance testing is required by the Technical Specifications in accordance with 10 CFR 50.36 to measure setpoint drift. This document describes the methodology for determining calibration uncertainty allowances, including as-found and as-left tolerances, used in plant surveillance tests to verify that setpoints for safety-related protective functions are within Technical Specification limits. The methodology for establishing performance and test acceptance criteria to evaluate setpoints during surveillance testing and calibration for setpoint drift is also described in this document.

1.2 Scope

The NuScale Instrument Setpoint Methodology is used to establish module protection system (MPS) setpoints for the safety-related instrumentation. The scope of this report documents the methodology for establishing safety-related trip setpoints and their associated uncertainties to ensure the analytical limit applied to safety-related MPS protective actions is satisfied in accordance with the plant safety analysis. This methodology is only applicable to instrumentation that supports the reactor trip and engineered safeguards actuation systems; this methodology does not apply to other nonsafety-related or important to safety instrumentation loops. Sample uncertainty and setpoint calculations based on the methodology described in this document are provided

2.0 Background

I&C safety systems control plant parameters to assure that safety limits will not be exceeded under the most severe design basis accident. Instrument setpoints and acceptable as-left and acceptable as-found bands for these I&C safety system functions are chosen so that potentially unsafe or damaging process excursions (transients) can be avoided and/or terminated before plant conditions exceed safety limits. Accident analyses establish the limits for credited protective actions. These analytical limits, as established by accident analyses, do not normally include considerations for the accuracy (uncertainty) of installed instrumentation. Additional analyses and procedures are necessary to assure that the limiting trip setpoint of each safety control function is appropriate.

Instrument channel uncertainties in these analyses are based on the characteristics of installed instrumentation, the environmental conditions present at the instrumentation's installed locations, and process conditions. A properly established setpoint initiates a plant protective action before the process parameter exceeds its analytical limit. This, in turn, assures that the transient will be avoided and/or terminated before the process parameters exceed the established safety limits.

Early versions of RTS and ESFAS Technical Specifications for existing plants contained only trip setpoint requirements with no allowance for setpoint drift. The setpoint values were specified as limits with inequality signs to indicate the direction of allowable drift. In order to maximize operating margin, instrument channels were sometimes calibrated without sufficient allowance for setpoint drift. This led to numerous abnormal occurrence reports, or Licensing Event Reports, as required by 10 CFR 50.36 when Technical Specification limits are exceeded.

The ISA sponsored a review of the setpoint drift problem in April 1975. Revision 1 to RG 1.105 was published in November 1976 in response to the large number of reported instances in which instrument setpoints in safety-related systems drifted outside the limits specified in the Technical Specifications. Using the method described in Revision 1 to RG 1.105 and additional criteria on establishing and maintaining setpoints, Subcommittee SP67.04, Setpoints for Safety-Related Instruments in Nuclear Power Plants, under the Nuclear Power Plant Standards Committee of the ISA developed a standard containing minimum requirements to be used for establishing and maintaining setpoints of individual instrument channels in safety-related systems (see Reference 9.11).

This standard was revised in 1987 to provide clarification and to reflect industry practice. The standard was revised further in 1994 and reflects the Improved Technical Specification Program (a cooperative effort between the industry and NRC staff) and current industry practice established in the Standard Technical Specifications (e.g., Reference 9.8), which included a nominal trip setpoint and an allowable value to establish limits of instrument channel operability during periodic~~period~~ surveillance testing.

2.1.2 Uncertainty Categories

Instrument uncertainties must be categorized to determine how they are combined in the overall instrument channel uncertainty calculation. The two basic categories, random and non-random are illustrated in Figure 2-1 and discussed below.

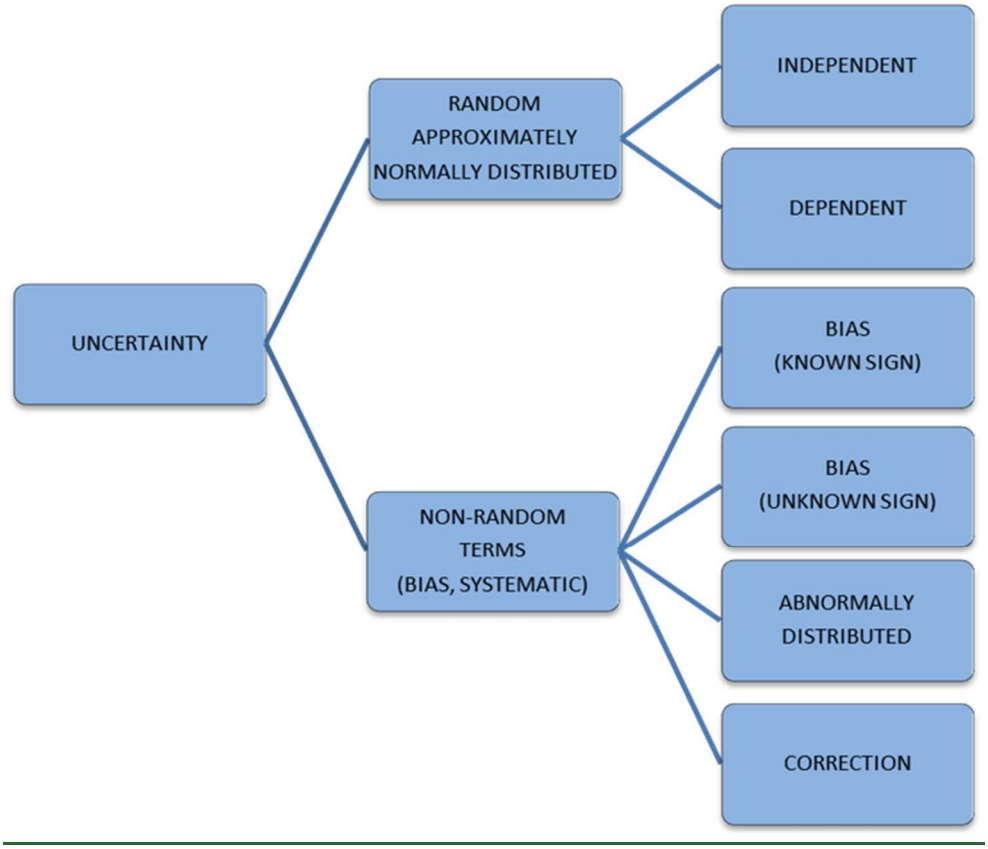


Figure 2-1 Statistical uncertainty

2.1.2.1 Random Uncertainties

Random uncertainties are referred to as a quantitative statement of the reliability of a single measurement or of a parameter, such as the arithmetic mean value, determined from a number of random trial measurements. This uncertainty is often called the statistical uncertainty and is one of the so-called precision indices. The most commonly used indices, usually in reference to the reliability of the mean, are the standard deviation, the standard error (also called the standard deviation of the mean), and the probable error.

It is usually expected that those instrument uncertainties that a manufacturer specifies as having a ± magnitude are random uncertainties. However, the uncertainty must be mean-centered and approximately normally distributed to be considered random. The

2.1.4 Bias (Unknown Sign)

Some bias effects may not have a known sign. The unpredictable sign should be conservatively treated by algebraically adding the bias in the worst (i.e., conservative) direction.

2.1.5 Correction

Errors or offsets that are of a known direction and magnitude are corrected for in the calibration of the module and are not included in the setpoint calculation. The fact that these corrections are made during calibration should be identified in the setpoint uncertainty calculation.

2.1.6 Combining Uncertainties

The total loop uncertainty (TLU) for an instrument or instrument loop/channel is typically a combination of several categories using the SRSS and algebraic methodologies described above. A simplified example illustrates how these uncertainties are combined.

An instrument channel has eight uncertainties: A, B, C, D, E, F, L and M, as categorized below. Values are scaled to units of percent calibrated span (CS) to ensure they are combined consistently with other values in the total channel uncertainty calculation. Direction signs are included to illustrate the combined effect.

A (random / independent) = ±1.0 % CS~~percent CS~~

B (random / independent) = ±1.0 % CS~~percent CS~~

C (random / independent) = ±1.0 % CS~~percent CS~~

D (random / dependent) = ±1.5 % CS~~percent CS~~ (D interacts with E)

E (random / dependent) = ±2.0 % CS~~percent CS~~ (E interacts with D)

F (Abnormally Distributed) = ±2.5 % CS~~percent CS~~ (Treated as ± Bias value)

L (Bias: Known Direction) = +3.0 % CS~~percent CS~~

M (Bias; Known Direction) = −4.0 % CS~~percent CS~~

The setpoint calculation ensures that protective actions occur before the analytical limits are reached. The SRSS technique applies only to those uncertainties that are characterized as independent, random, and approximately normally distributed (or otherwise allowed by versions of the central-limit theorem). All other uncertainty components are combined using the maximum possible uncertainty treatment (i.e., algebraic summation of absolute values as necessary).

The total loop uncertainty is calculated as follows using the SRSS method for random terms and algebraic summation of like signs for bias terms:

$$TLU = [(A)^2 + (B)^2 + (C)^2 + (D + E)^2]^{1/2} \pm |F| + L - M$$

$$TLU = \pm [(1)^2 + (1)^2 + (1)^2 + (1.5 + 2)^2]^{1/2} \pm |2.5| + 3 - 4$$

TLU = ±3.9 % CS~~percent CS~~ + 5.5 % CS~~percent CS~~ −6.5 % CS~~percent CS~~

TLU^{+} = (+)3.9 % CS~~percent CS~~ + 5.5 % CS~~percent CS~~

= +9.4 % CS~~percent CS~~

TLU^{-} = (-)3.9 % CS~~percent CS~~ - 6.5 % CS~~percent CS~~

= −10.4 % CS~~percent CS~~

This general example indicates how uncertainty calculations can be dominated by dependent and bias errors. The larger negative error can be significant if it is in the non-conservative direction with respect to the analytical limit for this instrument channel.

2.1.7 Sign Convention

The sign convention used in this setpoint methodology is consistent with the ISA definition of error (see Table 1-2). In this definition, error is equal to the difference between the indication and the ideal value of the measured signal. Therefore, a positive error indicates that the measured value is greater than the actual process value. The error direction is referenced to the ideal, or true value. This can be expressed mathematically in one or two ways:

Error = Indicated Value – Actual Value; or

Indicated Value = Actual Value + Error.

Using the example above, if the actual process value is 25 percent CS, the measured value may be anywhere from 14.6 percent CS to 34.4 percent CS.

Conversely, if the measured value is 25 percent CS, the actual process value may be anywhere between 15.6 percent CS and 35.4 percent CS.

2.2 Regulatory Requirements

2.2.1 NRC Regulations

10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with IEEE Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. (Reference 9.10) Clause 4.4 of IEEE Standard 603-1991 requires identification of the analytical limit

associated with the M&TE in use during the calibration process. ~~If the overall uncertainty of the M&TE is less than 1/10th of the reference accuracy of the device being tested, the M&TE uncertainty can be disregarded).~~

3.2.4 Sensor Calibration Accuracy

Sensor calibration accuracy (SCA) refers to the uncertainties introduced into the sensor during the calibration process. This accuracy is sometimes referred to as the "setting tolerance" or the "as-left tolerance." Sensor calibration errors are the result of measurement and test equipment uncertainties and human errors introduced during the calibration process. Time constraints, indicator readability, calibration procedures, and individual skills limit the precision of calibration data in the field.

The calibration, or performance verification, process involves the application of known values of the measured variable at the sensor input and recording corresponding output values over the entire sensor range in ascending and descending directions. If the method of calibration verifies all four attributes of reference accuracy, and the calibration tolerance is less than or equal to the reference accuracy, then the calibration tolerance does not need to be included in the total sensor error allowance.

Verification of all four attributes of reference accuracy requires multiple cycles of ascending and descending calibration data; however, this approach is not practical for field calibration, and plant procedures typically require only a single up-down cycle. Since this method of calibration does not verify all attributes of the reference accuracy such as repeatability, the potential exists to introduce an offset in the sensor output that is not identified in the calibration data. This offset is usually very small, but could be as large as the calibration tolerance limit allowed in the test procedure. In this case, an additional calibration tolerance is needed to account for the potential repeatability error. If adequate margin exists, the additional calibration tolerance is acceptable. Otherwise, verifying repeatability during the calibration process may be justified to reduce the calibration error allowance.

Reference 9.12 provides several methods to account for the potential calibration error. For the instrument setpoint methodology, it is conservatively assumed that the calibration process does not verify all attributes of the reference accuracy; therefore, a separate allowance for the calibration tolerance is included in the overall total loop uncertainty calculations. It is impossible to calibrate an instrument loop with a tolerance that is less than the reference accuracy – calibration of a component to a tolerance less than its reference accuracy cannot increase its accuracy. Therefore, the minimum requirement for the calibration tolerance should normally be equal to the reference accuracy.

For the purpose of determining the calibration error allowance, it is assumed that calibration is performed at essentially the same ambient temperature. Ambient temperature data is recorded in the calibration procedure to verify this assumption (see Section 3.2.2). If the calibration is performed at a different temperature, then the uncertainty calculation must consider this for inclusion of a temperature error term. This data can also be used to analyze calibration results, if needed.

This effect can typically be calibrated out using a correction factor provided by the manufacturer so that the transmitter will provide the desired output at high pressure operating conditions. To calculate the sensor pressure effect at the operating pressure, the maximum pressure variation above and below the operating pressure should be determined. The manufacturer's static pressure effect is then applied to the operating pressure variation to determine the sensor pressure effects. Normally the manufacturer specifies separate span and zero effects. For any of these effects that cannot be zeroed out during calibration must be accounted for in the calibration; typically the error is treated as a bias term for a sensor whose SPE is in a predictable magnitude and direction.

As an example, a differential pressure level transmitter is designed to operate at 1850 psig with a process pressure variation (PV) of 1600 to 2100 psig, or ±250 psig. The static pressure effect specified by the manufacturer for the transmitter in this example is ±0.5 percent CS per 1000 psig. It should be noted that static pressure effects are typically specified in percent upper range limit (URL). In this case the URL based value must be scaled to percent CS using the ratio of URL to CS.

Assuming the static pressure effect is linear over the pressure range, SPE is calculated as follows:

SPE = (±0.5 % CS~~percent CS~~) PV psig /1000 psig

SPE = (±0.5 % CS~~percent CS~~)(2100 – 1600) psig / 1000 psig

SPE = (±0.5 % CS~~percent CS~~)(500 psig /1000 psig)

SPE = ±0.25 % CS~~percent CS~~

3.2.7 Insulation Resistance Effects

The instrument channel uncertainty is dependent on the insulation resistance effects (IRE), which quantifies changes in the insulation resistance of the sensor and instrument cabling in harsh environments. Under high humidity and temperature events, the instrument channels may experience a reduction in insulation resistance such as during a high energy line break or loss-of-coolant-accident. During normal conditions, the leakage current is relatively small and typically is calibrated out during instrument channel calibrations. However, during conditions of high temperature and humidity, the leakage current may increase to a level that causes significant uncertainty in measurement. The effect is particularly a concern for sensitive, low signal level circuits such as neutron detector measurements, current transmitters, RTDs, and thermocouples. IRE is a known sign bias term.

3.2.8 Accident Environment Effects

Instruments which can be exposed to severe ambient conditions as a result of an accident, and which are required to remain functional during or after an accident, may have additional accident related error terms which must be considered in a loop

4.0 Setpoint Determination

4.1 Setpoint Relationships

It is important to understand the relationships between trip setpoints, analytical limits, and the plant safety limits in order to properly account for the total instrument channel uncertainty in the establishment of the setpoints. Figure 4-1 presents the relative position of these items with respect to both an increasing process and a decreasing process.

The safety limits are imposed on plant process variables, such as pressure, level, temperature, or these combinations. Some safety limits may also be defined in terms of indirectly calculated process conditions such as the critical heat flux ratio~~departure from nucleate boiling ratio~~ or linear heat generation rate. Requirements for establishing setpoints and relationships between the nominal trip setpoint, limiting trip setpoint, analytical limit, and safety limit are discussed in a safety analysis analytical limits report. This section discusses the concepts used to determine limiting trip setpoint and nominal trip setpoints.

variables such as pressure, temperature, and their combinations (e.g., critical heat flux ratio~~Departure from Nuclear Boiling Ratio~~).

4.1.2 Analytical Limits

The analytical limits are based on the results of plant safety analyses, and are used to ensure that the plant safety limits are not exceeded. The safety analyses should account for interaction activities between plant safety equipment during normal operation, anticipated operational occurrences, and postulated accidents. Based on the results of the plant safety analyses, the analytical limits are established for various plant safety parameters, processes, and variables. The determined analytical limits are applied in the determination of plant setpoints, which are designed to initiate protective functions.

4.1.3 Limiting Trip Setpoint

Trip setpoints are the predetermined values where the protective actuation devices of the instruments perform a protective function (e.g., trip a breaker, de-energize a solenoid). The LTSP is the least conservative value the trip setpoint can be accounting for all uncertainties and still ensure the analytical limits are not exceeded and safety limits are protected. For the NuScale Instrument Setpoint Methodology, the LTSP is the LSSS, as required by 10 CFR 50.36(c)(1)(ii)(A).

4.1.4 Nominal Trip Setpoint

The NTSP is the LTSP with margin added. The NTSP must be equal to or more conservative than the LTSP. The NTSP is the value of the trip setpoint chosen for plant operation to account for the Total As-Found Tolerance (Equation 4-15) and generally contains added margin based on engineering judgement to add a level of conservatism to ensure the LTSP is not exceeded. In all cases, the margin must be greater than or equal to the As-Found Tolerance. For the purposes of this document, the Total As-Found Tolerance is not applied to the NTSP; rather the NTSP value is rounded, where appropriate, to the nearest whole number in the conservative direction for simplification and to add margin. For example, the NTSP is rounded down for an increasing process, and rounded up for a decreasing process.

4.1.5 Actual Trip Setpoint

The actual trip setpoint is known only at the precise time of measurement or surveillance testing, since uncertainties due to instrument drift will cause the actual trip setpoint to vary over time. The actual trip setpoint is equal to the as-found or as-left value during surveillance testing and measurement.

4.2 Calculation of Trip Setpoint

The NuScale Instrument Setpoint Methodology uses a procedure based on evaluation of the as-found setpoint conditions in comparison to the NTSP for the instrument loop in question. This method is based on conditions established in NRC RIS 2006-17. These conditions are described below.

4.4 Performance Test and Acceptance Criteria

Periodic surveillances of instrument loops are required to ensure the loops are operating as expected. The instruments are tested to verify they perform their required safety function (i.e., initiate a protective action when a setpoint is exceeded~~exceed~~) within their prescribed limits within the time interval required. Channel operability using performance test acceptance criteria is based on determining the as-found values for the instrument loop components under test and comparing that using a double-sided band around the NTSP.

The performance and test acceptance criteria (PTAC) band is therefore equivalent to the value of the NTSP plus or minus the AFT and is evaluated as a double-sided band for evaluation of channel operability:

$$\pm PTAC_{Total} = NTSP \pm AFT_{Total} \qquad \text{Equation 4-18}$$

Building upon relationships of the various parameters shown in Figure 4-1, the surveillance test and calibration relationships are presented in Figure 4-2.

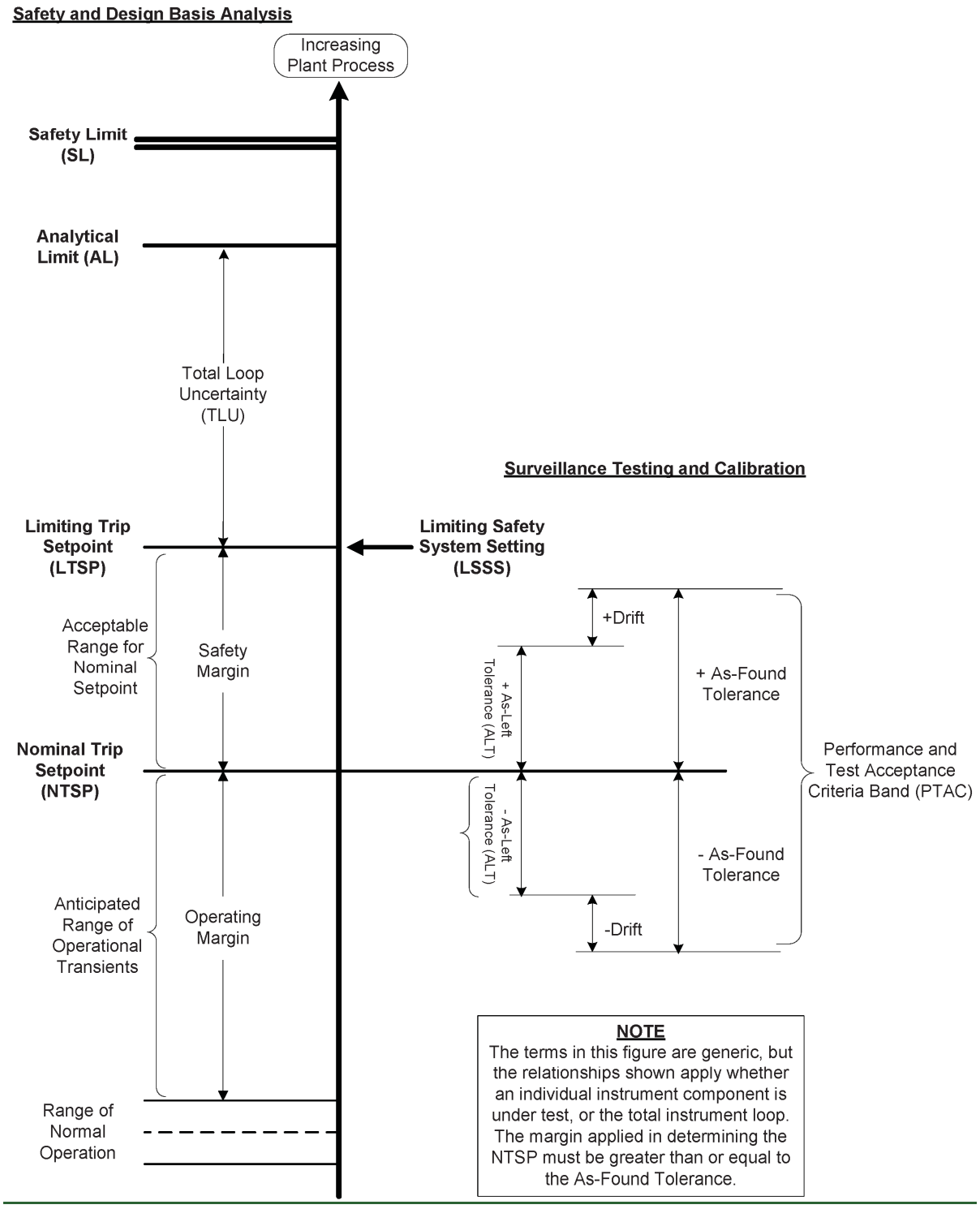


Figure 4-2 Setpoint relationships during surveillance testing and calibration

5.0 Assumptions

The NuScale Instrument Setpoint Methodology is based on the following assumptions listed below. Some assumptions apply generically to the NuScale Instrument Setpoint Methodology; other assumptions are made to account for lack of actual manufacturer or instrument loop data. Assumptions 5.1 through 5.5 apply generically to the NuScale Instrument Setpoint Methodology. Assumptions 5.6 to 5.18 are for purposes of performing the example setpoint calculations and will be adjusted based on actual instrument loop data.

The following assumptions apply generically to the NuScale Instrument Setpoint Methodology:

5.1 Any random independent term whose value is less than {{ }}$^{2(c)}$ of any of the other associated device random uncertainties can be statistically neglected.

5.2 Uncertainty terms of devices are calculated in terms of percent CS unless otherwise stated.

5.3 For the purposes of the setpoint analyses, the instrumentation is assumed to be calibrated at the reference ambient conditions for which the instrumentation is required to operate as specified in plant calibration procedures. The STE for the instrumentation is an allowance based on the maximum expected ambient temperature deviation from the reference calibration conditions. {{

}}$^{2(c)}$ (in units of ± X percent CS per Y degree Fahrenheit).

{{

}}$^{2(c)}$

5.4 The random terms are assumed to have approximately normal probability distribution functions for the purposes of this document. Common industry practice is to assume that published vendor specifications conform to a 95/95 confidence level unless specific information is available to indicate otherwise. ~~The insulation resistance error is {{ }}$^{2(c)}$~~

5.5 The sensor seismic effect error is {{ }}$^{2(c)}$ (see Section 3.2.9).~~The random terms are assumed to have approximately normal probability distribution functions for the purposes of this document. Common industry practice is to assume that published vendor specifications conform to a 95/95 confidence level unless specific information is available to indicate otherwise.~~

~~**5.5**~~ The following assumptions are made to demonstrate the application of the NuScale Instrument Setpoint Methodology. These assumptions are validated and updated if necessary in the application of this methodology based on final sensor selection and known instrumentation loop parameters.

5.6 The insulation resistance error is {{ }}[2(c)]

~~5.6~~**5.7** For all sensors except neutron detectors, the SDR is conservatively assumed to be {{ }}[2(c)]

~~5.7~~**5.8** For all sensors except neutron detectors, the SME is conservatively assumed to be {{ }}[2(c)] The M&TE readability error is assumed to be zero as it is assumed all M&TE will have digital readouts.

~~5.8~~**5.9** An aggregate value for the SAE is assumed to be {{ }}[2(c)] The SAE term is applied to the protective functions associated with protection against loss of coolant accident (LOCA) or high energy line break (HELB) events. Accident pressure effects will generally not be included in an error analysis except, as discussed in Section 3.2.8.2.

Table 5-1 lists the protective functions for which the ~~The~~ SAE uncertainty is applied ~~to the following protective functions~~ based on safety analysis analytical limits:

Table 5-1 Protective functions with accident environment effect uncertainties applied

Protective Function	Sensor	Mitigating Event
High narrow range containment pressure	Containment pressure	RCS or secondary leaks above allowable limits to protect RCS inventory and ECCS function during these events
Low pressurizer level	Pressurizer level	Primary HELB outside CNV
Low-low pressurizer level	Pressurizer level	LOCA and primary HELB outside CNV
Low pressurizer pressure	Pressurizer pressure	HELB outside CNV
Low-low pressurizer pressure	Pressurizer pressure	HELB outside CNV
Low main steam pressure	Main steam pressure	Secondary HELB outside CNV
Low-low main steam pressure	Main steam pressure	Secondary HELB outside CNV
Low RPV riser level	RPV riser level	LOCA
High containment water	CNV level	LOCA

level		
High under the bioshield temperature	Under the bioshield temperature	HELB outside CNV

~~**5.9** The sensor seismic effect error is {{ }}2(c) (see Section 3.2.9).~~

5.10 The sensor PME and SRA are shown for the sensors listed in Table 5-2. The PME terms were {{

}}2(c)

6.0 Calculation of Reactor Protection and Engineered Safeguards Actuation System Setpoints

This section provides a demonstration of the NuScale Instrument Setpoint Methodology described in this document and contains preliminary calculations of instrument uncertainties associated with analytical limits for credited protective actuation functions defined by the plant safety analyses. The protective actuation functions consist of RTS functions listed in Table 6-1 and ESFAS functions listed in Table 6-2. This methodology is not applied to any other process instrumentation setpoints. The uncertainty calculations and resultant NTSP and LTSP values in this section are based on preliminary estimates of device behavior using engineering judgement and vendor estimates and are provided to show the application of the instrument setpoint methodology described in this document, and are not intended to be the final NTSP and LTSP values for use in plant calibration procedures or Technical Specifications. Final calculations of instrument channel uncertainties and trip setpoints will be provided as part of the final, detailed system design using actual, verified instrument sensor uncertainty data.

Table 6-3 through Table 6-24 contain detailed individual TLU calculations (see Section 3.5) and Limiting Trip Setpoints (see Section 4.1.3) for the RTS functions listed in Table 6-1 and ESFAS functions listed in Table 6-2. The tables contain the parameter ranges, calibrated spans, and normal operating points for the parameters of interest and list values in both the engineering units and calibrated spans for the particular instrument loop.

Table 6-2 Engineered Safety Features Actuation System Functions

Safety Function	Protective Action Signal
Emergency core cooling system	High containment water level
	Low RPV riser level
	Low AC voltage 24 hour timer
DHRS actuation	High pressurizer pressure
	High RCS T_{hot} temperature
	High narrow range containment pressure
	Low pressurizer pressure
	Low-low pressurizer level
	Low main steam pressure
	Low-low main steam pressure
	High main steam pressure
	High steam superheat
	Low steam superheat
	Low AC voltage
	High under the bioshield temperature
Containment system isolation	High narrow range containment pressure
	Low-low pressurizer level
	Low AC voltage
	High under the bioshield temperature
Demineralized water system isolation	Reactor trip
	Low RCS flow
	High subcritical multiplication
Chemical and volume control system isolation	High pressurizer level
	Low pressurizer pressure
	Low-low pressurizer pressure
	High narrow range containment pressure
	Low-low pressurizer level
	Low-low RCS flow
Pressurizer heater trip	Low pressurizer level

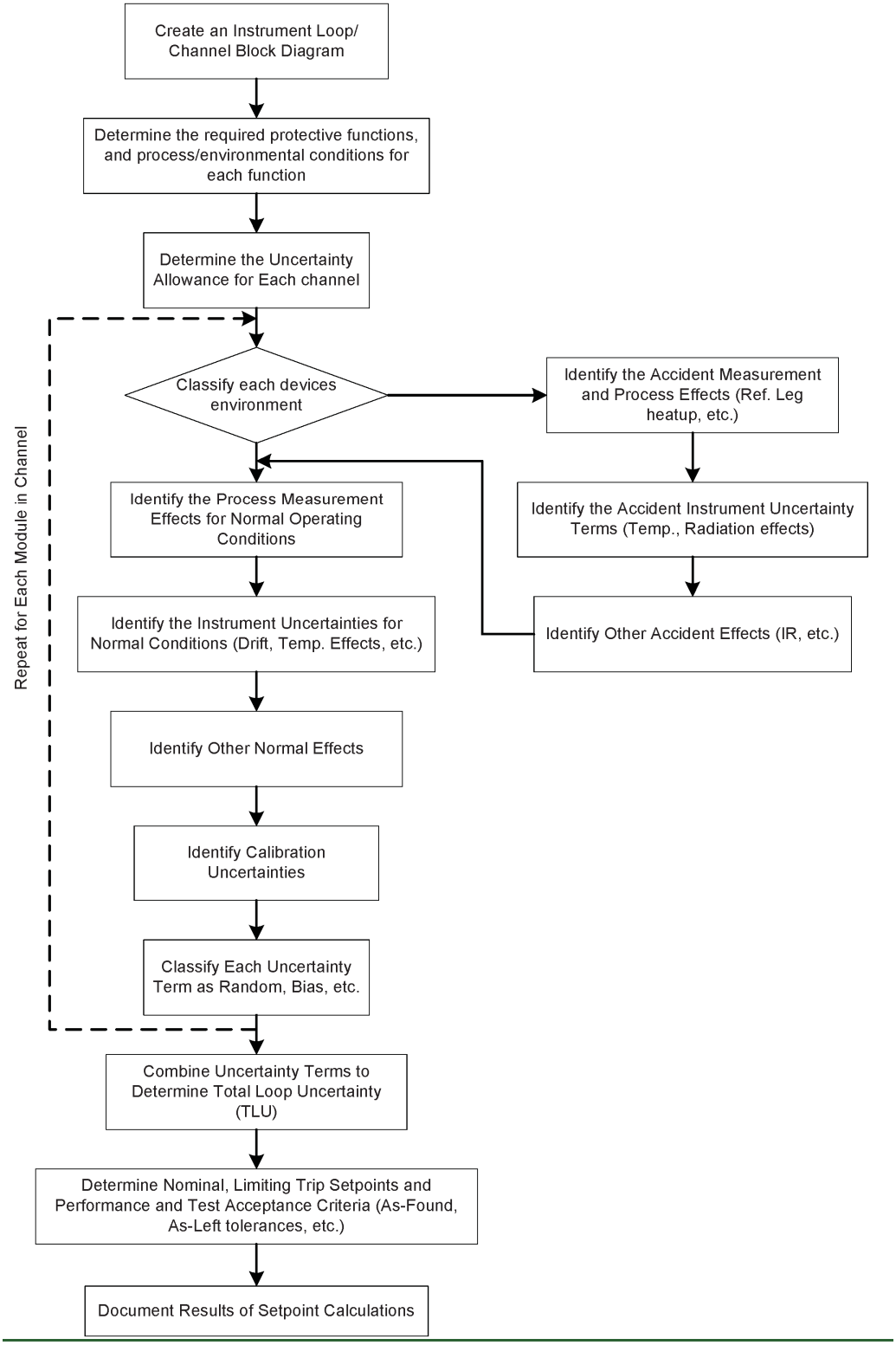


Figure 6-1 Setpoint calculation flowchart

Digital System Temperature Error (DTE)	{{ }}$^{2(c)}$	Assumption 5.12.2
Digital System Measurement and Test Equipment Error (DME)	{{ }}$^{2(c)}$	Assumption 5.12.2

Total Loop Uncertainty (TLU)	{{ }}$^{2(c)}$
Units	**CPS**

Analytical Limit	5.00E+05	CPS
Limiting Trip Setpoint (Equation 4-1)	{{ }}$^{2(c)}$	CPS
Nominal Trip Setpoint (Equation 4-2)	{{ }}$^{2(c)}$	CPS

Table 6-4 Setpoint calculation for high subcritical multiplication protective function

Actuation Function	**High Subcritical Multiplication**	
Sensor	**Source Range Detectors**	
Engineering Units of Measurement	Note 1	**Source/Reference**
Upper Limit	5.00	Note 2
Lower Limit	0.00	Note 2
Calibrated Span (CS)	5.00	Note 2
Process and Miscellaneous Effects Error	{{ }}2(c)	Assumption 5.11.5.4
Neutron Monitoring System Error	{{ }}2(c)	Assumption 5.11.5.4
Digital Processing Error	{{ }}2(c)	Assumption 5.11.5.4
Margin	{{ }}2(c)	Assumption 5.11.5.4
Total Loop Uncertainty (TLU)	{{ }}2(c)	
Units	Note 1	
Analytical Limit	3.2	
Limiting Trip Setpoint (Equation 4-1)	{{ }}2(c)	
Nominal Trip Setpoint (Equation 4-2)	{{ }}2(c)	

1. The subcritical multiplication factor (M) is calculated by the MPS and is defined as the current source range count rate (CR) divided by the average baseline source range count rate (CR_o) and is a unitless term:

$$M = \frac{CR}{CR_0}$$

2. For this protective function, a calibrated span for the subcritical multiplication factor is assumed to be 0 to 5.00.

Table 6-5 Setpoint calculation for SR and IR high startup rate protective functions

Actuation Function	**High SR and IR Log Power Rate**	**Source/Reference**
Sensor	**Source and Intermediate Range Detectors**	Note 1
Engineering Units of Measurement	DPM	
Upper Limit	5.00	Assumption 5.16
Lower Limit	0.00	Assumption 5.16
Calibrated Span (CS)	5.00	
Process and Miscellaneous Effects Error	{{ }}$^{2(c)}$	Assumption 5.16
Neutron Monitoring System Error	{{ }}$^{2(c)}$	Assumption 5.16
Digital Processing Error	{{ }}$^{2(c)}$	Assumption 5.16

Total Loop Uncertainty (TLU)	{{ }}$^{2(c)}$
Units	**DPM**

Analytical Limit	3.00 DPM
Limiting Trip Setpoint (Equation 4-1)	{{ }}$^{2(c)}$ DPM
Nominal Trip Setpoint (Equation 4-2)	{{ }}$^{2(c)}$ DPM

Note 1: The Source Range Log Power Rate Trip and Intermediate Range Log Power Rate Trip are separate trips which are developed by their respective NMS channels. A trip in either channel will initiate the trip logic in MPS.

Table 6-6 Setpoint calculation for high power rate protective function

Actuation Function	**High Power Range Rate**	
Sensor	**Power Range Neutron Detector**	
Engineering Units of Measurement	% RTP/min	**Source/Reference**
Upper Limit	N/A	Assumption 5.17
Lower Limit	N/A	Assumption 5.17
Calibrated Span (CS)	N/A	
Process and Miscellaneous Effects Error	{{ }}$^{2(c)}$	Assumption 5.17
Sensor Error	{{ }}$^{2(c)}$	Assumption 5.17
Neutron Monitoring System Error	{{ }}$^{2(c)}$	Assumption 5.17
Digital Processing Error	{{ }}$^{2(c)}$	Assumption 5.17
Margin	{{ }}$^{2(c)}$	Assumption 5.17
Total Loop Uncertainty (TLU)	{{ }}$^{2(c)}$	
Units	**% RTP/min**	

Analytical Limit	15.00	% RTP/min
Limiting Trip Setpoint (Equation 4-1)	{{ }}$^{2(c)}$	% RTP/min
Nominal Trip Setpoint (Equation 4-2)	{{ }}$^{2(c)}$	% RTP/min

Table 6-8 Setpoint calculation for high RCS T_{hot} temperature protective function

Actuation Function	**High RCS T_{hot} Temperature**
Sensor	**RCS Narrow Range RCS T_{hot}**
Engineering Units of Measurement	°F
Upper Limit	650
Lower Limit	400
Calibrated Span (CS)	250

Process and Miscellaneous Effects Error	**°F**	**% CS**	**Source/Reference**
Primary Element Accuracy (PEA)	0.00	0.00	
Process Measurement Error (PME)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Error			
Sensor Reference Accuracy (SRA)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Drift (SDR)	{{	}}$^{2(c)}$	Assumption ~~5.6~~5.7
Sensor Measurement and Test Equipment (SME)	{{	}}$^{2(c)}$	Assumption ~~5.7~~5.8
Sensor Calibration Accuracy (SCA)	{{	}}$^{2(c)}$	Equation 3-1
Sensor Temperature Effect (STE)	{{	}}$^{2(c)}$	Assumption 5.3
Sensor Static Pressure Effect (SPE)	{{	}}$^{2(c)}$	Assumption 5.15
Insulation Resistance Effect (IRE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.4~~5.6
Sensor Accident Effect (SAE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.8~~5.9
Sensor Seismic Effect (SenSE)	{{	}}$^{2(c)}$	Assumption ~~5.9~~5.5
Digital Processing Error			
Digital System Reference Accuracy (DRA)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Drift Error (DDR)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Temperature Error (DTE)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Measurement and Test Equipment Error (DME)	{{	}}$^{2(c)}$	Assumption 5.12

Total Loop Uncertainty (TLU)	{{	}}$^{2(c)}$
Units	**°F**	**% CS**

Analytical Limit	610.00	°F
Limiting Trip Setpoint (Equation 4-1)	{{ }}$^{2(c)}$	°F
Nominal Trip Setpoint (Equation 4-2)	{{ }}$^{2(c)}$	°F

Table 6-9 Calculation of main steam temperature loop uncertainty

Actuation Function	**Main Steam Temperature**		
Sensor	**Main Steam Temperature**		
Engineering Units of Measurement	°F		
Upper Limit	700		
Lower Limit	100		
Calibrated Span (CS)	600		
Process and Miscellaneous Effects Error	°F	% CS	
Primary Element Accuracy (PEA)	0.00	0.00	
Process Measurement Error (PME)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Error			
Sensor Reference Accuracy (SRA)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Drift (SDR)	{{	}}$^{2(c)}$	Assumption ~~5.6~~5.7
Sensor Measurement and Test Equipment (SME)	{{	}}$^{2(c)}$	Assumption ~~5.7~~5.8
Sensor Calibration Accuracy (SCA)	{{	}}$^{2(c)}$	Equation 3-1
Sensor Temperature Effect (STE)	{{	}}$^{2(c)}$	Assumption 5.3
Sensor Static Pressure Effect (SPE)	{{	}}$^{2(c)}$	Assumption 5.15
Insulation Resistance Effect (IRE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.4~~5.6
Sensor Accident Effect (SAE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.8~~5.9
Sensor Seismic Effect (SenSE)	{{	}}$^{2(c)}$	Assumption ~~5.9~~5.5
Digital Processing Error			
Digital System Reference Accuracy (DRA)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Drift Error (DDR)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Temperature Error (DTE)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Measurement and Test Equipment Error (DMTE)	{{	}}$^{2(c)}$	Assumption 5.12
Total Loop Uncertainty (TLU)	{{	}}$^{2(c)}$	
Units	**°F**	**% CS**	

To calculate the uncertainty associated with the superheat protective function, a simple equation for determining the steam superheat temperature (T_{SH}) for main steam is used. The degree of superheat is found by determining the saturation temperature (T_{SAT}) at the measured main steam pressure (P_{STM}), and subtracting this value from the measured main steam temperature (T_{STM}). The main steam saturation temperature is found via a simple steam table lookup function using the measured steam pressure value.

$$T_{SH} = T_{STM} - T_{SAT}(P_{STM}) \qquad \text{(Equation 6-1)}$$

Table 6-10 Setpoint calculation for high main steam pressure protective function

Actuation Function	**High Main Steam Pressure**
Sensor	**Main Steam Pressure**
Engineering Units of Measurement	psia
Upper Limit	1200
Lower Limit	0
Calibrated Span (CS)	1200

Process and Miscellaneous Effects Error	**psia**	**% CS**	**Source/Reference**
Primary Element Accuracy (PEA)	0.00	0.00	
Process Measurement Error (PME)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Error			
Sensor Reference Accuracy (SRA)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Drift (SDR)	{{	}}$^{2(c)}$	Assumption ~~5.6~~5.7
Sensor Measurement and Test Equipment (SME)	{{	}}$^{2(c)}$	Assumption ~~5.7~~5.8
Sensor Calibration Accuracy (SCA)	{{	}}$^{2(c)}$	Equation 3-1
Sensor Temperature Effect (STE)	{{	}}$^{2(c)}$	Assumption 5.3
Sensor Static Pressure Effect (SPE)	{{	}}$^{2(c)}$	Assumption 5.15
Insulation Resistance Effect (IRE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.4~~5.6
Sensor Accident Effect (SAE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.8~~5.9
Sensor Seismic Effect (SenSE)	{{	}}$^{2(c)}$	Assumption ~~5.9~~5.5
Digital Processing Error			
Digital System Reference Accuracy (DRA)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Drift Error (DDR)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Temperature Error (DTE)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Measurement and Test Equipment Error (DME)	{{	}}$^{2(c)}$	Assumption 5.12

Total Loop Uncertainty (TLU)	{{	}}$^{2(c)}$
Units	**psia**	**% CS**

Analytical Limit	800.0	psia
Limiting Trip Setpoint (Equation 4-1)	{{ }}$^{2(c)}$	psia
Nominal Trip Setpoint (Equation 4-2)	{{ }}$^{2(c)}$	psia

Table 6-13 Setpoint calculation for high containment pressure protective function

Actuation Function	**High Containment Pressure**
Sensor	**Narrow Range Containment Pressure**
Engineering Units of Measurement	psia
Upper Limit	20
Lower Limit	0
Calibrated Span (CS)	20

Process and Miscellaneous Effects Error	**psia**	**% CS**	**Source/Reference**
Primary Element Accuracy (PEA)	0.00	0.00	
Process Measurement Error (PME)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Error			
Sensor Reference Accuracy (SRA)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Drift (SDR)	{{	}}$^{2(c)}$	Assumption ~~5.6~~5.7
Sensor Measurement and Test Equipment (SME)	{{	}}$^{2(c)}$	Assumption ~~5.7~~5.8
Sensor Calibration Accuracy (SCA)	{{	}}$^{2(c)}$	Equation 3-1
Sensor Temperature Effect (STE)	{{	}}$^{2(c)}$	Assumption 5.3
Sensor Static Pressure Effect (SPE)	{{	}}$^{2(c)}$	Assumption 5.15
Insulation Resistance Effect (IRE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.4~~5.6
Sensor Accident Effect (SAE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.8~~5.9
Sensor Seismic Effect (SenSE)	{{	}}$^{2(c)}$	Assumption ~~5.9~~5.5
Digital Processing Error			
Digital System Reference Accuracy (DRA)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Drift Error (DDR)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Temperature Error (DTE)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Measurement and Test Equipment Error (DME)	{{	}}$^{2(c)}$	Assumption 5.12

Total Loop Uncertainty (TLU)	{{	}}$^{2(c)}$
Units	**psia**	**% CS**

Analytical Limit	9.50	psia
Limiting Trip Setpoint (Equation 4-1)	{{ }}$^{2(c)}$	psia
Nominal Trip Setpoint (Equation 4-2)	{{ }}$^{2(c)}$	psia

Table 6-14 Setpoint calculation for high pressurizer pressure protective function

Actuation Function	**High Pressurizer Pressure**
Sensor	**Pressurizer Pressure**
Engineering Units of Measurement	psia
Upper Limit	2200
Lower Limit	1500
Calibrated Span (CS)	700

Process and Miscellaneous Effects Error	**psia**	**% CS**	**Source/Reference**
Primary Element Accuracy (PEA)	0.00	0.00	
Process Measurement Error (PME)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Error			
Sensor Reference Accuracy (SRA)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Drift (SDR)	{{	}}$^{2(c)}$	Assumption ~~5.6~~5.7
Sensor Measurement and Test Equipment (SME)	{{	}}$^{2(c)}$	Assumption ~~5.7~~5.8
Sensor Calibration Accuracy (SCA)	{{	}}$^{2(c)}$	Equation 3-1
Sensor Temperature Effect (STE)	{{	}}$^{2(c)}$	Assumption 5.3
Sensor Static Pressure Effect (SPE)	{{	}}$^{2(c)}$	Assumption 5.15
Insulation Resistance Effect (IRE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.4~~5.6
Sensor Accident Effect (SAE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.8~~5.9
Sensor Seismic Effect (SenSE)	{{	}}$^{2(c)}$	Assumption ~~5.9~~5.5
Digital Processing Error			
Digital System Reference Accuracy (DRA)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Drift Error (DDR)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Temperature Error (DTE)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Measurement and Test Equipment Error (DME)	{{	}}$^{2(c)}$	Assumption 5.12

Total Loop Uncertainty (TLU)	{{	}}$^{2(c)}$
Units	**psia**	**% CS**

Analytical Limit	2000.0	psia
Limiting Trip Setpoint (Equation 4-1)	{{ }}$^{2(c)}$	psia
Nominal Trip Setpoint (Equation 4-2)	{{ }}$^{2(c)}$	psia

Table 6-15 Setpoint calculation for low and low-low pressurizer pressure protective function

Actuation Function	**Low and Low-Low Pressurizer Pressure**
Sensor	**Pressurizer Pressure**
Engineering Units of Measurement	psia
Upper Limit	2200
Lower Limit	1500
Calibrated Span (CS)	700

Process and Miscellaneous Effects Error	**psia**	**% CS**	**Source/Reference**
Primary Element Accuracy (PEA)	0.00	0.00	
Process Measurement Error (PME)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Error			
Sensor Reference Accuracy (SRA)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Drift (SDR)	{{	}}$^{2(c)}$	Assumption ~~5.6~~5.7
Sensor Measurement and Test Equipment (SME)	{{	}}$^{2(c)}$	Assumption ~~5.7~~5.8
Sensor Calibration Accuracy (SCA)	{{	}}$^{2(c)}$	Equation 3-1
Sensor Temperature Effect (STE)	{{	}}$^{2(c)}$	Assumption 5.3
Sensor Static Pressure Effect (SPE)	{{	}}$^{2(c)}$	Assumption 5.15
Insulation Resistance Effect (IRE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.4~~5.6
Sensor Accident Effect (SAE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.8~~5.9
Sensor Seismic Effect (SenSE)	{{	}}$^{2(c)}$	Assumption ~~5.9~~5.5
Digital Processing Error			
Digital System Reference Accuracy (DRA)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Drift Error (DDR)	{{	}}$^{2(c}$	Assumption 5.12
Digital System Temperature Error (DTE)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Measurement and Test Equipment Error (DME)	{{	}}$^{2(c)}$	Assumption 5.12

Total Loop Uncertainty (TLU)	{{	}}$^{2(c)}$
Units	**psia**	**% CS**

	Low Pzr Pressure	
Analytical Limit	1720.00	psia
Limiting Trip Setpoint (Equation 4-1)	{{ }}$^{2(c)}$	psia
Nominal Trip Setpoint (Equation 4-2)	{{ }}$^{2(c)}$	psia

Table 6-16 Setpoint calculation for low and low-low main steam pressure protective function

Actuation Function	**Low and Low-Low Main Steam Pressure**
Sensor	**Main Steam Pressure**
Engineering Units of Measurement	psia
Upper Limit	1200
Lower Limit	0
Calibrated Span (CS)	1200

Process and Miscellaneous Effects Error	**psia**	**% CS**	**Source/Reference**
Primary Element Accuracy (PEA)	0.00	0.00	
Process Measurement Error (PME)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Error			
Sensor Reference Accuracy (SRA)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Drift (SDR)	{{	}}$^{2(c)}$	Assumption ~~5.6~~5.7
Sensor Measurement and Test Equipment (SME)	{{	}}$^{2(c)}$	Assumption ~~5.7~~5.8
Sensor Calibration Accuracy (SCA)	{{	}}$^{2(c)}$	Equation 3-1
Sensor Temperature Effect (STE)	{{	}}$^{2(c)}$	Assumption 5.3
Sensor Static Pressure Effect (SPE)	{{	}}$^{2(c)}$	Assumption 5.15
Insulation Resistance Effect (IRE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.4~~5.6
Sensor Accident Effect (SAE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.8~~5.9
Sensor Seismic Effect (SenSE)	{{	}}$^{2(c)}$	Assumption ~~5.9~~5.5
Digital Processing Error			
Digital System Reference Accuracy (DRA)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Drift Error (DDR)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Temperature Error (DTE)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Measurement and Test Equipment Error (DME)	{{	}}$^{2(c)}$	Assumption 5.12

Total Loop Uncertainty (TLU)	{{	}}$^{2(c)}$
Units	**psia**	**% CS**

	Power > 15%	Power ≤15%
Analytical Limit	300 psia	100 psia
Limiting Trip Setpoint (Equation 4-1)	{{ }}$^{2(c)}$ psia	{{ }}$^{2(c)}$ psia
Nominal Trip Setpoint (Equation 4-2)	{{ }}$^{2(c)}$ psia	{{ }}$^{2(c)}$ psia

Table 6-17 Setpoint calculation for high containment water level protective function

Actuation Function	**High Containment Water Level**		
Sensor	**Containment Water Level**		
Engineering Units of Measurement	Inches		
Upper Limit	270		Note 1
Lower Limit	170		Note 1
Calibrated Span (CS)	100		

Process and Miscellaneous Effects Error	**Inches**	**% CS**	**Source/ Reference**
Primary Element Accuracy (PEA)	0.00	0.00	
Process Measurement Error (PME)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Error			
Sensor Reference Accuracy (SRA)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Drift (SDR)	{{	}}$^{2(c)}$	Assumption ~~5.6~~5.7
Sensor Measurement and Test Equipment (SME)	{{	}}$^{2(c)}$	Assumption ~~5.7~~5.8
Sensor Calibration Accuracy (SCA)	{{	}}$^{2(c)}$	Equation 3-1
Sensor Temperature Effect (STE)	{{	}}$^{2(c)}$	Assumption 5.3
Sensor Static Pressure Effect (SPE)	{{	}}$^{2(c)}$	Assumption 5.15
Insulation Resistance Effect (IRE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.4~~5.6
Sensor Accident Effect (SAE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.8~~5.9
Sensor Seismic Effect (SenSE)	{{	}}$^{2(c)}$	Assumption ~~5.9~~5.5
Digital Processing Error			
Digital System Reference Accuracy (DRA)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Drift Error (DDR)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Temperature Error (DTE)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Measurement and Test Equipment Error (DME)	{{	}}$^{2(c)}$	Assumption 5.12

Total Loop Uncertainty (TLU)	{{	}}$^{2(c)}$
Units	**Inches**	**% CS**

Table 6-18 Setpoint calculation for high pressurizer level protective function

Actuation Function	**High Pressurizer Level**
Sensor	**Pressurizer Level**
Engineering Units of Measurement	% Level
Upper Limit	100
Lower Limit	0
Calibrated Span (CS)	100

Process and Miscellaneous Effects Error	**% Level**	**% CS**	**Source/Reference**
Primary Element Accuracy (PEA)	0.00	0.00	
Process Measurement Error (PME)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Error			
Sensor Reference Accuracy (SRA)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Drift (SDR)	{{	}}$^{2(c)}$	Assumption ~~5.6~~5.7
Sensor Measurement and Test Equipment (SME)	{{	}}$^{2(c)}$	Assumption ~~5.7~~5.8
Sensor Calibration Accuracy (SCA)	{{	}}$^{2(c)}$	Equation 3-1
Sensor Temperature Effect (STE)	{{	}}$^{2(c)}$	Assumption 5.3
Sensor Static Pressure Effect (SPE)	{{	}}$^{2(c)}$	Assumption 5.15
Insulation Resistance Effect (IRE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.4~~5.6
Sensor Accident Effect (SAE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.8~~5.9
Sensor Seismic Effect (SenSE)	{{	}}$^{2(c)}$	Assumption ~~5.9~~5.5
Digital Processing Error			
Digital System Reference Accuracy (DRA)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Drift Error (DDR)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Temperature Error (DTE)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Measurement and Test Equipment Error (DME)	{{	}}$^{2(c)}$	Assumption 5.12

Total Loop Uncertainty (TLU)	{{	}}$^{2(c)}$
Units	**% Level**	**% CS**

Analytical Limit	80.00	% Level
Limiting Trip Setpoint (Equation 4-1)	{{ }}$^{2(c)}$	% Level
Nominal Trip Setpoint (Equation 4-2)	{{ }}$^{2(c)}$	% Level

Table 6-19 Setpoint calculation for low and low-low pressurizer level protective function

Actuation Function	**Low and Low-Low Pressurizer Level**
Sensor	**Pressurizer Level**
Engineering Units of Measurement	% Level
Upper Limit	100
Lower Limit	0
Calibrated Span (CS)	100

Process and Miscellaneous Effects Error	**% Level**	**% CS**	**Source/Reference**
Primary Element Accuracy (PEA)	0.00	0.00	
Process Measurement Error (PME)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Error			
Sensor Reference Accuracy (SRA)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Drift (SDR)	{{	}}$^{2(c)}$	Assumption ~~5.6~~5.7
Sensor Measurement and Test Equipment (SME)	{{	}}$^{2(c)}$	Assumption ~~5.7~~5.8
Sensor Calibration Accuracy (SCA)	{{	}}$^{2(c)}$	Equation 3-1
Sensor Temperature Effect (STE)	{{	}}$^{2(c)}$	Assumption 5.3
Sensor Static Pressure Effect (SPE)	{{	}}$^{2(c)}$	Assumption 5.15
Insulation Resistance Effect (IRE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.4~~5.6
Sensor Accident Effect (SAE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.8~~5.9
Sensor Seismic Effect (SenSE)	{{	}}$^{2(c)}$	Assumption ~~5.9~~5.5
Digital Processing Error			
Digital System Reference Accuracy (DRA)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Drift Error (DDR)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Temperature Error (DTE)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Measurement and Test Equipment Error (DME)	{{	}}$^{2(c)}$	Assumption 5.12

Total Loop Uncertainty (TLU)	{{	}}$^{2(c)}$
Units	**% Level**	**% CS**

	Low Pressurizer Level	
Analytical Limit	35.00	% Level
Limiting Trip Setpoint (Equation 4-1)	{{ }}$^{2(c)}$	% Level
Nominal Trip Setpoint (Equation 4-2)	{{ }}$^{2(c)}$	% Level

Table 6-20 Setpoint calculation for low RCS level protective function

Actuation Function	**Low RPV Riser Level**	
Sensor	**RPV Riser Water Level**	
Engineering Units of Measurement	Inches	
Upper Limit	420	Note 1
Lower Limit	320	Note 1
Calibrated Span (CS)	100	

Process and Miscellaneous Effects Error	**Inches**	**% CS**	**Source/Reference**
Primary Element Accuracy (PEA)	0.00	0.00	
Process Measurement Error (PME)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Error	0	0	
Sensor Reference Accuracy (SRA)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Drift (SDR)	{{	}}$^{2(c)}$	Assumption ~~5.6~~5.7
Sensor Measurement and Test Equipment (SME)	{{	}}$^{2(c)}$	Assumption ~~5.7~~5.8
Sensor Calibration Accuracy (SCA)	{{	}}$^{2(c)}$	Equation 3-1
Sensor Temperature Effect (STE)	{{	}}$^{2(c)}$	Assumption 5.3
Sensor Static Pressure Effect (SPE)	{{	}}$^{2(c)}$	Assumption 5.15
Insulation Resistance Effect (IRE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.4~~5.6
Sensor Accident Effect (SAE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.8~~5.9
Sensor Seismic Effect (SenSE)	{{	}}$^{2(c)}$	Assumption ~~5.9~~5.5
Digital Processing Error			
Digital System Reference Accuracy (DRA)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Drift Error (DDR)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Temperature Error (DTE)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Measurement and Test Equipment Error (DME)	{{	}}$^{2(c)}$	Assumption 5.12

Total Loop Uncertainty (TLU)	{{	}}$^{2(c)}$
Units	**Inches**	**% CS**

	High Limit (Note 2)	Low Limit (Note 2)
Analytical Limit	390.00 Inches	350.00 Inches
Limiting Trip Setpoint (Equation 4-1)	{{ }}$^{2(c)}$ Inches	{{ }}$^{2(c)}$ Inches
Nominal Trip Setpoint (Equation 4-2)	{{ }}$^{2(c)}$ Inches	{{ }}$^{2(c)}$ Inches

Note 1: All levels are reported in terms of module elevation with the global zero elevation at the bottom of the reactor pool.

Table 6-21 Setpoint calculation for low RCS flow protective function

Actuation Function	**Low RCS Flow**	
Sensor	**RCS Flow**	
Engineering Units of Measurement	ft^3/s	
Upper Limit	26.19	
Lower Limit	0.00	
Calibrated Span (CS)	26.19	

Process and Miscellaneous Effects Error	**ft^3/s**	**% CS**	**Source/Reference**
Primary Element Accuracy (PEA)	0.00	0.00	
Process Measurement Error (PME)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Error			
Sensor Reference Accuracy (SRA)	{{	}}$^{2(c)}$	
Sensor Drift (SDR)	{{	}}$^{2(c)}$	Assumption ~~5.6~~5.7
Sensor Measurement and Test Equipment (SME)	{{	}}$^{2(c)}$	Assumption ~~5.7~~5.8
Sensor Calibration Accuracy (SCA)	{{	}}$^{2(c)}$	Equation 3-1
Sensor Temperature Effect (STE)	{{	}}$^{2(c)}$	Assumption 5.3
Sensor Static Pressure Effect (SPE)	{{	}}$^{2(c)}$	Assumption 5.15
Insulation Resistance Effect (IRE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.4~~5.6
Sensor Accident Effect (SAE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.8~~5.9
Sensor Seismic Effect (SenSE)	{{	}}$^{2(c)}$	Assumption ~~5.9~~5.5
Digital Processing Error			
Digital System Reference Accuracy (DRA)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Drift Error (DDR)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Temperature Error (DTE)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Measurement and Test Equipment Error (DME)	{{	}}$^{2(c)}$	Assumption 5.12

Total Loop Uncertainty (TLU)	{{	}}$^{2(c)}$
Units	**ft^3/s**	**% CS**

Analytical Limit	1.70	ft^3/s
Limiting Trip Setpoint (Equation 4-1)	{{ }}$^{2(c)}$	ft^3/s
Nominal Trip Setpoint (Equation 4-2)	{{ }}$^{2(c)}$	ft^3/s

Table 6-22 Setpoint calculation for low-low RCS flow protective function

Actuation Function	**Low-Low RCS Flow**
Sensor	**Narrow Range RCS Flow**
Engineering Units of Measurement	ft^3/s
Upper Limit	26.19
Lower Limit	0.00
Calibrated Span (CS)	26.19

Process and Miscellaneous Effects Error	**ft^3/s**	**% CS**	**Source/Reference**
Primary Element Accuracy (PEA)	0.00	0.00	
Process Measurement Error (PME)	{{	}}$^{2(c)}$	Assumption 5.10
Sensor Error			
Sensor Reference Accuracy (SRA)	{{	}}$^{2(c)}$	
Sensor Drift (SDR)	{{	}}$^{2(c)}$	Assumption ~~5.6~~5.7
Sensor Measurement and Test Equipment (SME)	{{	}}$^{2(c)}$	Assumption ~~5.7~~5.8
Sensor Calibration Accuracy (SCA)	{{	}}$^{2(c)}$	Equation 3-1
Sensor Temperature Effect (STE)	{{	}}$^{2(c)}$	Assumption 5.3
Sensor Static Pressure Effect (SPE)	{{	}}$^{2(c)}$	Assumption 5.15
Insulation Resistance Effect (IRE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.4~~5.6
Sensor Accident Effect (SAE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.8~~5.9
Sensor Seismic Effect (SenSE)	{{	}}$^{2(c)}$	Assumption ~~5.9~~5.5
Digital Processing Error			
Digital System Reference Accuracy (DRA)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Drift Error (DDR)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Temperature Error (DTE)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Measurement and Test Equipment Error (DME)	{{	}}$^{2(c)}$	Assumption 5.12

Total Loop Uncertainty (TLU)	{{	}}$^{2(c)}$
Units	**ft^3/s**	**% CS**

Analytical Limit	0.00	ft^3/s
Limiting Trip Setpoint (Equation 4-1)	{{ }}$^{2(c)}$	ft^3/s
Nominal Trip Setpoint (Equation 4-2)	{{ }}$^{2(c)}$	ft^3/s

Table 6-24 Setpoint calculation for high bioshield temperature protective function

Actuation Function	**High Under the Bioshield Temperature**
Sensor	**Under the Bioshield Temperature**
Engineering Units of Measurement	°F
Upper Limit	700
Lower Limit	40
Calibrated Span (CS)	660

Process and Miscellaneous Effects Error	**°F**	**% CS**	**Source/Reference**
Primary Element Accuracy (PEA)	{{	}}$^{2(c)}$	Section 3.1.2
Process Measurement Error (PME)	{{	}}$^{2(c)}$	Assumption 1.1
Sensor Error			
Sensor Reference Accuracy (SRA)	{{	}}$^{2(c)}$	Assumption 1.1
Sensor Drift (SDR)	{{	}}$^{2(c)}$	Assumption ~~5.6~~5.7
Sensor Measurement and Test Equipment (SME)	{{	}}$^{2(c)}$	Assumption ~~5.7~~5.8
Sensor Calibration Accuracy (SCA)	{{	}}$^{2(c)}$	Equation 3-1
Sensor Temperature Effect (STE)	{{	}}$^{2(c)}$	Assumption 5.3
Sensor Static Pressure Effect (SPE)	{{	}}$^{2(c)}$	
Insulation Resistance Effect (IRE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.4~~5.6
Sensor Accident Effect (SAE) [Bias]	{{	}}$^{2(c)}$	Assumption ~~5.8~~5.9
Sensor Seismic Effect (SenSE)	{{	}}$^{2(c)}$	Assumption ~~5.9~~5.5
Digital Processing Error			
Digital System Reference Accuracy (DRA)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Drift Error (DDR)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Temperature Error (DTE)	{{	}}$^{2(c)}$	Assumption 5.12
Digital System Measurement and Test Equipment Error (DME)	{{	}}$^{2(c)}$	Assumption 5.12

Total Loop Uncertainty (TLU)	{{	}}$^{2(c)}$
Units	**°F**	**% CS**

Analytical Limit	250.00	°F
Limiting Trip Setpoint (Equation 4-1)	{{ }}$^{2(c)}$	°F
Nominal Trip Setpoint (Equation 4-2)	{{ }}$^{2(c)}$	°F

8.0 Summary and Conclusions

This technical report described the instrument setpoint determination methodology applied to the safety-related I&C functions. The methodology ensures that the RTS and ESFAS setpoints are consistent with the assumptions made in the safety analysis and conform to the setpoint-related requirements of industry standard, Reference 9.11, which is endorsed by RG 1.105 Revision 3, and addresses the regulatory issues identified in RIS 2006-17.

Setpoints for the RTS and ESFAS have been selected to provide sufficient allowance between the trip setpoint and the safety limit to account for instrument channel uncertainties to ensure that the analytical limit applied to safety-related MPS protective actions satisfy the plant~~Chapter 15~~ safety analysis requirements.

The instrument setpoint methodology determines calibration uncertainty allowances, including as-found and as-left tolerances, used in plant surveillance tests to verify that setpoints for safety-related protective functions are within Technical Specification limits. The methodology also establishes performance and test acceptance criteria to evaluate setpoints during surveillance testing and calibration for setpoint drift.

9.14 Highly Integrated Protection System Platform Topical Report, TR-1015-18653, Revision ~~1~~2.

Enclosure 3:

Affidavit of Zackary W. Rad, AF-0617-54702

NuScale Power, LLC

AFFIDAVIT of Zackary W. Rad

I, Zackary W. Rad, state as follows:

(1) I am the Director of Regulatory Affairs of NuScale Power, LLC (NuScale), and as such, I have been specifically delegated the function of reviewing the information described in this Affidavit that NuScale seeks to have withheld from public disclosure, and am authorized to apply for its withholding on behalf of NuScale

(2) I am knowledgeable of the criteria and procedures used by NuScale in designating information as a trade secret, privileged, or as confidential commercial or financial information. This request to withhold information from public disclosure is driven by one or more of the following:

(a) The information requested to be withheld reveals distinguishing aspects of a process (or component, structure, tool, method, etc.) whose use by NuScale competitors, without a license from NuScale, would constitute a competitive economic disadvantage to NuScale.

(b) The information requested to be withheld consists of supporting data, including test data, relative to a process (or component, structure, tool, method, etc.), and the application of the data secures a competitive economic advantage, as described more fully in paragraph 3 of this Affidavit.

(c) Use by a competitor of the information requested to be withheld would reduce the competitor's expenditure of resources, or improve its competitive position, in the design, manufacture, shipment, installation, assurance of quality, or licensing of a similar product.

(d) The information requested to be withheld reveals cost or price information, production capabilities, budget levels, or commercial strategies of NuScale.

(e) The information requested to be withheld consists of patentable ideas.

(3) Public disclosure of the information sought to be withheld is likely to cause substantial harm to NuScale's competitive position and foreclose or reduce the availability of profit-making opportunities. The accompanying report reveals distinguishing aspects about the process and method by which NuScale develops its Instrument Setpoint Methodology.

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

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

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

(4) The information sought to be withheld is in the enclosed report entitled "NuScale Instrument Setpoint Methodology Technical Report".The enclosure contains the designation "Proprietary" at the top of each page containing proprietary information. The information considered by NuScale to be proprietary is identified within double braces, "{{ }}" in the document.

(5) The basis for proposing that the information be withheld is that NuScale treats the information as a trade secret, privileged, or as confidential commercial or financial information. NuScale relies

upon the exemption from disclosure set forth in the Freedom of Information Act ("FOIA"), 5 USC § 552(b)(4), as well as exemptions applicable to the NRC under 10 CFR §§ 2.390(a)(4) and 9.17(a)(4).

(6) Pursuant to the provisions set forth in 10 CFR § 2.390(b)(4), the following is provided for consideration by the Commission in determining whether the information sought to be withheld from public disclosure should be withheld:

(a) The information sought to be withheld is owned and has been held in confidence by NuScale.

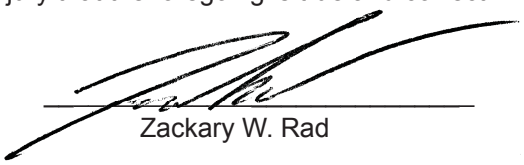
(b) The information is of a sort customarily held in confidence by NuScale and, to the best of my knowledge and belief, consistently has been held in confidence by NuScale. The procedure for approval of external release of such information typically requires review by the staff manager, project manager, chief technology officer or other equivalent authority, or the manager of the cognizant marketing function (or his delegate), for technical content, competitive effect, and determination of the accuracy of the proprietary designation. Disclosures outside NuScale are limited to regulatory bodies, customers and potential customers and their agents, suppliers, licensees, and others with a legitimate need for the information, and then only in accordance with appropriate regulatory provisions or contractual agreements to maintain confidentiality.

(c) The information is being transmitted to and received by the NRC in confidence.

(d) No public disclosure of the information has been made, and it is not available in public sources. All disclosures to third parties, including any required transmittals to NRC, have been made, or must be made, pursuant to regulatory provisions or contractual agreements that provide for maintenance of the information in confidence.

(e) Public disclosure of the information is likely to cause substantial harm to the competitive position of NuScale, taking into account the value of the information to NuScale, the amount of effort and money expended by NuScale in developing the information, and the difficulty others would have in acquiring or duplicating the information. The information sought to be withheld is part of NuScale's technology that provides NuScale with a competitive advantage over other firms in the industry. NuScale has invested significant human and financial capital in developing this technology and NuScale believes it would be difficult for others to duplicate the technology without access to the information sought to be withheld.

I declare under penalty of perjury that the foregoing is true and correct. Executed on June 29, 2017.



Zackary W. Rad

Enclosure 4:

Changes to Final Safety Analysis Report Tier 1 Section 2.5 and Tier 2 Chapter 1 and Chapter 7

Table 2.5-7: Module Protection System and Safety Display and Indication System Inspections, Tests, Analyses, and Acceptance Criteria

No.	Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
1.	The MPS design and software are implemented using a quality process composed of the following ~~software~~system design lifecycle phases, with each phase having outputs which satisfy the requirements of that phase. • System Functional Specification Phase • System Design Phase • System Prototype Development Phase • Equipment Requirements Specification Phase • Hardware Planning Phase • Hardware Requirements Phase • Hardware Design Phase • Software Planning Phase • Software Requirements Phase • Software Design Phase • Software Implementation Phase • Software Configuration Phase • System Testing Phase • System Installation Phase	i. An analysis will be performed of the output documentation of the System Functional Specification Phase. ii. An analysis will be performed of the output documentation of the System Design Phase. iii. An analysis will be performed of the output documentation of the System Prototype Development Phase. iv. An analysis will be performed of the output documentation of the Equipment Requirements Specification Phase. v. An analysis will be performed of the output documentation of the Hardware Planning Phase. vi. An analysis will be performed of the output documentation of the Hardware Requirements Phase. vii. An analysis will be performed of the output documentation of the Hardware Design Phase. viii. An analysis will be performed of the output documentation of the Software Planning Phase. ix. An analysis will be performed of the output documentation of the Software Requirements Phase. x. An analysis will be performed of the output documentation of the Software Design Phase. xi. An analysis will be performed of the output documentation of the Software Implementation Phase.	i. The output documentation of the MPS Functional Specification Phase satisfies the requirements of the System Functional Specification Phase. ii. The output documentation of the MPS Design Phase satisfies the requirements of the System Design Phase. iii. The output documentation of the MPS Prototype Development Phase satisfies the requirements of the System Prototype Development Phase. iv. The output documentation of the MPS Equipment Requirements Specification Phase satisfies the requirements of the Equipment Requirements Specification Phase. v. The output documentation of the MPS Hardware Planning Phase satisfies the requirements of the Hardware Planning Phase. vi. The output documentation of the MPS Hardware Requirements Phase satisfies the requirements of the Hardware Requirements Phase. vii. The output documentation of the MPS Hardware Design Phase satisfies the requirements of the Hardware Design Phase. viii. The output documentation of the MPS Software Planning Phase satisfies the requirements of the Software Planning Phase. ix. The output documentation of the MPS Software Requirements Phase satisfies the requirements of the Software Requirements Phase. x. The output documentation of the MPS Software Design Phase satisfies the requirements of the Software Design Phase. xi. The output documentation of the MPS Software Implementation Phase satisfies the requirements of the Software Implementation Phase.

Table 1.9-2: Conformance with Regulatory Guides (Continued)

RG	Division Title	Rev.	Conformance Status	COL Applicability	Comments	Section
1.101	Emergency Response Planning and Preparedness for Nuclear Power Reactors	5	Not Applicable	Applicable	This RG is limited to providing emergency response guidance for co-located licensees. As such, this RG is the responsibility of the COL applicant proposing to site a power plant such that the definition of co-located is met. Since RG 1.101, Revision 4, is the most current revision that endorses NUREG-0654/FEMA-REP-1, Revision 1, Revision 4 of RG 1.101 is applicable to the extent that it endorses (through NUREG-06554/FEMA-REP-1) the design-specific aspects of NUREG-0696.	Not Applicable
1.102	Flood Protection for Nuclear Power Plants	1	Not Applicable	Not Applicable	The design assumes the NPP is located above the maximum flood height (including wind induced wave run-up).	2.4 3.4
1.105	Setpoints for Safety-Related Instrumentation	3	Partially Conforms	Applicable	Chapter 15 analyses utilize the safety-related setpoints described in Chapter 7. This RG endorses ISA-67.04.01-1994, however, the NuScale Instrument Setpoint Methodology Technical Report (TR-0616-49121) applies the guidance contained in ISA-67.04.01-2006. A key difference is that the 1994 version of ISA-67.04.01 uses an allowable value to determine instrument channel operability during surveillance testing and calibration. The 2006 version of ISA-67.04.01 provides updated guidance for evaluating instrument channel operability based on the comparison of the as-found to the as-left value from the previous instrument calibration for the instrument setpoint.	7.2 15.1 15.2 15.4 15.5 15.6 15.7
1.106	Thermal Overload Protection for Electric Motors on Motor-Operated Valves	2	Not Applicable	Not Applicable	This RG governs the application of thermal overload protection devices to ensure that safety-related motor-operated valves perform their safety function. The design does not use safety-related motor operated valves.	Not Applicable

7.0.1 Regulatory Requirements

Table 7.0-1 provides a cross-reference of regulatory requirements, guidance, and industry standards with the Chapter 7 subsections in which the requirements and guidance are specifically addressed.

7.0.2 Instrumentation and Control System Classification

NuScale I&C structures, systems, and components are classified in accordance with the classification criteria described in Section 3.2. The I&C systems classified as safety-related are the MPS and the NMS. The remaining NuScale I&C systems (e.g., PPS, SDIS, MCS, PCS, ICIS, HPN and RM) are classified as nonsafety-related.

7.0.3 System Architecture

The architectural design of I&C systems is based on providing clear interconnection interfaces for plant I&C structures, systems, and components. Each NuScale Power Module (NPM) has a safety-related MPS and NMS, and a nonsafety-related MCS and ICIS. One nonsafety-related PPS, SDIS, PCS, HPN and RM serve the non-NPM-specific plant systems.

A simplified block diagram of the overall I&C system architecture is provided in Figure 7.0-1. The classification of I&C systems is also depicted in Figure 7.0-1.

More detail of the architectural design is provided in Section 7.1 and Section 7.2.

7.0.4 System Descriptions

7.0.4.1 Module Protection System

The primary purpose of the MPS is to monitor process ~~parameters~~variables and provide automatic initiating signals in response to out-of-normal conditions, providing protection against unsafe NPM operation during steady state and transient power operation. There is one MPS for each NPM. The two major functions that the MPS performs are:

- monitors plant ~~parameters~~variables and trips the reactor when specified setpoints, which are based on the plant safety analysis analytical limits described in Chapter 15, are reached or exceeded during anticipated operational occurrences. The NPM reactor trip functions for the reactor trip system (RTS) are listed in Table 7.1-3
- monitors plant ~~parameters~~variables and actuates engineered safety features actuation system (ESFAS) equipment when specified setpoints, which are based on the plant safety analysis analytical limits described in chapter 15, are reached or exceeded during anticipated operational occurrences. Actuation of ESFAS equipment prevents or mitigates damage to the reactor core and reactor coolant system components and ensures containment integrity. The ESFAS functions are summarized in Table 7.1-4

The MPS also transmits status and information signals to the nonsafety-related MCS, maintenance workstation (MWS), and SDIS, and performs monitoring for post-accident monitoring (PAM) functionality.

The MPS is built on the highly integrated protection system platform (Reference 7.0-3), which is a field programmable gate array (FPGA)-based system. The MPS incorporates the fundamental I&C design principles of independence, redundancy, predictability and repeatability, and diversity and defense-in-depth as used by TR-1015-18653 (Reference 7.0-3).

The MPS includes the following safety-related (except where noted otherwise) elements:

- separation group sensor electronics and input panels
- four separation groups of signal conditioning
- four separation groups of trip determination
- division power distribution panels
- Class 1E components to provide isolation from the nonsafety-related highly reliable DC power system (EDSS) power supply
- power supplies for sensors and MPS components, which also provide isolation from the nonsafety-related EDSS
- eight voltage sensors for detecting loss of 480 VAC to the EDSS battery chargers
- four reactor trip breakers
- four pressurizer heater trip breakers
- two nonsafety-related MWSs
- two nonsafety-related MPS gateways
- three 24-hour timers per division for PAM-only mode
- two divisions of RTS voting and actuation equipment (see Section 7.0.4.1.2)
- two divisions of ESFAS voting and actuation equipment (see Section 7.0.4.1.3)
- reactor trip breakers and associated cabling
- pressurizer heater trip breakers and associated cabling
- low voltage AC electrical distribution system (ELVS) 480 VAC bus voltage sensors and associated cabling for input to the MPS

The MPS boundary extends from the output connections of the sensors and detectors to the input connections of the actuated components as shown in Figure 7.0-2.

7.0.4.1.1 Safety Function Modules

The safety function module (SFM) signal conditioning receives inputs from the process sensors and detectors to measure the process ~~parameters~~variables as shown in Figure 7.0-3. The interconnections of the process sensors and detectors to the signal conditioning block are dedicated copper wires and are routed according to the separation group with which they are associated. Loop power supplies are provided where needed based on the sensor requirements.

updates for each safety function. The safety function must be out of service and a temporary cable from the MWS to the MIB communication module is required to allow changing parameters or calibration of a channel. An MWS can only access one separation group at a time using a temporary cable. For additional information on access controls of the MWS see Section 7.2.9.1.

An MIB communication module is included for each separation group and each division. A divisional MIB communication module only serves the function of monitoring and indication as there is no calibration available for the divisional RTS and ESFAS.

7.0.4.1.2 Reactor Trip System

The RTS uses four redundant trip determination signals, one from each separation group, to complete the logic decisions necessary to automatically open the reactor trip breakers as shown in Figure 7.0-3. The analytical limits for the RTS are listed in Table 7.1-3.

When an RTS parameter exceeds a predetermined limit as defined by the NuScale Power, LLC, TR-616-49121, "NuScale Instrument Setpoint Methodology Technical Report," (Reference 7.0-4). The SFM for each separation group generates a trip signal that is sent through an SBM to an SVM in both RTS divisions. The SVM performs two-out-of-four coincident logic voting on the trip determination status. If two or more trip determination signals generate a reactor trip, a trip signal is generated in the SVM and sent to the associated equipment interface modules (EIM) to open the reactor trip breakers.

Each EIM in the RTS receives redundant trip signals from outputs created in the SFM and provides a trip signal based on two-out-of-three voting from the incoming signals as shown in Figure 7.0-5. Two divisions of RTS circuitry and reactor trip breakers are provided to ensure that a single failure does not cause the loss of an RTS function. The reactor trip breakers are configured in a series-parallel configuration as shown in Figure 7.0-6.

An EIM is included for each reactor trip breaker in both RTS divisions that are actuated by the MPS. Each reactor trip breaker EIM has two separate logic paths. The primary coil is connected to the undervoltage trip circuit and the secondary coil is connected to the shunt trip circuit for each reactor trip breaker. Each RTS division controls one reactor trip breaker in each parallel path. This configuration allows for either division to accomplish a reactor trip. ~~When a reactor trip signal is generated in the SVM, the under-voltage trip circuit is de-energized, and the shunt trip circuit is energized. Either action causes all four reactor trip breakers to open. Power is then interrupted from the control rod drive power supply and the control rods are inserted into the core by gravity.~~When a reactor trip signal is generated, the EIM outputs to the undervoltage and shunt trip circuits are de-energized, causing the undervoltage coils and the shunt trip relays to de-energize. When the shunt trip relays drop out, the shunt trip coils are energized with power from EDSS-MS. Either action causes the reactor trip breakers to open. The shunt trip circuit and coil are provided as a nonsafety-related, diverse means to open the reactor trip breakers for increased reliability should de-energization of the

undervoltage coil fail to cause a reactor trip breaker to open, and nonsafety-related electrical power from EDSS-MS is still available. Power from the control rod drive power supply is then interrupted and the control rods are inserted into the core by gravity. The undervoltage and shunt trip circuits are shown in Figure 7.1-1ad through Figure 7.1-1ae and Figure 7.1-1ak through Figure 7.1-1al for the Division I and II reactor trip breakers, respectively.

The RTS also provides manual trip capability. Manual switches in the main control room (MCR) allow the operator to manually initiate a reactor trip. Two manual switches, one per division, are provided to manually initiate a reactor trip. The manual switches are input into the actuation and priority logic (APL) associated with the reactor trip system EIM via the hard-wired module (HWM).

The APL accepts commands from three sources:

- digital trip signal from the SFM
- non-digital manual trip signal from its associated RTS division
- non-digital manual control signals from the MCS

The non-digital signals are diverse from the digital portion of the MPS. Discrete logic is used by the APL for actuating a single device based on the highest priority. Regardless of the state of the digital system, manual initiation can always be performed at the division level. If the enable nonsafety control permissive is active and there are no automatic or manual actuation signals present, the MCS is capable of operating the reactor trip breaker.

The result from the APL is used to actuate equipment connected to the EIM. Reactor trip breaker status is transmitted to the EIM. Breaker status information is sent to the MIB, along with the status of the SDB signals.

7.0.4.1.3 Engineered Safety Feature Actuation System

The ESFAS uses four redundant actuation determination signals, one from each separation group, to complete the logic decisions necessary to automatically initiate the operation of necessary engineered safety features (ESFs) as shown in Figure 7.0-3. The analytical limits for the ESFAS are listed in Table 7.1-4.

When an ESFAS parameter exceeds a predetermined limit, the SFM for each separation group generates an actuation signal that is sent through an SBM to the SVM in both ESFAS divisions. The SVM performs two-out-of-four coincident logic voting on the trip determination status. If two or more actuation signals generate an actuation of an ESF system, an actuation signal is generated in the SVM. The signal is then sent to the associated EIMs to de-energize the solenoids of the associated ESF system or open the breakers of the associated ESF system.

An EIM is included in each division for each ESF component actuated by the MPS. Each EIM has two separate logic paths to allow for connection to separate ESF components. Each component is connected to two separate EIMs, resulting in two EIMs providing redundant control to each component as shown in Figure 7.0-7.

This allows an EIM to be taken out of service and replaced online without actuating the connected equipment.

When an ESFAS actuation signal is generated in the SVM, all four switching outputs from the EIM open, as shown in Figure 7.0-8, power is interrupted to the component solenoids, the solenoids are de-energized, and the components change state to their de-energized position. ~~For the pressurizer heater, the under-voltage trip circuit is de-energized, and the shunt trip circuit is energized. Either action causes all four breakers to open. Power is then removed from the pressurizer heaters.~~For the pressurizer heater trip breakers, the EIM outputs to the undervoltage trip and shunt trip circuits are de-energized, causing the undervoltage coils and the shunt trip relays to de-energize. When the shunt trip relays drop out, the shunt trip coils are energized with power from EDSS-MS. Either action causes pressurizer heater trip breakers to open. The shunt trip circuit and coil are provided as a nonsafety-related, diverse means to open the pressurizer heater trip breakers for increased reliability should de-energization of the undervoltage coil fail to cause a pressurizer heater trip breaker to open, and nonsafety-related electrical power from EDSS-MS is still available. Power is then removed from the pressurizer heaters. The undervoltage and shunt trip circuits are shown in Figure 7.1-1af through Figure 7.1-1ag and Figure 7.1-1am through Figure 7.1-1an for the proportional and backup pressurizer heater trip breakers, respectively.

Similarly to the reactor trip breakers, only one division of pressurizer heater breakers is required to trip to remove power to heaters. The pressurizer heater breakers are configured as two separate series connections as shown in Figure 7.0-9.

The ESFAS also provides manual actuation capability. Manual switches in the MCR allow the operator to manually initiate an ESF function. Two manual switches, one per division, are provided to manually initiate each ESF function. These manual switches are inputs into the APL associated with the engineering safety features actuation system EIM via the HWM.

The APL accepts commands from three sources:

- digital trip signal from the SFM
- non-digital manual trip signal from its own ESFAS division
- non-digital manual control signals from the MCS

The non-digital signals are diverse from the digital portion of the MPS. Discrete logic is used by the APL for actuating a single component based on the highest priority. Regardless of the state of the digital system, manual initiation always can be performed at the division level. If the enable nonsafety-related control permissive is active and there are no automatic or manual actuation signals present, the MCS is capable of controlling the ESF components.

An NMS-excore sub-system includes the following components for each NPM:

- four wide-range ex-core detectors functioning over the source, intermediate, and power ranges distinguished by processing electronics
- four pre-amplifiers
- NMS-excore cabinets with electronics needed to monitor flux levels from reactor shutdown to 200% full-rated power
- associated cabling
- Class 1E components to provide isolation from the nonsafety-related EDSS power supply

The NMS-excore detectors are qualified to Seismic Category I and located within the operation bays of the Reactor Building (RXB). They are placed outside the containment vessel. The NMS-excore detectors are installed in support mechanisms that are connected to the NPM operating bay structure. During operation, the support mechanisms are positioned to place the NMS-excore detectors just outside the containment vessel to monitor neutron flux leakage from the reactor which is directly proportional to reactor power level.

To support NPM movement, the NMS-excore detector support mechanisms are retracted to reposition the NMS-excore detectors away from the containment vessel to allow for NPM movement.

The NMS-excore signal processing cabinets are located in the RXB. Separation Group A and C cabinets are located in the MPS equipment rooms on the 75'0" elevation of the RXB (see ~~Figure 1.2-13~~Figure 1.2-14). The NMS-excore separation group B and D equipment is located in the MPS equipment rooms on the 86' elevation of the RXB (see ~~Figure 1.2-14~~Figure 1.2-15). Figure 7.0-12 shows the NMS-excore block diagram.

7.0.4.2.2 Neutron Monitoring System-Refuel

The NMS-refuel detectors are located within the refueling bay of the plant. There is one NMS-refuel subsystem for the plant as each NPM is relocated to the refueling bay for the refueling process and only one NPM is refueled at a time. The NMS-refuel monitors neutron flux from the point of reactor pressure vessel (RPV) head lift, until the replacement of the RPV head.

The NMS-refuel subsystem includes the detector array, pre-amplifiers, NMS-refuel cabinets with electronics, and associated cabling. The NMS-refuel detectors are proportional counter source range detectors located near the core mid-plane. The detectors monitor neutron flux in counts per second over a five decade range from 10^0 to 10^5 counts per second with a 5 percent sensor accuracy.

The NMS-refuel neutron monitoring capability ensures the neutron flux level is continuously monitored during the refueling process and also provides an audible count rate to the operator with the ability to detect and alert a spurious increase in

7.0.4.3 Plant Protection System

The PPS monitors ~~parameters~~process variables at the plant level and executes actuations in response to normal and off-normal conditions. The PPS monitors and controls systems common to up to 12 NPMs. Selected variables monitored and equipment actuated by the PPS require an augmented level of quality. The PPS consists of two independent and redundant divisions. Either of the divisions is capable of accomplishing PPS functions.

The PPS is built on the highly integrated protection system platform (Reference 7.0-3) and is an FPGA-based system. Figure 7.0-13 displays the system diagram of the PPS architecture.

Division I and Division II of the PPS are located in separate rooms in the Control Building. The boundaries of the PPS extend from the output connections of the sensors and detectors to the input connections of the actuated devices. Also included in the PPS boundary are the ELVS AC voltage sensors, which are classified as part of the PPS. The nonsafety-related displays, which receive data from the PPS, are either part of the SDIS or the PCS as described in Section 7.0.4.4 and Section 7.0.4.6, respectively.

The process sensors measure different process ~~parameters~~variables, such as radiation, level, and voltage. Separate sensors supply information to the two PPS divisions. Sensors are qualified for the environmental conditions before, during, and after a design basis event. The sensors provide input to the PPS, but are classified as part of the system in which they are installed.

An individual SFM is included in each division for each function performed by the PPS. Each SFM can accept input from up to four sensors. Signal conditioning is performed to convert the sensor signals into a digital representation. With the digital signals, the SFM performs algorithms and setpoint comparisons necessary to determine if actuation is required for the function. The actuation decision is output to three separate communication buses to provide redundant communication between the SFMs and EIMs. The SFMs also provide communication outputs for parameter values, status information, and alarms to be sent to the PCS and SDIS. Diagnostic information for each SFM is also sent to the MWS.

The architecture of the PPS uses three independent data busses dedicated to actuation signals. The three communication safety data buses (SDB1, SDB2, and SDB3) are each configured in a master-slave communication protocol. The three redundant SBMs (SBM1, SBM2, and SBM3) are the masters for their associated bus and provide the redundant SDB communications from the SFM to the EIM. The SDB1, SDB2, and SDB3 are dedicated to processing the actuation signals.

The MIB communication module is independent of the three SDB communication modules and is the master of the MIB. It processes the information using the same master-slave communication protocol and interfaces with registers on the SFM, communication module, and EIM. These registers are different from the registers that are used for the actuation data path. The MIB communication module uses the MIB to communicate to the CTB communication module to update the MWS. One-way data to the PCS and SDIS are transmitted through the MIB communication module isolated

The HPN includes communications cabling and equipment mounting racks.

For more information on radiation protection, see Chapter 12.

7.0.4.9 Fixed Area Radiation Monitoring

Radiation monitoring is performed by fixed area radiation monitors and continuous air monitors throughout the plant.

The principal functions of radiation monitoring are:

- continuously monitoring in-plant radiation and airborne radioactivity as appropriate for routine and accident conditions,
- informing plant personnel immediately when predetermined exposure rates are exceeded in various areas within the plant, and
- alerting control room operators of changing plant radiation levels.

Area radiation monitors consist of a detector or detectors that are connected to an electronic control unit in local proximity. The electronic control unit interfaces with the corresponding I&C system depending on functionality. Airborne monitors are self-contained and consist of modular components that are assembled on an open frame for ease of accessibility. The detectors are connected to a local electronic control unit which interfaces with the corresponding I&C system depending on functionality. Location of area and airborne radiation monitors are provided in Section 11.5.

7.0.5 References

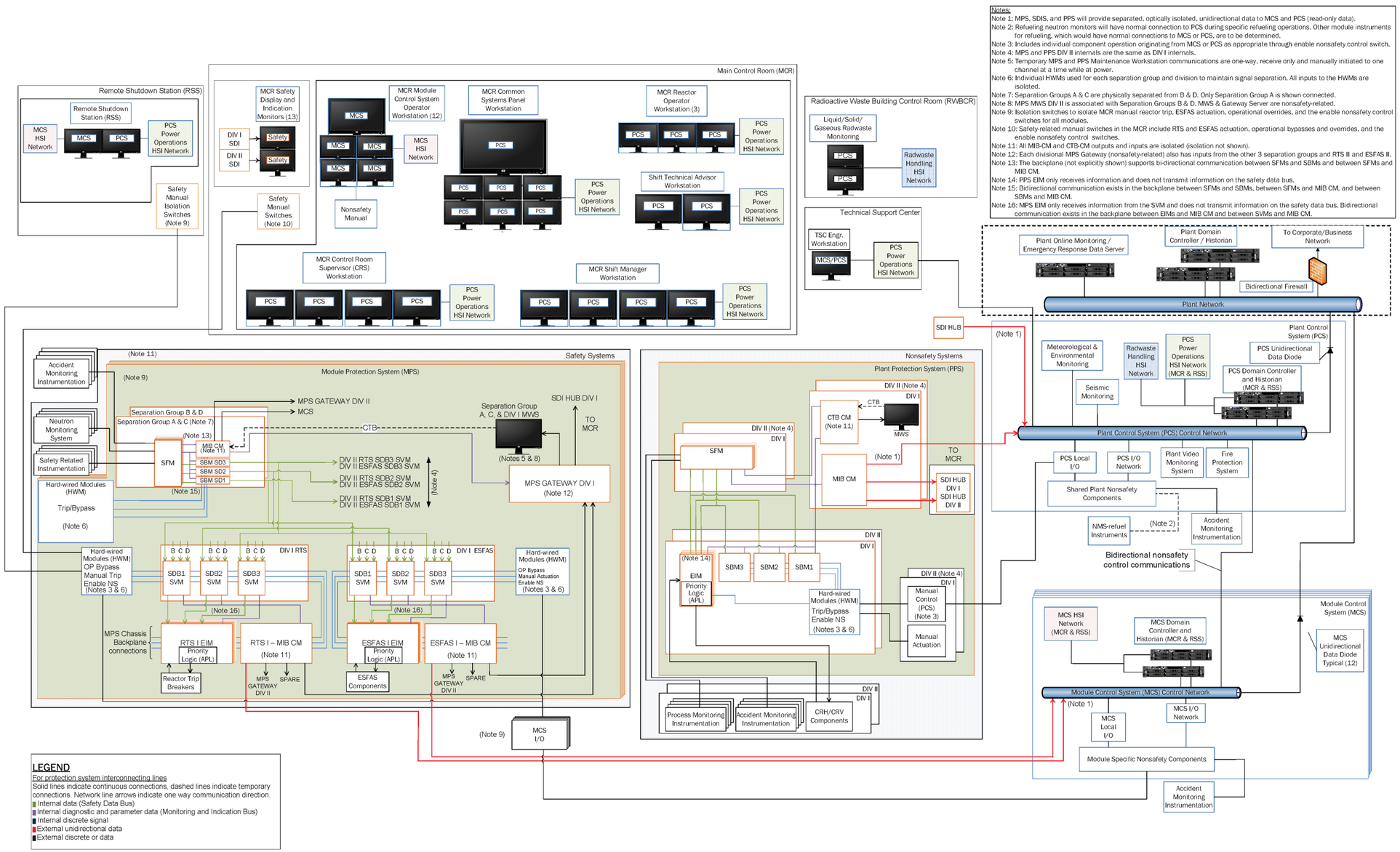
7.0-1 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Standard 603-1991, Piscataway, NJ.

7.0-2 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," IEEE Standard 7-4.3.2 - 2003, Piscataway, NJ.

7.0-3 NuScale Power, LLC, "Highly Integrated Protection System Topical Report," TR-1015-18653, Revision 2.

7.0-4 NuScale Power, LLC, "NuScale Instrument Setpoint Methodology Technical Report," TR-616-49121, Revision ~~0~~1.

Figure 7.0-1: Overall Instrumentation and Controls System Architecture Diagram



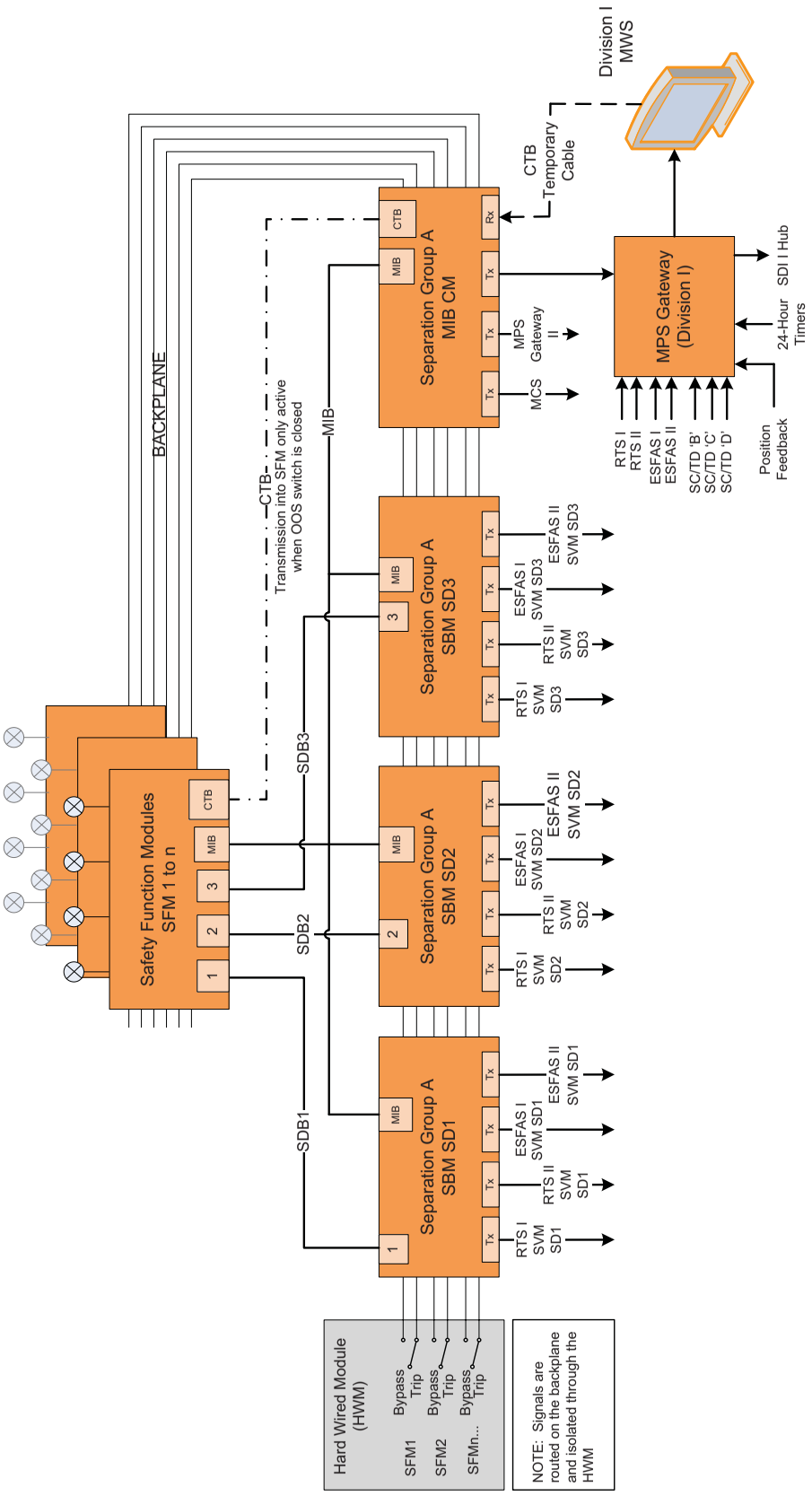


Figure 7.0-4: Separation Group A Communication Architecture

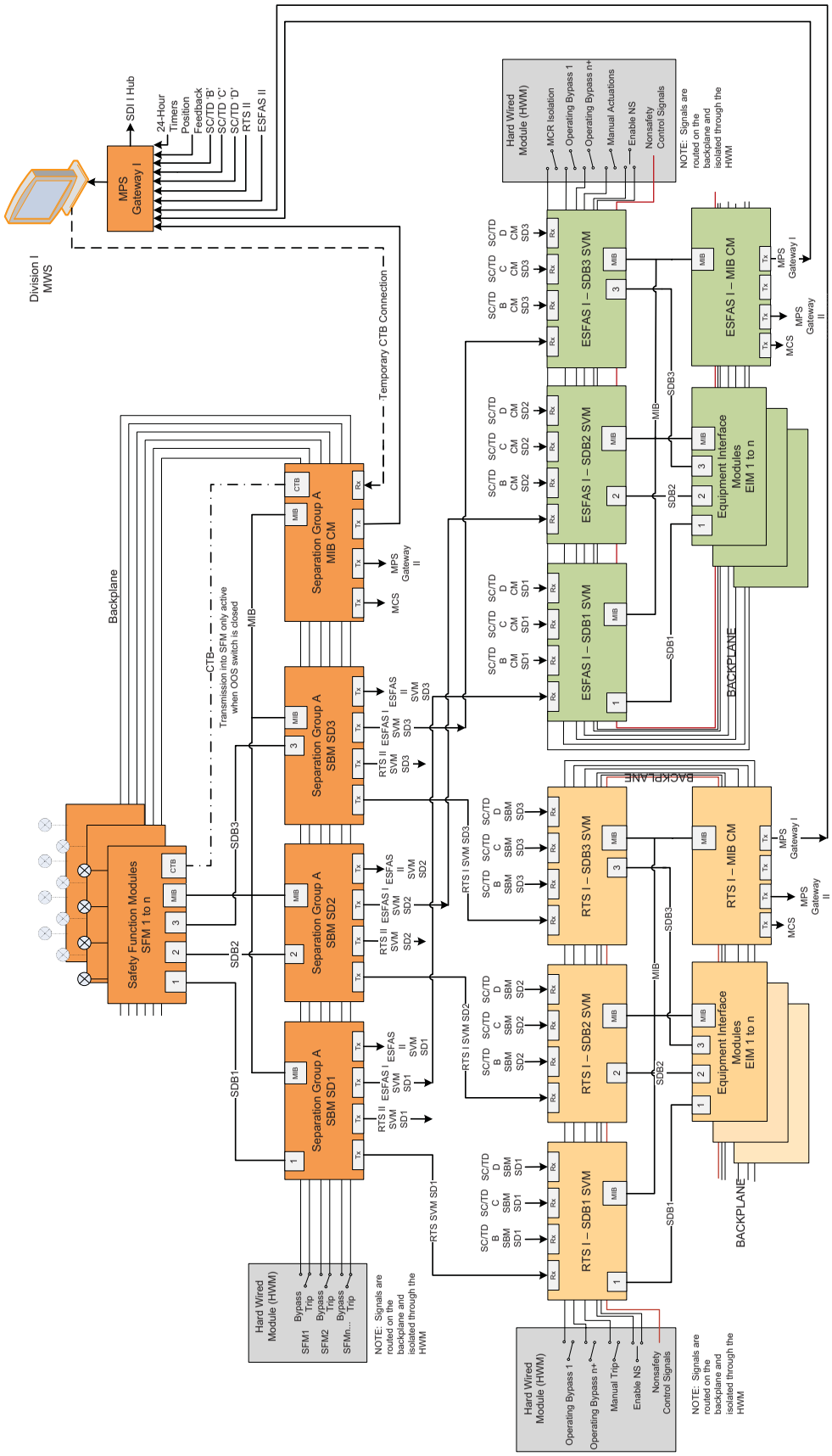


Figure 7.0-5: Separation Group A and Division I Reactor Trip System and Engineered Safety Features Actuation System Communication Architecture

Figure 7.0-10: Module Protection System Gateway Diagram

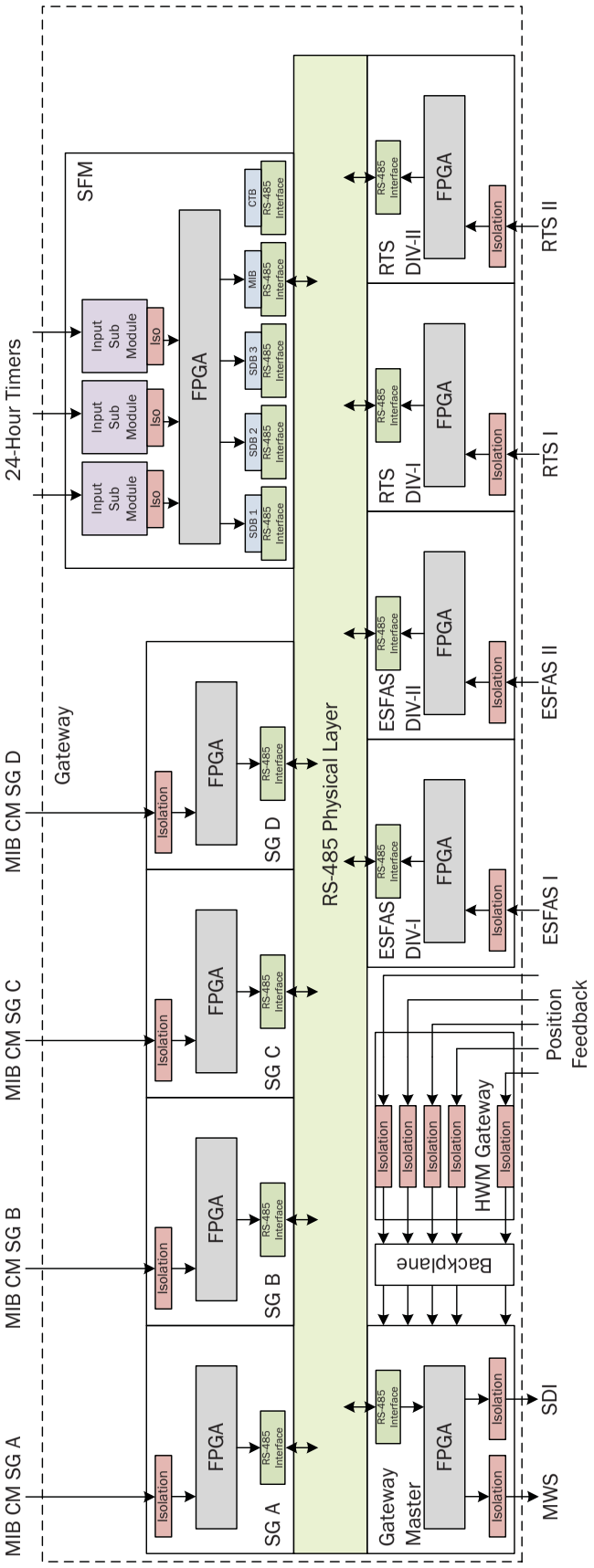


Figure 7.0-13: Plant Protection System Block Diagram

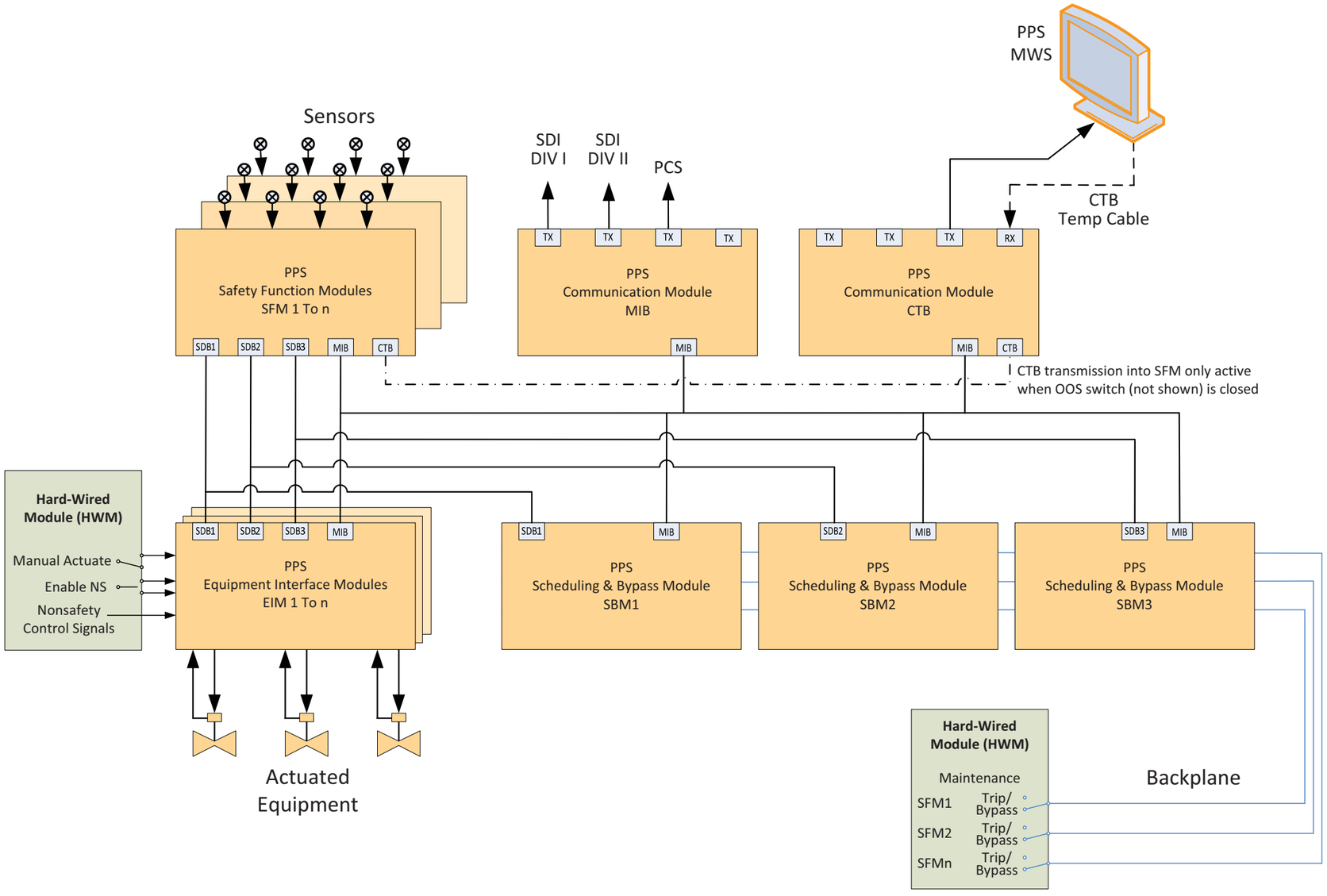
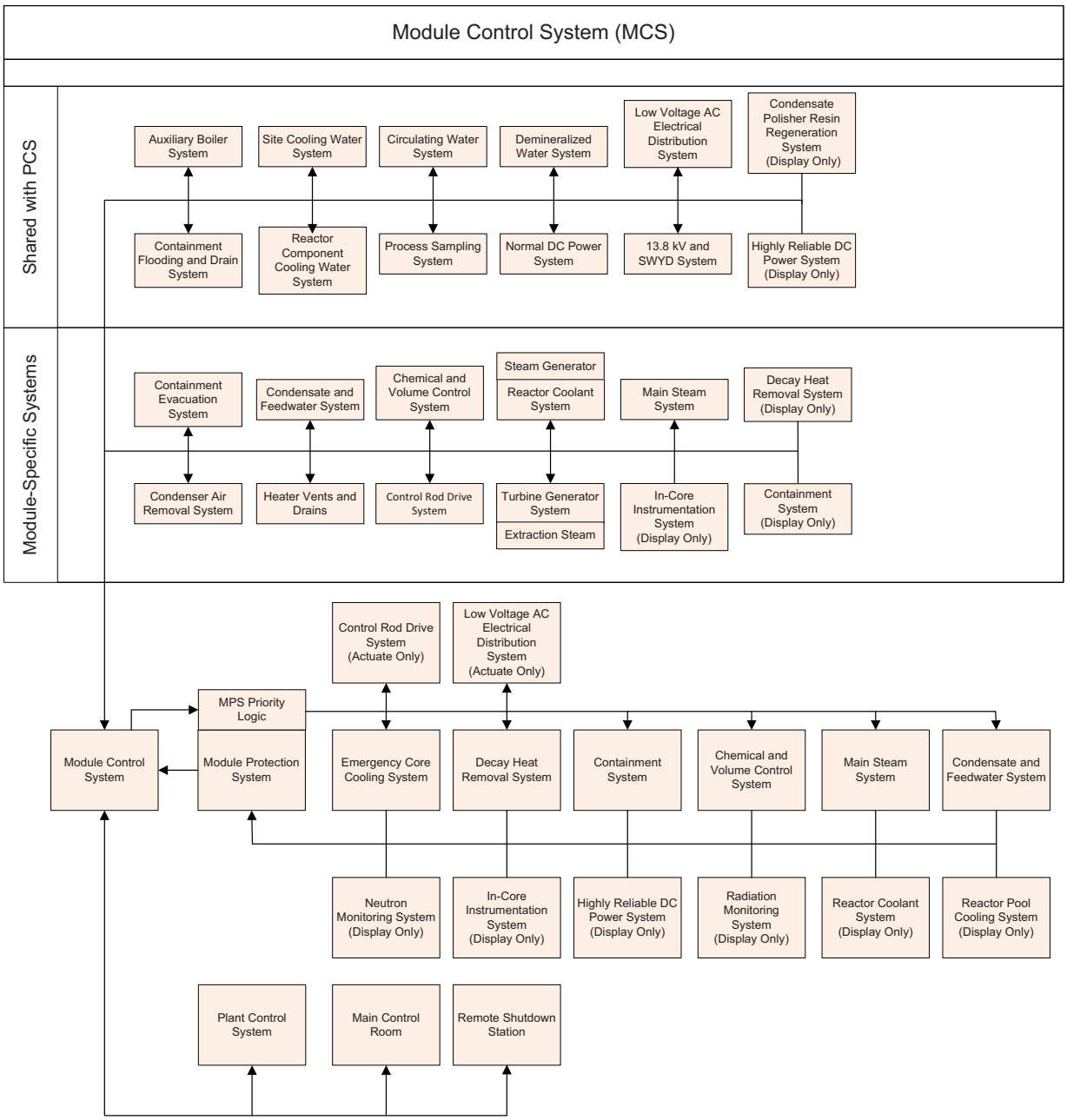


Figure 7.0-17: Module Control System Internal Functions and External Interfaces



Section 7.1.1.1

maintenance, testing, and postulated accidents, and to withstand the effects of natural phenomena.

Consistent with GDC 23, the MPS fails into a safe state upon loss of electrical power or if adverse environmental conditions are experienced.

Consistent with GDC 24, the MPS has physical, electrical, communication, and functional independence within the system and from associated nonsafety-related systems and components.

Consistent with GDC 25, the MPS initiates reactor trip functions to ensure that specified fuel design limits are not exceeded for any single malfunction of the reactivity control system. Compliance with GDC 25 is discussed in Section 4.6.2

Consistent with GDC 28, the MPS initiates reactor trip functions to limit the potential amount and rate of reactivity increase and to ensure sufficient protection from reactivity accidents. Compliance with GDC 28 is discussed in Section 4.6.2.

Consistent with GDC 29, the MPS and NMS are designed with redundancy and diversity to ensure a high probability their safety-related functions are performed in the event of AOOs.

Consistent with GDC 64, the MCS and PCS monitor radioactivity releases, the reactor containment atmosphere, and plant environments for radioactivity that may be released from normal operations, AOOs, and postulated accidents.

Consistent with 10 CFR 50.34(b)(2)(i), the design of the I&C systems and auxiliary features of the I&C system design is discussed in Section 7.0.4 and Section 7.2.8 respectively.

Consistent with 10 CFR 50.34(f)(2)(iv), the I&C systems provide the capability to display key plant ~~parameters~~variables over their anticipated ranges for normal operation, AOOs, and accident conditions.

Consistent with 10 CFR 50.34(f)(2)(v), the MCS provides bypassed and operable status indication of safety systems.

Consistent with 10 CFR 50.34(f)(2)(xi), the displays in the main control room (MCR) indicate reactor safety valve position.

Consistent with 10 CFR 50.34(f)(2)(xiv), the MPS initiates containment isolation and ensures that isolation valves do not re-open upon isolation signal reset.

Consistent with 10 CFR 50.34(f)(2)(xvii), I&C systems are designed to display appropriate variables in the MCR for monitoring specified containment ~~parameters~~variables and site radioactive gaseous effluents from potential accident releases.

Consistent with 10 CFR 50.34(f)(2)(xviii), the I&C systems provide MCR indications of inadequate core cooling.

Consistent with 10 CFR 50.34(f)(2)(xix), the I&C systems provide instrumentation for monitoring plant conditions following an accident, including potential core damage.

Consistent with 10 CFR 50.36(c)(1)(ii)(A), the MPS initiates automatic protective actions prior to exceeding a safety limit.

Consistent with 10 CFR 50.36(c)(3), the I&C systems are designed meet surveillance requirements to ensure that the necessary quality of SSC is maintained such that operation is within safety limits and limiting conditions of operations are met.

Consistent with 10 CFR 50.49, the I&C equipment that performs the functions in 10 CFR 50.49(b) will remain functional during and following design basis events (DBEs).

Consistent with 10 CFR 50.54(jj) and 10 CFR 50.55(i), I&C systems are designed, tested, and inspected to quality standards commensurate with the safety function to be performed.

Consistent with 10 CFR 50.55a(h), the MPS and NMS are designed in accordance with IEEE Std. 603-1991 (Reference 7.1-3) and the correction sheet dated January 30, 1995.

Compliance with these regulatory requirements is described in Section 7.1.6.

10 CFR 50.34(f)(2)(xii), 10 CFR 50.34(f)(2)(xx), and 10 CFR 50.34(f)(2)(xxii) are not applicable to the NuScale design, as discussed in Table 1.9-5.

7.1.1.2 Additional Design Considerations

7.1.1.2.1 Protection Systems

The protection systems are used to facilitate protective actions of the MPS (reactor trip and ESF functions) in response to monitored variables exceeding pre-established limits. Table 7.1-1 identifies the specific DBEs and classifications for which MPS protective actions are credited in Chapter 15 analyses. The DBEs, including AOOs, infrequent events (IEs), and postulated accidents for the NuScale Power Plant design are listed in Table 15.0-2. The MPS functional logic diagrams are shown in Figure 7.1-1a through Figure 7.1-1ao.

Table 7.1-2 identifies the specific NPM ~~parameters~~variables that provide input to the MPS and includes the instrument range for covering normal, abnormal and accident conditions, and the nominal operating value at 100% rated thermal power (RTP).

The NMS-excore subsystem monitors the continuous reactor neutron flux from shutdown to full-rated power across three overlapping detector ranges: the source range, intermediate range, and power range.

Certain monitored variables are relied upon to execute protective actions ~~if~~when setpoints based on the analytical limits are exceeded. The analytical limits and permissive conditions for operational bypasses are summarized in Table 7.1-3 and Table 7.1-5 for the reactor trip system (RTS) and Table 7.1-4 and Table 7.1-5 for the

engineered safety features actuation system (ESFAS). For additional information on the MPS interlocks and permissive, see Table 7.1-5. The NMS provides safety-related input to the MPS to support its functions.

The ESFAS delays assumed in the plant safety analysis are a ~~product~~combination of sensor response time, ~~signal~~MPS timing budget allocation~~processing time~~, and actuation device delays. A standard 1.0-second ~~signal~~MPS ~~processing time~~timing budget allocation is applied for all ESFAS signals. A 1.0-second ~~delay~~MPS timing budget allocation is also added to the RTS signal ~~which~~that includes reactor trip breaker response time and control rod delatch time. ~~Additional~~The sensor response delays are defined in Table 7.1-6. The delay times in Table 7.1-6 associated with ESFAS signals don't include the delay times associated with the actuation device (e.g. valve stroke times) with the exception of opening the pressurizer heater breakers.

There are manual trip or actuate switches for each automatic trip or actuate function in the MCR. These switches are connected to the hard-wired modules (HWMs) in the RTS and ESFAS chassis where the signals are isolated and converted to logic-level signals and placed on the backplane. These signals are provided to the associated equipment interface module (EIM) actuation priority logic circuits downstream of the field programmable gate array (FPGA) programmable logic.

All of the variables monitored by the MPS listed in Table 7.1-2 are sent to the safety display and indication system (SDIS) and the MCS to be displayed in the MCR as required by those systems. These ~~parameters~~variables include all that are needed for reactor trip and ESF actuations, and post-accident monitoring (PAM) variables that would be required for monitoring after an event. When allowed by plant procedures to reconfigure systems after a reactor trip or an ESF actuation, the components can be repositioned using the nonsafety-related MCS when the enable nonsafety control switch is activated and no automatic or manual safety actuation signal is present.

All required protective actions by the MPS are automatic. There are no credited manual actuations required for the MPS to accomplish its safety functions; however, manual initiation at the division level of the automatically initiated protective actions is provided in the MCR. The MCR environmental conditions during manual operation are described in Section 9.4.1.

Each MPS and NMS variable used to initiate a protective action is monitored by four independent separation groups, with one or more sensors in each separation group. The separation of redundant sensors creates a potential for spatial dependence for some variables as discussed below.

The physical separation of redundant MPS pressure and level sensors is not a spatial dependence concern. Pressure and level are distributed within the vessel or pipe so that redundant sensors do not see varying process conditions as a function of location.

The control room habitability systems are designed to allow continuous occupancy in the MCR during radiation, hazardous chemical, or hazardous gas release. In addition, the MCR is protected in case of a security event.

Despite these considerations, events for the RSS design and licensing basis include:

- smoke due to fire in the MCR
- impact of a commercial aircraft into the Control Building
- loss of the Control Building as part of loss of a large area

At the onset of an MCR evacuation, the operators trip the reactors and initiate decay heat removal and containment isolation for each reactor prior to leaving the MCR. Following evacuation of the MCR, the ability to isolate the MPS manual switches to prevent spurious actuations is provided in the RSS as described in Section 7.2.12. An alarm is annunciated in the MCR when the MCR hard-wired switches are isolated using the MCR isolation switches in the RSS, see Figure 7.1-1j.

The MPS manual isolation switches are mounted in a Seismic Class I enclosure to allow them to remain functional following an earthquake. The MCS equipment in the RSS provides an independent alternative shutdown capability that is physically and electrically separate from the controls in the MCR. The MCS equipment in the RSS provides nonsafety-related human-system interface (HSI) and direct readings of the process variables necessary to monitor safe shutdown of each NPM. Figure 1.2-16 shows the location of the RSS equipment.

The alternative shutdown capability is independent of specific fire areas and accommodates post-fire conditions when offsite power is available and when offsite power is not available for 72 hours, dependent on the conditions described in the fire hazards analysis as described in Section 9.0.

The controls necessary for the operator to monitor the plant status of an immediate hot shutdown of the reactor, maintain the unit in a safe condition during hot shutdown, and perform subsequent cold shutdown of the unit are provided in the RSS.

Access to the RSS is under administrative controls~~, as described in Section 7.2.9~~.

7.1.1.2.4 Safety Display and Indication System

The safety display and indication system (SDIS) as described in Section 7.0.4.4, provides HSI for the MPS and PPS to monitor and display PAM variables, and provides the capability for control inputs and status information. The SDIS is a nonsafety-related, nonrisk-significant system; however, because it supports the PAM function, the SDIS meets augmented quality and regulatory requirements as described in Table 3.2-1.

The physical and electrical independence attributes of the MPS and NMS meet the guidance in RG 1.75 Rev.3, which endorses IEEE Std. 384-1992 (Reference 7.1-14).

The communication independence attributes of the MPS meet the guidance in RG 1.152, which endorses IEEE Std. 7-4.3.2-2003 (Reference 7.1-5).

This information satisfies the application specific information in the NuScale Power, LLC, TR-1015-18653, "Design of the Highly Integrated Protection System Platform Topical Report," (Reference 7.1-1) listed in Table 7.0-2 for IEEE-603-1991, Sections 5.6 and 8 (Reference 7.1-3); IEEE-7-4.3.2-2003, Section 5.6 (Reference 7.1-5); and ISG-04, Section 1, Staff Positions 1, 2, 3, 8, 16, 18, and Section 3, Staff Positions 2 and 3 (Reference 7.1-6).

7.1.2.1 Physical Independence

The MPS structures, systems, and components that comprise a separation group or division are independent and physically separated to retain the capability of performing required safety functions during and following a DBE.

Separation group and division independence is maintained throughout the system, extending from the sensor to the devices actuating the protective function. Physical separation is used to achieve separation of redundant sensors. Wiring for redundant divisions uses physical separation and isolation to provide independence of the circuits. Separation of wiring is achieved using separate wireways and cable trays. Separate power feeds energize redundant protection divisions. The MPS Separation Groups A, C, and Division I equipment are located in rooms on the 75'-0" elevation of the Reactor Building (RB) and Separation Groups B, D, and Division II equipment are located on the 86'-0" elevation (see ~~Figure 1.2-13 and Figure 1.2-14,~~Figure 1.2-14 and Figure 1.2-15, respectively). The MPS equipment rooms are seismically qualified and located in separate fire zones. The rooms containing Separation Group A and C (Division I) MPS and NMS equipment are in a separate fire zone from the MPS equipment rooms containing Separation Group B and D (Division II) MPS and NMS equipment.

The NMS separation groups are physically independent and separate. The NMS-excore neutron detectors are installed 90 degrees equidistant around the NPM, and the associated cabling is routed in physically separate cable trays and raceways. The NMS hardware and signal processing equipment associated with the MPS divisions is installed in separate, seismically qualified equipment rooms. The NMS Separation Group A and C signal processing equipment is located in the MPS Separation Group A and C (Division I) equipment rooms on the 75'-0" elevation of the RB, and NMS Separation Group B and D signal processing equipment is located in the MPS Separation Groups B and D (Division II) equipment rooms on the 86'-0" elevation of the RB (see ~~Figure 1.2-13 and Figure 1.2-14,~~Figure 1.2-14 and Figure 1.2-15, respectively).

The SDIS has two separate and independent hubs. The SDIS hubs are located in the seismically qualified Control Building (CRB) at the 50' level in the same divisionally separate rooms as the PPS.

Safety-related and nonsafety-related SSC are physically separated in accordance with NuScale electrical design guidelines and meet the criteria established in

IEEE Std. 384-1992 (Reference 7.1-14), which is endorsed by RG 1.75. See Section 8.3 for additional details on the design and routing of nonsafety-related cabling.

7.1.2.2 Electrical Independence

The MPS electrical isolation devices used as a safety system boundary are considered part of the MPS and are qualified as part of the MPS in accordance with IEEE Std. 384-1992 (Reference 7.1-14). The isolation devices are tested to confirm that credible failures on the nonsafety side of the isolation device do not prevent the associated safety system channel from meeting the minimum performance requirements.

Electrical isolation between the safety-related MPS and associated nonsafety-related systems is provided by the following devices (see Figure 7.0-2):

- Nonsafety-related sensor inputs. The safety function module (SFM) provides Class 1E isolation by galvanic isolation between the nonsafety sensors inputs to the MPS. For additional information, see Section 4.2 of the NuScale Power, LLC, TR-1015-18653, "Design of the Highly Integrated Protection System Platform Topical Report," (Reference 7.1-1).
- Safety-related to nonsafety-related communication interface. Communication to nonsafety-related systems is provided through transmit-only or receive-only fiber optic ports. These ports provide Class 1E electrical isolation for either receive or transmit data through uni-directional communication links. The monitoring and indication bus (MIB) communications module provides Class 1E isolation from the safety-related MPS to nonsafety-related MCS by using four copper-to-fiber optic ports on the device. Three of the copper to fiber data ports for the MIB communications module in the separation groups and the RTS and ESFAS Divisions are configured for transmit only and send information to the MCS, the Division I MPS gateway, and the Division II MPS gateway. The remaining copper-to-fiber data port on the separation group MIB communications module is configured as receive only and receives information from the maintenance workstation (MWS) through a temporary cable that is connected during maintenance activities. ~~The MPS gateway provides Class 1E isolation from the safety-related MPS to the nonsafety-related SDIS hubs by using copper-to-fiber optic ports on the MPS gateway.~~
- Hard-wired inputs to MPS. The HWM receives signals from the manual switches in the MCR; from the discrete, hard-wired nonsafety-related control signals from MCS; and from the trip/bypass switch panels. The HWM is constructed of discrete logic components only; there are no programmable devices. The HWM provides direct current (DC)-to-DC and galvanic isolation between the safety-related MPS and nonsafety-related MCS.
- Electrical power supply. The MPS receives electrical power from the nonsafety-related highly reliable DC power system (EDSS). The MPS provides Class 1E isolation from the nonsafety-related EDSS by using Class 1E isolation devices that are part of the MPS and are used as the safety system boundary (see Figure 7.0-2). The DC-to-DC voltage converters are used for Class 1E isolation and protection of the MPS equipment. The DC power sources are redundant and an alarm is generated if one of the redundant supplies fails (see Figures 7.0-11a and 7.0-11b).

device failure. In addition, redundant process system components are segregated onto alternate I/O modules to ensure that MCS and PCS component-level failures do not impact redundant process equipment.

Redundancy is incorporated into the RSS by providing redundant MCS and PCS operator workstations for plant monitoring when the MCR is evacuated. When the operators evacuate the MCR and occupy the RSS, two manual isolation switches for the MPS divisions are provided to isolate the MPS manual actuation switches in the MCR to prevent fires in the MCR from causing spurious actuations of associated equipment.

The PPS consists of two independent and redundant divisions. A single failure within either division does not prevent the PPS from performing required protection functions. The PPS failure modes and effects analysis also considered the effects of cascaded failures expected as a consequence of a single failure. Either of the PPS divisions is capable of accomplishing the PPS functions.

The SDIS receives inputs from the MPS and PPS through communication interface modules. The SDIS consists of two independent divisions of data paths to the display panels. A single failure within either division does not prevent the SDIS from performing required functions. Either of the SDIS divisions is capable of accomplishing the SDIS function.

7.1.4 Predictability and Repeatability

The predictability and repeatability design principles for the NuScale I&C systems are designed and meet the criteria for system integrity in IEEE Std. 603-1991, Section 5.5 (Reference 7.1-3) and GDC 13, 21, and 29 as described in this section. This information satisfies the application specific information in the NuScale Power, LLC, TR-1015-18653, "Design of the Highly Integrated Protection System Platform Topical Report," (Reference 7.1-1) listed in Table 7.0-2 for IEEE-603-1991, Sections 5.5 and 5.15 (Reference 7.1-3); IEEE-7-4.3.2-2003, Section 5.5 and 5.15 (Reference 7.1-5); and ISG-04, Section 1, Staff Positions 5, 19, and 20 (Reference 7.1-6).

The MPS architecture uses the HIPS platform. This platform is designed to produce the same outputs for a given set of input signals within well-defined response time limits to allow timely completion of credited actions. The NuScale Power, LLC, TR-1015-18653, "Design of the Highly Integrated Protection System Platform Topical Report," (Reference 7.1-1) Section 7.0 describes how the platform and components function, and provides functional block diagrams to demonstrate how it meets the criteria for predictability and repeatability.

The MPS response time analysis demonstrates that the MPS performs and completes its required safety functions in a predictable and repeatable manner. The NuScale Power, LLC, TR-1015-18653, "Design of the Highly Integrated Protection System Platform Topical Report," (Reference 7.1-1) Section 7.7 describes the calculation used to determine worst-case digital time response for an MPS channel.

The actuation delays assumed in the plant safety analysis are listed in Table 7.1-6. The RTS timing analysis is defined from the point in time when the monitoring process variable exceeds its predetermined setpoint to when the control rods fall into the reactor core. The

MPS digital portion of the RTS function is allocated a timing budget in the safety analysis of 1.0 second. ~~For this portion of the RTS, protective actuation function is defined from the sensor input to the SFM input terminals, to the opening of the RTBs, which includes the control rod de-latch time.~~ For the RTS protective function, the MPS time allocation response time budget is comprised of the analog input delay plus the digital time response delay plus the analog output delay and includes the reactor trip breaker cycle time and CRDM delatch time. The MPS digital time response delay is described in section 7.7 of NuScale Power, LLC, TR-1015-18653, "Design of the Highly Integrated Protection System Platform Topical Report," (Reference 7.1-1).The MPS is designed to complete this function in less than or equal to 1.0 second.

For the ESFAS protective functions, the actuation delays in Table 7.1-6 are assumed in the plant safety analysis and are defined as the time from when the monitored process variable exceeds the predetermined setpoint until the actuation signal is received at the component (e.g., valve solenoid). The MPS ~~digital~~ portion of the ESFAS functions is allocated a timing budget in the safety analysis of 1.0 second. This time allocation ~~is~~budget is comprised of the analog input delay plus the digital time response delay plus the analog output delay and is defined from the sensor input to the ~~separation groups~~SFM input terminals to the EIM ~~outputs.~~output command to the final actuation device. ~~The MPS is designed to complete this function in less than or equal to 1.0 second.~~ For the pressurizer heater trip function, this time requirement includes the time for the pressurizer heater trip breakers to open. The MPS is designed to complete the pressurizer heater trip function in less than or equal to 1.0 second.

7.1.5 Diversity and Defense-in-Depth

The NuScale I&C system design includes features and processes to mitigate a common cause failure (CCF) in the MPS because of digital-based failures which could disable a safety function.

The D3 assessment of the NuScale I&C design is consistent with the guidelines in NUREG/CR-6303. This assessment focused on the MPS which is the only safety-related digital I&C system. The assessment is summarized in Section 7.1.5.1.

The D3 coping analysis methodology and results for postulated digital-based CCF vulnerabilities are summarized in Section 7.1.5.2.2. Coping strategies include identification of signals or components unaffected by the postulated CCF that can be used to perform the safety function, different functions that can provide adequate protection, or justification for taking no action based on meeting analytical acceptance criteria without diverse mitigation actuation.

Conformance to the applicable regulatory guidance from the staff requirement memorandum to SECY- 93-087 is summarized in Section 7.1.5.3. Conformance to 10 CFR 50.62, and 10 CFR 50.34(f)(2)(xiv) are summarized in Section 7.1.6. See Section 15.8 for the discussion on ATWS.

This information satisfies the application specific information in the NuScale Power, LLC, TR-1015-18653, "Design of the Highly Integrated Protection System Platform Topical Report," (Reference 7.1-1) listed in Table 7.0-2 for SRM to SECY-93-087, items 1 through 4 (Reference 7.1-7).

overview from Figure 7.0-3; however, for purposes of clarity, some communication lines from the separation groups have been removed.

Because each separation group provides a trip determination status to both divisions of RTS and ESFAS, links between both safety blocks are required. Additionally, information from the safety block is provided to the SDIS blocks.

The safety-related manual controls within the manual controls blocks provide division-level initiation of safety-related components; however, component-level control of these safety-related components requires that non-Class 1E control logic within the actuation priority logic of the EIM is enabled by a safety-related switch as described in Section 7.0.4.1. If the operator has enabled non-Class 1E controls in the actuation priority logic of an EIM and there are no active manual or automatic actuation signals present, the operator can use MCS to control safety-related components.

Sensor Blocks

Sensor Blocks I and II encompass the sensors used as inputs to the MPS. The inputs to MPS are summarized in Table 7.1-9. For the purpose of the D3 assessment, the evaluation of Sensor Block I and II is focused on digital sensors that have safety-related functions. ~~Parameters~~Variables that are calculated by MPS (e.g., degrees of subcooling, high power range positive rate) are not included as part of the sensor blocks. Analog and discrete sensors are identified for completeness, but they are not considered to be vulnerable to digital-based CCF.

Module Control System

The MCS provides for NPM-specific control of nonsafety-related systems and, with the appropriate permissives, control of safety-related equipment. The MCS block provides information to the operators and receives input from the operators through the non-Class 1E Monitoring and Indication block. The MCS block consists of the control network, controllers, remote I/O network, and remote I/O modules.

7.1.5.1.2 Guideline 2 - Determining Diversity

The identification of blocks in the previous section allows for diversity assessment against the following six diversity attributes:

- design diversity
- equipment diversity
- functional diversity
- human diversity
- signal diversity
- software diversity

Two types of diversity assessments were performed: diversity attributes within a block and diversity attributes between blocks.

Sensor Block I or II

Assessment of diversity within this block is intended to demonstrate how a digital-based CCF of a safety-related sensor would be limited to a single function type.

The safety-related digital sensors from Table 7.1-9 can be grouped into the following function types as described in the NuScale Power, LLC, TR-0316-22048 "Nuclear Steam Supply Systems Advanced Sensor Technical Report," (Reference 7.1-15):

- digital-based level measurements
- digital-based pressure measurement
- digital-based flow measurement

Equipment Diversity

Each function type depends on different physical effects that require unique processing algorithms to obtain the desired ~~parameter~~variable (e.g., flow, pressure, level). Within a sensor block, each function type is based on different designs from different manufacturers.

Design Diversity

The equipment diversity within each sensor block creates inherent design diversity. Each function type is based on a different architecture (i.e., arrangement and connection of components).

Functional Diversity

Each function type is used for a particular function: digital based level, pressure, and flow sensors are used for these process measurements.

Human Diversity

Within a sensor block, each function type represents sensors from a different design organization (i.e., vendor or supplier).

Software Diversity

Each function type relies on different physical effects that require different algorithms and logic to obtain the desired ~~parameter~~variable.

Signal Diversity

The equipment diversity within each sensor block creates inherent signal diversity. Each function type represents different process ~~parameters~~variables sensed by different physical effects.

Division I or II of SDIS

There are no diversity attributes within this block.

Division I or II of Manual Controls

There are no diversity attributes within this block.

Non-Class 1E Monitoring and Indication Block

There are no diversity attributes within this block.

Module Control System

There are no diversity attributes within this block for the monitoring functions.

Diversity Attributes between Blocks

Equipment Diversity

Initiation of protective actions can be done manually by operators using physical switches or done automatically by Safety Block I or II.

Between Safety Block I and II, different FPGA technology is used to achieve equipment diversity. The FPGA equipment diversity in the form of two different FPGA technologies coupled with the different development tools is an effective solution for the digital-based CCF vulnerabilities present in the MPS, as described in the NuScale Power, LLC, TR-1015-18653, "Design of the Highly Integrated Protection System Platform Topical Report," (Reference 7.1-1). Table 7.1-17 describes the effect of a digital-based CCF across diverse FPGA technologies between each safety block.

Between Sensor Block I and II, there are two sets of digital-based level measurement sensors and each set is from a different design organization (i.e., vendor or supplier). Although the process ~~parameter~~variable is sensed by the same physical effect, the digital processing electronics from different companies result in different designs. When compared to a digital I&C platform, digital-based level measurement sensors have a simpler and specific function. As a result, equipment diversity is an effective solution for the digital-based CCF vulnerability that may be present in the digital-based level measurement electronics.

Design Diversity

To limit the potential for and the consequences of a digital-based CCF, Safety Block I and Division I SDIS block use a different FPGA chip architecture than Safety Block II and Division II SDIS block. The diverse FPGA technologies have additional design diversity attributes, as described in the NuScale Power, LLC, TR-1015-18653, "Design of the Highly Integrated Protection System Platform Topical Report," (Reference 7.1-1) and summarized in Table 7.1-10.

The MCS block and non-Class 1E Monitoring and Indication blocks are based on a programmable technology diverse from safety block I and II, and Division I and II

SDIS. Along with other attributes discussed below, different hardware designs have different failure modes that reduce the possibility of a digital-based CCF affecting more than one block.

Human Diversity

The use of different I&C platforms creates inherent human diversity between certain blocks. The SDIS and safety blocks are based on an FPGA platform while the non-Class 1E Monitoring and Indication block and MCS block are based on a microprocessor-based or computer-based platform as described in Section 7.0.4.4.

Human diversity is an implicit attribute of the FPGA equipment, chip design, and software tool diversity of the SDIS and safety blocks; however, it is neither explicitly defined nor verified for these blocks.

Similar to the SDIS and sensor blocks, human diversity is an implicit attribute of the digital-based level measurements provided by different companies; however, it is neither explicitly defined nor verified for these blocks.

Software Diversity

Software diversity is a subset of design diversity and is the use of different programs designed and implemented by different development groups with different key personnel to accomplish the same safety goals (NUREG/CR-6303).

Due to the design diversity discussed for the FPGA equipment, the use of different programmable technologies results in the use of different design tools that would not introduce the same failure modes.

Functional Diversity

Functional diversity is introduced by having different purposes and functions between blocks.

Safety Blocks I and II form the MPS. These blocks initiate, as needed, to initiate a reactor trip and ESF actuations to mitigate a DBE.

The monitoring and indication blocks allow for an operator to monitor and control both safety and nonsafety systems. The operator can maintain a plant within operating limits or initiate necessary protective actions.

The MCS provides automatic control of systems to maintain the plant within operating limits including constraining certain operational transients.

Sensor Block I and II function is to provide ~~parameter~~process variable information to Safety Block I or II.

Signal Diversity

Between blocks, signal diversity is provided by having automatic and manual means of actuating equipment and protective actions. The MCS and non-Class 1E Monitoring and Indication blocks provide control at the component-level while the manual controls blocks provide control at the division-level.

7.1.5.1.3 Guideline 3 - System Failure Types

Type 1, 2 and 3 system failures as described in NUREG/CR-6303 are considered in Guidelines 10 and 11.

Type 1 Failures

Type 1 failures occur when a plant transient is induced by the instrumentation system for which reactor trip or ESF function is needed, but may not occur, because of an interaction between echelons of defense. Type 1 failures typically begin with a challenge presented by the control system to the RTS or to the ESFAS due to failure of a common sensor or signal source. Defense against such failures depends upon means of accomplishing safety functions that are diverse to the shared signals or equipment (i.e., not impaired by the postulated CCF). Defense-in-depth analysis of Type 1 failures is required by general analysis Guideline 12.

Type 2 Failures

Type 2 failures do not directly cause plant transients, but are undetected until environmental effects or physical equipment failures cause a plant transient or DBE to which protective equipment may not respond. Failure to respond is due to postulated CCF of redundant protection system divisions or portions thereof. Type 2 failures can have serious consequences only if the event needing safety action occurs while the protection system is in the failed state and before the failure is repaired. Defense against type 2 failures depends upon some combination of diverse control system, RTS, ATWS mitigation equipment, ESFAS, and monitoring and indication functions that are sufficient to mitigate the postulated incident. Defense-in-depth analysis of Type 2 failures is required by general analysis Guidelines 10 and 11.

Type 3 Failures

Type 3 failures occur because the primary sensors expected to respond to a DBE produce anomalous readings. For instance, accident conditions may have modified instrument response or an unanticipated event sequence may have modified the ~~parameters~~process variable values seen by the instrumentation. Because Type 3 failures are unpredictable by definition, a strategy dictated by experience is to ensure sufficient signal diversity that alternate means of detecting significant events exist. At a minimum, there is sufficient signal diversity to ensure that for each AOO in the design basis in conjunction with postulated CCFs, the plant is brought to a stable hot standby condition. For each accident in the design basis in conjunction with postulated CCFs, the plant response calculated using best-estimate (using realistic assumptions) analyses does not result in exceedance of the 10 CFR 100 dose limits, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment. Defense-in-depth

Section 7.1.5.1.6

Non-Class 1E Monitoring and Indication Block

Non-Class 1E Monitoring and Indication block includes controls for safety and nonsafety equipment. Because non-Class 1E Monitoring and Indication is used for normal day-to-day operations, any spurious actuation of a major control function (e.g., rod control, feedwater control) by a digital-based CCF within non-Class 1E Monitoring and Indication block is immediately identifiable and, if it exceeds operating limits, is mitigated by Safety Blocks I or II. Figure 7.1-10 identifies the assumed digital-based CCF in red and shows in green outline the available blocks and signals used to resolve information discrepancy.

The actuation priority logic can be used to allow control of safety-related components using non-Class 1E controls; however, this can only be enabled by the operator using a safety-related switch. Without this feature being enabled, the non-Class 1E signals to the actuation priority logic are ignored. Because of the limited period in time in which safety-related components are controlled by non-Class 1E controls, it is not considered credible for a digital based CCF to occur while the enable nonsafety control permissive is active. The limitations on when the enable nonsafety control switch can be positioned to allow control of safety-related components from nonsafety-related controls are controlled by the plant operating procedures described in Section 13.5.2. As a result, no digital-based CCF within the non-Class 1E Monitoring and Indication can directly prevent or spuriously initiate protective actions.

Module Control System

The MCS block is a subset of the actual MCS. The MCS block consists of the control network, controllers, remote I/O network, and remote I/O modules. These components are segmented or explicitly incorporate other functional defensive measures to inhibit the propagation of failures across major control functions. These major control functions are relied on to maintain day-to-day plant operations within operating limits including constraining certain operational transients. Hazards from MCS digital-based CCF are addressed in Section 7.1.8.

The actuation priority logic can be used to allow control of safety-related components using non-Class 1E controls; however, this can only be enabled by the operator using a safety-related switch. Without this feature being enabled, the non-Class 1E signals to the actuation priority logic are ignored. Because of the limited period in time in which safety-related components are controlled by non-Class 1E controls, it is not considered credible for a digital-based CCF to occur while the enable nonsafety control permissive is active. The limitations on when the enable nonsafety control switch can be positioned to allow control of safety-related components from nonsafety-related controls are controlled by the plant operating procedures described in Section 13.5.2. As a result, a digital-based CCF within the MCS block cannot directly prevent MPS from initiating protective actions and cannot directly command MPS to spuriously initiate protective actions.

Sensor Block I or II

These blocks have been included in the analysis because safety-related sensors that depend on digital electronics are being used as inputs to the MPS and are subject to a digital-based CCF. Using the function types and the diversity attributes discussed in Section 7.1.5.1.2, Table 7.1-13 through Table 7.1-16 identify how a digital-based CCF affects either one or both sensor blocks. For Table 7.1-13, there is sufficient diversity in the digital-based level measurement between Sensor Block I and II such that a digital-based CCF is limited to one block.

Postulated outputs of a sensor block with a digital based CCF are fail as-is, fail low, or fail high.

Digital-Based CCF of Level Function Type

A digital-based CCF of level function type for Sensor Block I (Figure 7.1-11) causes:

- spurious actuations from MPS
- incorrect information provided to SDIS, and
- incorrect information provided to MCS

Failed Low Signal

The affected ~~parameters~~variables are pressurizer level, RPV water level, and containment water level. Because protective actions are actuated when at least two-out-of-four separation groups demand a reactor trip or ESF actuation, a failed low signal results in a spurious reactor trip, containment isolation, decay heat removal system (DHRS) actuation, chemical and volume control system (CVCS) isolation, emergency core cooling system (ECCS) actuation, and pressurizer heater trip.

Failed low signals received by Safety Block I are transmitted to MCS, displayed in the MCR, and used for nonsafety control functions. With the spurious actuation of a reactor trip, CNTS isolation, and pressurizer heater trip, the MCS response to two correct and two incorrect sensor values has no further impact. Out of the failed low signals, pressurizer level is the only signal used for nonsafety-related controls; however, with CVCS isolated, MCS cannot use CVCS makeup and letdown pumps to change pressurizer level.

Failed High Signal

The affected ~~parameters~~variables are pressurizer level, RPV water level, and containment water level. Because protective actions are actuated when at least two-out-of-four separation groups demand a reactor trip or ESF actuation, a failed high signal results in a spurious reactor trip, CVCS isolation, and ECCS actuation.

Failed high signals received by Safety Block I are transmitted to MCS, displayed in the MCR, and used for nonsafety control functions. With the spurious actuation of a reactor trip, and CVCS isolation, the MCS response to two correct and two incorrect sensor values has a no further impact. Out of the failed high signals, pressurizer level is the only signal used for nonsafety controls; however, with CVCS isolated,

MCS cannot use CVCS makeup and letdown pumps to change pressurizer level. With Sensor Block II still capable of actuating on low-level signals (e.g., containment isolation on low-low pressurizer level), capability to initiate other ESFs is not lost.

Failed As-Is

The affected ~~parameters~~variables are pressurizer level, RPV water level, and containment water level. The failed as-is condition for two of the four sensors for each affected ~~parameter~~variable does not prevent the initiation of a reactor trip or ESF actuation. Sensor Block II is still capable of identifying plant conditions requiring protective actions.

Failed as-is signals do not lead to spurious initiation of protective actions. Failed as-is signals may go unnoticed until the valid signals significantly deviate from the failed signals.

Digital-Based CCF of Pressure Measuring System Function Type

A digital-based CCF of pressure measuring system function type for Sensor Block I (Figure 7.1-12) causes

- spurious actuations from MPS
- incorrect information provided to SDIS
- incorrect information provided to MCS

Failed Low Signal

The affected ~~parameters~~variables are pressurizer pressure and wide-range RCS pressure. Failed low signals in the four sensors for each affected ~~parameter~~variable can result in a spurious reactor trip, DHRS actuation, CVCS isolation, and pressurizer heater trip.

Failed low signals received by Safety Block I and II are provided to MCS to be displayed in the MCR and to be used for nonsafety controls. With the spurious reactor trip, DHRS actuation, and CVCS isolation, the MCS response to four incorrect sensor values has no further impact. The automatic MCS response to a drop in pressure is to turn on the pressurizer heaters; however, with the pressurizer heater trip, pressurizer heaters are unavailable.

Failed High Signal

The affected ~~parameters~~variables are pressurizer pressure and wide-range RCS pressure. A failed high signal affecting the four sensors for the affected ~~parameters~~variables can result in a spurious reactor trip, CNTS isolation, DHRS actuation, CVCS isolation, and pressurizer heater trip.

Failed high signals received by Safety Block I and II are provided to MCS to be displayed in the MCR and to be used for nonsafety controls. With the spurious

reactor trip, CVCS isolation, and pressurizer heater trip, the MCS response to four incorrect sensor values has a no further impact. The automatic MCS response to a rise in pressure is to use pressurizer spray; however, with the isolation of the CVCS, pressurizer spray is unavailable.

Failed As-Is

The affected ~~parameters~~variables are pressurizer pressure and wide-range RCS pressure. The failed as-is condition for the four sensors of each affected ~~parameter~~variable does not result in spurious actuations; however, it can prevent initiation of protective actions if a DBE were to occur. This failure can be considered a Type 3 failure and is discussed in Section 7.1.5.1.10 and Section 7.1.5.1.11.

Digital-Based CCF of Flow Measurement Function Type

A digital-based CCF of flow measurement function type for Sensor Block I (Figure 7.1-13) causes

- spurious actuations from MPS
- incorrect information provided to SDIS
- incorrect information provided to MCS

Failed Low Signal

The affected ~~parameter~~variable is RCS flow. A failed low signal for the four channels results in a spurious demineralized water system (DWS) isolation and CVCS isolation. There is no further impact associated with a failed low signal.

Failed High Signal

The affected ~~parameter~~variable is RCS flow. A failed high signal for the four channels does not result in spurious actuations; however, the safety blocks would be unable to identify a low RCS flow condition and the operator would have incorrect information.

Failure to identify a low RCS flow condition failure can be considered a Type 3 failure and is discussed in Section 7.1.5.1.10 and Section 7.1.5.1.11.

Failed As-Is

The affected ~~parameter~~variable is RCS flow. The failed as-is condition for the four channels do not result in spurious actuations; however, it can prevent initiation of protective actions if a DBE were to occur. This failure can be considered a Type 3 failure and is discussed in Section 7.1.5.1.10 and Section 7.1.5.1.11.

7.1.5.1.7 Guideline 7 - Use of Identical Hardware and Software Modules

The digital-based flow and pressure measuring system function type found in Sensor Block I and II are considered to be identical. The other blocks are considered

Although there are no Type A variables, Division I and II manual controls blocks provide an independent and diverse method of manually actuating the automatic safety-related functions at the Division-level. The actuation priority logic within the EIMs of both safety blocks is implemented in discrete analog components and downstream of the automatic digital portion of the safety system. The SDIS and manual controls blocks are sufficiently diverse that any failure does not prevent the operator from obtaining or resolving conflicting information as described in Section 7.1.5.1.6. As shown in Section 7.1.2 and Section 7.1.5.1.4, the SDIS and manual controls blocks are considered to be independent of the RTS, ESFAS, and control system echelon.

7.1.5.2 Results and Conclusions

7.1.5.2.1 Vulnerabilities to Spurious Actuations resulting from Digital-Based Common Cause Failures

After applying the guidelines of NUREG/CR-6303, the following potential vulnerabilities have been identified:

1) Potential digital-based CCF within a safety block may lead to spurious initiation of a protective action, as described in Section 7.1.5.1.6:

   - reactor trip
   - DHRS actuation
   - ECCS actuation
   - containment isolation
   - CVCS isolation
   - pressurizer heater trip
   - DWS isolation
   - low temperature overpressure protection (LTOP)

2) Potential digital-based CCF within a safety block may lead to spurious partial initiation of protective actions (Section 7.1.5.1.6). The identified consequences are provided in Table 7.1-11.

3) Potential digital-based CCF of level function type within Sensor Block I or II may result in one of the following (Section 7.1.5.1.6):

   - spurious reactor trip, containment isolation, DHRS actuation, CVCS isolation, ECCS actuation, demineralized water system isolation, and pressurizer heater trip
   - spurious reactor trip, CVCS isolation, demineralized water system isolation, and ECCS actuation

4) Potential digital-based CCF of pressure measuring system function type within Sensor Block I and II may result in one of the following (Section 7.1.5.1.6):

- spurious reactor trip, DHRS actuation, CVCS isolation, demineralized water system isolation, and pressurizer heater trip
- spurious reactor trip, containment isolation, DHRS actuation, CVCS isolation, demineralized water system isolation, and pressurizer heater trip
- Type 3 failure for the digital-based pressure measuring system function type sensors

5) Potential digital-based CCF of flow function type within Sensor Block I and II may result in one of the following (Section 7.1.5.1.6):

   - ~~spurious DWS isolation and CVCS isolation~~spurious reactor trip, demineralized water system isolation, and CVCS isolation
   - Type 3 failure of flow function type sensors (See Item 6 and 7 below)

6) Type 3 failures of digital sensors may lead to failure of MPS to initiate protective action(s) during AOOs and PAs. Table 7.1-18 identifies the digital sensors credited for AOOs and PAs that were addressed with a D3 coping analysis. A failure of two of the four MPS separation groups that leads to the spurious initiation of a protection action or combination of protective actions was evaluated by the D3 coping analysis using best-estimate methods. While there are a very large number of possible actuation combinations, the analysis of these events can be simplified without addressing each possible combination specifically.

   The D3 coping analysis determined that the spurious actuation of containment system isolation due to a digital-based CCF is the bounding analysis with regard to the reactor coolant pressure boundary integrity. Concurrent actuations of any combination of RTS, DHRS or PZR heater trip have been evaluated to be less limiting due to the additional heatup effects on the delay of reactor trip, DHRS actuation valve opening or PZR heaters being tripped off. CSI actuation includes CVCSI actuation which increases the heatup event slightly and negates any possible effects of DWSI actuation. The consequences of a digital-based CCF that leads to spurious initiation of any combination of MPS protective actions at normal operating pressure and temperature are bounded by the existing inadvertent DHRS analysis.

   A postulated digital-based CCF affecting digital-based sensors that lead to a partial spurious initiation of protective actions at normal operating pressure and temperature is bounded by the existing plant safety analyses described in Chapter 15 or have no immediate impact and are non-limiting events.

7.1.5.2.2 Results of Coping Analyses for Postulated Digital-Based Common Cause Failure Vulnerability

As identified in Section 7.1.5.2.1, several postulated digital-based CCF vulnerabilities were identified that required a coping analysis to verify the consequences for the digital-based CCF were acceptable. For the AOOs and PAs identified in Table 7.1-18, the events were analyzed with postulated digital-based CCFs of the identified sensors that are relied upon and credited for the event in

question. The results of the coping analysis concluded the AOO and postulated accident acceptance criteria were met. For the postulated spurious actuations analyzed, none resulted in a plant response or consequence that created conditions which were not bounded by the plant safety analysis described in Chapter 15. As a result, no additional coping strategies have been identified for prevention or mitigation of the postulated spurious actuations analyzed.

The acceptance criteria for the coping analysis is to demonstrate a SCCF of a credited signal and all sensors of the same type, concurrent with a DBE does not violate the integrity of the primary coolant pressure boundary, or result in radiation release exceeding 10 percent of 10 CFR 100 dose limits for AOOs and 100 percent of 10 CFR 100 dose limits for postulated accidents. The analysis summary is provided below for the flow~~, level~~ and pressure safety-related digital-based ~~sensors for pressure, level and flow.~~ sensors.

High Pressurizer Pressure

The plant safety analyses described in Chapter 15 credit high PZR pressure for detection and mitigation of heatup and reactivity excursion DBEs. The best-estimate transient analysis performed concluded that credit for the pressure mitigating effect of the PZR spray system would exclude the high pressure trip from being the primary credited signal. Even if the spray was insufficient to mitigate the pressure response, the result would be the lifting of a reactor safety valve.

There are two reactor safety valves each of which are sized to relieve the pressure generated by a total loss of secondary cooling without credit for a reactor trip. The D3 coping analysis concluded that a conservative postulated heatup event that did not trip on high pressure would not violate the RCS pressure boundary integrity due to the sizing of the reactor safety valves.

For the events described in Chapter 15 and listed in Table 7.1-18 that result in a high RCS pressure condition, the analyses conservatively do not take credit for normal pressurizer spray control. In the secondary plant events that result in the loss of main steam flow, the high main steam pressure signal is credited to generate reactor trip and DHRS actuations in addition to the high PZR pressure. In the case of the loss of feedwater and feedwater line break events, the high RCS hot temperature is a diverse signal. Therefore, sufficient signal diversity exists such that postulated digital-based CCFs of the high pressurizer pressure function are bounded by the plant safety analyses in Chapter 15. In most of these event scenarios, the best estimate analysis determined that the plant response would not reach the high pressurizer pressure actuation setpoint due to the realistic treatment of PZR spray and its ability to control the RCS pressure increase.

Low Pressurizer Pressure

The plant safety analyses described in Chapter 15 credit low PZR pressure in the steam generator tube failure and CVCS line breaks outside containment events. The limiting radiological scenarios include assumed loss of AC power concurrent with the breaks which results in an RCS pressurization that delays the low

Division I and II manual control switches are provided to manually initiate at the division-level the automatic safety-related functions. Manual actuation signals are inputs to the actuation priority logic within an EIM. The actuation priority logic within the EIMs is implemented in discrete analog components and is downstream of the automatic digital portion of the safety system. The SDIS and manual controls are sufficiently diverse that any failure does not prevent the operator from obtaining or resolving conflicting information (Section 7.1.5.1.6).

7.1.6 Safety Evaluation

Conformance with 10 CFR 50 Appendix A

General Design Criterion 1

The I&C systems are designed to the quality assurance program requirements as described in Section 7.1.1, Section 7.2.1, and Section 17.5.

General Design Criterion 2

The I&C systems and components required to function during natural phenomena events are located within structures that protect them against natural phenomena. See Section 7.1.1 and Section 7.2.2.

General Design Criterion 4

The I&C systems are designed for the environmental conditions that are associated with normal operation, maintenance, testing, and postulated accidents to which they may be subjected and required to function. See Section 7.1.1 and Section 7.2.2.

General Design Criterion 5

The MPS, NMS, MCS, and ICISs are not shared between NPMs. The PCS and PPS are shared between multiple NPMs and are designed to not adversely affect the ability of I&C platforms to perform safety-related functions. See Section 7.1.1 and Section 7.2.11.

General Design Criterion 10

The MPS provides the reactor trips and ESF actuations based on analytical limits with appropriate margin to ensure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of AOOs. The MPS also monitors NPM ~~parameters~~variables and provides these signals to the MCS for control and indication. The NMS monitors and provides neutron flux levels to the MPS. See Section 7.1.1.

General Design Criterion 13

The I&C systems monitor variables and systems over their anticipated ranges for normal operations, AOOs, and accident conditions to ensure adequate safety. See Section 7.1.2, Section 7.1.4, Section 7.1.5, Section 7.2.7, and Section 7.2.13.

The MPS has sufficient separation of the protection and the control systems to satisfy reliability, redundancy, and independence requirements even with a component or channel failed or removed from service. See Section 7.1.2, Section 7.1.3, and Section 7.1.5.

General Design Criterion 25

The MPS initiates reactor trip functions to ensure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control system. See Section 4.6.2 and Section 7.1.1.

General Design Criterion 28

The MPS initiates reactor trip functions to limit the potential amount and rate of reactivity increase and to ensure sufficient protection from reactivity accidents. See Section 4.6.2, and Section 7.1.1.

General Design Criterion 29

The MPS and NMS are designed with sufficient redundancy and diversity to ensure high probability of accomplishing their safety-related functions in the event of AOOs. See Section 7.1.3.

General Design Criterion 64

The MCS and PCS provide monitoring of radioactivity releases, reactor containment atmosphere, and plant environments for radioactivity that may be released from normal operations, AOOs, and postulated accidents. See Section 7.1.1.

Conformance with Other 10 CFR 50 Requirements

10 CFR 50.34(b)(2)(i)

The NuScale I&C systems and auxiliary features of the I&C system design are discussed in Section 7.0.4 and Section 7.2.8 respectively.

10 CFR 50.34(f)(2)(iv)

The SDIS, MCS, and PCS provide the capability to display important plant ~~parameters~~variables over their anticipated ranges for normal operation, AOOs, and accident conditions. See Section 7.2.13.

10 CFR 50.34(f)(2)(v)

The MCR displays bypassed and operable status indication of safety interlocks. See Section 7.2.4 and Section 7.2.13.

10 CFR 50.34(f)(2)(xi)

The MCR displays reactor safety valve position indication. See Section 7.2.13.

10CRD 50.34(f)(2) (xiv)

Containment isolation is initiated by two diverse signals from the MPS that ensure the isolation valves do not re-open upon logic reset, as shown in Table 7.1-4 and Section 7.1.5.

10 CFR 50.34(f)(2)(xvii)

The I&C systems are designed to display appropriate variables in the MCR for monitoring specified containment ~~parameters~~variables and site radioactive gaseous effluents from potential accident releases. See Section 7.2.13.

10 CFR 50.34(f)(2)(xviii)

The MPS and NMS provide MCR indications of inadequate core cooling. See Section 7.2.13.

10 CRF 50.34(f)(2)(xix)

The MPS and NMS provide instrumentation for monitoring plant conditions following an accident that includes potential core damage. See Section 7.2.13.

10 CFR 50.36(c)(1)(ii)(A)

The MPS initiates automatic protective actions prior to exceeding a safety limit. See Section 7.2.7.

10 CFR 50.36(c)(3)

The I&C systems are designed to meet surveillance requirements to ensure that the necessary quality of SSC is maintained such that operation is within safety limits and limiting conditions of operations are met. See Section 7.2.7 and Section 7.2.15.

10 CFR 50.49

The I&C equipment that perform the functions in 10 CFR 50.49(b) remain functional during and following DBEs. See Section 7.2.2.

10 CFR 50.44(jj) and 10 CFR 50.55(i)

The I&C systems are designed, tested, and inspected to quality standards commensurate with the safety function to be performed. See Section 7.2.1.

10 CFR 50.55a(h)

The MPS and the NMS meet the requirements for protection systems and safety systems in accordance with IEEE Std. 603-1991 (Reference 7.1-3) and the correction sheet dated January 30, 1995 as described in Section 7.1 and Section 7.2.

10 CFR 50.62

- no additional hazards have been introduced by the work done during the software life cycle activity.

7.1.8.2 Hazards Analysis Methodology

A hazard analysis is a process for examining an I&C system to identify hazards (i.e., factors and causes) and system requirements or constraints to eliminate, prevent, or control them.

The scope of the NuScale I&C system hazard analysis encompasses the system design basis described in Section 7.1.1. The analyses performed for the system design examined the associated I&C system, subsystems, and components and their interrelationships and interactions with other systems, subsystems, and components during all modes of system operation to identify unintended or unwanted I&C system operation, including the impairment or loss of the ability to perform a safety function.

The NuScale I&C system hazard analysis is intended to evaluate those conditions and factors associated with the system under analysis and the systems that directly interact with it that can result in unintended or unwanted system operation, including a failure to initiate a protective action. These conditions are designated in the analysis as "Unsafe." Additional analysis is performed to provide guidance for the development process where a control action could affect continuity of operation or create other abnormal operating conditions without causing failure of a required protective action. These conditions are designated in the analysis as "Undesired."

The methodology for the hazard analysis is based on STAMP (Systems-Theoretic Accident Model and Processes) and STPA (Systems-Theoretic Process Analysis) developed at the Massachusetts Institute of Technology (Reference 7.1-9). The STPA methodology departs from the standard FMEA and fault-tree analysis by going beyond potential system failure caused by component failures. The STPA includes potential failures caused by interactions between system components, including human operators, which result in inadequate control actions, which can occur without component or logic faults.

Systems-Theoretic Accident Model and Processes

The STAMP model of accident causation is built on three basic concepts: safety constraints, a hierarchical control structure, and process models, along with basic systems theory concepts.

In STAMP, systems are viewed as interrelated components kept in a state of dynamic equilibrium by feedback control loops. Systems are not treated as static, but as dynamic processes that are continually adapting to achieve their ends and to react to changes in themselves and their environment.

Safety is viewed as an emergent property of the system that is achieved when constraints on the behavior of the system and its components are satisfied. The design of the system must not only satisfy these constraints but must also continue to enforce the constraints as changes and adaptations to the system occur over time.

Section 7.1.8.3.4

components for maintenance, system alignment following an actuation or other, nonsafety-related operations.

Example Neutron Monitoring Control Structure

The control structure for the NMS ex-core sensors and process instrumentation consists of the control and monitoring systems, process instrumentation, and sensors. This structure is shown in Figure 7.1-17. Beginning at the top of Figure 7.1-17, the control and monitoring systems manipulate the different functions and ~~parameters~~variables that affect the reactor power level that the NMS is monitoring. The NMS monitors the neutron flux levels of the controlled process and supplies the control and monitoring systems with current levels and conditions. The NMS also updates the control and monitoring systems with the status and condition of the NMS circuits. The control and monitoring systems use this information to update the operator.

Example Low-Level Logic Structure - Safety Function Module

The SFM logic (Figure 7.1-18) is a non-standard control structure in that there are three controllers (the operator, the signal conditioning, and the trip determination logic) and minimal control feedback. The only feedback provided is loopback input signal verification for the signal conditioning, actuated component position information, and ~~parameter~~process variable display feedback to the operator.

The control structure diagram shows the configuration of the input signal conditioning and trip determination controllers with output, through the triple redundant communications bus, directed to the associated SBMs. The division level processes are analyzed separately.

The control actions considered in this portion of the analysis begin with the signal conditioning. The signal conditioner is a controller to the extent that it accepts an input from an analog or digital sensor, performs conditioning on the signal, such as filtering and scaling, and then performs an analog-to-digital conversion, if necessary. Signal validation is performed on the signal to reduce the possibility of an inadvertent protective action or the failure to initiate a required protective action. The digital representation of the original analog input signal is sent to the associated trip determination portion of the SFM. The ~~parameter~~process variable value signal, along with generated signal quality information, is sent to the MIB communications module.

CP-0138

Control Action Analysis

The control actions are analyzed by investigating the control objects in each diagram and the interactions between them. Each interaction, command or event, is evaluated to determine if a hazardous condition results if the interaction fails to occur, if it occurs in an incorrect manner, if it is late or early in occurring, if it occurs out of sequence, or if it is stopped too soon. For example, looking at the signal conditioning in Figure 7.1-18, an input event that is expected is an analog signal

that is received from a sensor. If this does not occur, an unsafe condition could exist with a ~~parameter~~process variable out of its normal operating range without an appropriate protective action. This unsafe condition results from a failure to execute a correct control action in response to an out-of-normal plant ~~parameter~~process variable. Similarly, if the analog signal does not accurately reflect plant conditions, it could result in the same type of unsafe control action. Table 7.1-23 reflects this in the first row by showing that the control action is unsafe and identifies the hazardous condition as HC-1. The remaining potential hazardous conditions, too early, too late, out of sequence, and stopped too soon, are not indicated as unsafe conditions. This is because the input signal is a continuous stream and is not impacted by timing issues in the MPS. A too-late condition caused by a slow response time of the ~~parameter~~process sensor is identified by a hazard analysis of the sensing device.

In this hazard analysis, the following conventions are used:

- Hazardous conditions are identified by the designation HC followed by a unique number that is incremented for each identified HC.
- Possible causes are identified by the designation PC followed by a number. Possible causes are not classified according to related hazardous conditions because of their more generic nature.
- Safety constraints are identified by the designation SC followed by a two part number. The first number identifies the hazardous condition that the constraint is intended to mitigate. The second number is a unique number that is incremented for each identified SC.
- Possible causes that refer to "algorithm" errors may be due to requirements, design, or implementation. Any FPGA errors, after proper design and implementation, could only be the result of physical damage or component failure.
- Board level clock errors may be due to mistiming or loss of clock signals that control the sequencing of FPGA logic. These clock signals are independent for each FPGA board and allow asynchronous operation between FPGA modules.
- Communication errors may be data or signal faults. Data media errors or faults would be the result of physical damage or failure.
- Control actions identified as "Undesired" are actions that do not directly result in an unsafe condition, but may result in an abnormal operation condition or an unnecessary shutdown.

Correlation of Possible Causes to Preliminary Hazard List

Table 7.1-24 shows the basic causes of unsafe control actions identified by the MPS hazard analysis and the system preliminary hazard list (PHL). The hazards identified in the hazard list correlate well with the hazard analysis. The table is not intended to indicate a one-to-one correspondence between the first (Hazards Analysis Identified Cause) and second (PHL Identified Cause) column. For example, the damaged cable from the hazard analysis could be caused by many of the causes from the hazard list. The most significant differences between the lists are that the

preliminary hazard list focused primarily on failures due to physical events. The hazard analysis identified causes such as operator error and procedural error as well as possible design deficiencies such as software and algorithm error. These differences support the use of the STPA methodology for analyzing complex systems such as the MPS.

The NuScale I&C system hazard analysis is based on a view of the processes that are performed by the systems described in Section 7.0. The hazards analysis does not explicitly analyze the effects of redundancy and defense-in-depth; however, the hazard conditions identified in the hazards analysis are partially or fully mitigated through application of the fundamental design principles of redundancy (Section 7.1.3) and D3 (Section 7.1.5). The hazards analysis methodology described is a living process, performed through the system design life cycle. The cross-referencing of hazard conditions, safety constraints, and functional design requirements ensures that potentially hazardous conditions not previously identified by other analysis methods are mitigated by feedback into the design of the system functional requirements.

7.1.9 References

7.1-1 NuScale Power, LLC, Topical Report, "Design of the Highly Integrated Protection System Platform," TR-1015-18653 ~~Rev.~~Revision 2~~1~~.

7.1-2 NuScale Power, LLC, Topical Report, "Quality Assurance Program Description," NP-TR-1010-859-NP-A, Revision 3.

7.1-3 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Standard 603-1991, Piscataway, NJ.

7.1-4 Institute of Electrical and Electronics Engineers, "IEEE Standard for Seismic Qualification of Equipment for Nuclear Power Generating Stations," IEEE Standard 344-2004, Piscataway, NJ.

7.1-5 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Digital Computers and Safety Systems of Nuclear Power Generating Stations," IEEE Standard 7-4.3.2-2003, Piscataway, NJ.

7.1-6 U.S. Nuclear Regulatory Commission, “Highly-Integrated Control Rooms--Communication Issues (HICRc),” Interim Staff Guidance, DI&C-ISG-04, Rev. 1, March 2009.

7.1-7 U.S. Nuclear Regulatory Commission, SRM for SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactors (ALWR) Designs,” July 21, 1993.

7.1-8 Institute of Electrical and Electronics Engineers, "IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," IEEE Standard 379-2000, Piscataway, NJ.

Table 7.1-1: Module Protection System Design Basis Events

Event	Event Type	Credited Signals
Decrease in Feedwater Temperature	Cooldown Event	Described in Section 15.1.1.2
~~Decrease~~Increase in Feedwater ~~Temperature~~Flow	Cooldown Event	Described in Section 15.1.2.2
Increase in Steam Flow	Cooldown Event	Described in Section 15.1.3.2
Inadvertent Opening of Turbine Bypass System	Cooldown Event	Described in Section 15.1.4.2
Steam System Piping Failures Inside and Outside of Containment	Cooldown Event	Described in Section 15.1.5.2
Loss of Containment Vacuum	Cooldown Event	Described in Section 15.1.6.2
Loss of External Load	Heatup Event	Described in Section 15.2.1.2
Turbine Trip	Heatup Event	Described in Section 15.2.2.2
Loss of Condenser Vacuum	Heatup Event	Described in Section 15.2.3.2
Closure of Main Steam Isolation Valve	Heatup Event	Described in Section 15.2.4.2
Loss of Nonemergency AC Power to the Station Auxiliaries	Heatup Event	Described in Section 15.2.6.2
Loss of Normal Feedwater Flow	Heatup Event	Described in Section 15.2.7.2
Feedwater System Pipe Breaks Inside and Outside of Containment	Heatup Event	Described in Section 15.2.8.2
Uncontrolled Control Rod Assembly Withdrawal from a Subcritical or Low Power	Reactivity Event	Described in Section 15.4.1.2
Uncontrolled Control Rod Assembly Withdrawal at Power	Reactivity Event	Described in Section 15.4.2.2
Control Rod Misoperation	Reactivity Event	Described in Section 15.4.3.2
Inadvertent Decrease in Boron Concentration in the Reactor Coolant System	Reactivity Event	Described in Section 15.4.6.2
Spectrum of Rod Ejection Accidents	Reactivity Event	Described in Section 15.4.8.2
System Malfunction that Increases Reactor Coolant Inventory	Increase in RCS Inventory Event	Described in Section 15.5.1.2
Failure of Small Lines Carrying Primary Coolant Outside CNV	Decrease in RCS Inventory Event	Described in Section 15.6.2.2
Steam Generator Tube Failure	Decrease in RCS Inventory Event	Described in Section 15.6.3.2
Loss-of-Coolant Accidents from a Spectrum of Postulated Piping Breaks inside CNV	Decrease in RCS Inventory Event	Described in Section 15.6.5.2
Spurious Opening of an RPV Valve	Decrease in RCS Inventory Event	Described in Section 15.6.6.2
Inadvertent Operation of DHRS	Heatup/Cooldown Event	Described in Section 15.2.9.2
Instability Events	Special Event	Described in Section 15.9

Table 7.1-3: Reactor Trip Functions

~~Parameter~~Process Variable	Analytical Limit	Number of Channels	Logic
High Power Range Linear Power	High-1 = 25% RTP High-2 = 120% RTP	4	2/4↑
High Intermediate Range Log Power Rate	3 dpm	4	2/4↑
High Power Range Positive and Negative Rate	+/- 15% RTP/minute	4	2/4↕
High Source Range Count Rate	$5x10^5$ cps	4	2/4↑
High Source Range Log Power Rate	3 dpm	4	2/4↑
High Narrow Range RCS Hot Temperature (NR RCS T_{hot})	610°F	4	2/4↑
High Narrow Range Containment Pressure	9.5 psia	4	2/4↑
High Pressurizer Pressure	2000 psia	4	2/4↑
Low Pressurizer Pressure	1720 psia	4	2/4↓
Low Low Pressurizer Pressure	1600 psia	4	2/4↓
High Pressurizer Level	80%	4	2/4↑
Low Pressurizer Level	35%	4	2/4↓
High Main Steam Pressure	800 psia	4	2/4↑
Low Main Steam Pressure	300 psia	4	2/4↓
Low Low Main Steam Pressure	100 psia	4	2/4↓
High Steam Superheat (MS Temperature and Pressure)	150°F	4	2/4↑
Low Steam Superheat (MS Temperature and Pressure)	0.0°F	4	2/4↓
Low Low RCS Flow	0.0 ft^3/s	4	2/4↓
Low AC Voltage to Battery Chargers	Actuation Delay of 60 seconds (Note 1)	4	2/4↓
High Under-the-Bioshield Temperature	250°F	4	2/4↑

Note 1: Normal AC voltage is monitored at the bus(es) supplying the battery chargers for the highly reliable DC power system. The Analytical Limit is based on loss of AC power to plant busses (0 volts); the actual bus voltage used is based upon the voltage ride-thru characteristics of the EDSS battery chargers.

Table 7.1-4: Engineered Safety Feature Actuation System Functions

ESF Function	~~Parameter~~Process Variable	Analytical Limit	Number of Channels	Logic	System Automated Function
Emergency Core Cooling System (ECCS)	High Containment Water Level	260″ - 220″ (elevation) (Note 3)	4	2/4↑	Removes Electrical Power to the trip solenoids of the reactor vent valves. Removes electrical power to the trip solenoids of the reactor recirculation valves
	Low RPV Riser Level	390″- 350″ (elevation) (Note 3)	4	2/4↓	
	Low ELVS voltage 24-hour Timer	24 hours	3	2/3	
Decay Heat Removal System (DHRS)	High Pressurizer Pressure	2000 psia	4	2/4↑	Removes electrical power to the trip solenoids of the decay heat removal valves Removes electrical power to the trip solenoids of the of the following valves in the containment system: • main steam isolation valves • main steam isolation bypass valves • secondary main steam isolation valves • secondary main steam isolation ~~bypass~~ valve bypass valves • feedwater isolation valves • feedwater ~~regulation~~regulating valves
	High Narrow Range RCS Hot Temperature (NR RCS Thot)	610°F	4	2/4↑	
	Low Main Steam Pressure	300 psia (> 15% RTP)	4	2/4↓	
	Low Low Main Steam Pressure	100 psia (≤ 15% RTP)	4	2/4↓	
	High Main Steam Pressure	800 psia	4	2/4↑	
	Low Steam Superheat (MS Temperature and Pressure)	0.0°F	4	2/4↓	
	High Steam Superheat (MS Temperature and Pressure)	150°F	4	2/4↑	
	High Narrow Range Containment Pressure	9.5 psia	4	2/4↑	
	Low Pressurizer Pressure	1720 psia (Note 1)	4	2/4↓	
	Low Low Pressurizer Pressure	1600 psia (Note 2)	4	2/4↓	
	Low Low Pressurizer Level	20%	4	2/4↓	
	Low AC Voltage to Battery Chargers	Actuation Delay of 60 seconds (~~See~~ Note 4~~1~~)~~s~~	4	2/4↓	
	High Under-the-Bioshield Temperature	250°F	4	2/4↑	

Table 7.1-4: Engineered Safety Feature Actuation System Functions (Continued)

ESF Function	~~Parameter~~Process Variable	Analytical Limit	Number of Channels	Logic	System Automated Function
Containment System Isolation (CSI) Signal	High Narrow Range Containment Pressure	9.5 psia	4	2/4↑	Removes electrical power to the trip solenoids of the following valves: • RCS injection valves • RCS discharge valves • PZR spray valves • RPV high point degasification line valves • feedwater isolation valves • feedwater ~~regulation~~regulating valves • main steam isolation valves • main steam isolation bypass valves • secondary main steam isolation valves • secondary main steam isolation ~~bypass~~ valve bypass valves • containment evacuation system valves • reactor component cooling water system supply and return valves • containment flooding and drain system valves
	Low Low Pressurizer Level	20%	4	2/4↓	
	Low AC Voltage to Battery Chargers	Actuation Delay of 60 seconds (~~See~~ Note ~~4~~1)	4	2/4↓	
	High Under-the-Bioshield Temperature	250°F	4	2/4↑	
Demineralized Water System Isolation (DWSI)	High Power Range Linear Power	High-1 = 25% RTP High-2 = 120% RTP	4	2/4↑	Removes electrical power to the trip solenoids of the demineralized water supply valves
	High Intermediate Range Log Power Rate	3 dpm	4	2/4↑	
	High Power Range Positive and Negative Rate	+/- 15% RTP/minute	4	2/4↕	
	High Source Range Count Rate	$5x10^5$ cps	4	2/4↑	
	High Source Range Log Power Rate	3 dpm	4	2/4↑	
	High Narrow Range RCS Hot Temperature (NR RCS Thot)	610°F	4	2/4↑	
	High Narrow Range Containment Pressure	9.5 psia	4	2/4↑	
	High Pressurizer Pressure	2000 psia	4	2/4↑	
	Low Pressurizer Pressure	1720 psia (Note 1)	4	2/4↓	

Table 7.1-4: Engineered Safety Feature Actuation System Functions (Continued)

ESF Function	~~Parameter~~Process Variable	Analytical Limit	Number of Channels	Logic	System Automated Function
Demineralized Water System Isolation (DWSI) (continued)	Low Low Pressurizer Pressure	1600 psia (Note 2)	4	2/4↓	
	High Pressurizer Level	80%	4	2/4↑	
	Low Pressurizer Level	35%	4	2/4↓	
	High Main Steam Pressure	800 psia	4	2/4↑	
	Low Main Steam Pressure	300 psia (> 15% RTP)	4	2/4↓	
	Low Low Main Steam Pressure	100 psia (≤ 15% RTP)	4	2/4↓	
	High Steam Superheat (MS Temperature and Pressure)	150°F	4	2/4↑	
	Low Steam Superheat (MS Temperature and Pressure)	0.0°F	4	2/4↓	
	Low RCS Flow	1.7 ft^3/s	4	2/4↓	
	Low Low RCS Flow	0.0 ft^3/s	4	2/4↓	
	Low AC Voltage to Battery Chargers	Actuation Delay of 60 seconds (Note 4~~1~~)	4	2/4↓	
	High Under-the-Bioshield Temperature	250°F	4	2/4↑	
	High Subcritical Multiplication (SCM)	3.2	4	2/4↑	
Chemical and Volume Control System Isolation (CVCSI)	High Pressurizer Level	80%	4	2/4↑	Removes electrical power to the trip solenoids of the following valves: • RCS injection valves • RCS discharge valves • PZR spray valves • RCS high point degasification valves
	High Narrow Range Containment Pressure	9.5 psia	4	2/4↑	
	Low Pressurizer Pressure	1720 psia (Note 1)	4	2/4↓	
	Low Low Pressurizer Pressure	1600 psia (Note 2)	4	2/4↓	
	Low Low Pressurizer Level	20%	4	2/4↓	
	Low Low RCS Flow	0.0 ft^3/s	4	2/4↓	
Pressurizer Heater Trip	Low Pressurizer Level	35%	4	2/4↓	Removes electrical power to the PZR heaters
	Any DHRS Actuation - See DHRS Actuation ~~Parameters~~Variables	See DHRS Actuation Analytical Limits	4	2/4	

Table 7.1-4: Engineered Safety Feature Actuation System Functions (Continued)

ESF Function	~~Parameter~~Process Variable	Analytical Limit	Number of Channels	Logic	System Automated Function
Low Temperature Overpressure Protection (LTOP)	Low Temperature Interlock with High Pressure (WR RCS cold temperature and WR RCS Pressure)	Variable based on WR RCS cold temperature and WR RCS Pressure	4	2/4↑	Removes electrical power to the trip solenoids of the reactor vent valves

~~Note 1: Normal AC voltage is monitored at the bus(es) supplying the battery chargers for the highly reliable DC power system. The Analytical Limit is based on loss of AC power to plant busses (0 volts); the actual bus voltage used is based upon the voltage ride-thru characteristics of the EDSS battery chargers.~~

Note 1: If RCS hot temperature is above 600°F.

Note 2: If RCS hot temperature is below 600°F.

Note 3: RPV riser level and CNV water level are presented in terms of elevation where reference zero is the bottom of the reactor pool. The ranges allow ±20" from the nominal ECCS level setpoint of 370" and 240", respectively.

Note 4: Normal AC voltage is monitored at the bus(es) supplying the battery chargers for the highly reliable DC power system. The Analytical Limit is based on loss of AC power to plant busses (0 volts); the actual bus voltage used is based upon the voltage ride-thru characteristics of the EDSS battery chargers.

Table 7.1-9: Sensor Inputs to Module Protection System

~~Parameter~~Process Variable	Sensor Type	Output Signal	Safety-Related?	Type A, B, or C PAM Variable?	Sensor Block I			Sensor Block II		
					SG A	SG C	DIV. I	SG B	SG D	DIV. II
Pressurizer~~/RPV water~~ level (Note 1)	Digital	Analog	Y	N	X	X	-	X	X	-
RPV riser level (Note 1)	Digital	Analog	Y	Y	X	X	-	X	X	-
PZR pressure (Note 1)	Digital	Analog	Y	N	X	X	-	X	X	-
Wide-range reactor coolant system (RCS) pressure (Note 1)	Digital	Analog	Y	Y	X	X	-	X	X	-
Containment water level (Note 1)	Digital	Analog	Y	Y	X	X	-	X	X	-
Narrow-range containment pressure	Analog	Analog	Y	N	X	X	-	X	X	-
Wide-range containment pressure	Digital	Analog	N	Y	-	X	-	X	-	-
Containment isolation valve positions	Discrete (Analog)	Discrete (Analog)	N	Y	-	-	X	-	-	X
~~MSIV position~~	~~Discrete (Analog)~~	~~Discrete (Analog)~~	~~N~~	~~Y~~	~~-~~	~~-~~	~~X~~	~~-~~	~~-~~	~~X~~
~~MSIV bypass isolation valve position~~	~~Discrete (Analog)~~	~~Discrete (Analog)~~	~~N~~	~~Y~~	~~-~~	~~-~~	~~X~~	~~-~~	~~-~~	~~X~~
Secondary MSIV position	Discrete (Analog)	Discrete (Analog)	N	N	-	-	X	-	-	X
Secondary MSIV bypass isolation valve position	Discrete (Analog)	Discrete (Analog)	N	N	-	-	X	-	-	X
~~Feedwater isolation valve position~~	~~Discrete (Analog)~~	~~Discrete (Analog)~~	~~N~~	~~Y~~	~~-~~	~~-~~	~~X~~	~~-~~	~~-~~	~~X~~
Feedwater regulation valve position	Discrete (Analog)	Discrete (Analog)	N	N	-	-	X	-	-	X
ECCS valve position	Discrete (Analog)	Discrete (Analog)	N	N	-	-	X	-	-	X
Narrow-range RCS hot temperature	Analog	Analog	Y	N	X	X	-	X	X	-
Wide-range RCS hot temperature	Analog	Analog	Y	Y	X	X	-	X	X	-
Wide-range RCS cold temperature	Analog	Analog	Y	N	X	X	-	X	X	-
Core exit temperature	Analog	Analog	N	Y	-	X	-	X	-	-
Core inlet temperature	Analog	Analog	N	Y	-	X	-	X	-	-
RCS flow (Note 1)	Digital	Analog	Y	N	X	X	-	X	X	-
Main steam pressure (decay heat removal inlet pressure)	Analog	Analog	Y	N	X	X	-	X	X	-
Main steam temperature (decay heat removal inlet temperature)	Analog	Analog	Y	N	X	X	-	X	X	-
Power range linear power	Analog	Analog	Y	~~N~~Y	X	X	-	X	X	-
Intermediate range log power	Analog	Analog	Y	Y	X	X	-	X	X	-
Source range count rate	Analog	Analog	Y	Y	X	X	-	X	X	-
Source/intermediate range fault	Discrete (Analog)	Discrete (Analog)	Y	N	X	X	-	X	X	-

Table 7.1-9: Sensor Inputs to Module Protection System (Continued)

~~Parameter~~Process Variable	Sensor Type	Output Signal	Safety-Related?	Type A, B, or C PAM Variable?	Sensor Block I			Sensor Block II		
					SG A	SG C	DIV. I	SG B	SG D	DIV. II
Power range fault	Discrete (Analog)	Discrete (Analog)	Y	N	X	X	-	X	X	-
NMS Supply Fault	Discrete (Analog)	Discrete (Analog)	Y	N	X	X	-	X	X	-
Inside bioshield area radiation monitor	Digital	Analog	N	Y	-	X	-	X	-	-
Reactor trip breaker position feedback	Discrete (Analog)	Discrete (Analog)	Y~~N~~	N	-	-	X	-	-	X
Pressurizer heater breaker status	Discrete (Analog)	Discrete (Analog)	N	N	-	-	X	-	-	X
DHRS valve position	Discrete (Analog)	Discrete (Analog)	N	N	-	-	X	-	-	X
DHRS outlet temperature	Analog	Analog	N	N	-	X	-	X	-	-
DHRS outlet pressure	Analog	Analog	N	N	X	X	-	X	-	-
Demineralized water system isolation valve position	Discrete (Analog)	Discrete (Analog)	N	N	-	-	X	-	-	X
Reactor pool temperature	Analog	Analog	N	N	-	X	-	X	-	-
EDS voltage	Analog	Analog	N	N	-	X	-	X	-	-
ELVS voltage	Analog	Analog	Y	N	X	X	-	X	X	-
Reactor safety valve position	Discrete (Analog)	Discrete (Analog)	N	N	-	X~~-~~	~~-X~~	X~~-~~	-	~~-X~~
Under-the-bioshield temperature	Analog	Analog	Y	N~~Y~~	X	X	-	X	X	-
NMS-Flood	Analog	Analog	N	Y	-	X	-	X	-	-
NMS-Flood Faults	Discrete (Analog)	Discrete (Analog)	N	Y	-	X	-	X	-	-
Containment evacuation vacuum pump suction pressure	Analog	Analog	N	N	X	-	-	-	X	-

Note 1: These sensors are digital-based and perform safety-related functions.

Table 7.1-11: Partial Spurious Actuation Scenarios for Engineered Safety Features Actuation System within Safety Block I

Scenario	Protective Action(s) on EIM	Components Actuated
1	Containment isolation and DHRS	DHRS actuation valves MSIVs~~;~~ ~~MSIV bypass~~MS isolation bypass valves Feedwater isolation valves Secondary MSIVs Secondary MSIV bypass valves Feedwater regulating valves
2	ECCS	ECCS reactor recirculation valve (Note 1)
3	ECCS and LTOP	ECCS reactor vent valves (Note 1)
4	Containment isolation	Containment evacuation CIV Containment flood & drain CIV Reactor component cooling water CIVs
5	CVCS isolation and containment isolation	CVCS containment isolation valves
6	DWS isolation and loss of AC power	DWS isolation valve
7	PZR heater trip	PZR heater breakers

Note 1: The ECCS valves include an inadvertent actuation block (IAB) described in Section 7.2.5.2 that is designed to prevent the spurious opening of the ECCS valves at normal operating pressures. The spurious opening of the ECCS valves below the IAB setpoint is bounded by the plant safety analysis described in Chapter 15.

Table 7.1-13: Effects of Digital-Based Common Cause Failure of Level Function Type on Sensor Block I

Function Type	~~Parameter~~Process Variable	Sensor Block I	Sensor Block II
Digital-based level measurement	PZR level	Digital-based CCF	OK
	RPV water level	Digital-based CCF	OK
	Containment water level	Digital-based CCF	OK
Digital-based pressure measurement	PZR pressure	OK	OK
	Wide-range RCS pressure	OK	OK
	~~Wide-range containment pressure~~	~~OK~~	~~OK~~
Digital-based flow measurement	RCS flow	OK	OK

Table 7.1-14: Effects of Digital-Based Common Cause Failure of Digital-Based Pressure Measuring System Function Type on Sensor Block I and II

Function Type	~~Parameter~~Process Variable	Sensor Block I	Sensor Block II
Digital-based level measurement	PZR level	OK	OK
	RPV water level	OK	OK
	Containment water level	OK	OK
Digital-based pressure measurement	PZR pressure	Digital-based CCF	Digital-based CCF
	Wide-range RCS pressure	Digital-based CCF	Digital-based CCF
Digital-based flow measurement	RCS flow	OK	OK

Table 7.1-15: Effects of Digital-Based Common Cause Failure of Digital-Based Flow Function Type on Sensor Block I and II

Function Type	~~Parameter~~Process Variable	Sensor Block I	Sensor Block II
Digital-based level measurement	PZR level	OK	OK
	RPV water level	OK	OK
	Containment water level	OK	OK
Digital-based pressure measurement	PZR pressure	OK	OK
	Wide-range RCS pressure	OK	OK
Digital-based flow measurement	RCS flow	Digital-based CCF	Digital-based CCF

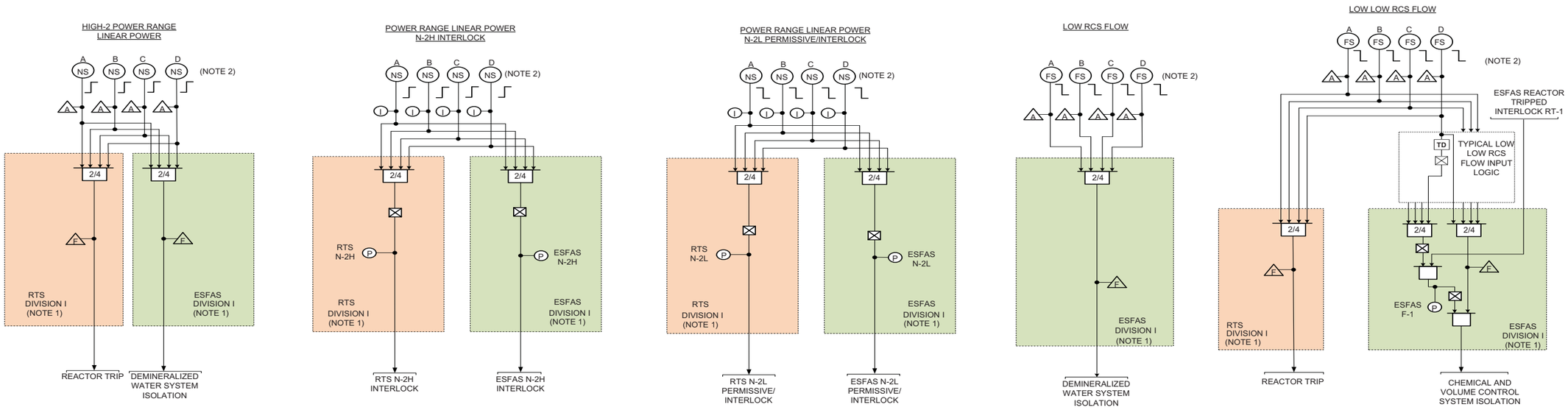
Table 7.1-18: Digital Sensors Credited for Mitigating Anticipated Operational Occurrences and Postulated Accidents (Continued)

Design Basis Event	Signals Credited in Plant Safety Analysis Described in Chapter 15	Signals Credited in D3 Best-Estimate Coping Analysis	Comments
Category 4 Events			
For the design basis events listed below, while the deterministic plant safety analyses described in Chapter 15 credit the function provided by the digital-based sensors that are subject to a CCF; however, the evaluation of the plant response for these events using best-estimate analysis methods determined that the plant response does not progress to the point where the digital-based sensor is relied upon to provide required protection. In these events, other sensors that do not use digital-based technology and are not subject to a digital-based CCF provide the required safety function and the FPGA technology diversity in the MPS divisions ensures a digital-based CCF does not prevent the MPS from performing its required safety function (note 2).			
Control Rod Misoperation	high power range linear power high RCS hot temperature high PZR pressure (digital-based) high power range negative rate (control rod drop)	high power range linear power high RCS hot temperature high power range negative rate (control rod drop)	Diverse sensors not subject to a digital-based CCF provide required protection. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Inadvertent Operation of Emergency Core Cooling System (ECCS)	high CNV pressure low RPV water level (note 1)	high CNV pressure low RPV water level (note 1)	Diverse sensors not subject to a digital-based CCF provide required protection. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Failure of Small Lines Carrying Primary Coolant Outside Containment	low PZR level (see note 1) low PZR pressure (digital-based)	low PZR level (see note 1)	Diverse sensors not subject to a digital-based CCF provide required protection. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.
Instability Events	high RCS hot temperature low pressurizer level (note 1) low PZR pressure (digital-based)	high RCS hot temperature low pressurizer level (note 1)	Diverse sensors not subject to a digital-based CCF provide required protection. FPGA technology diversity within the MPS limits digital-based CCF impact to one of two divisions - the other division remains fully functional.

Note 1: The digital-based level measurement function incorporates equipment diversity between sensor blocks I and II such that a postulated CCF of the digital-based level measurement function is limited to one sensor block only. Since the other sensor block remains functional, sufficient diversity exists for those functions that rely on the digital-based level measurement function, see Section 7.1.5.1.2.

Note 2: The design basis for the digital-based RCS flow sensor is to ensure minimum RCS flow rates exist during dilution events to ensure proper mixing within the RCS. Best-estimate analysis of this event concludes the event is non-limiting, and does not rely on the digital-based RCS flow sensor to function. The FPGA technology diversity in the MPS divisions ensures a digital-based CCF does not prevent the MPS from performing its required safety function.

Figure 7.1-1c: Power Range High-2 Power Trip and N-2 Interlocks, Low and Low Low RCS Flow Trips



P	RTS/ESFAS N-2H	INTERLOCK STATUS
○	ACTIVE	3oo4 PR INPUTS < N-2H SETPOINT
●	NOT ACTIVE	2oo4 PR INPUTS ≥ N-2H SETPOINT

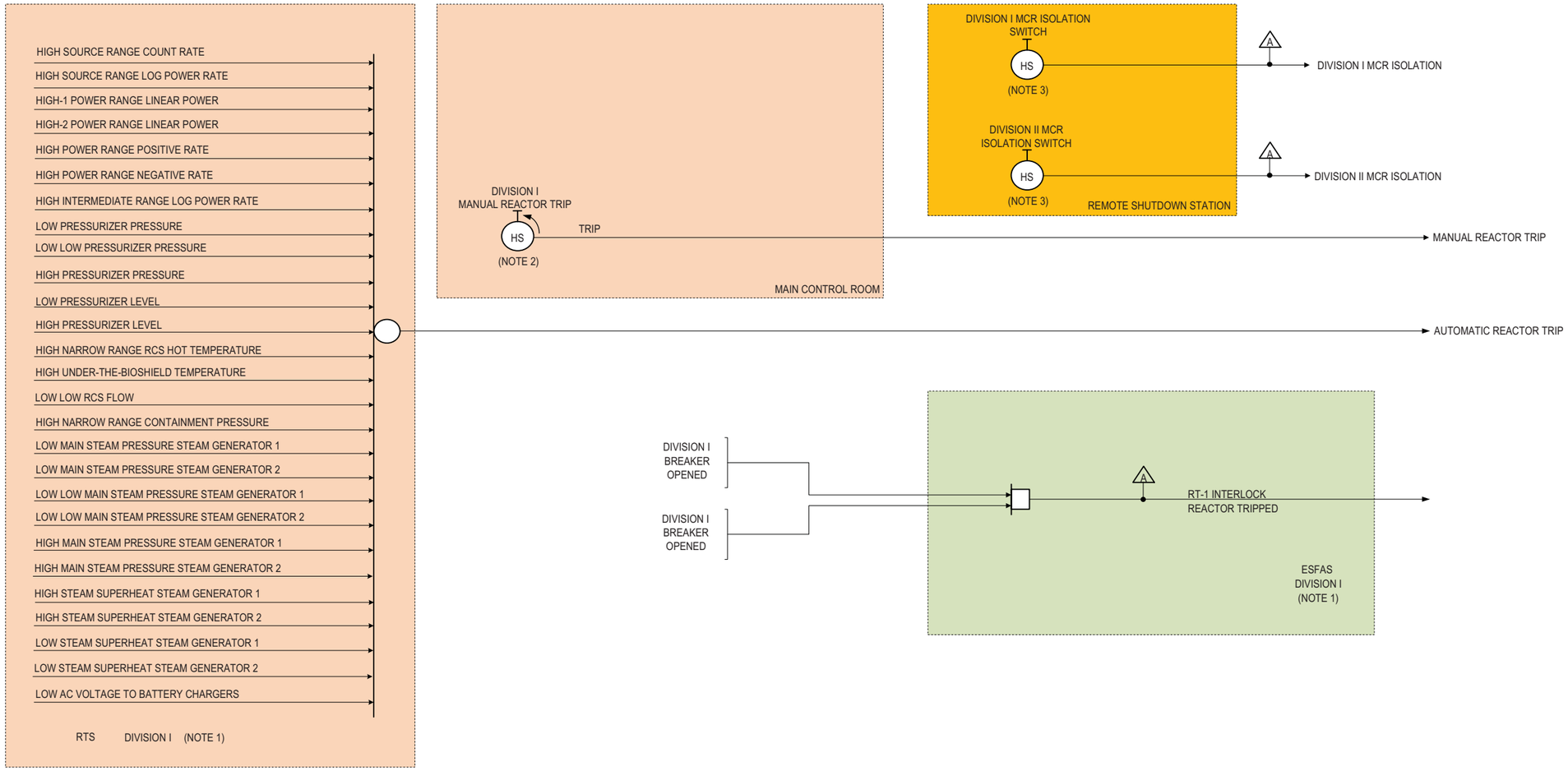
P	RTS/ESFAS N-2L	PERMISSIVE/INTERLOCK STATUS
○	ACTIVE	3oo4 PR INPUTS > N-2L SETPOINT
●	NOT ACTIVE	2oo4 PR INPUTS ≤ N-2L SETPOINT

P	ESFAS F-1	LOW LOW RCS FLOW CVCSI ACTUATION INTERLOCK STATUS
○	ACTIVE	3oo4 FLOW INPUTS < LOW LOW SETPOINT FOR MORE THAN TD, AND RT-1 ACTIVE
●	NOT ACTIVE	2oo4 RCS FLOW INPUTS > LOW LOW SETPOINT FOR MORE THAN TD, OR 3oo4 RCS FLOW INPUTS < LOW LOW SETPOINT FOR LESS THAN TDM OR RT-1 NOT ACTIVE

NOTE 1: LOGIC IS SHOWN FOR DIVISION I ONLY. LOGIC FOR DIVISION II IS THE SAME AS DIVISION I.

NOTE 2: THERE IS A TRIP/BYPASS SWITCH FOR EACH SFM THAT HAS A SAFETY FUNCTION THAT SUPPORTS REMOVING THE SFM FROM SERVICE.

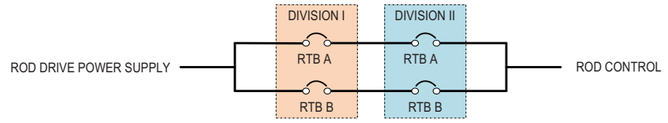
Figure 7.1-1j: Reactor Trip and Reactor Tripped Interlock RT-1



NOTE 1: LOGIC IS SHOWN FOR DIVISION I ONLY. LOGIC FOR DIVISION II IS THE SAME AS DIVISION I.

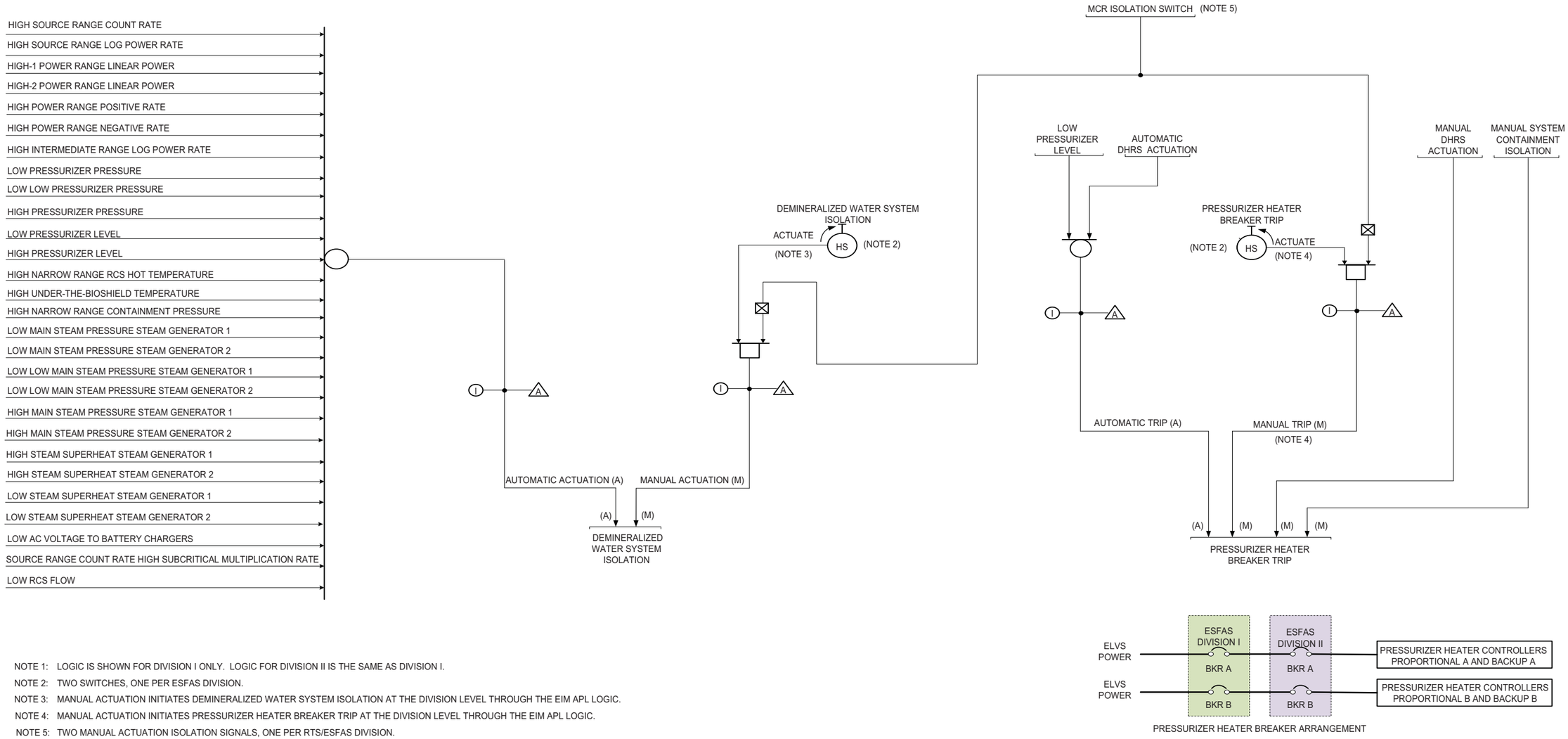
NOTE 2: TWO MOMENTARY REDUNDANT SWITCHES, ONE PER RTS DIVISION.

NOTE 3: TWO MANUAL ACTUATION ISOLATION REDUNDANT SWITCHES LOCATED IN THE REMOTE SHUTDOWN STATION, ONE PER RTS AND ESFAS DIVISION.



REACTOR TRIP BREAKER ARRANGEMENT

Figure 7.1-1m: ESFAS - Demineralized Water System Isolation, Pressurizer Heater Trip



PRESSURIZER HEATER BREAKER ARRANGEMENT

NOTE 1: LOGIC IS SHOWN FOR DIVISION I ONLY. LOGIC FOR DIVISION II IS THE SAME AS DIVISION I.

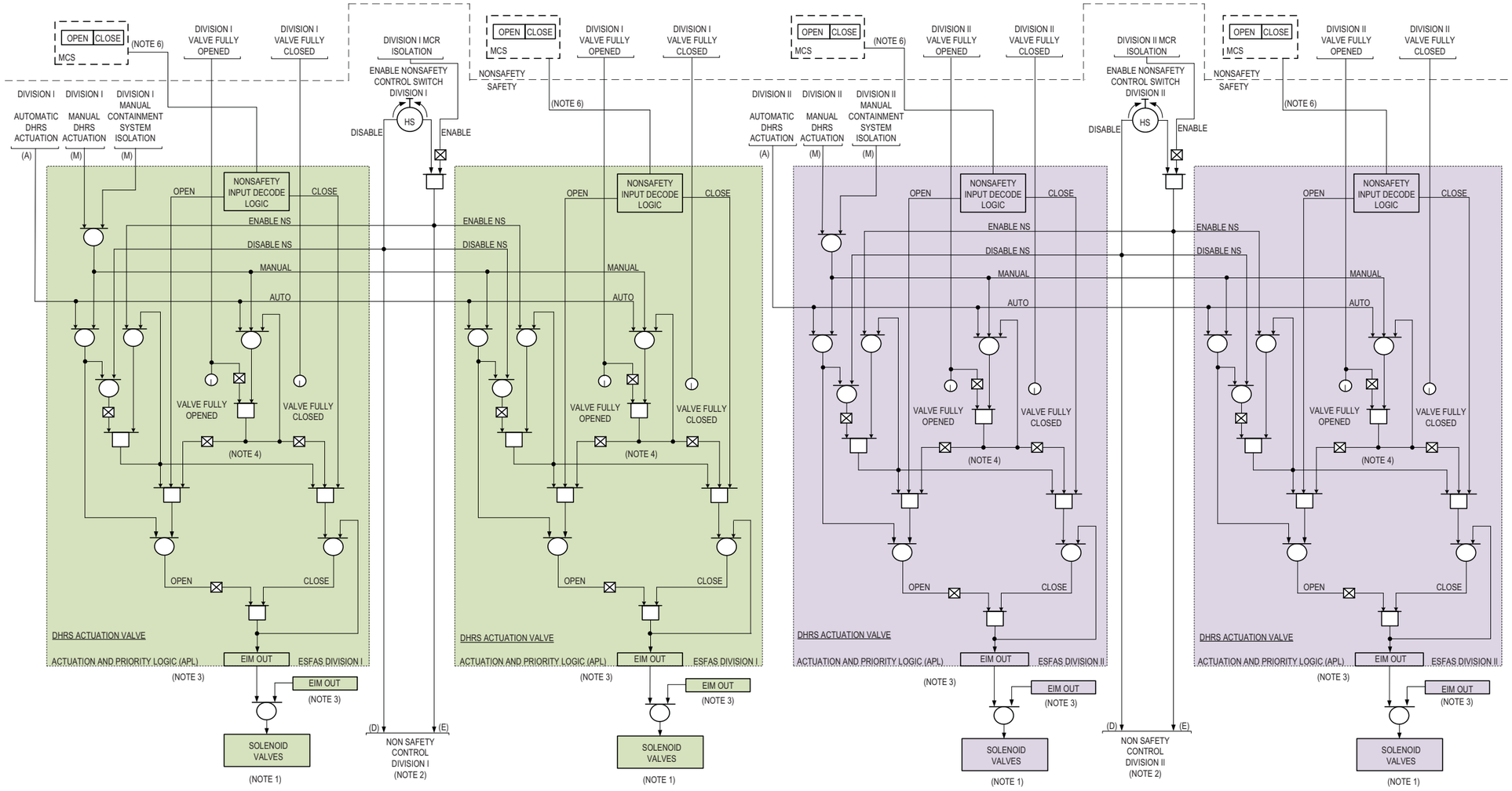
NOTE 2: TWO SWITCHES, ONE PER ESFAS DIVISION.

NOTE 3: MANUAL ACTUATION INITIATES DEMINERALIZED WATER SYSTEM ISOLATION AT THE DIVISION LEVEL THROUGH THE EIM APL LOGIC.

NOTE 4: MANUAL ACTUATION INITIATES PRESSURIZER HEATER BREAKER TRIP AT THE DIVISION LEVEL THROUGH THE EIM APL LOGIC.

NOTE 5: TWO MANUAL ACTUATION ISOLATION SIGNALS, ONE PER RTS/ESFAS DIVISION.

Figure 7.1-1o: Decay Heat Removal System Valve Actuation



NOTE 1: SOLENOIDS ARE ENERGIZED BY REDUNDANT EIMS TO CLOSE VALVE; SOLENOIDS ARE DE-ENERGIZED TO OPEN VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.

NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

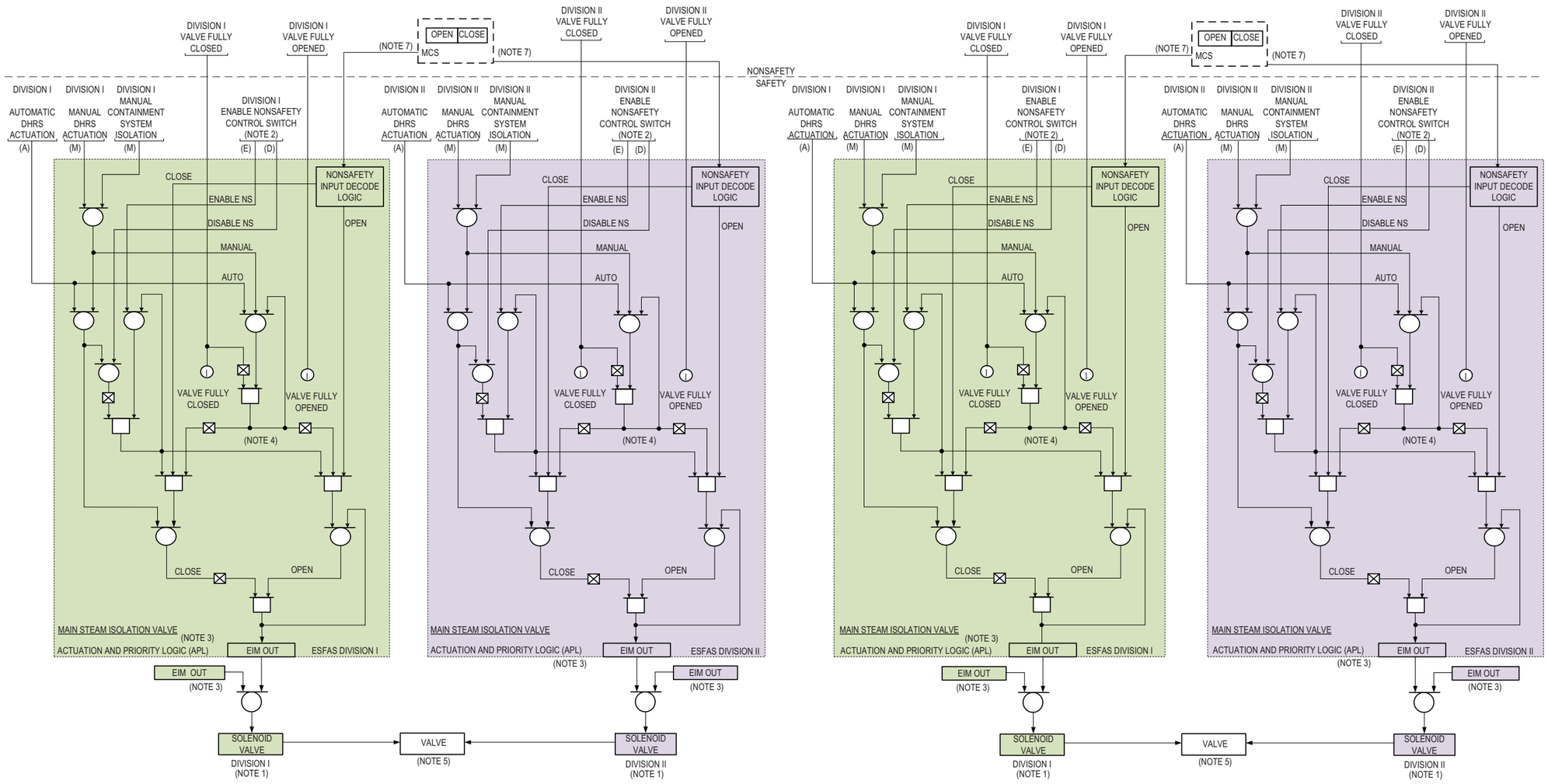
NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.

NOTE 6: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1p: Main Steam Isolation Valve Actuation



NOTE 1: SOLENOIDS ARE ENERGIZED BY REDUNDANT EIMS TO OPEN VALVE; SOLENOIDS ARE DE-ENERGIZED TO CLOSE VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.

NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

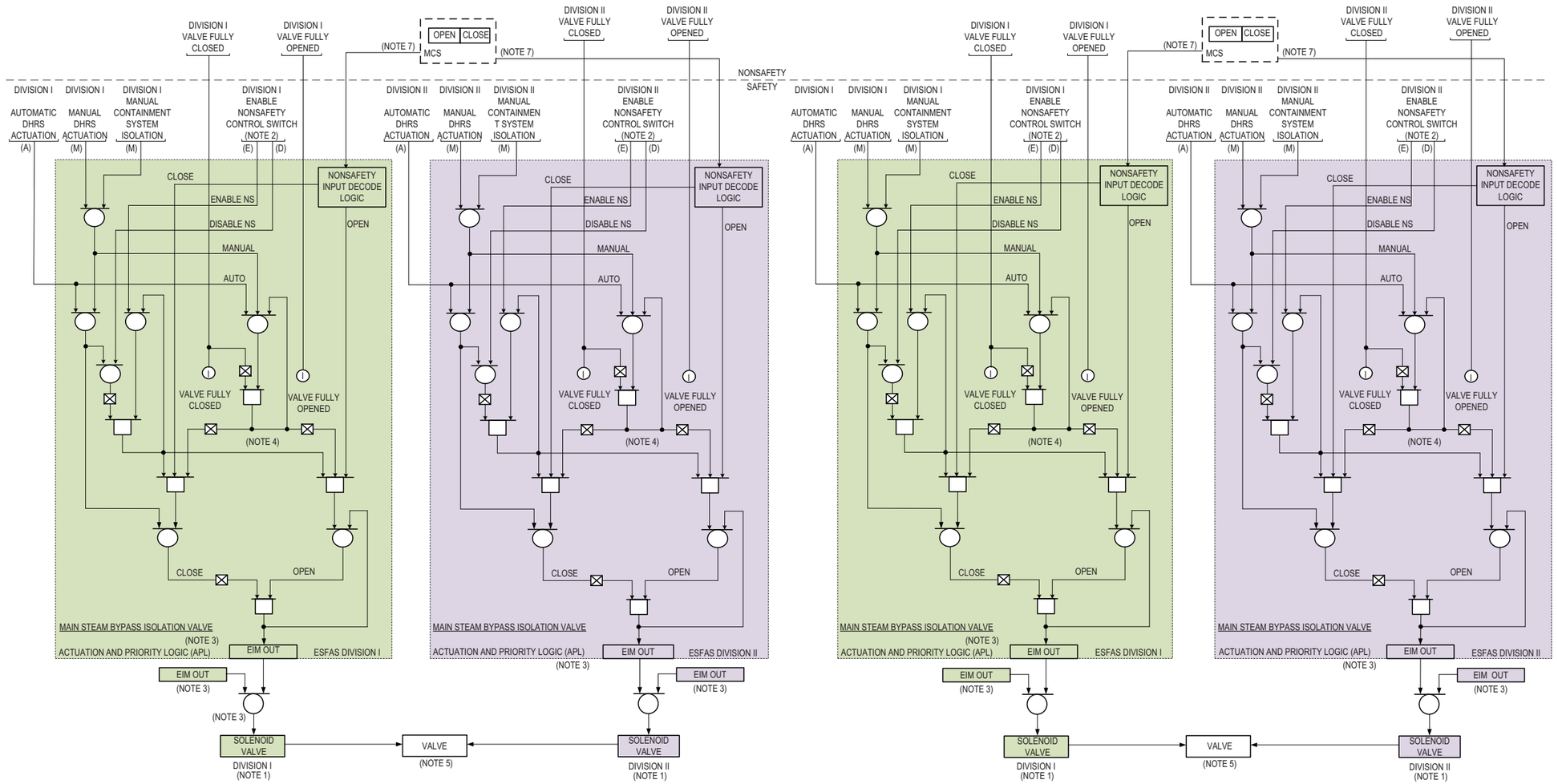
NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: VALVE IS CONTROLLED BY TWO REDUNDANT SOLENOIDS. ONE FROM EACH DIVISION. THE VALVE CLOSES WHEN EITHER THE DIVISION I OR DIVISION II SOLENOID IS DE-ENERGIZED. THE VALVE OPENS ONLY WHEN BOTH THE DIVISION I AND DIVISION II SOLENOIDS ARE ENERGIZED.

NOTE 6: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.

NOTE 7: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1q: Main Steam Isolation Bypass Valve Actuation



NOTE 1: SOLENOIDS ARE ENERGIZED BY REDUNDANT EIMS TO OPEN VALVE; SOLENOIDS ARE DE-ENERGIZED TO CLOSE VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.

NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

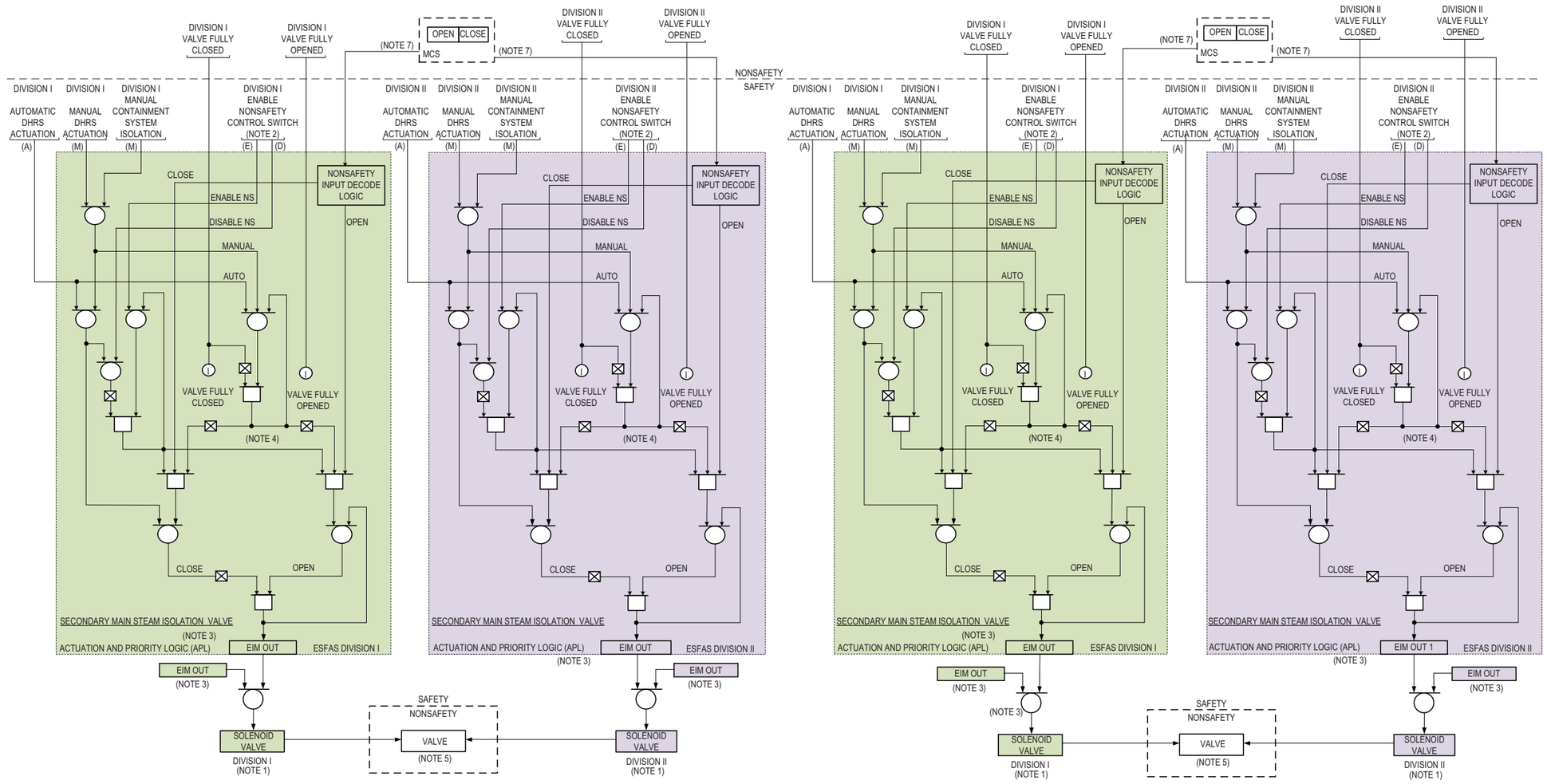
NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: VALVE IS CONTROLLED BY TWO REDUNDANT SOLENOIDS. ONE FROM EACH DIVISION. THE VALVE CLOSES WHEN EITHER THE DIVISION I OR DIVISION II SOLENOID IS DE-ENERGIZED. THE VALVE OPENS ONLY WHEN BOTH THE DIVISION I AND DIVISION II SOLENOIDS ARE ENERGIZED.

NOTE 6: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.

NOTE 7: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1r: Secondary Main Steam Isolation Valve Actuation



NOTE 1: SOLENOIDS ARE ENERGIZED BY REDUNDANT EIMS TO OPEN VALVE; SOLENOIDS ARE DE-ENERGIZED TO CLOSE VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.

NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

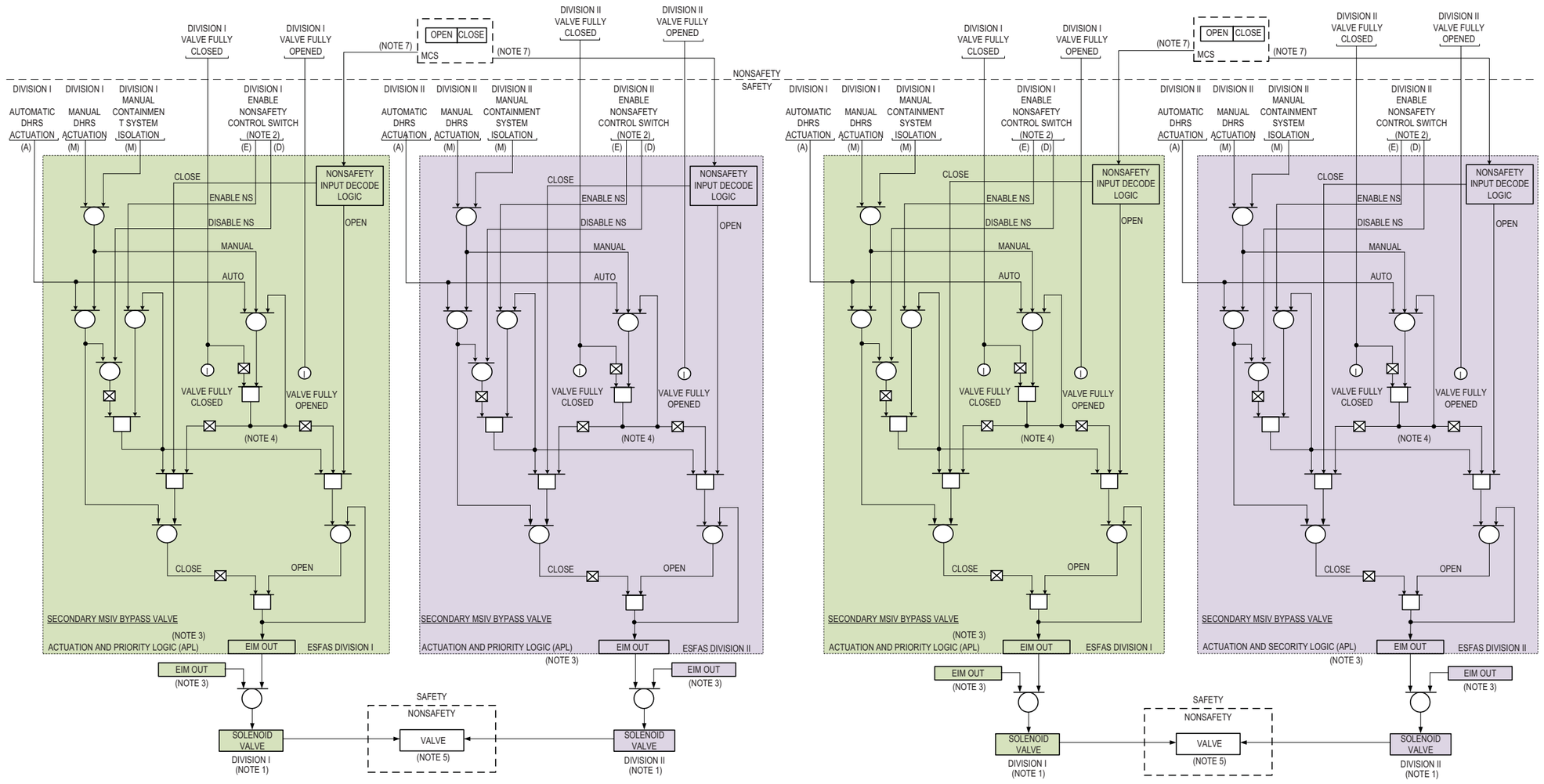
NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: VALVE IS CONTROLLED BY TWO REDUNDANT SOLENOIDS. ONE FROM EACH DIVISION. THE VALVE CLOSES WHEN EITHER THE DIVISION I OR DIVISION II SOLENOID IS DE-ENERGIZED. THE VALVE OPENS ONLY WHEN BOTH THE DIVISION I AND DIVISION II SOLENOIDS ARE ENERGIZED.

NOTE 6: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.

NOTE 7: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1s: Secondary ~~Main Steam Isolation~~MSIV Bypass Valve Actuation



NOTE 1: SOLENOIDS ARE ENERGIZED BY REDUNDANT EIMS TO OPEN VALVE; SOLENOIDS ARE DE-ENERGIZED TO CLOSE VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.

NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

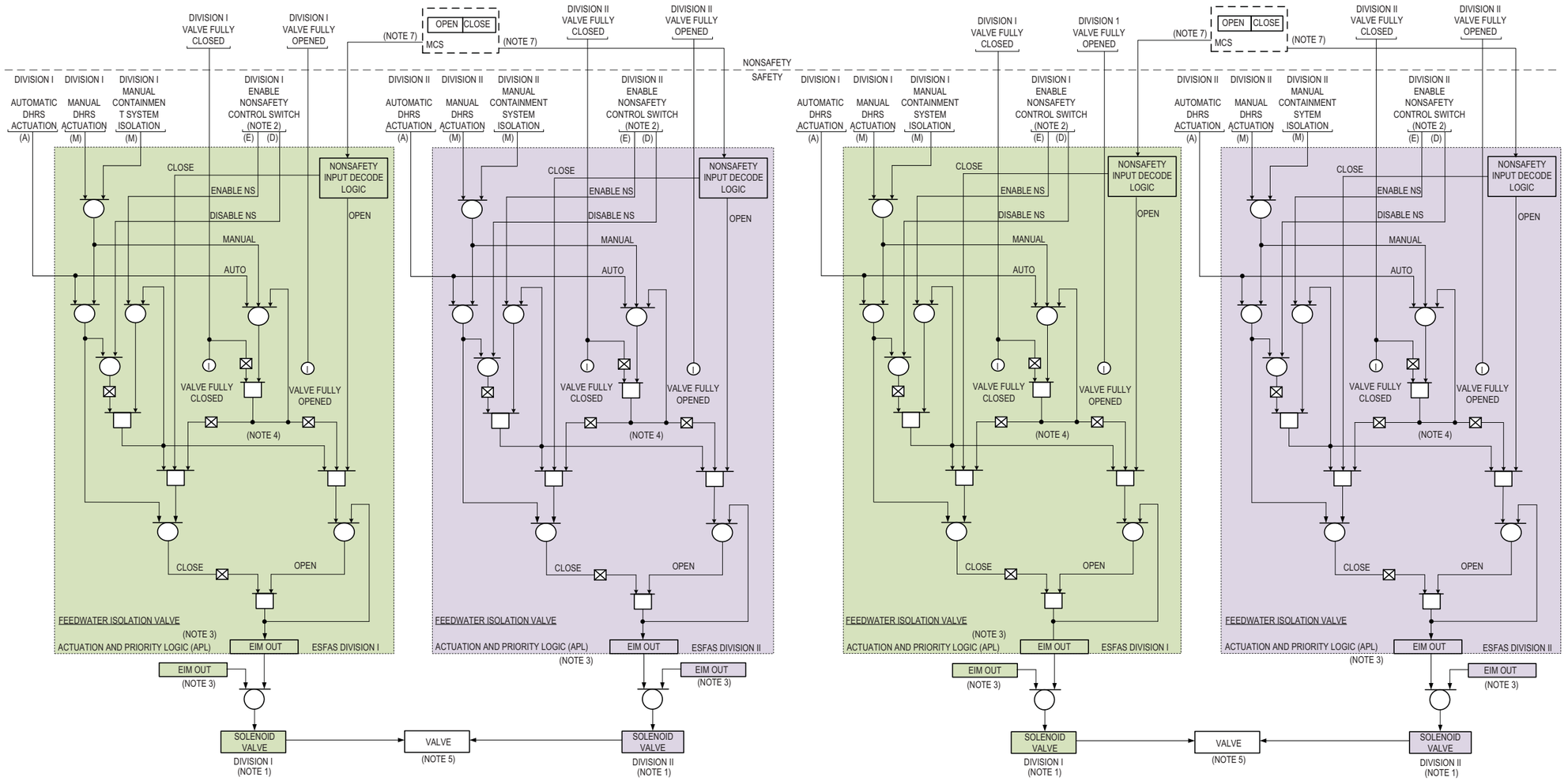
NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: VALVE IS CONTROLLED BY TWO REDUNDANT SOLENOIDS. ONE FROM EACH DIVISION. THE VALVE CLOSES WHEN EITHER THE DIVISION I OR DIVISION II SOLENOID IS DE-ENERGIZED. THE VALVE OPENS ONLY WHEN BOTH THE DIVISION I AND DIVISION II SOLENOIDS ARE ENERGIZED.

NOTE 6: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.

NOTE 7: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1t: Feedwater Isolation Valve Actuation



NOTE 1: SOLENOIDS ARE ENERGIZED BY REDUNDANT EIMS TO OPEN VALVE; SOLENOIDS ARE DE-ENERGIZED TO CLOSE VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.

NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

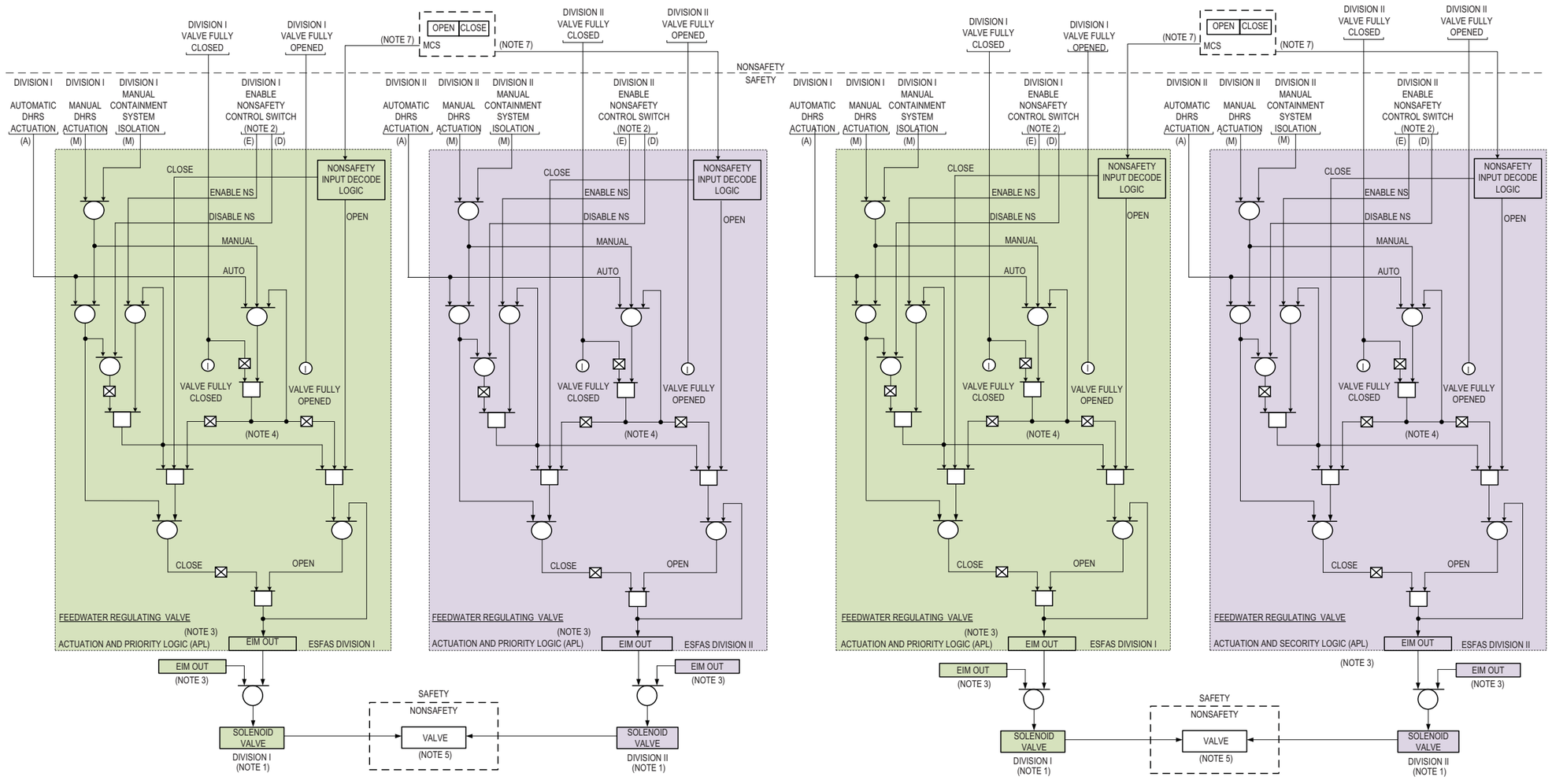
NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: VALVE IS CONTROLLED BY TWO REDUNDANT SOLENOIDS. ONE FROM EACH DIVISION. THE VALVE CLOSES WHEN EITHER THE DIVISION I OR DIVISION II SOLENOID IS DE-ENERGIZED. THE VALVE OPENS ONLY WHEN BOTH THE DIVISION I AND DIVISION II SOLENOIDS ARE ENERGIZED.

NOTE 6: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.

NOTE 7: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1u: Feedwater ~~Regulation~~Regulating Valve Isolation



NOTE 1: SOLENOID IS ENERGIZED BY REDUNDANT EIMS TO ALLOW NONSAFETY CONTROL OF VALVE; SOLENOID IS DE-ENERGIZED TO CLOSE VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.

NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

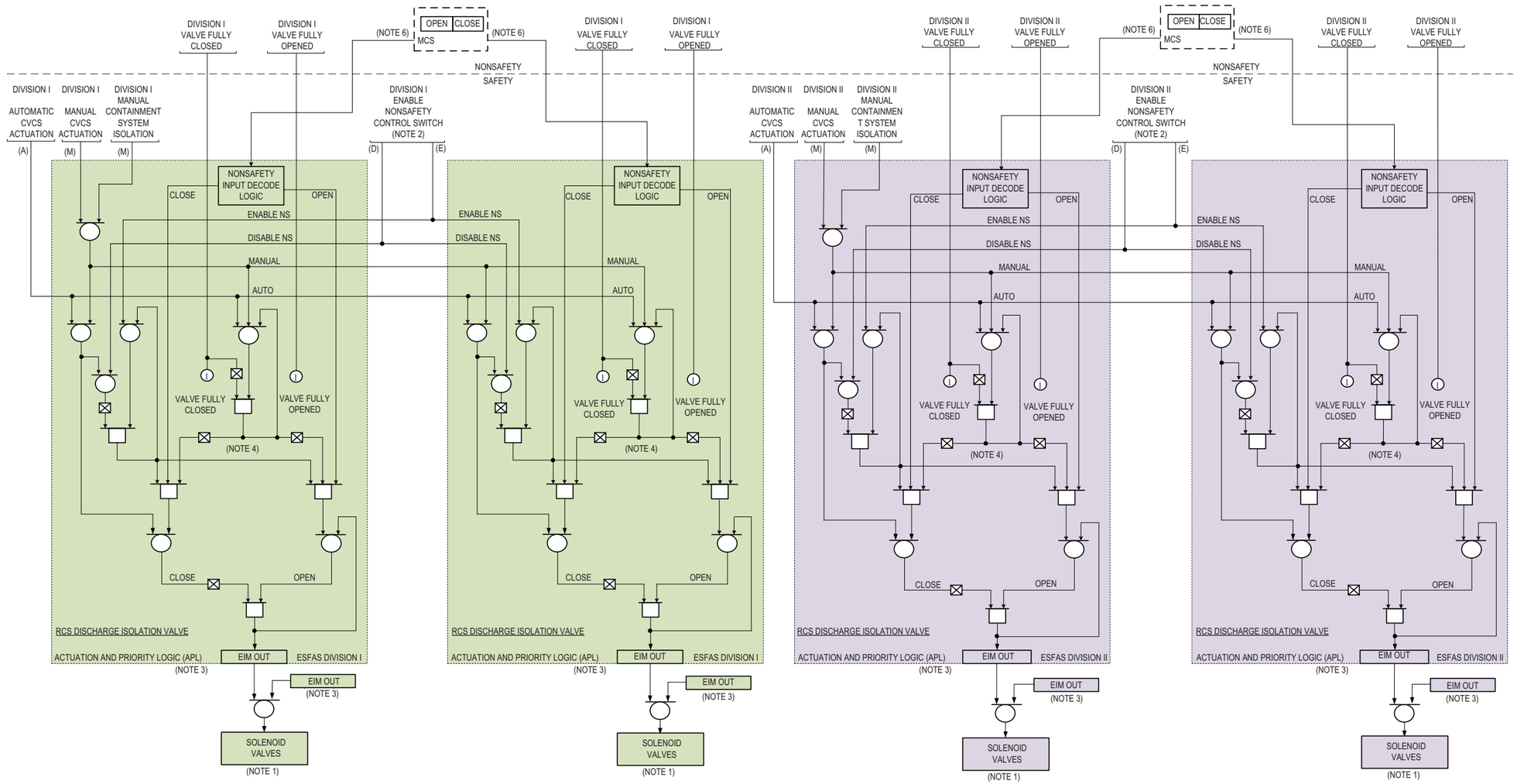
NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: VALVE IS CONTROLLED BY TWO REDUNDANT SOLENOIDS. ONE FROM EACH DIVISION. THE VALVE CLOSES WHEN EITHER THE DIVISION I OR DIVISION II SOLENOID IS DE-ENERGIZED. THE VALVE OPENS ONLY WHEN BOTH THE DIVISION I AND DIVISION II SOLENOIDS ARE ENERGIZED.

NOTE 6: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.

NOTE 7: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1v: Chemical and Volume Control System RCS ~~Injuection~~Injection ~~Dishargе~~and Discharge Valve Actuation



NOTE 1: SOLENOIDS ARE ENERGIZED BY REDUNDANT EIMS TO OPEN VALVE; SOLENOIDS ARE DE-ENERGIZED TO CLOSE VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.

NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

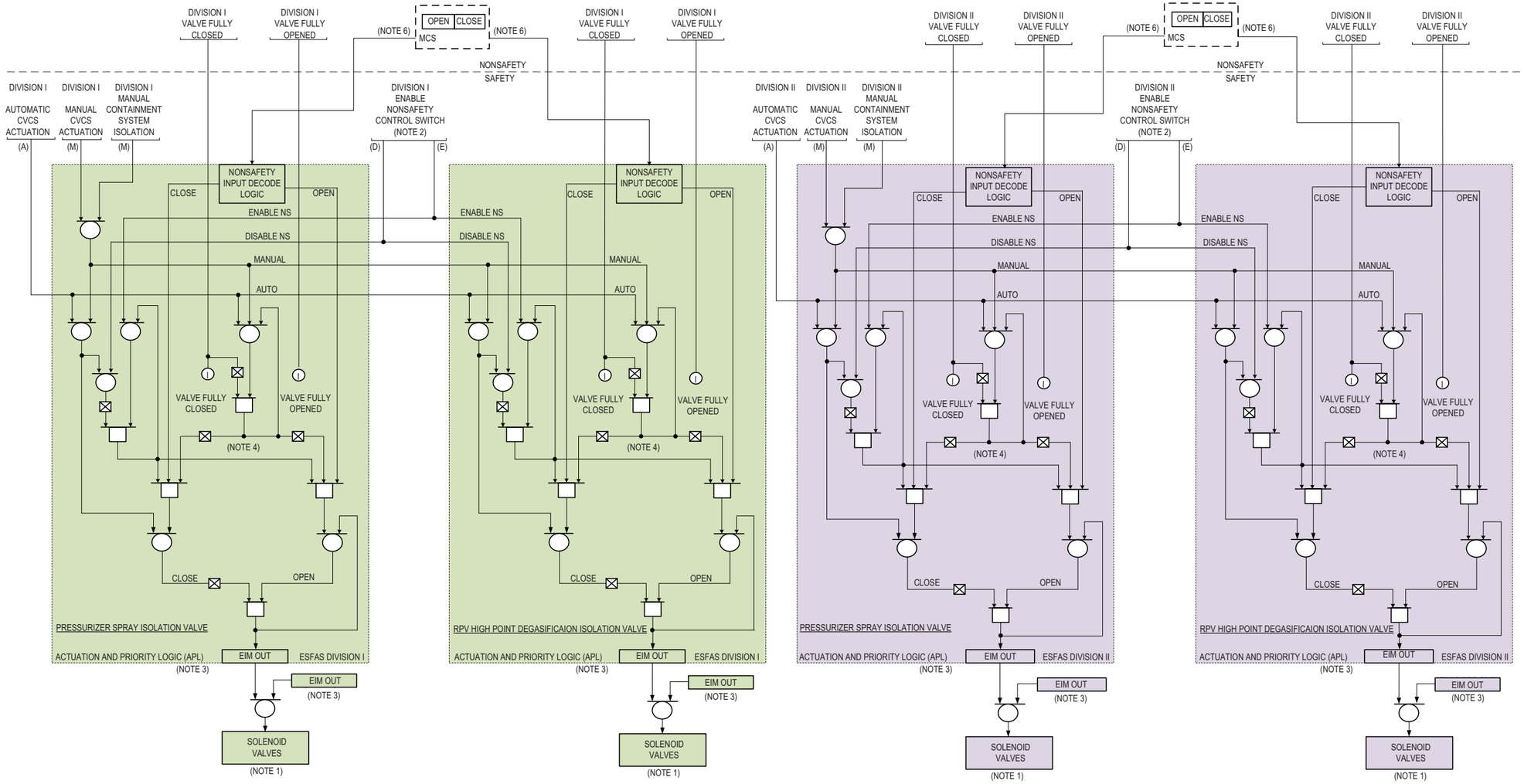
NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.

NOTE 6: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1w: Chemical and Volume Control System Pressurizer Spray and High Point Degasification Valve Actuation



NOTE 1: SOLENOIDS ARE ENERGIZED BY REDUNDANT EIMS TO OPEN VALVE; SOLENOIDS ARE DE-ENERGIZED TO CLOSE VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.

NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

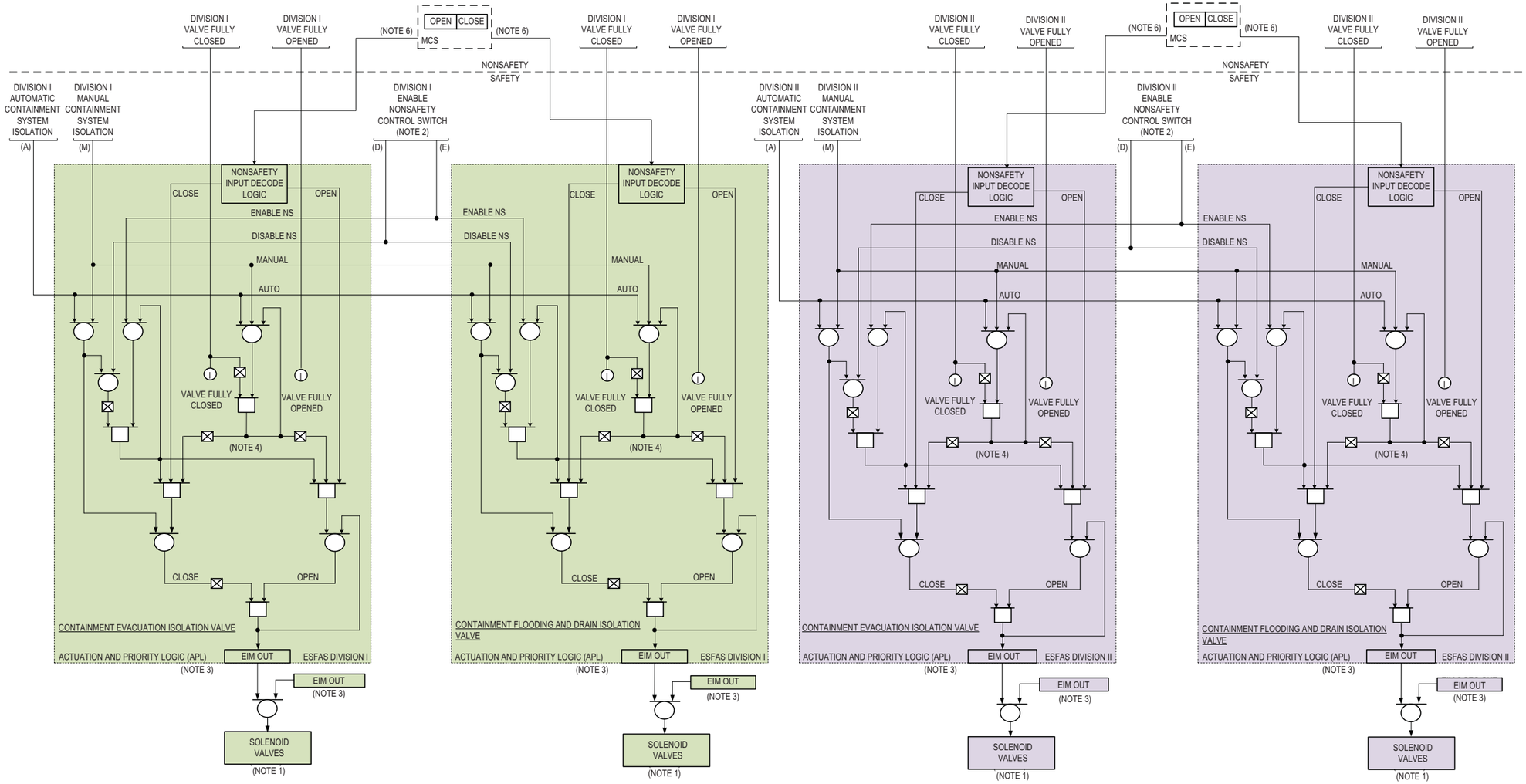
NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.

NOTE 6: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1x: Containment Flooding and Drain and Containment Evacuation Valve Actuation



NOTE 1: SOLENOIDS ARE ENERGIZED BY REDUNDANT EIMS TO OPEN VALVE; SOLENOIDS ARE DE-ENERGIZED TO CLOSE VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.

NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

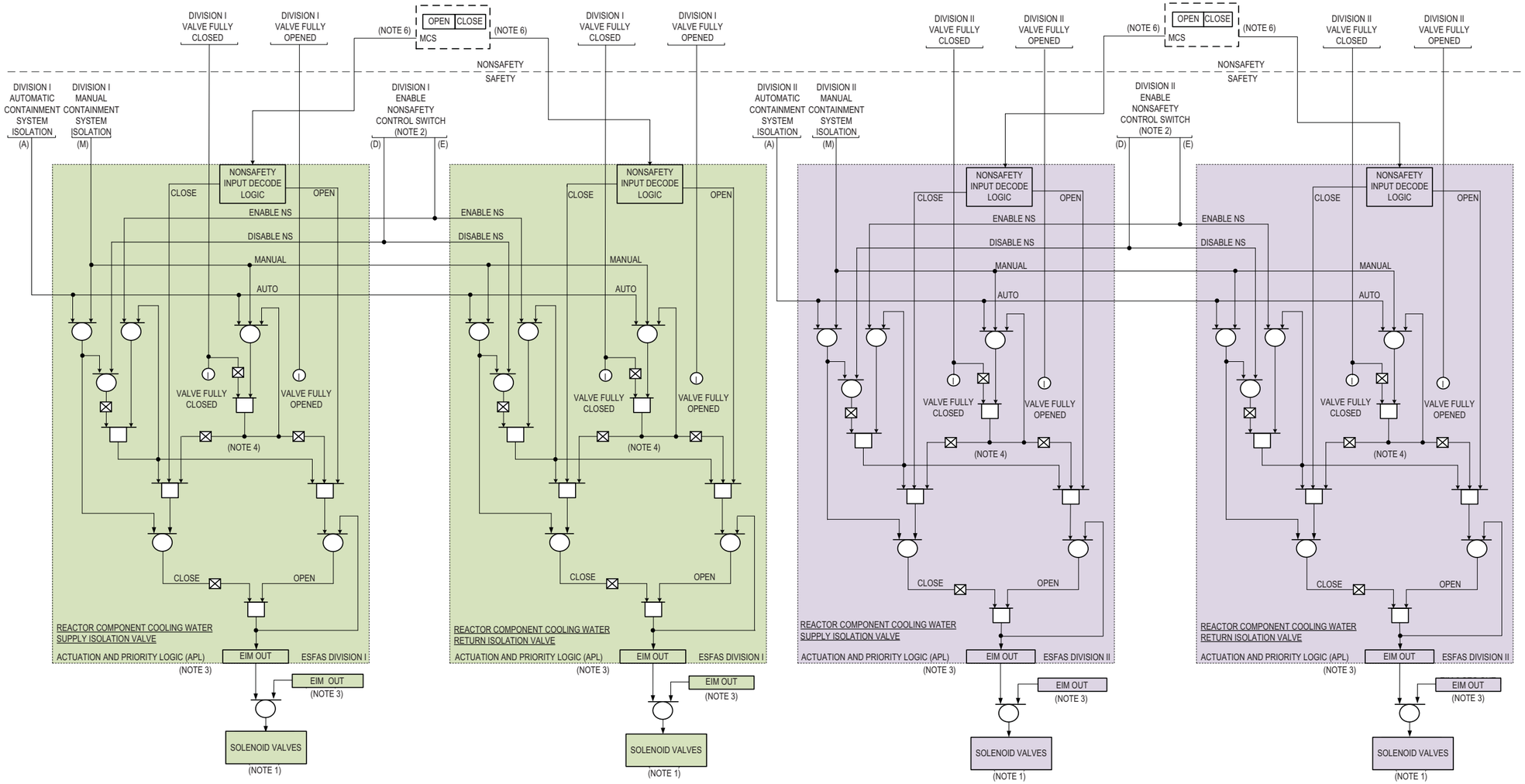
NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.

NOTE 6: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1y: Reactor Component Cooling Water System Valve Actuation



NOTE 1: SOLENOIDS ARE ENERGIZED BY REDUNDANT EIMS TO OPEN VALVE; SOLENOIDS ARE DE-ENERGIZED TO CLOSE VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.

NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

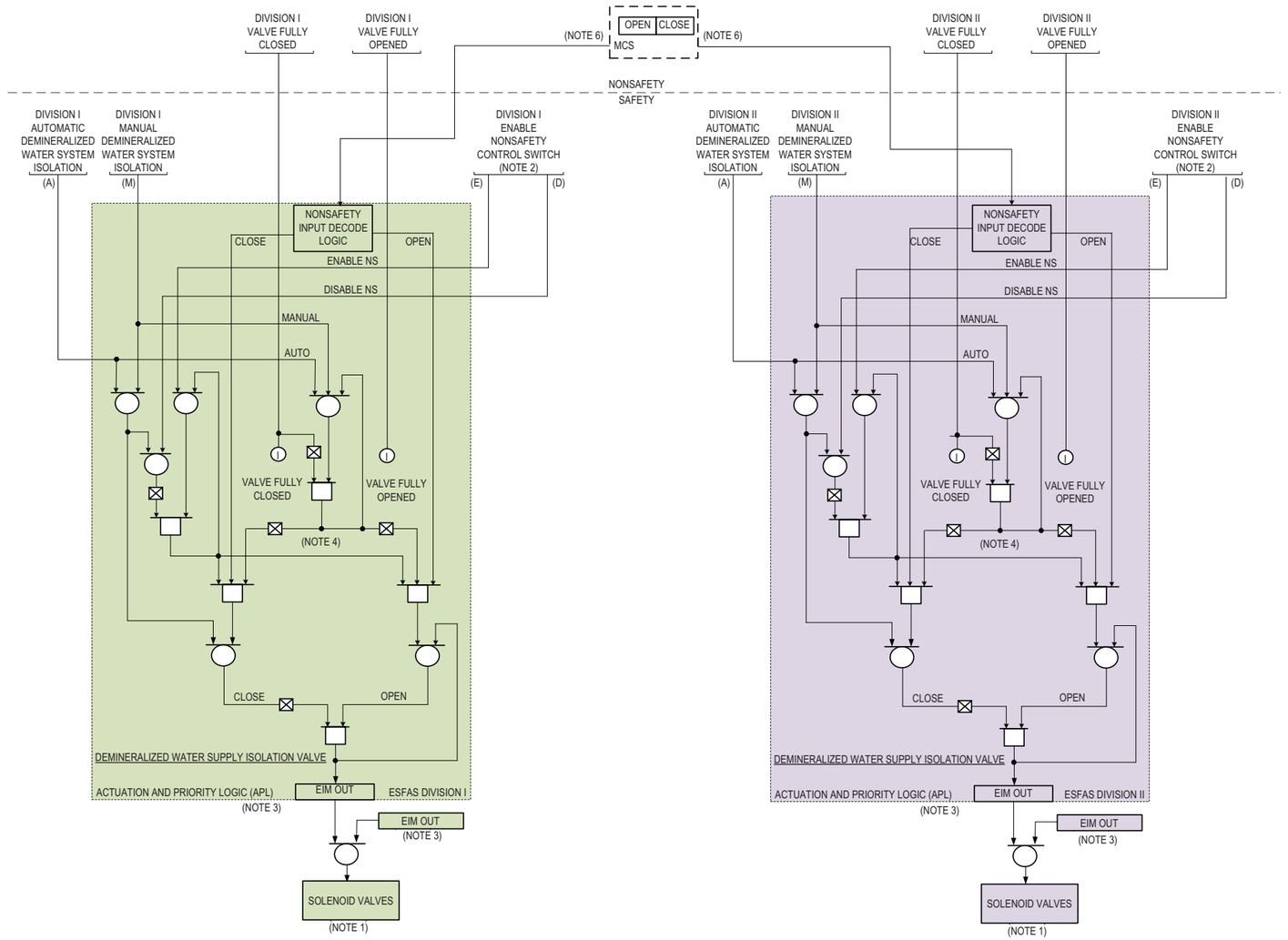
NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.

NOTE 6: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1z: Demineralized Water Supply Valve Actuation



NOTE 1: SOLENOIDS ARE ENERGIZED BY REDUNDANT EIMS TO OPEN VALVE; SOLENOIDS ARE DE-ENERGIZED TO CLOSE VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.

NOTE 2: ONE ENABLE NONSAFETY SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

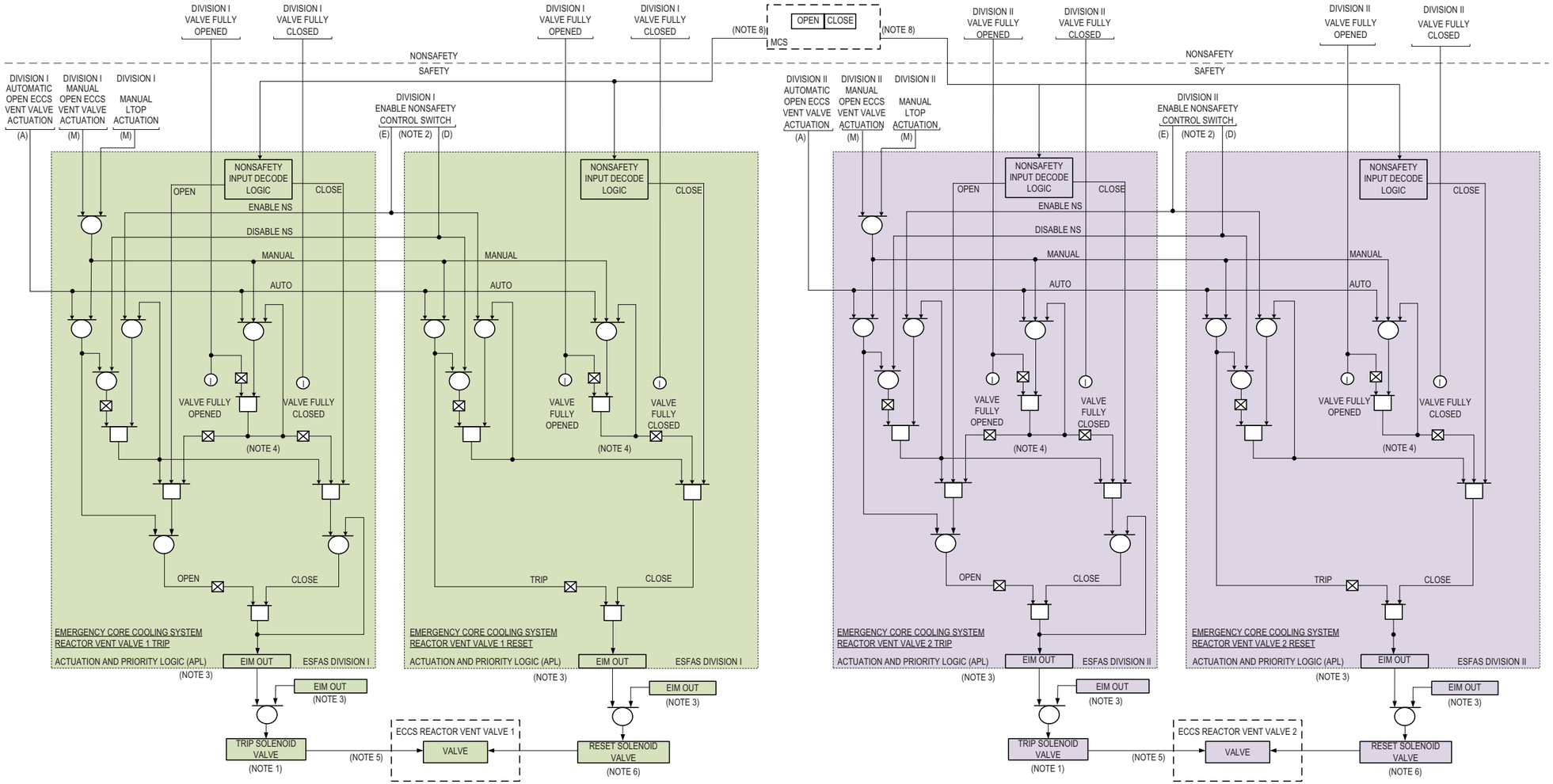
NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTUATION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

NOTE 5: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.

NOTE 6: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1aa: Emergency Core Cooling System Reactor Vent Valve 1 & 2 Actuation



NOTE 1: THE ECCS VENT VALVE IS CLOSED WITH THE TRIP SOLENOID VALVE ENERGIZED BY REDUNDANT EIMS; THE TRIP SOLENOID IS DE-ENERGIZED TO OPEN THE ECCS VENT VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.

NOTE 2: ONE ENABLE NONSAFTEY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

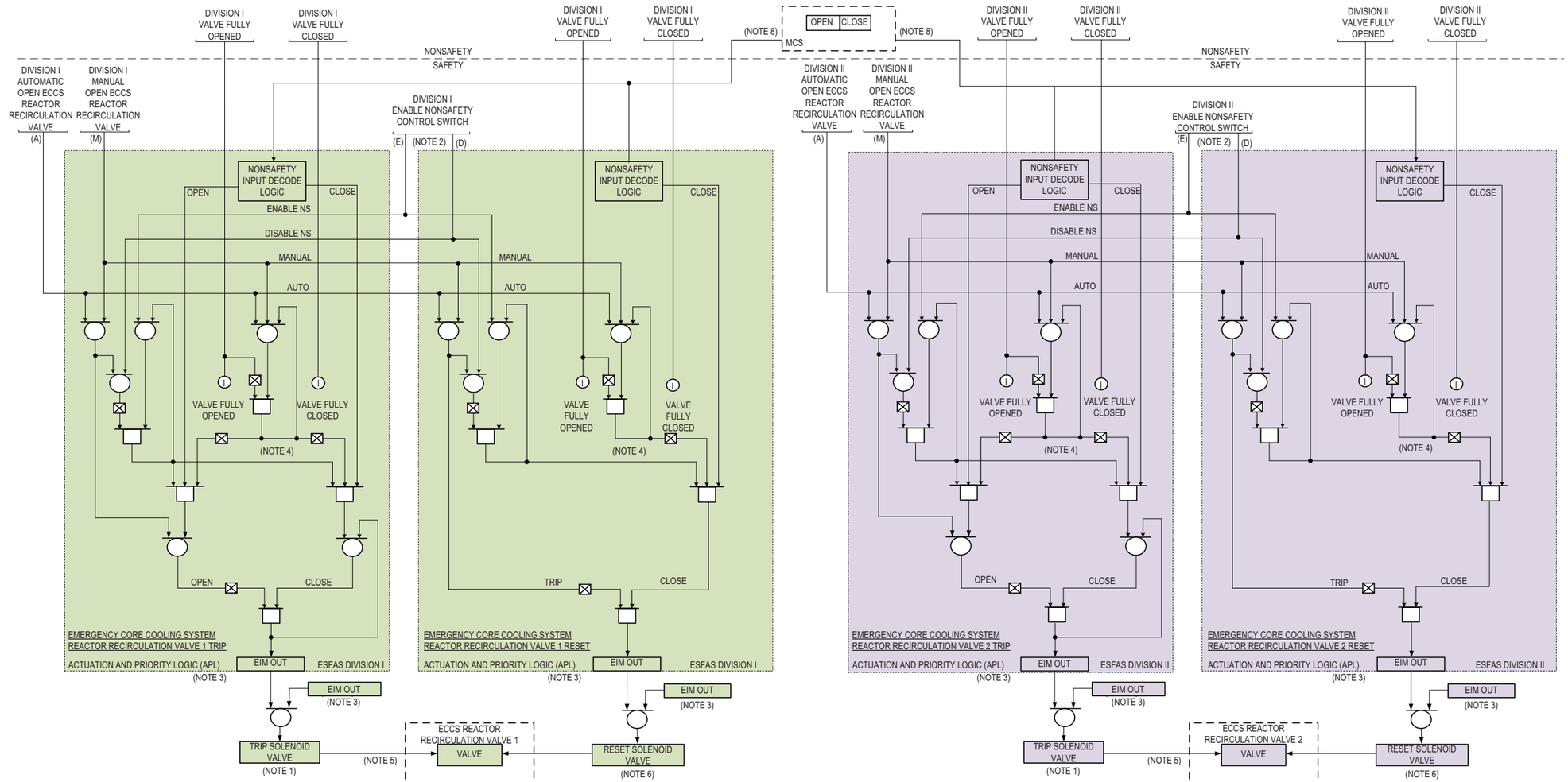
NOTE 5: THE ECCS VENT VALVE DESIGN INCLUDES AN ARMING VALVE. THE ARMING VENT VALVE IMPLEMENTS THE INADVERTENT ACTUATION BLOCK (IAB) FUNCTION THAT DELAYS OPENING OF THE ECCS VENT VALVE WHEN THE TRIP SOLENOID DE-ENERGIZES UNTIL RPV TO CNV DIFFERENTIAL PRESSURE IS BELOW THE ARMING VENT VALVE SET PRESSURE.

NOTE 6: THE ECCS RESET SOLENOID VALVE IS NORMALLY DE-ENERGIZED (CLOSED). THE RESET SOLENOID MUST BE ENERGIZED (OPENED) TO CLOSE THE ECCS VALVE. THIS PROVIDES A PATH FOR CVCS MAKEUP TO THE MAIN VALVE CONTROL CHAMBER UNTIL RPV PRESSURE IS SUFFICIENT TO OVERCOME THE SPRING FORCE HOLDING THE VALVE OPEN.

NOTE 7: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.

NOTE 8: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1ab: Emergency Core Cooling System Reactor Recirculation Valve Actuation



NOTE 1: THE ECCS RECIRCULATION VALVE IS CLOSED WITH THE TRIP SOLENOID VALVE ENERGIZED BY REDUNDANT EIMS; THE TRIP SOLENOID IS DE-ENERGIZED TO OPEN THE ECCS RECIRCULATION VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.

NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

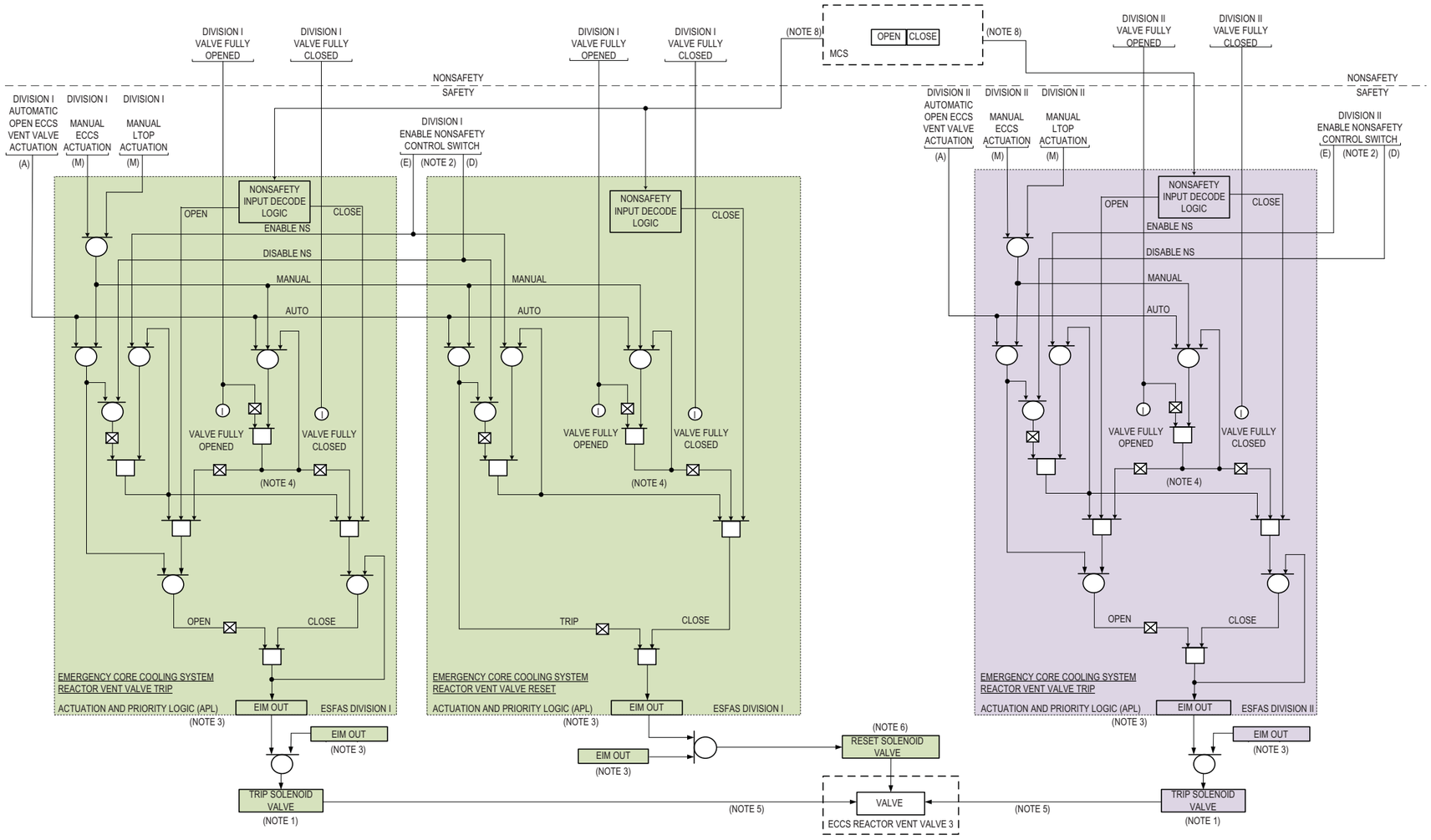
NOTE 5: THE ECCS RECIRCULATION VALVE DESIGN INCLUDES AN ARMING VALVE. THE ARMING VALVE IMPLEMENTS THE INADVERTENT ACTUATION BLOCK (IAB) FUNCTION THAT DELAYS OPENING OF THE ECCS RECIRCULATION VALVE WHEN THE TRIP SOLENOID DE-ENERGIZES UNTIL RPV TO CNV DIFFERENTIAL PRESSURE IS BELOW THE ARMING VALVE SET PRESSURE.

NOTE 6: THE ECCS RESET SOLENOID VALVE IS NORMALLY DE-ENERGIZED (CLOSED). THE RESET SOLENOID MUST BE ENERGIZED (CLOSED) TO OPEN THE ECCS RECIRCULATION VALVE. THIS PROVIDES A PATH FOR CVCS MAKEUP TO THE MAIN VALVE CONTROL CHAMBER UNTIL RPV PRESSURE IS SUFFICIENT TO OVERCOME THE SPRING FORCE HOLDING THE VALVE OPEN.

NOTE 7: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.

NOTE 8: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1ac: Emergency Core Cooling System Reactor Vent Valve 3 Actuation



NOTE 1: THE ECCS VENT VALVE IS CLOSED WITH THE TRIP SOLENOID VALVE ENERGIZED BY REDUNDANT EIMS; THE TRIP SOLENOID IS DE-ENERGIZED TO OPEN THE ECCS VENT VALVE WHEN BOTH EIM OUTPUTS ARE DE-ENERGIZED.

NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

NOTE 3: THE LOGIC SHOWN IS IMPLEMENTED IN REDUNDANT EIM ACTUATION PRIORITY LOGIC (APL) MODULES. A SINGLE EIM CAN BE REMOVED FOR MAINTENANCE, AND THE VALVE LOGIC WILL REMAIN FUNCTIONAL WITH THE EIM THAT REMAINS IN SERVICE.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE VALVE HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO ACTUATE.

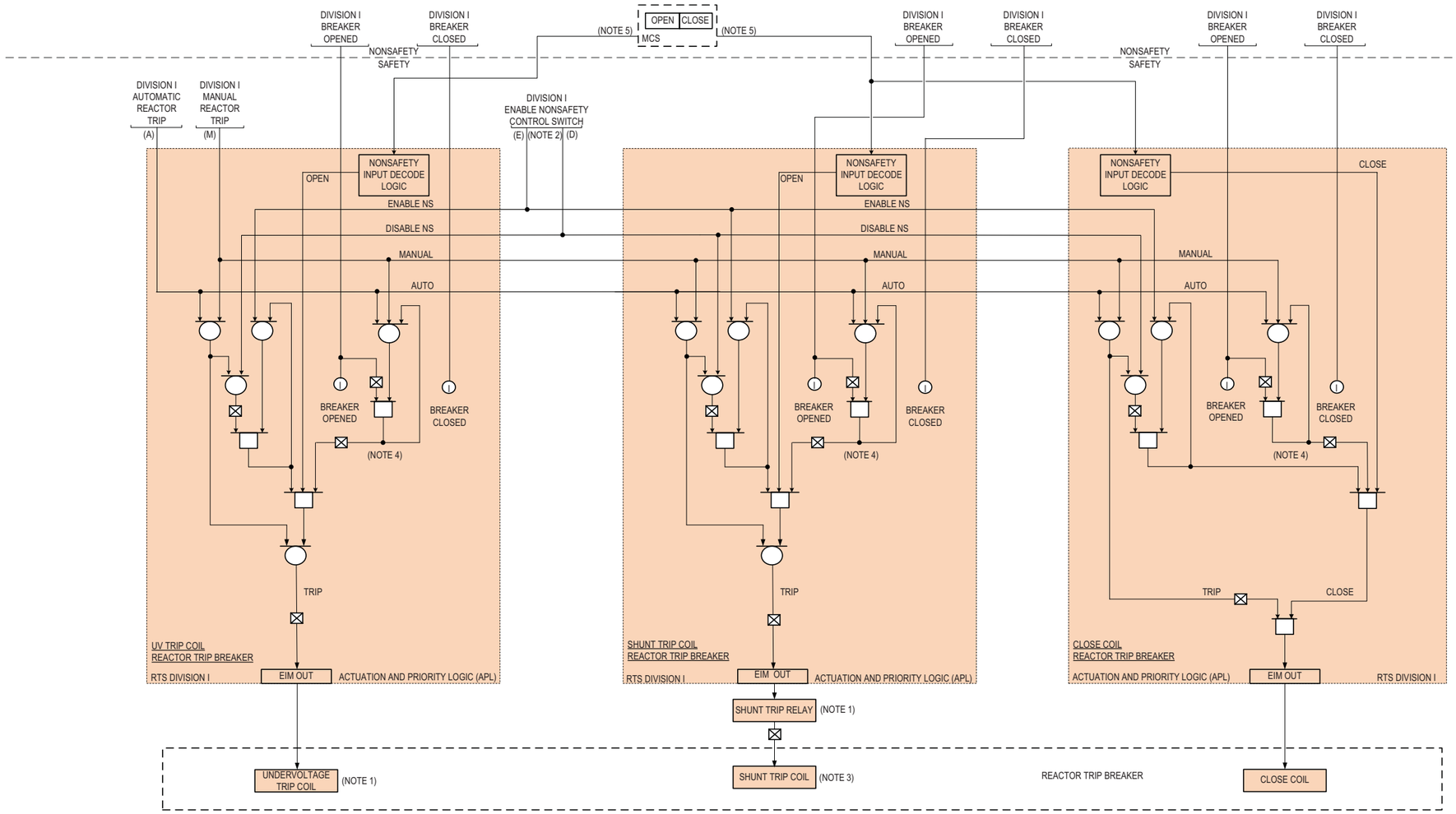
NOTE 5: THE ECCS VENT VALVE DESIGN INCLUDES AN ARMING VALVE. THE ARMING VALVE IMPLEMENTS THE INADVERTENT ACTUATION BLOCK (IAB) FUNCTION THAT DELAYS OPENING OF THE ECCS VENT VALVE WHEN THE TRIP SOLENOID DE-ENERGIZES UNTIL RPV TO CNV DIFFERENTIAL PRESSURE IS BELOW THE ARMING VALVE SET PRESSURE.

NOTE 6: THE ECCS RESET SOLENOID VALVE IS NORMALLY DE-ENERGIZED (CLOSED). THE RESET SOLENOID MUST BE ENERGIZED (CLOSED) TO OPEN THE ECCS VENT VALVE. THIS PROVIDES A PATH FOR CVCS MAKEUP TO THE MAIN VALVE CONTROL CHAMBER UNTIL RPV PRESSURE IS SUFFICIENT TO OVERCOME THE SPRING FORCE HOLDING THE VALVE OPEN.

NOTE 7: LOGIC IS SHOWN FOR DIVISION I AND II. BOTH DIVISIONS ARE SHOWN TO INDICATE UNIQUE ACTUATED EQUIPMENT NUMBERS ASSOCIATED WITH EACH REDUNDANT DIVISION.

NOTE 8: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1ad: Reactor Trip Breaker Division I A



NOTE 1: THE UNDERVOLTAGE (UV) TRIP COIL AND SHUNT TRIP RELAY ARE ENERGIZED WHEN OPERATING; WHEN THE EIM OUTPUTS ARE DE-ENERGIZED, THE UV TRIP COIL AND SHUNT TRIP RELAY ARE DE-ENERGIZED TO TRIP THE BREAKER OPEN.

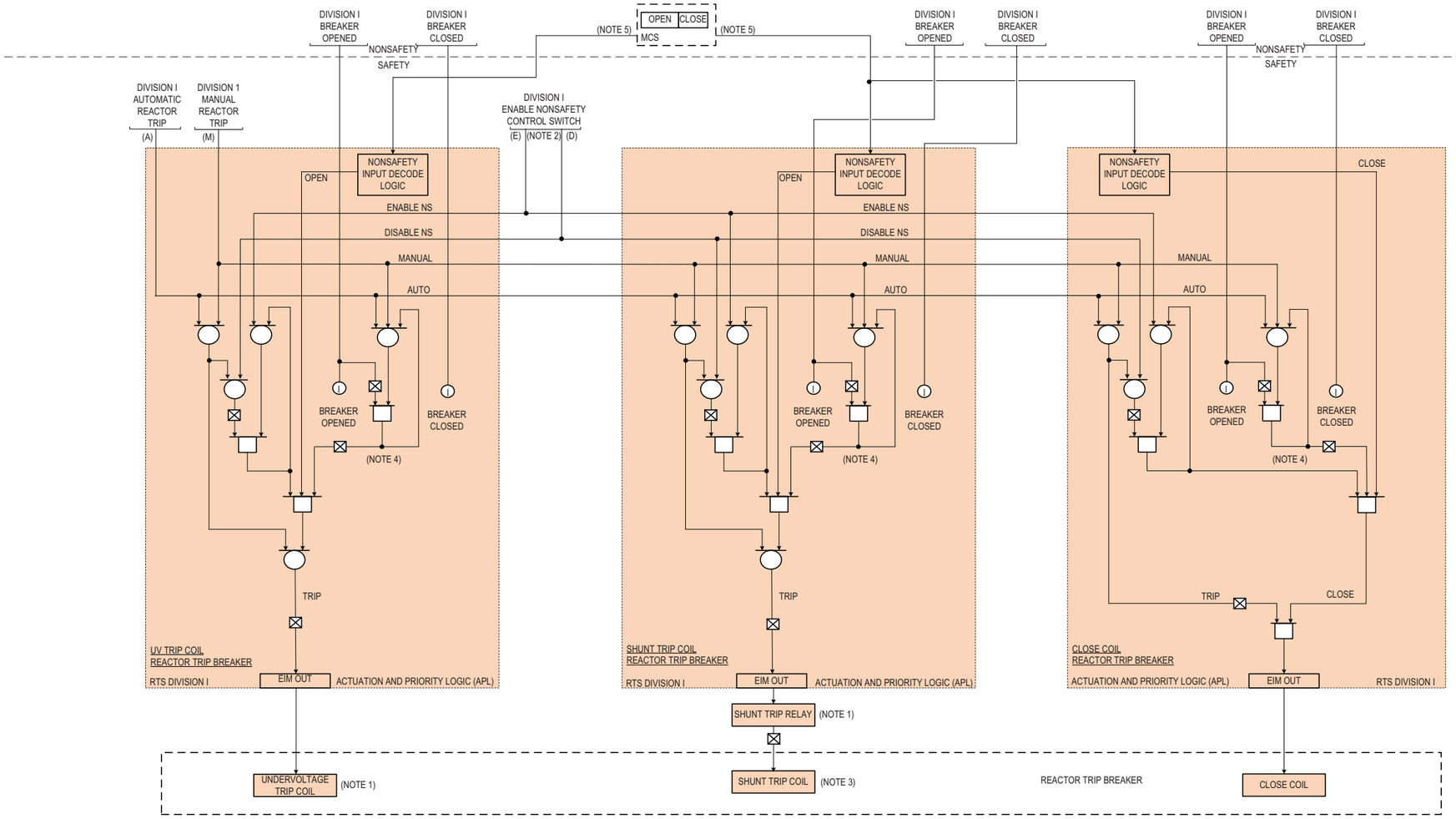
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

NOTE 3: THE SHUNT TRIP COIL IS NORMALLY DE-ENERGIZED; WHEN THE SHUNT TRIP RELAY IS DE-ENERGIZED, SHUNT TRIP COIL IS ENERGIZED TO TRIP THE BREAKER OPEN.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE TRIP BREAKER HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO TRIP.

NOTE 5: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1ae: Reactor Trip Breaker Division I B



NOTE 1: THE UNDERVOLTAGE (UV) TRIP COIL AND SHUNT TRIP RELAY ARE ENERGIZED WHEN OPERATING; WHEN THE EIM OUTPUTS ARE DE-ENERGIZED, THE UV TRIP COIL AND SHUNT TRIP RELAY ARE DE-ENERGIZED TO TRIP THE BREAKER OPEN.

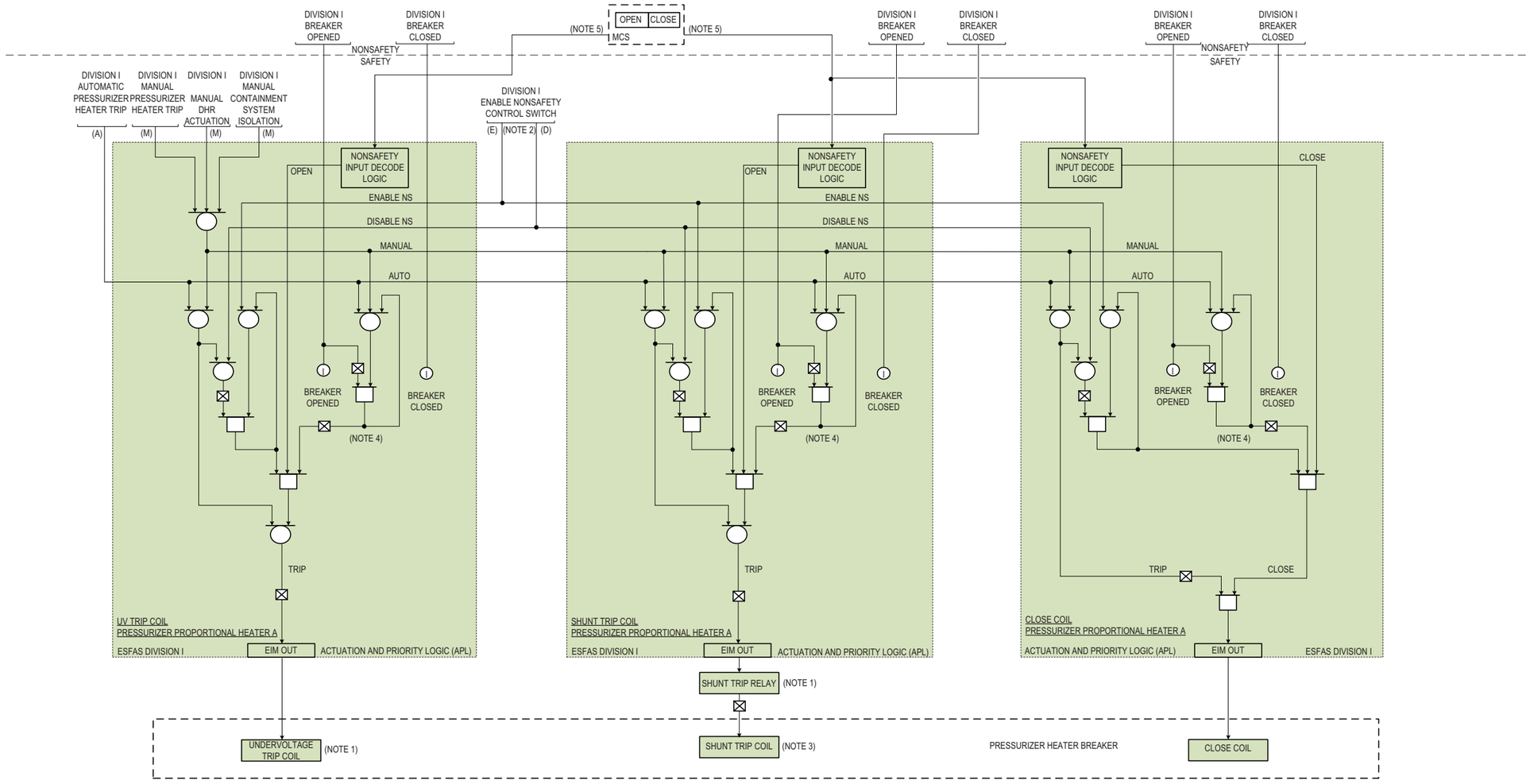
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

NOTE 3: THE SHUNT TRIP COIL IS NORMALLY DE-ENERGIZED; WHEN THE SHUNT TRIP RELAY IS DE-ENERGIZED, SHUNT TRIP COIL IS ENERGIZED TO TRIP THE BREAKER OPEN.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE TRIP BREAKER HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO TRIP.

NOTE 5: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1af: Pressurizer Heater Trip Breaker Proportional Heater A



NOTE 1: THE UNDERVOLTAGE (UV) TRIP COIL AND SHUNT TRIP RELAY ARE ENERGIZED WHEN OPERATING; WHEN THE EIM OUTPUT IS DE-ENERGIZED, THE UV TRIP COIL AND SHUNT TRIP RELAY ARE DE-ENERGIZED TO TRIP THE BREAKER OPEN.

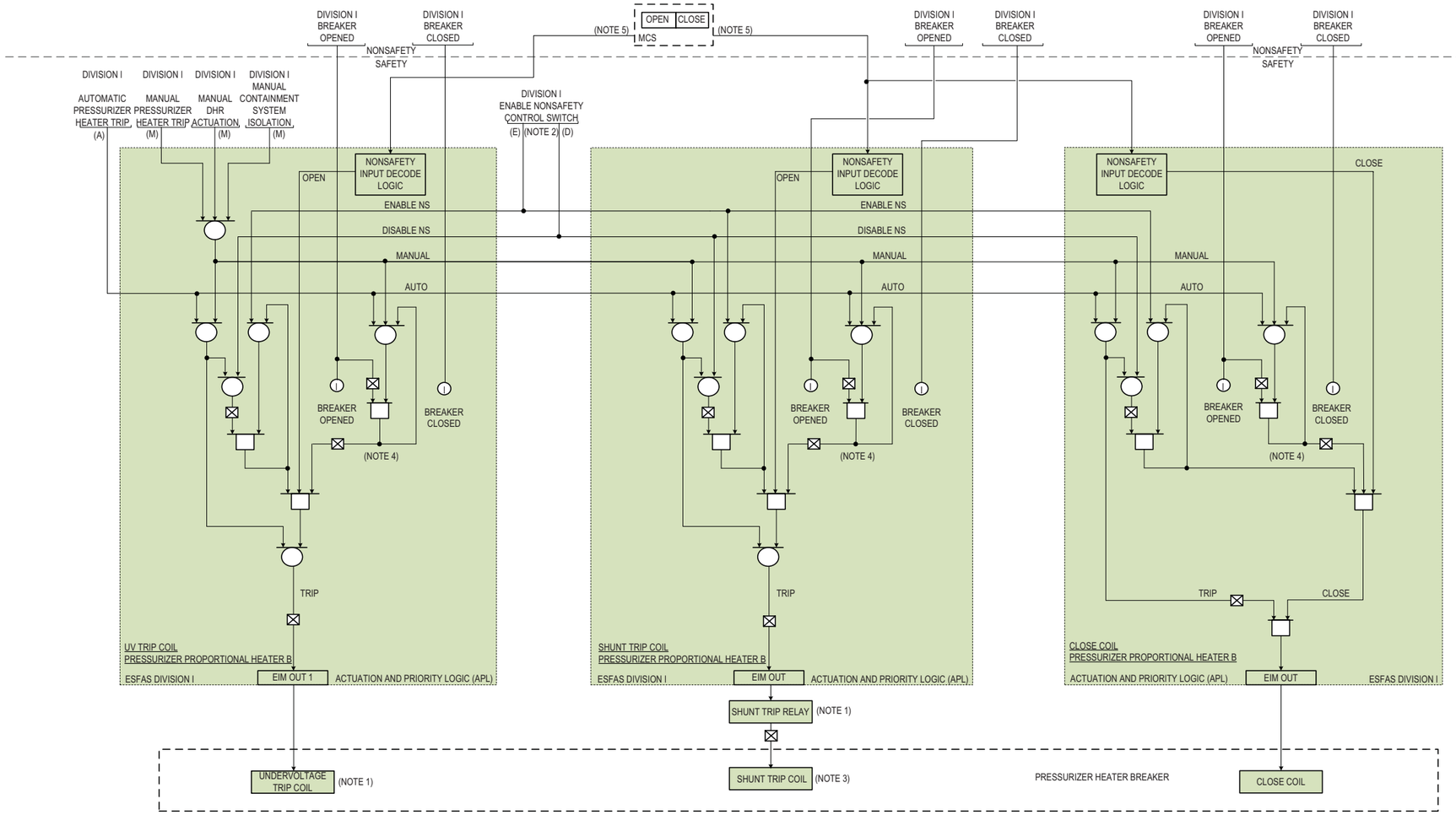
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

NOTE 3: THE SHUNT TRIP COIL IS NORMALLY DE-ENERGIZED; WHEN THE SHUNT TRIP RELAY IS DE-ENERGIZED, SHUNT TRIP COIL IS ENERGIZED TO TRIP THE BREAKER OPEN.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE TRIP BREAKER HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO TRIP.

NOTE 5: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1ag: Pressurizer Heater Trip Breaker Proportional Heater B



NOTE 1: THE UNDERVOLTAGE (UV) TRIP COIL AND SHUNT TRIP RELAY ARE ENERGIZED WHEN OPERATING; WHEN THE EIM OUTPUT IS DE-ENERGIZED, THE UV TRIP COIL AND SHUNT TRIP RELAY ARE DE-ENERGIZED TO TRIP THE BREAKER OPEN.

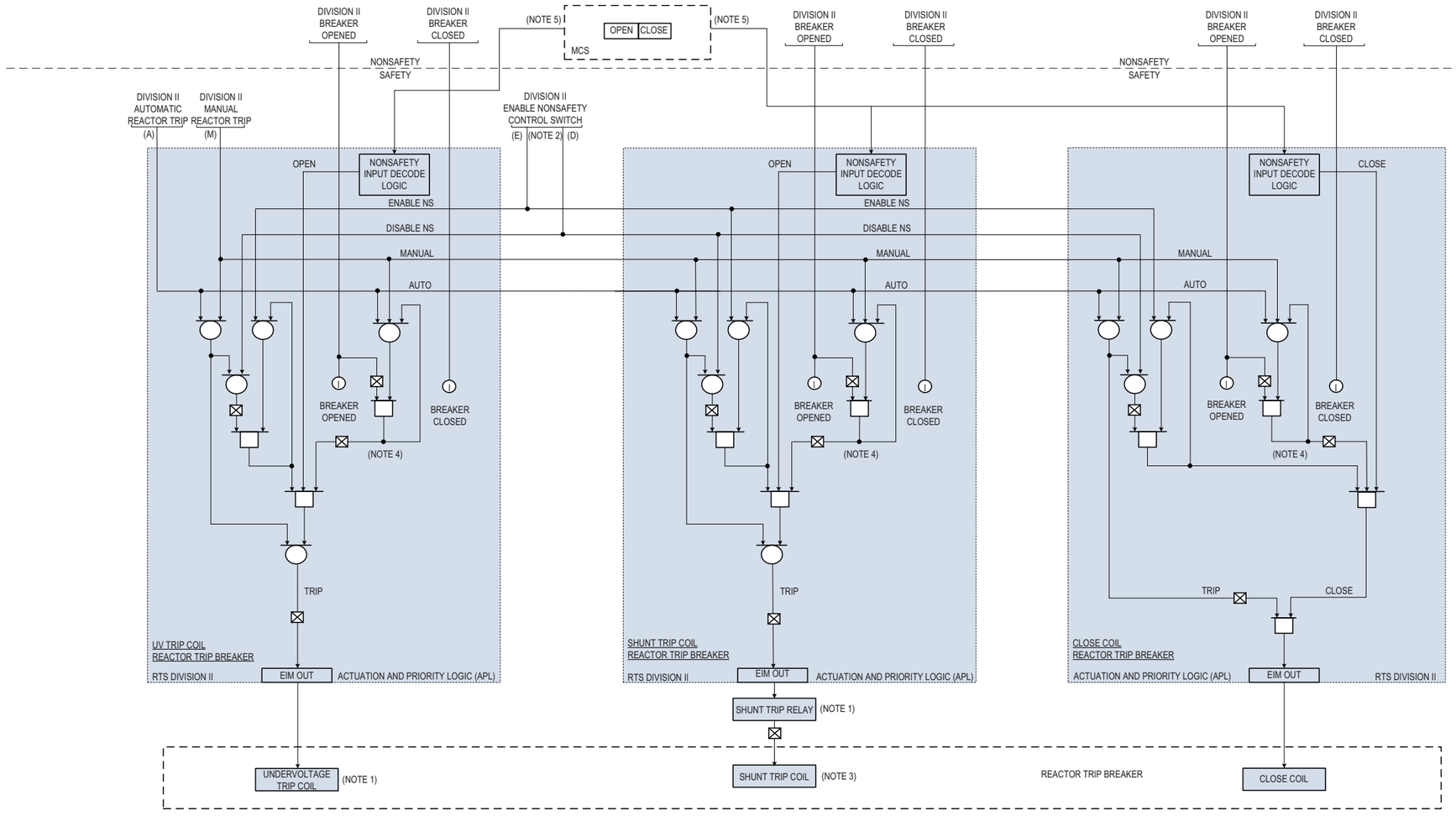
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

NOTE 3: THE SHUNT TRIP COIL IS NORMALLY DE-ENERGIZED; WHEN THE SHUNT TRIP RELAY IS DE-ENERGIZED, SHUNT TRIP COIL IS ENERGIZED TO TRIP THE BREAKER OPEN.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE TRIP BREAKER HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO TRIP.

NOTE 5: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1ak: Reactor Trip Breaker Division II A



NOTE 1: THE UNDERVOLTAGE (UV) TRIP COIL AND SHUNT TRIP RELAY ARE ENERGIZED WHEN OPERATING; WHEN THE EIM OUTPUTS ARE DE-ENERGIZED, THE UV TRIP COIL AND SHUNT TRIP RELAY ARE DE-ENERGIZED TO TRIP THE BREAKER OPEN.

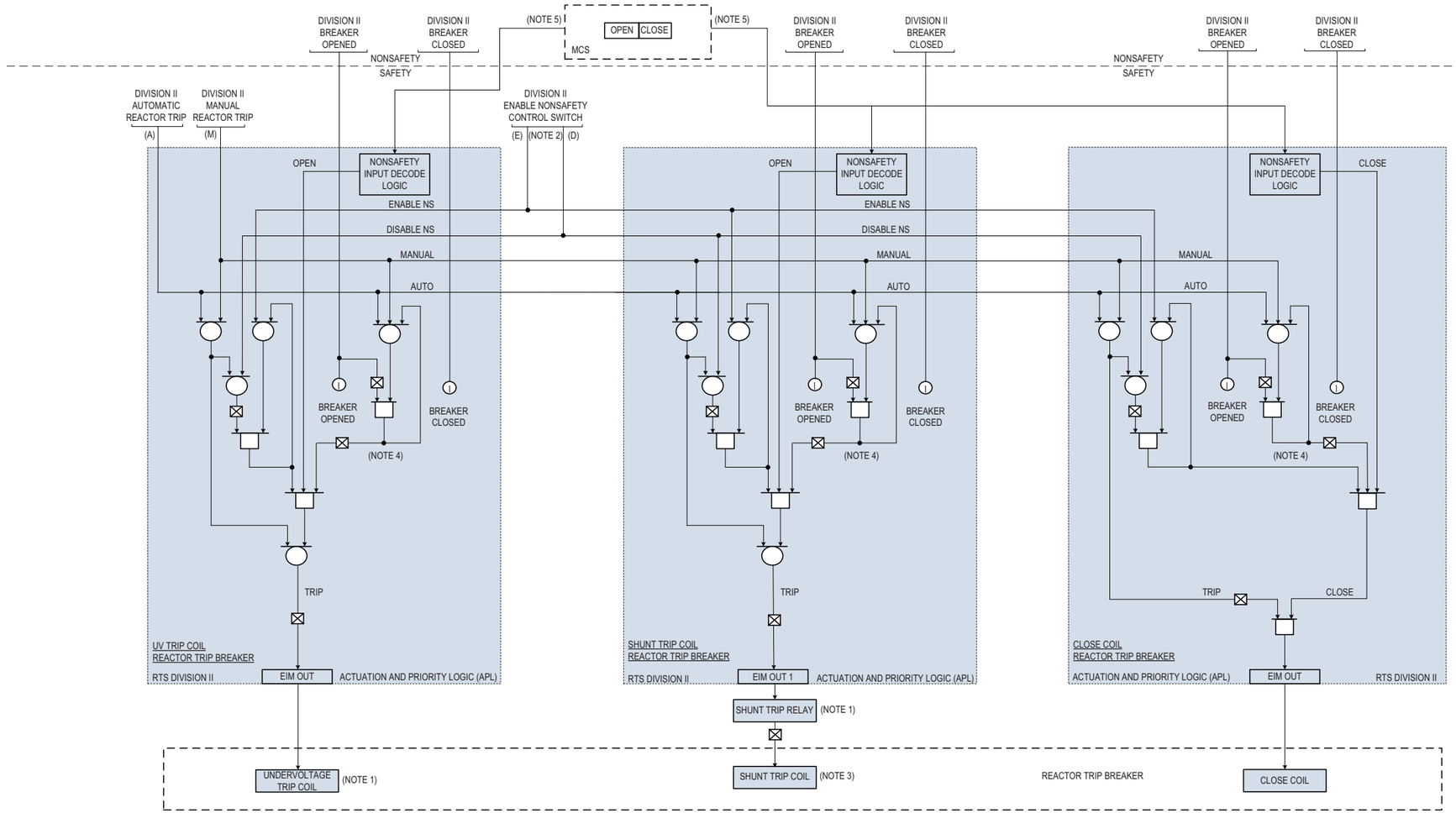
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

NOTE 3: THE SHUNT TRIP COIL IS NORMALLY DE-ENERGIZED; WHEN THE SHUNT TRIP RELAY IS DE-ENERGIZED, SHUNT TRIP COIL IS ENERGIZED TO TRIP THE BREAKER OPEN.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE TRIP BREAKER HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO TRIP.

NOTE 5: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1al: Reactor Trip Breaker Division II B



NOTE 1: THE UNDERVOLTAGE (UV) TRIP COIL AND SHUNT TRIP RELAY ARE ENERGIZED WHEN OPERATING; WHEN THE EIM OUTPUTS ARE DE-ENERGIZED, THE UV TRIP COIL AND SHUNT TRIP RELAY ARE DE-ENERGIZED TO TRIP THE BREAKER OPEN.

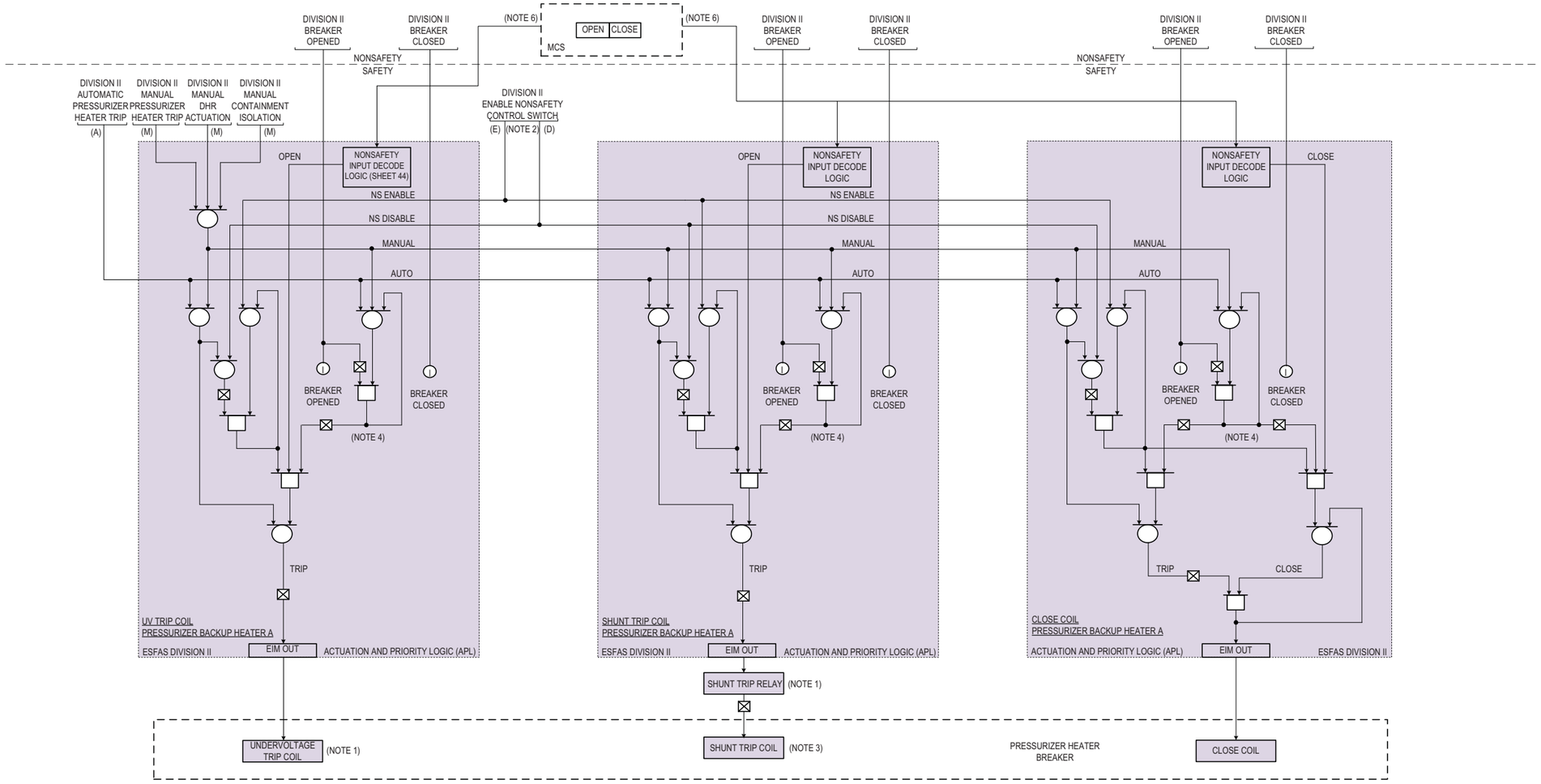
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

NOTE 3: THE SHUNT TRIP COIL IS NORMALLY DE-ENERGIZED; WHEN THE SHUNT TRIP RELAY IS DE-ENERGIZED, SHUNT TRIP COIL IS ENERGIZED TO TRIP THE BREAKER OPEN.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE TRIP BREAKER HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO TRIP.

NOTE 5: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1am: Pressurizer Heater ~~Breaker Trip~~Trip Breaker Backup Heater A



NOTE 1: THE UNDERVOLTAGE (UV) TRIP COIL AND SHUNT TRIP RELAY ARE NORMALLY ENERGIZED; WHEN THE EIM OUTPUT IS DE-ENERGIZED, THE UV TRIP COIL AND SHUNT TRIP RELAY ARE DE-ENERGIZED TO TRIP THE BREAKER OPEN.

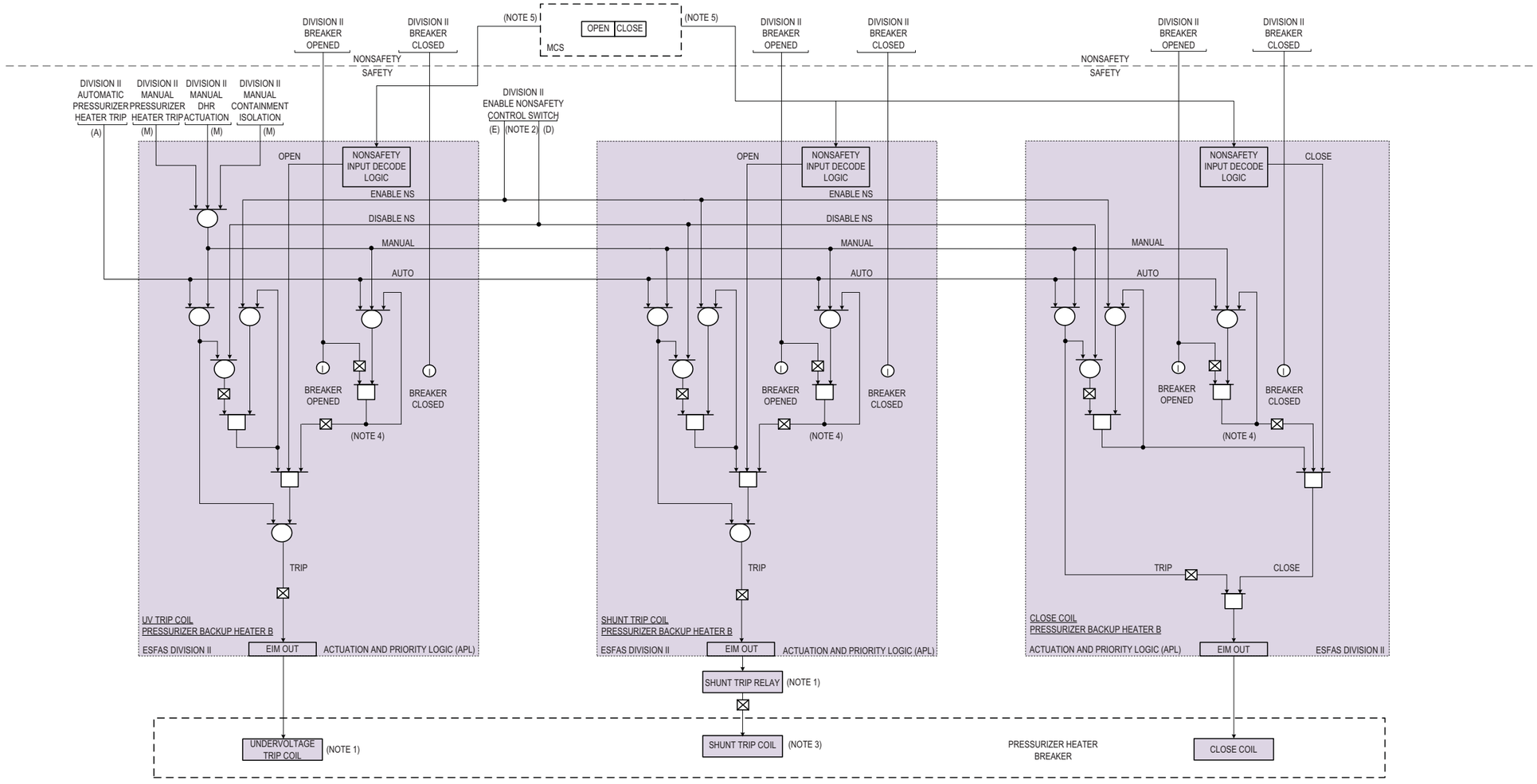
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

NOTE 3: THE SHUNT TRIP COIL IS NORMALLY DE-ENERGIZED; WHEN THE SHUNT TRIP RELAY IS DE-ENERGIZED, SHUNT TRIP COIL IS ENERGIZED TO TRIP THE BREAKER OPEN.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE TRIP BREAKER HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO TRIP.

NOTE 5: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1an: Pressurizer Heater ~~Breaker Trip~~Trip Breaker Backup Heater B



NOTE 1: THE UNDERVOLTAGE (UV) TRIP COIL AND SHUNT TRIP RELAY ARE NORMALLY ENERGIZED; WHEN THE EIM OUTPUT IS DE-ENERGIZED, THE UV TRIP COIL AND SHUNT TRIP RELAY ARE DE-ENERGIZED TO TRIP THE BREAKER OPEN.

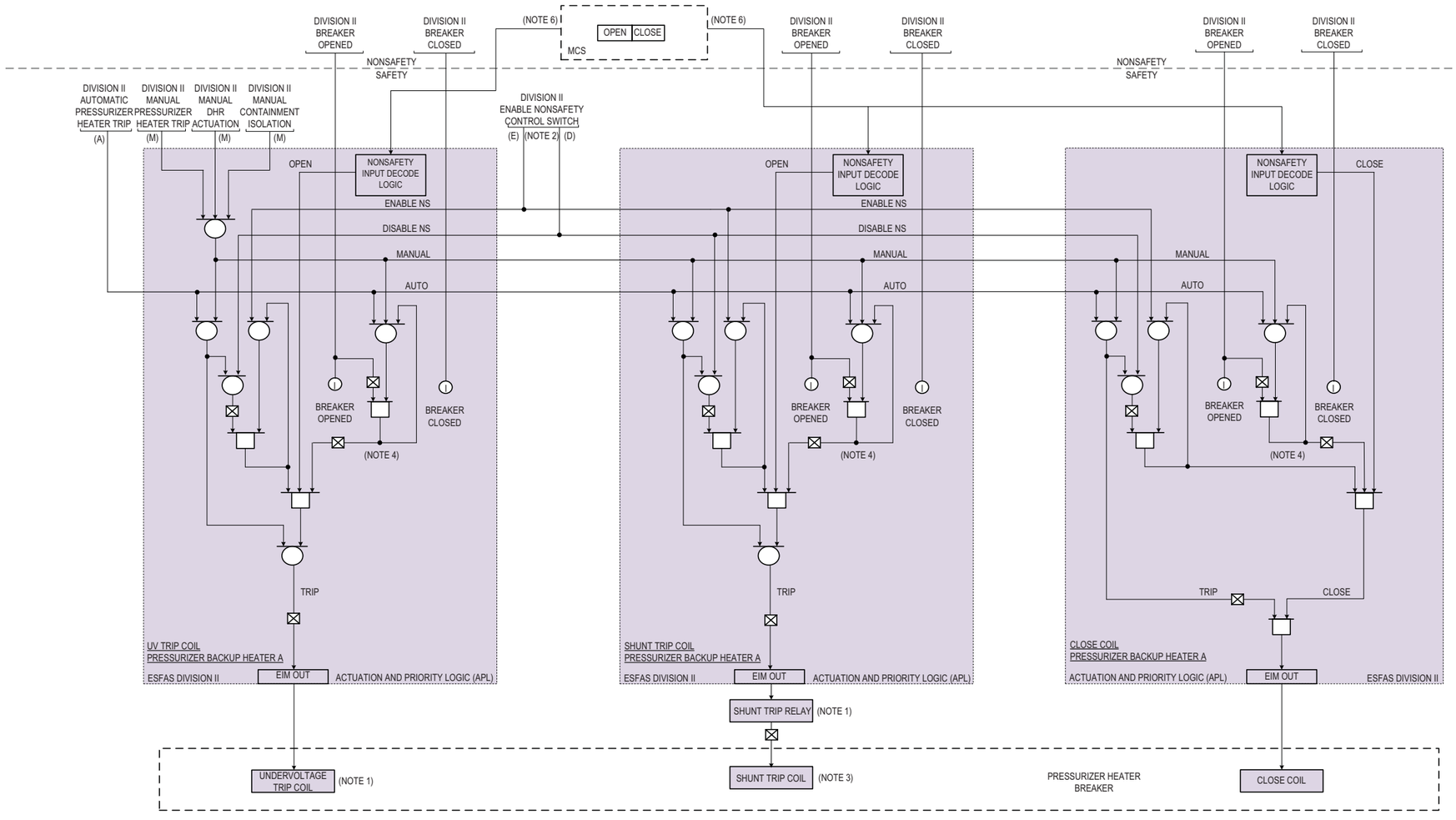
NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

NOTE 3: THE SHUNT TRIP COIL IS NORMALLY DE-ENERGIZED; WHEN THE SHUNT TRIP RELAY IS DE-ENERGIZED, SHUNT TRIP COIL IS ENERGIZED TO TRIP THE BREAKER OPEN.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE TRIP BREAKER HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO TRIP.

NOTE 5: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-1am: Pressurizer Heater ~~Breaker Trip~~Trip Breaker Backup Heater A



NOTE 1: THE UNDERVOLTAGE (UV) TRIP COIL AND SHUNT TRIP RELAY ARE NORMALLY ENERGIZED; WHEN THE EIM OUTPUT IS DE-ENERGIZED, THE UV TRIP COIL AND SHUNT TRIP RELAY ARE DE-ENERGIZED TO TRIP THE BREAKER OPEN.

NOTE 2: ONE ENABLE NONSAFETY CONTROL SWITCH PER DIVISION. THE SINGLE SWITCH ENABLES NONSAFETY CONTROL TO ALL ESF COMPONENTS.

NOTE 3: THE SHUNT TRIP COIL IS NORMALLY DE-ENERGIZED; WHEN THE SHUNT TRIP RELAY IS DE-ENERGIZED, SHUNT TRIP COIL IS ENERGIZED TO TRIP THE BREAKER OPEN.

NOTE 4: THE EIM APL LOGIC INCLUDES A SEAL-IN TO ENSURE COMPLETION OF THE PROTECTIVE ACTION. THE SEAL-IN REMAINS IN PLACE UNTIL POSITION FEEDBACK INDICATES THAT THE TRIP BREAKER HAS REACHED THE POSITION DEMANDED BY THE PROTECTIVE ACTION. THE PROTECTIVE ACTION IS FAIL-SAFE, OR DE-ENERGIZE TO TRIP.

NOTE 5: NONSAFETY CONTROL INPUTS CONSIST OF 14 INDIVIDUAL HARDWIRED SIGNALS.

Figure 7.1-2: Post-Accident Monitoring ~~System~~ General Arrangement Drawing

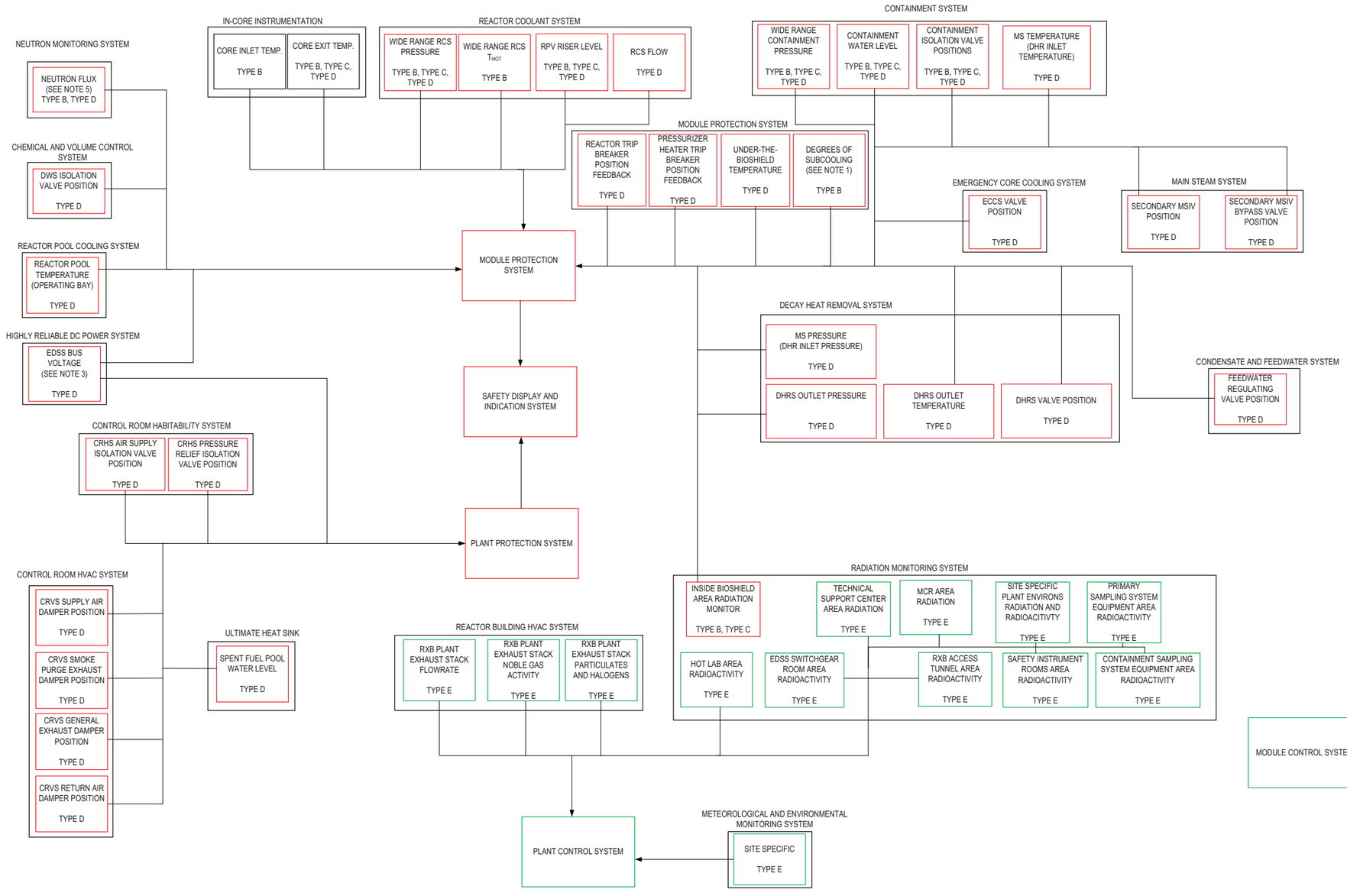


Figure 7.1-16: Example Module Protection System High Level Control Structure

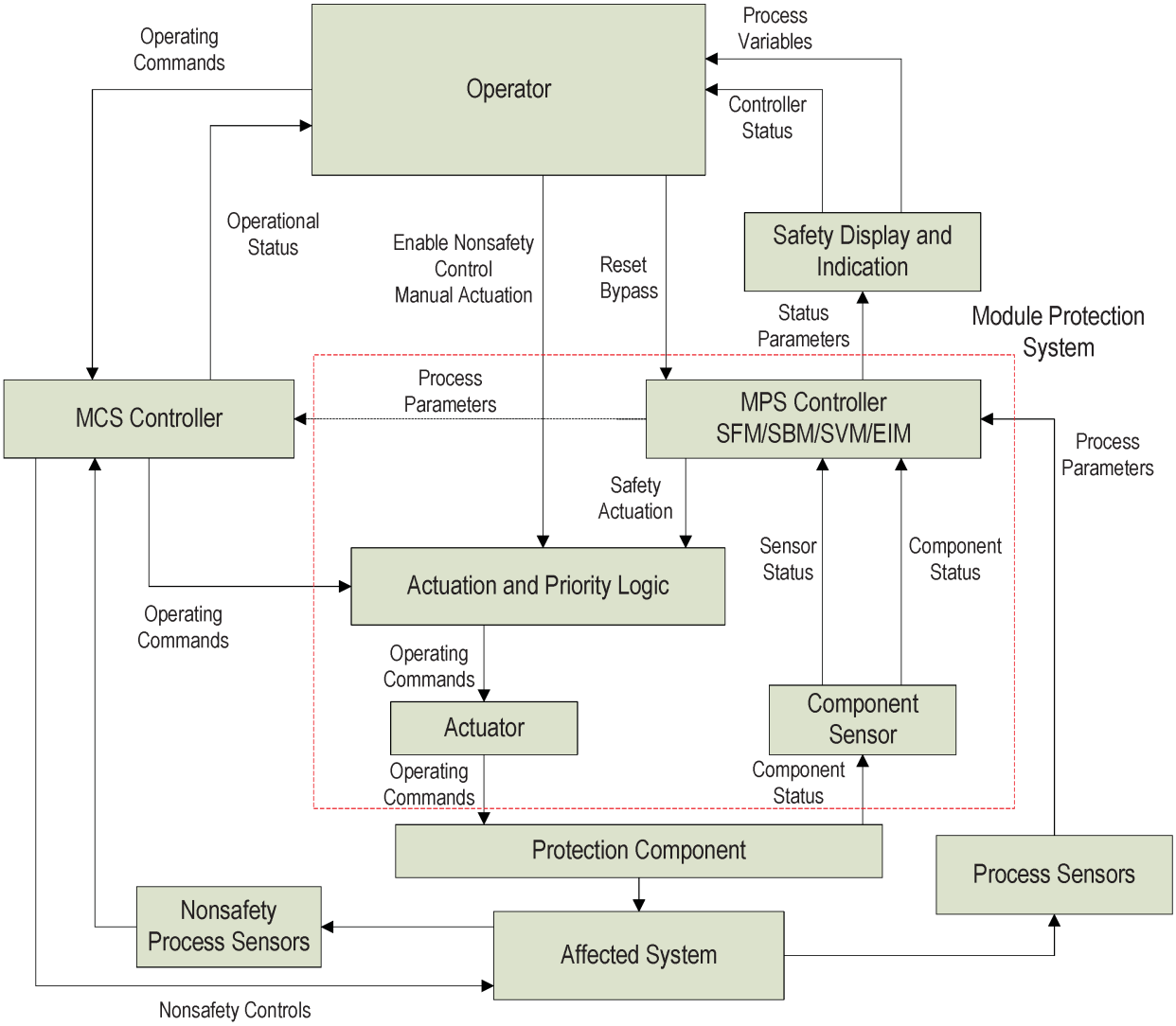


Figure 7.1-17: Example Neutron Monitoring System High Level Control Structure

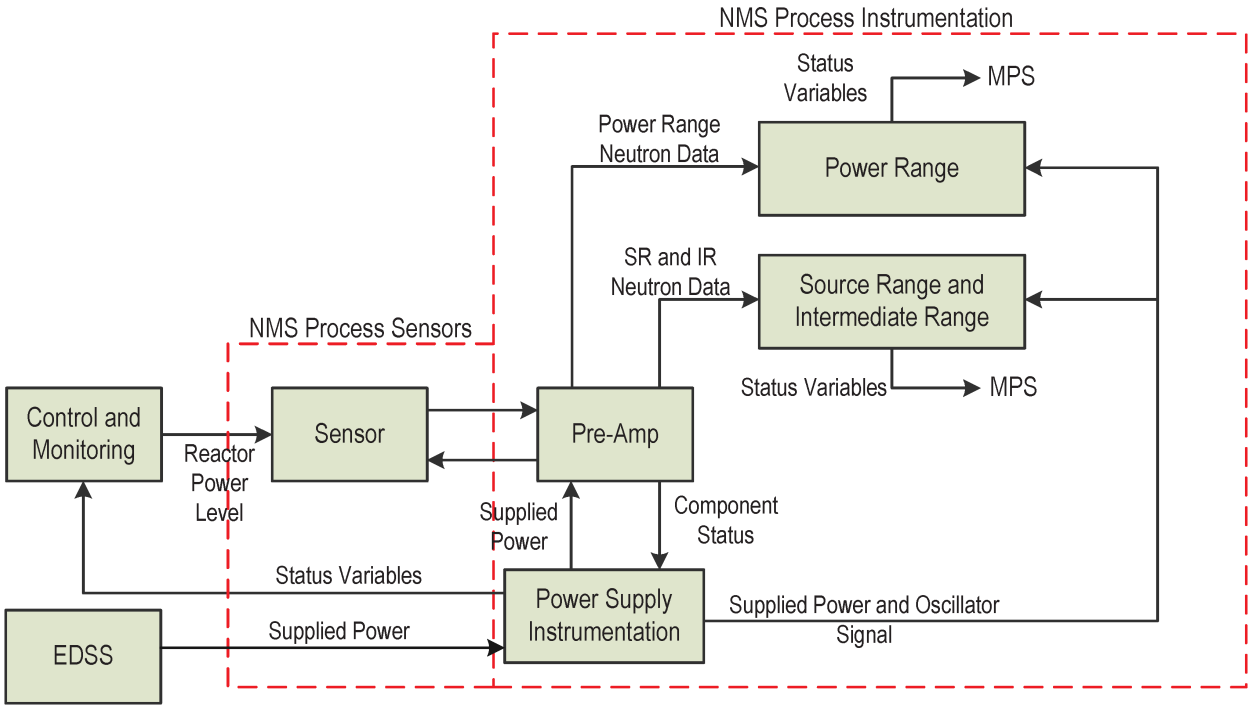
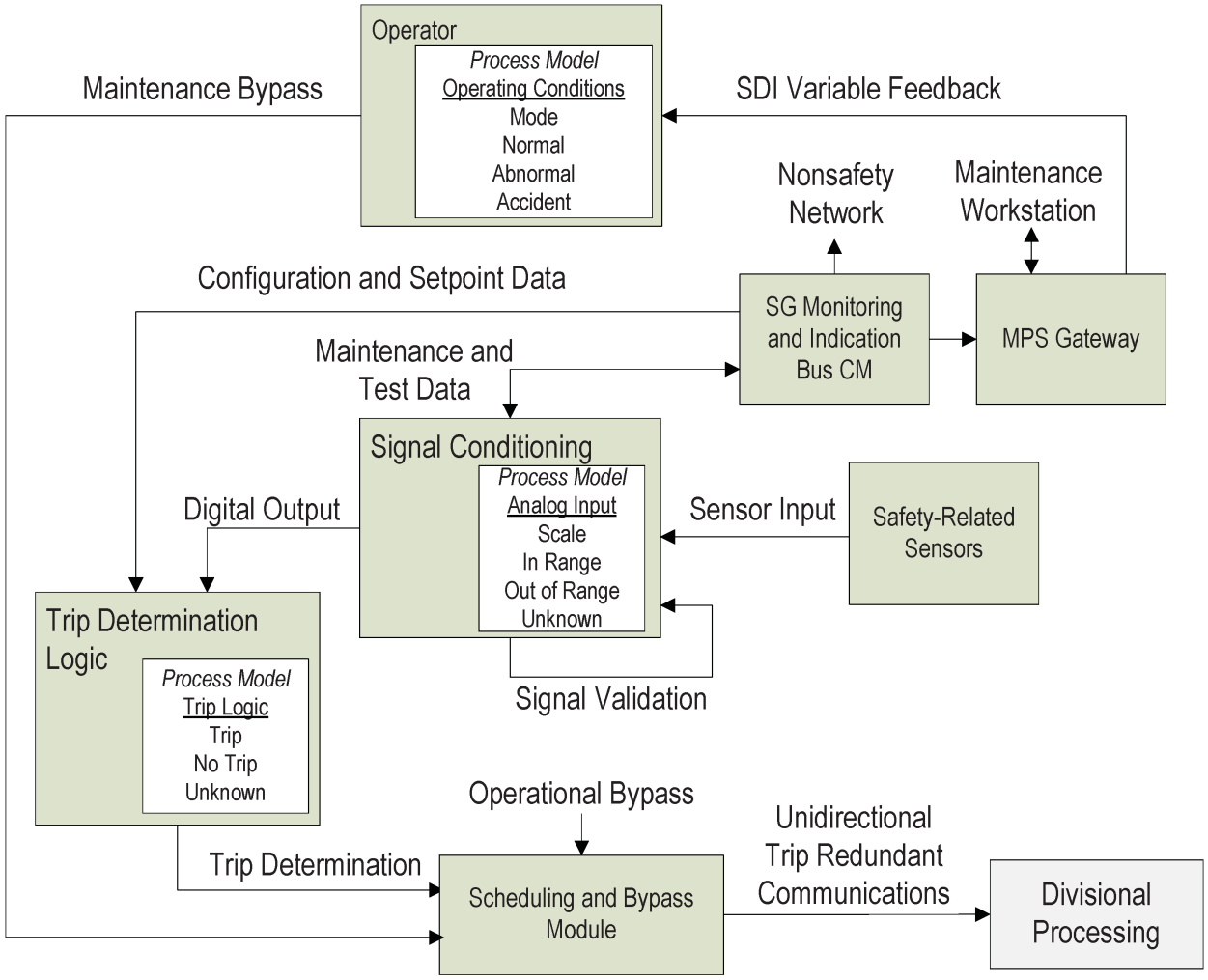


Figure 7.1-18: Safety Function Module Logic Structure



Section 7.2.1

conflict with NuScale standard engineering documentation practices or QAP requirements.

5) Regulatory Guide 1.169, Revision 1 endorses IEEE Standard 828-2005 as an acceptable approach for safety system software configuration management. The NuScale Digital I&C Software Configuration Management Plan specifies the requirements for software configuration management, consistent with the guidance in RG 1.169, Revision 1 and IEEE Standard 828-2005. The NuScale Digital I&C Software Configuration Management Plan conforms to complies with the requirements in IEEE Standard 828-2005, as endorsed by RG 1.169, Revision 1.

6) Regulatory Guide 1.168, Revision 2 endorses IEEE Standard 1012-2004 as an acceptable approach for V&V of safety system software. The RG also endorses IEEE Standard 1028-2008 "IEEE Standard for Software Reviews and Audits" (Reference 7.2-20) as an acceptable approach for carrying out software reviews, inspections, walkthroughs, and audits typically used in association with software QA activities. The NuScale Software Verification and Validation Plan is based on IEEE Standard 1012-2004, as endorsed by RG 1.168 Revision 2. The V&V program for safety-related software (i.e., SIL 4) is implemented by a V&V team that is independent from the design development team. The NuScale Digital I&C Software Verification and Validation Plan conforms to IEEE Standard 1012-2004 with adaptations and exceptions as follows:

Adaptations

- V&V activities adapted to NuScale life cycle and Complex Logic Device technology. In the application of different FPGA technologies within the MPS, the V&V activities are the same; they do not differentiate between different FPGA technologies.
- V&V tasks adapted to Complex Logic Device technology

Exceptions

- ~~Documentation requirement details in Sections 6 and 7 of the standard that conflict with NuScale standard documentation practices or QAP requirements or are inconsistent with the platform neutral strategy (where flexibility is retained to adopt established vendor documentation formats)~~Consistent with the guidance in RG 1.170, Revision 1, exceptions are taken for documentation requirement details in Sections 6 and 7 of IEEE-1012-2004 that conflict with NuScale standard documentation practices or are inconsistent with the platform neutral strategy (where flexibility is retained to adopt established vendor documentation formats). In all cases, the approved NuScale QAP (see Section 17.5) takes precedence.

NuScale performs software reviews, inspections, walkthroughs, and audits as part of software design, V&V, and quality assurance activities. These activities are performed and documented in accordance with methods defined in NuScale procedures and QA program requirements. NuScale takes exception to the methods and documentation requirement specified in IEEE Std 1028-2008, since these details conflict with NuScale standard documentation practices or QA program requirements or are inconsistent with the platform neutral strategy (where flexibility is retained to adopt established vendor methods and documentation formats for these activities). NuScale does not conform to the requirements in IEEE Standard 1028-2008.

- For SIL 3 and 4 software, an independent V&V team performs a V&V of the Software Requirements Specification in accordance with the NuScale Digital I&C Software Verification and Validation Plan.
- For SIL 1 and 2 software, an independent verifier within the engineering team performs this function.

The Software Requirements Specification is baselined, updated as necessary, and placed under configuration management in accordance with the NuScale Digital I&C Software Configuration Management Plan.

7.2.1.2.6 Software Design

A Software Design Description is developed for the software product to document the detailed design for the software or Complex Logic Device logic elements of the software system and how the software units are to be constructed. It addresses the methods by which software units are refined into lower levels including software modules to allow coding programming, compiling (not applicable for Complex Logic Device logic), and testing. The software or Complex Logic Device logic is also divided into a set of interacting units, including the description of those units, the interfaces, and dependencies in a structured fashion. The IDD supplements the Software Design Description as described in Section 7.2.1.1.2.6.

The design of the software module is restricted to one clearly identified function that involves minimum interaction with other functions to minimize the impact of changes. The interfaces between the various units are simple, completely identified, and documented.

The applicable software design is incorporated from the Software Requirements Phase into the software design and implementation and traceability is established between software unit(s) and software module(s).

~~The software design is assessed to ensure it adequately covers the requirements in the Software Requirements Specification and does not contain unnecessary functions.~~

~~For pre-developed digital platforms, pre-existing software (e.g., operating system software) may contain features that are not used (or not configured for use) in a specific I&C system. In those instances, the design is assessed to:~~The NuScale Digital I&C Software Development Plan requires that an assessment of the software design is performed to ensure the software design adequately covers the requirements in the Software Requirements Specification and does not contain unnecessary software, complex programmable logic, or functions. The software design is assessed to:

- ~~identify unused capabilities~~
- ~~evaluate the safety benefit of the intended function and whether those functions may adversely impact performance of the safety function~~
- ~~identify compensatory measures taken~~identify unused capabilities

- evaluate the safety benefit of the intended function and whether those functions may adversely impact performance of the safety function
- identify compensatory measures taken

Security analysis verification is performed as part of the verification and validation activities to ensure the secure development environment requirements are met and the developer has removed hidden functions or code that may have been used in development or unit testing and is not required to meet the system design requirements.

The NuScale Digital Safety System SDOE Plan requires that vulnerability assessments be performed on software and complex programmable logic that is developed and classified as SIL 4. The vulnerability assessments evaluate that the design configuration items of the secure development environment are reviewed to ensure they are correctly translated from the system design specification and are correct, accurate, and complete. Details of the NuScale Secure Development Environment are described in Section 7.2.9.1.

In cases where previously developed software or commercial off-the-shelf software is used, the NuScale Digital Safety System SDOE and Digital I&C Software Development Plans contain requirements during the implementation phase of software development for evaluating and assessing that both developed code and previously developed or commercial off-the-shelf software meets the specified design requirements for system reliability and secure development and operating environments.

For commercial off-the-shelf software, previously developed software or complex programmable logic classified as SIL 4, the NuScale Digital I&C Quality Assurance Plan requires an evaluation of vendors and suppliers of digital I&C systems to verify that the software or complex programmable logic adheres to the secure development and operational environment design requirements and does not adversely affect system reliability.

The NuScale Digital I&C Software Quality Assurance Plan and the NuScale Digital I&C Software Verification and Validation Plan govern the use of support software and tools (e.g., software and hardware description language code generating tools, software compilers, software assemblers, software operating systems, software or Complex Logic Device logic coverage analyzers). The NuScale Digital I&C Software Configuration Management Plan governs the process for controlling code change requests and modifications.

The completed Software Requirements Specification is used as input to the ongoing software safety analysis activity for SIL 3 and 4 software or Complex Logic Device logic.

For SIL 3 and 4, an independent V&V team performs a V&V of the Digital I&C Software Design Description in accordance with the NuScale Digital I&C Software Verification and Validation Plan. For SIL 1 and 2 software, an independent verifier performs this function.

This information satisfies the application specific information for the NuScale Power, LLC, TR-1015-18653, "Design of the Highly Integrated Protection System Platform Topical Report," (Reference 7.2-25) listed in Table 7.0-2 for IEEE-603-1991, Sections 5.4 and 5.5 (Reference 7.2-11) and IEEE-7-4.3.2-2003, Section 5.4 (Reference 7.1-5).

7.2.2.1 Instrumentation and Controls Qualification

MPS and Neutron Monitoring System-Excore Equipment Operating Environment

MPS and neutron monitoring system (NMS)-excore rack-mounted equipment is installed in a mild environment and is designed to meet the environmental conditions described in Section 3.11 and Appendix 3C. The MPS and NMS rack-mounted equipment do not require environmental controls to perform their safety functions. The NMS-excore detectors are located in support mechanisms submerged in the reactor pool next to the reactor module which is a harsh environment. The MPS and NMS-excore equipment rooms provide an environment that would at no time be more severe than the environment that would occur during normal plant operation, including anticipated operational occurrences.

The MPS and NMS-excore components are environmentally qualified in accordance with IEEE-323-2003, "IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations" (Reference 7.2-7) as endorsed by RG 1.209 for mild environments as described in Section 3.11 and in accordance with IEEE-323-1974 "IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Stations" (Reference 7.2-8) as endorsed by RG 1.89 for harsh environments.

Protection from natural phenomena for the MPS and NMS-excore processing electronics is provided by the location of the MPS and NMS-excore cabinets in the reactor building on the 75'-0" and 86'-0" elevations (~~Figures 1.2-13 and 1.2-14~~Figures 1.2-14 and Figure 1.2-15, respectively) which is a Seismic Category I, reinforced concrete structure. This location is remote from the NMS-excore detectors and in a mild environment which provides protection for the processing electronics portion of the NMS-excore detectors.

Separation Groups A, C, and Division I of the reactor trip system (RTS), engineered safety features actuation system (ESFAS) and Separation Groups A and C NMS-excore signal processing equipment are in one room, and separation groups B, D, and Division II of the RTS, ESFAS and Separation Groups B and D NMS-excore equipment are located in a different room.

The Reactor Building and Control Building arrangement and design enable systems and components required for safe plant operation and shutdown to withstand or to be protected from the effects of sabotage, environmental conditions, natural phenomena, postulated design-basis accidents, and design-basis threats. The Reactor Building and the Control Building (at and below elevation 120′-0″) are Seismic Category I, reinforced concrete structures, except as noted in Section 1.2.2.2. See Section 3.2 for more details on the design of the reactor and control buildings.

The MPS is an FPGA-based system, which does not use software in a traditional manner; therefore, there is no software which executes while the system is in operation.

7.2.3.2 System Integrity Characteristics

The MPS maintains the capability to initiate protective functions during and following anticipated operational occurrences (AOOs), postulated accidents, and design basis events (DBEs) resulting from natural external phenomena such as earthquakes, tornadoes, hurricanes, floods and winds. The functional capability of the system is maintained during internal events such as fires, flooding, explosions, missiles, electrical faults, and pipe whip. The equipment is environmentally and seismically qualified in accordance with RG1.209 and IEEE-323-1974 as described in Section 7.2.2.

Rack-mounted MPS and NMS equipment is located in an environmentally controlled area. However, the ~~equipment is~~MPS and NMS rack-mounted equipment do not require environmental controls to perform their safety functions and are designed to accommodate abnormal conditions due to the loss of normal heating, ventilation, and air conditioning (HVAC) in the area for a minimum of 72 hours, coincident with AOOs and postulated accidents. The MPS equipment is designed to meet the normal and abnormal environmental conditions as described in Section 3.11 and Appendix 3C.

The design of the MPS is based on FPGA technology. The MPS platform is designed with redundancy and embedded self-test capability to ensure system integrity by detecting and alarming faults in the MCR. Diagnostics and testing capabilities are designed into the MPS platform to ensure there is a systematic approach to maintaining and testing the system, see Section 7.2.15.

The MPS platform implements advanced failure detection and mitigation to ensure system or component failures do not remain undetected. The operation of the system is deterministic in nature and allows the system to monitor in order to validate functional performance. The MPS is designed such that it can be tested and calibrated while retaining the capability to accomplish the required safety functions (Reference 7.2-25). Testing from the sensor inputs to the MPS through the actuated equipment is accomplished through a series of overlapping sequential tests with the majority of the tests capable of being performed with the plant at full power. Where testing final equipment at power has the potential to upset plant operation or damage equipment, provisions are made to test the equipment at reduced power or when the reactor is shut down. Periodic surveillance testing capability is incorporated to ensure that functional tests and checks, calibration verification, and time response measurements are validated. Periodic surveillance testing of sensors that are part of the MPS is performed in accord with the plant technical specifications.

Diagnostics data for the separation group and division of the MPS are provided to the maintenance workstation (MWS). The MWS is located close to the equipment to facilitate troubleshooting activities. The interface between the MPS and the MWS is an optically-isolated, one-way diagnostic interface connected to the calibration and test bus that is used to update tunable parameters. The calibration and test bus is configured as a one-way, receive-only interface. Diagnostics data are communicated via the monitoring and indication bus (MIB) which is a physically separate, isolated communications path from the safety data communication paths associated with the MPS safety functions (e.g., the safety data bus), thereby ensuring the diagnostics functionality is independent of the safety functionality. The diagnostic data comes

across the MIB communications module via a one-way transmit-only connection through the MPS gateway to the MWS.

The MPS is designed such that in the event of a condition such as a system disconnection or loss of power, it fails into a safe state. The equipment interface module (EIM) outputs are designed to remove power to the final actuation devices causing them to go to a safe-state (e.g., reactor trip breakers open, ECCS valves open). This ensures that a loss of power or other detected fault that causes the EIM to go into a faulted state also causes the interface to remove power to the final actuated device.

The NMS operates throughout normal reactor operation and provides PAM data to the MPS during and after a DBE. Failures of the NMS equipment are identified through system health monitoring of the NMS detectors and signal processing equipment. Periodic surveillance testing is performed on the NMS in accordance with the plant technical specifications. Failure of NMS-excore components generate a fault signal and an actuate/trip signal for that particular NMS-excore channel. The fault signal is transmitted to the MPS for display to the control room operators.

The NMS incorporates four redundant sets of detectors that are completely independent so that a failure in one redundant channel does not affect the other three.

7.2.3.3 Completion of Protective Action

The MPS is designed such that once a protective action is initiated, either automatically or manually, the sequence of protective actions continues until it has reached completion.

Seal-in of ESFAS actuation logic is provided at the EIM to account for transient process conditions that may change during a DBE (e.g., containment pressure). This seal-in prevents logic and final actuated devices from returning to the non-trip or non-actuated state due to changing process conditions. Seal-in is also provided at the EIM for the RTS actuation logic functions. The reactor trip function is inherently latched by removing electrical power from the control rod drive mechanisms causing the control rods to fall into the reactor core by gravity.

After the initiation of a protective action that requires components to go to an actuated position or safe-state, the MPS continues to hold the requested state after the initiating signal goes away. The EIM in the MPS functions as a state machine in that it accepts a request for a particular positon of a final actuation device and retains that position until a new position has been requested.

~~The MPS EIM and actuation priority logic circuitry maintains command prioritization. If the actuation priority logic receives a signal to initiate a protective action from a safety-related source, all nonsafety signals are automatically ignored. Re-initiation of manual controls from nonsafety equipment is possible only if the protective action has gone to completion and the operator deliberately blocks the safety signal using the override function via the manual override switches provided or the initiating signal is no longer present.~~

~~After a protective action has returned to normal or non-actuated state, the following conditions automatically block the manual nonsafety related signals:~~

1) ~~enable nonsafety-related control permissive no longer present~~

2) ~~manual re-initiation of the protective action at the division level~~

3) ~~conditions requiring automatic protective action are re-established~~

~~The actuation priority logic is based on discrete logic which allows for testing of possible combinations of inputs and the evaluation the associated outputs.~~

~~MPS functional logic diagrams indicate how this criterion is implemented for the functions, see Figure 7.1-1a through Figure 7.1-1ag.~~

The APL circuit is designed to give priority to safety-related RTS and ESF signals over nonsafety-related signals in all modes of operation. The APL circuit does not contain digital technology; it is constructed of discrete logic components and functions separately from the FPGA logic within the EIM.

The APL circuit accepts inputs from three sources:

1) Automatic reactor trip or ESF actuation signals from its own safety division.

2) Manual reactor trip or ESF actuation signals from its own divisional manual actuation switches in the main control room.

3) Enable nonsafety control switch and nonsafety-related control input signals from the module control system. If the enable nonsafety control switch is not active (i.e., nonsafety-related inputs are disabled), the nonsafety-related control signal is ignored.

The actuation priority logic evaluates these signals, and generates and provides output signals to the EIM to actuate or trip the final actuation devices based on the logic described in this section.

In all cases, the highest priority is given to the automatic and manual RTS and ESFAS actuation signals. As shown in Figure 7.1-1k through 7.1-1an, these actuation signals have equal, highest priority; they are differentiated only by the sequence by which they are received by the APL circuit, such that the first active signal received is used to generate the output.

If an automatic or manual RTS or ESF actuation signal is active, these signals have the highest logic priority; the RTS and ESF signals are processed and an actuation command is sent directly to the EIM output to actuate or trip the final actuation device. In all cases, it does not matter what the position of the enable nonsafety control switch is. The enable nonsafety control switch does not impede the handling and evaluation of active automatic or manual RTS or ESF actuation signals as these are processed at the highest logic priority.

If the nonsafety control inputs are disabled by the enable nonsafety control switch, then nonsafety control inputs are rejected and not processed by the APL circuit.

For cases when the enable nonsafety control switch is enabled to allow nonsafety control inputs, there must be no active RTS or ESF manual or automatic active signal present. If the enable nonsafety control switch is enabled, and there is no active RTS or ESF signal, then the nonsafety manual control inputs from the MCS are used by the APL circuit to control the final component (e.g., containment isolation valve).

During the time the nonsafety control inputs are enabled, if an automatic or manual RTS or ESF signal is generated and received by the APL circuit, the actuation priority logic immediately disables the enable nonsafety control logic permissive and rejects all nonsafety control inputs. The actuation priority logic circuit processes the RTS or ESF command to position the final actuation device to its safe state.

Re-initiation of manual controls from nonsafety equipment is possible only if the protective action has gone to completion and the operator deliberately blocks the safety signal using the override function via the manual override switches provided or the initiating signal is no longer present.

The actuation priority logic is based on discrete logic which allows for testing of possible combinations of inputs and the evaluation of the associated outputs.

7.2.4 Operating and Maintenance Bypasses

An operating bypass is provided for certain protective actions when they are not necessary in a particular mode of plant operation. Different modes of plant operation may necessitate an automatic or manual bypass of a safety function. Operating bypasses are used to permit mode changes. A maintenance bypass is provided to bypass safety system equipment during maintenance, testing, or repair. A maintenance bypass may reduce the degree of redundancy of equipment, but it does not result in the loss of a safety function. Operating and maintenance bypasses are described in the following sections.

The MPS operating and maintenance bypasses conforms to Sections 6.6, 6.7, 7.4 and 7.5 of IEEE-603-1991 (Reference 7.2-11) and the guidance contained in RG 1.47, Revision 1. The display of bypassed and inoperable status information is described in Section 7.2.13 which conforms to 10 CFR 50.34(f)(2)(v).

This section addresses the application specific information from NuScale topical report TR-1015-18653, "Highly Integrated Protection System Platform Topical Report" (Reference 7.1-1 listed in Table 7.0-2 for Sections 6.6, 6.7, 7.4, and 7.5 of IEEE-603-1991 (Reference 7.2-11).

7.2.4.1 Operating Bypasses

The MPS includes interlocks, permissives, and operational and maintenance bypasses that prohibit or permit certain protective actions either automatically or through a combination of automatic and manual actions to allow plant mode changes.

Information on displaying system bypass status information is provided in Section 7.2.13.

7.2.5 Interlocks

Interlocks ensure the reactor trip and engineered safety feature actuations are in the correct configuration for the current plant status. They ensure protection system functions are available and operational during plant conditions under which the interlocks are assumed to function in the plant safety analyses.

The design of MPS interlocks conforms to the requirements of IEEE 603-1991 (Reference 7.2-11). Computer-based interlocks conform to the requirments of IEEE 7-4.3.2. (Reference 7.2-13)

7.2.5.1 Instrumentation and Controls System Interlocks

The I&C interlocks performed within the MPS are summarized in Table 7.1-5. The I&C interlocks used to maintain the ESFAS variables within the ranges of values specified in the safety analyses are summarized in Table 7.1-5.

The MPS interlocks and operating bypasses are implemented within the individual divisions, which ensures that the applicable requirements of IEEE Standard 603-1991 (Reference 7.2-11) for redundancy, independence, satisfaction of the single failure criterion, qualification, bypasses, status indication, and testing are met.

NMS sensors and signal processing equipment are used to provide signal inputs for reactor trip functions and MPS interlocks. The NMS equipment used to provide the MPS functions meet the NMS single failure requirements.

The MPS interlocks are compatible with the functions and performance assumed in the events analyzed in Chapter 15.

7.2.5.2 Mechanical System Interlocks

The emergency core cooling system (ECCS) valves contain an inadvertent actuation block feature which minimizes the probability of a spurious opening of an ECCS valve at operating pressure (see Section 6.3). In the unlikely event of an inadvertent signal from MPS to actuate the ECCS valves at nominal plant pressure, the valves will not open until a sufficiently low differential pressure between the reactor pressure vessel and the containment vessel is reached. This allows the operator to respond to the inadvertent signal without the opening of the ECCS valves and the resulting plant transient.

Plant conditions during a valid ECCS actuation per the nominal trip setpoint should allow the ECCS valves to open when the inadvertent actuation block interlock is satisfied. If plant conditions do not allow the inadvertent actuation block interlock to be satisfied, the completion of the ECCS protective action will not occur until the inadvertent actuation block has allowed the ECCS valves to fully open and the open valve position signal is received by the MPS. There are no other safety-related mechanical system interlocks.

7.2.6 Derivation of System Inputs

This section describes the derivation of system inputs to the MPS used for the safety-related protective functions performed by the MPS. The MPS and NMS sensor and process measurement design conforms to the requirements of Section 6.4 of IEEE-603-1991 (Reference 7.2-11).

This section addresses the application specific information for NuScale topical report TR-1015-18653, "Highly Integrated Protection System Platform Topical Report" (Reference 7.1-1) listed in Table 7.0-2 for IEEE-603-1991 (Reference 7.2-11), Section 6.4.

The ~~parameters~~process variables associated with MPS safety-related functions are listed in Table 7.1-3 and Table 7.1-4. These ~~parameters~~process variables are used by the redundant sense and command features of MPS to generate required protective actions. These ~~parameters~~variables are monitored by variables identified in Table 7.1-2. The instrument range that accounts for normal, abnormal, and accident conditions is also specified for each variable. All but one MPS variable identified and used for safety-related functions is derived from process signals that are direct measurements of the process ~~parameters~~variables credited in the plant safety analysis (see Chapter 15). The exception is steam superheat, that is a ~~parameter~~variable calculated from steam pressure and steam temperature. Use of steam pressure and temperature is the only practical and feasible approach to obtaining the steam superheat ~~parameter~~variable credited in the plant safety analysis. Additional sensor measurement details for variables associated with the nuclear steam supply system are provided in the NuScale Power, LLC, TR-0316-22048 "Nuclear Steam Supply Systems Advanced Sensor Technical Report," (Reference 7.2-26).

The safety-related NMS sense and command features provide input to the MPS. The four redundant inputs to the MPS are direct measurements of the variables credited in the plant safety analysis. The ranges which account for normal, abnormal, and accident conditions for these variables are also provided in Table 7.1-2.

7.2.7 Setpoints

This section addresses the application specific information in NuScale topical report TR-1015-18653, "Design of the Highly Integrated Protection System Platform Topical Report" (Reference 7.1-1) listed in Table 7.0-2 for IEEE-603-1991 (Reference 7.2-11), Section 6.8.

NuScale Power, LLC, TR-616-49121 "NuScale Instrument Setpoint Methodology Technical Report," (Reference 7.2-27) describes the instrument setpoint determination methodology applied to the safety-related I&C functions. This methodology establishes performance and test acceptance criteria to evaluate setpoints during surveillance testing and calibration for setpoint drift. The analytical limits, uncertainties, and setpoints for the RTS and ESFAS functions are summarized in the NuScale Power, LLC, TR-616-49121 "NuScale Instrument Setpoint Methodology Technical Report," (Reference 7.2-27).

The methodology described has been established to ensure that the RTS and ESFAS setpoints are consistent with the assumptions made in the plant safety analysis and conform to the setpoint-related requirements of industry standard ISA-~~S~~67.04.01-~~1994~~2006, "Setpoints for Nuclear Safety-Related Instrumentation," (~~Reference 7.2-23~~Reference 7.2-29) ~~which is endorsed by RG 1.105 Revision 3, and~~

~~addresses the regulatory issues identified in U.S. Nuclear Regulatory Commission Regulatory Issue Summary 2006-17.~~and addresses the regulatory issues identified in U.S. Nuclear Regulatory Commission Regulatory Issue Summary 2006-17. Table 1.9-2 addresses the partial to conformance with Regulatory Guide 1.105, revision 3 that endorses ISA-S67.04-1994, "Setpoints for Nuclear Safety-Related Instrumentation," (Reference 7.2-23).

Setpoints for the RTS and ESFAS are selected to provide sufficient allowance between the trip setpoint and the analytical limit to account for instrument channel uncertainties. The instrument setpoint methodology determines calibration uncertainty allowances, including as-found and as-left tolerances, that are used in plant surveillance tests to verify that setpoints for safety-related protective functions are within technical specification limits. The methodology also establishes acceptance criteria to evaluate setpoints during surveillance testing and calibration for setpoint drift.

The methodology includes uncertainty and ~~setpoint calculations.~~calculated setpoints based on assumptions for instrument uncertainties. The detailed setpoint calculation processes for the MPS are described in the NuScale Power, LLC, TR-616-49121 "NuScale Instrument Setpoint Methodology Technical Report," (Reference 7.2-27) and may change according to the plant-specific ~~data~~instrument accuracy and uncertainty data. This methodology only applies to safety-related instrumentation used for RTS and ESFAS functions and does not include provisions for using a graded approach for nonsafety-related or less important instrumentation.

7.2.8 Auxiliary Features

I&C systems provide functionality to the auxiliary supporting features and other auxiliary features. These features meet the requirements of IEEE Standard 603-1991 (Reference 7.2-11), Section 5.12~~, and 10 CFR 50.34(f)(2)(xxiii)~~.

The information in this section addresses the application specific information in NuScale topical report TR-1015-18653, "Highly Integrated Protection System Platform Topical Report" (Reference 7.1-1) listed in Table 7.0-2 for the following sections: Section 5.12 of IEEE-603-1991 (Reference 7.2-11); DI&C-ISG-04, Section 1, staff position 16 (Reference 7.2-4).

7.2.8.1 Auxiliary Supporting Features

MPS Auxiliary Supporting Features

The auxiliary features within the MPS that are not required for the MPS to accomplish the safety function and are not isolated from MPS include the following:

- continuous online checking and self-diagnostics
- communication from safety function modules (SFMs), SBM, scheduling and voting modules, or EIMs to the MIB communications module in order to provide data to nonsafety systems and nonsafety displays
- capability for control of safety-related components by using nonsafety controls via the actuation priority logic function within the EIM
- isolation devices and circuitry

The NMS is an analog system with no digital components, and therefore has no vulnerabilities that require assessment.

7.2.9.2 Identification

Redundant divisions of MPS equipment are marked so that equipment can be clearly identified without frequent referral to reference material. Redundant divisions are distinguished by color-coded equipment tags or nameplates.

The MPS equipment is divided into four separation groups and two divisions. Non-rack mounted MPS SSCs are provided with an identification tag or nameplate. Small electrical components such as power supplies and logic cards have nameplates on the enclosure that houses them. Cables are provided with identification tags.

Electrical and control equipment, assemblies, devices, and cables are grouped into separate divisions and are identified such that the electrical divisional assignment is apparent. The identification method utilizes color coding and the markers within a division are the same color.

The cables and raceways for Class 1E systems (except those routed in conduits) are tagged at periodic intervals prior to or during installation. Cables and raceways are marked in a manner of sufficient durability to be legible throughout the life of the plant, and to facilitate initial verification that the installation is in conformance with the separation criteria. Cable and raceway markings are colored to uniquely identify the division (or non-division) of the cable. Any non-divisional cable within such cabinets is appropriately marked to distinguish it from the divisional cables. The method used for identification is readily distinguished between different divisions of Class 1E systems, between Class 1E and non- Class 1E systems, and between associated cables of different divisions. Associated cables are uniquely identified as such by a longitudinal stripe or other color-coded method.

Class 1E cable raceways are marked with the division color, and with their proper raceway identification at periodic intervals. Neutron-monitoring cables carry the unique voltage class markings superimposed on the divisional color markings, and placed at the same nominal intervals.

For computer systems, software and hardware identification is used to verify that the correct software is installed in the correct hardware component. A configuration control document or drawing is used to identify the correct software, including version, installed in digital I&C systems in accordance with IEEE Standard 7-4.3.2-2003, as endorsed by RG 1.152, Revision 3 (see Section 7.2.1).

MPS programming information is stored in the board's non-volatile memory device attached to the FPGA device. This configuration information is local to the board, and contains local settings, such as channel setup, sequencer setup, timing setup, and build information, including the version and revision of the programming. FPGA build information is created when the FPGA image is generated and is integral to the FPGA logic. The information can be read by the MWS.

- demineralized water system isolation
- chemical and volume control system isolation
- pressurizer heater trip
- low temperature over pressure protection

Because the hard-wired manual actuation switch input is downstream of digital components within the MPS, failure of the MPS automatic function does not prevent the manual initiation of the required protective action.

If enabled by the operator using the safety-related enable nonsafety control switch, the capability for manual component level control of ESF equipment is possible using nonsafety discrete hard-wired inputs from the MCS to the HWM. These signals are then input to the actuation priority logic circuit on the EIM. Any automatic or manual safety-related signal will override the nonsafety signal and is prioritized within the actuation priority logic. For beyond DBEs and for a limited number of actuated equipment, a safety-related override switch can be used to prioritize a nonsafety signal over an automatic signal. Override switches are provided for the following function.

Override - two switches / one per division

- The manual override switches override the containment flooding and drain system and valves.
- The manual override switches will generate an alarm when activated.

See the MPS functional logic diagrams (Figure 7.1-1j through Figure 7.1-1ao). The manual controls are controlled administratively through approved plant procedures.

No manually controlled actions are assumed in the NuScale Power Plant safety analyses in order to accomplish required safety-related functions. No Type A post-accident monitoring variables have been identified as defined in IEEE 497-2002 (Reference). The MPS provides outputs of monitored variables to two redundant divisions of the MCR SDIS displays for accident monitoring and to aid in manual operations. MCS human system interface displays in the MCR are also used to support manual controls.

In the event of a fire in the MCR, the operators evacuate the MCR and relocate to the RSS. There are two MCR isolation switches for each NPM that when repositioned, isolate the MPS manual actuation switches and the enable nonsafety switch for each NPM's MPS in the MCR to prevent spurious actuation of equipment due to fire damage. An alarm is annunciated in the MCR when the MCR hard-wired switches are isolated using the MCR isolation switches in the RSS, see Figure 7.1-1j.

7.2.13 Displays and Monitoring

This section describes the I&C display and monitoring systems, which provide information for the safe operation of the plant during normal operation, AOOs and postulated accidents, for supporting manual initiation and control of safety systems, for the normal status and the bypassed and inoperable status of safety systems, and for satisfying applicable requirements of 10 CFR 50.34(f).

The design of the SDIS conforms to IEEE-603-1991 (Reference 7.2-11), Section 5.8, and the guidance in RG 1.97, Revision 4 with exceptions as described in this section.

This section provides the application specific information from NuScale topical report TR-1015-18653, "Highly Integrated Protection System Platform Topical Report" (Reference 7.2-25) listed in Table 7.0-2 in the following sections: IEEE-603-1991 (Reference 7.2-11), Sections 5.8 and 5.14.

The displays for the SDIS are located in the MCR and provide accurate, complete, and timely information pertinent to MPS and PPS status and informational displays. These displays minimize the possibility of ambiguous indications to the operator. SDIS displays may be used to support manual initiation of protective actions, but the SDIS does not directly initiate protective actions.

MCR displays are developed following the guidance contained in NUREG-0700 as described in the NuScale Power Human-System Interface Design Results Summary Report (Reference 18.7-2). Display ambiguity factors have been addressed to minimize the chances of operational error due to misreading or misunderstanding displayed data. Each SDIS display panel presents data and status information derived from both divisions of MPS or PPS. There are two separate SDIS display panels, both panels independently display the same variables. This provides the operators in the MCR the ability to cross check data from independent divisions, independent sensors, on independent displays.

The SDIS receives inputs from the MPS and PPS through communication modules. Status information regarding ~~parameter~~process variable values, logic status, equipment status, and actuation device status are provided to the SDIS from the separation group and each division of the RTS, ESFAS, and PPS. The MPS interfaces through the divisional MPS gateway while the PPS interfaces through its MIB communication module.

The principal function of the SDIS is to display PAM variables used by plant operators to assess plant conditions during and following an accident. The principal functions of PAM instrumentation are to provide

- primary information to the control room operators to assess the plant critical safety functions
- primary information to the control room operators to indicate the potential for breach or the actual breach of fission product barriers
- information to the control room operators indicating the performance of those safety systems and auxiliary supporting features necessary for mitigating DBEs
- information to the control room operators indicating the performance of other systems necessary to achieve and maintain a safe shutdown condition
- information to the control room operators to verify safety system status
- information to the control room operators for determining the magnitude of the release of radioactive materials and continually assessing such releases

7.2.13.1 Displays for Manually Controlled Actions

Manual controls are a backup to the automatic functions provided by the MPS. There are no credited manual actions required to mitigate DBEs, and there are no Type A post-accident monitoring variables. There are no safety-related information displays in the MCR.

7.2.13.2 System Status Indication

The initiation of a protective action is identified and indicated down to the channel-level. Status information is nonsafety-related. As such, it is transmitted to the MCR for indication and recording from the MPS using the SDIS and MCS. PPS uses the PCS in conjunction with the SDIS.

MPS and PPS status information is provided in four types:

- ~~parameter~~process variable values and setpoints
- logic status
- equipment status
- actuation device status

Deviations from normal operating conditions using any combination of these four variable types are alerted to the operator through the use of alarms and annunciators. The task analysis process that was used to identify the controls, alarms, and displays needed in the MCR to manage the plant safety functions and remote shutdown capability are detailed in Section 18.7.2.

The Human Factors Program is described in Chapter 18, which includes the application of Functional Requirements Analysis and Function Allocation (Section 18.3) and Task Analysis (Section 18.4) in the design of the I&C human system interfaces for the NuScale Power Plant design.

Post-accident monitoring variables are displayed in the MCR on the SDIS, MCS, and PCS. The PAM variables displayed on SDIS are also displayed on MCS or PCS. Some PAM variables are only displayed on MCS and PCS. Additional description on PAM is in the PAM Section 7.1.1.2.2.

An interdisciplinary team consisting of I&C engineering, probabilistic risk assessment and severe accidents, reactor systems, and HFE have conducted a review of the variables identified for PAM based on the criteria established in IEEE Standard 497-2002. The SDIS meets the display criteria of IEEE-497-2002. The SDIS display panels display variables required for mitigation of design basis accidents, and the required variables for PAM requirements identified in Table 7.1-1. The ranges of the identified variables are presented in Table 7.1-2. The accuracies for the variables listed in Table 7.1-2 are presented in the NuScale Power, LLC, TR-616-49121 "NuScale Instrument Setpoint Methodology Technical Report," (Reference 7.2-27).

The SDIS is designed in accordance with the requirements of IEEE Standard 1023-1988. The NuScale HFE Program Management Plan (Reference 18.1-1) outlines how human

Alarms are not required to support manually controlled actions relied upon to enable the safety systems to accomplish their safety functions. Manually controlled actions are not assumed in the safety analyses in order to accomplish required safety functions. Operator actions are not required to maintain the plant in a safe and stable condition.

The MCS provides the operators with alarm and status information for viewing and historical trending. The MCS provides the alarms, alarm history, and trending information to the plant operators via the MCS human-system interfaces.

The alarms generated by the MCS for each NPM and PCS, are aggregated for display to the operator by the PCS HSIs in the MCR and RSS. The MCS and PCS operator workstations are separate and independent from the control processors such that a failure of the control processors will not affect the MCS or PCS operator workstations' alarm functions. Additionally, an independent monitoring system monitors the mutual status of the MCS and PCS to detect and alert the operator to a loss of the overall I&C system.

The MCS and PCS provide redundancy in the control processors, networking components, power supplies, power sources and operator workstation displays to maintain alarm system reliability in the MCR and RSS in accordance with item II.T of SECY-93-087 (Reference 7.1-7).

The MCS provides a first-out alarm resolution capacity. In the case of an avalanche of alarms, the system is able to discriminate between them and date tag the alarms in order of their occurrence. Process alarms are logged with a time stamp that includes the year, month, day, hour, minutes, and second which provides the operator the ability to understand and diagnose major plant upsets.

7.2.13.6 Three Mile Island Action Items

Control room indication is provided to measure, record, and readout containment pressure, containment water level, and noble gas effluents at the potential accident release points to satisfy the requirements of 10 CFR 50.34(f)(2)(xix) as well as the following ~~parameters~~variables that are used to identify inadequate core cooling to satisfy the requirements of 10 CFR 50.34(f)(2)(xviii):

- core exit temperatures
- wide range reactor coolant system pressure
- degrees of subcooling
- wide range reactor coolant system hot temperature
- RPV water level
- containment water level

The bypassed and operable status indication of safety interlocks is automatically provided in the control room as described in Section 7.2.13.6 and satisfies the requirements of 10 CFR 50.34(f)(2)(v) and RG 1.47.

The SDIS conforms to 10 CFR 50.34(f)(2)(iv) by providing the capability to display the Type B and Type C variables identified in Table 7.1-7 over anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions.

The reactor safety valve position indication is processed by the MPS and then sent to the SDIS and the MCS for display in the MCR. The reactor safety valve position indication is seismically qualified to Seismic Category I requirements and meets the requirements of 10 CFR 50.34(f)(2)(xi).

Consistent with 50.34(f)(2)(xvii) the SDI system provides the capability to monitor containment pressure, containment water level, and the reactor containment atmosphere for radioactivity released from postulated accidents. The MCS provides the recording function for the containment parameters.

Consistent with 10 CFR 50.34(f)(2)(xvii)(~~c~~C) and 10 CFR 50.44(c)(4), The PSS containment sampling system includes oxygen and hydrogen analyzers to monitor the containment environment. These monitors are non-safety related instruments that continuously monitor oxygen and hydrogen concentrations in containment during operation and are capable of monitoring during beyond design-basis conditions. The analyzers are designed to be functional, reliable, and will meet design criteria discussed in Regulatory Position C.2 of RG 1.7. The hydrogen analyzer output signal is sent to the MCS, which can provide readout in the main control room. Additionally, local indication is also provided as a backup display/indication in event that information from MCS cannot be displayed in the control room post-accident.

Consistent with 10 CFR 50.34(f)(2)(xvii)(E), the PCS displays and records in the MCR information on noble gas effluent release points for the NuScale plant.

Reactor coolant system level indication is powered with highly reliable DC power from EDSS rather than Class 1E power. This satisfies the requirements of 10 CFR 50.34(f)(2)(xx).

7.2.13.7 Other Information Systems

There is a unidirectional communication interface between the MCS and PCS networks and the plant network. The MCS and PCS systems provide monitoring data via one-way communication interfaces to the plant network which provides data recording, trending, and historical retention that can be called up on the emergency operations facility stations and technical support center (TSC) engineering workstations.

Additionally, there is a link from the plant network to the NRC emergency response data system via dedicated communication servers that connect to the plant network and provide data communication of required plant data to offsite emergency response facilities.

The TSC engineering work stations are located on the 100' level of the Control Building and separated from the operator workstations, which are located in the MCR on the 76'-6" level in the control building. The TSC engineering work stations have fully licensed operating systems, all configuration software, and a software package for complete configuration, tuning, trending, and diagnostics of the system. The TSC

engineering work stations provide a means to make changes and test software code prior to loading into the controllers.

The non-operator workstation PCS displays (TSC engineering, shift manager, shift technical advisor, and emergency operations facility) provide monitoring functionality to plant process and equipment controls.

7.2.14 Human Factors Considerations

The NuScale HFE program is described in Chapter 18. The program provides a systematic method for integrating HFE into plant analysis, design, evaluation, and implementation to achieve safe, efficient, and reliable operation, maintenance, testing, inspection, and surveillance of the plant. It also ensures the application of HFE principles in the design and verification of the following:

- physical control room structures
- MCR and RSS equipment and furnishings
- environments and structures where human tasks must be performed
- control panels and instruments throughout the plant
- controls and tools
- operating procedures
- operator training
- staffing planning

This information satisfies the application specific information in the NuScale Power, LLC, TR-1015-18653, "Design of the Highly Integrated Protection System Platform Topical Report," (Reference 7.2-25) listed in Table 7.0-2 for IEEE-603-1991 (Reference 7.2-11), Section 5.8, 5.13, and 5.14.

Human interface considerations for the MPS, PPS, and SDIS alarms and plant status information, as well as the nonsafety-related MCS and PCS are provided in this section.

7.2.14.1 Module Protection System

There are four types of MPS status information:

1) ~~parameter~~process variable values and setpoints

2) logic status

3) equipment status

4) actuation device status

The alarms and status information provided by MPS are used to confirm that protective actions have been actuated as required and that plant conditions have stabilized. Alarms and status information may be used for manual initiation of protective actions;

however, there are no manual protective actions for which no automatic action exists. Alarms associated with MPS are designed to alert the operator of abnormal conditions that may lead to automatic reactor trip or engineered safety feature (ESF) actuation, of inoperable channel or division-level components, or of a need for maintenance activities.

~~Parameter~~Process Variable Values and Setpoints

The MPS provides status information for all its sensors and equipment to the SDIS and the MCS for indication and alarms. The display instrumentation provides accurate, complete, and timely information which improves operator awareness and assists in making appropriate decisions. The MPS provides information for PAM variables through the MPS gateway to the SDIS displays in the MCR.

Logic Status

MPS utilizes four separation groups to make an reactor trip or ESF actuation determination. An alarm is provided at the separation group and division-level for the protective action. As an example, when an overpower condition is identified in one separation group, an alarm is generated. With two or more separation groups indicating an overpower condition, a first out alarm is generated to indicate the cause of the reactor trip. A first out alarm identifies the first condition to cause a major change in plant state. This is illustrated in the MPS functional logic diagrams in Figure 7.1-1a through Figure 7.1-1ao. This information is made available to the operators in the MCR and, in more detail, through the MWS.

Equipment Status

A trouble alarm is generated if there are equipment errors or inoperable channels or divisions, which are monitored continuously. Detailed information regarding the trouble alarm is available from the MWS. This aids in determining the course of action to correct problems.

These notifications allow operators to remain aware of system status during the performance of maintenance or testing.

Actuation Device Status

Execute features relied on by the MPS to accomplish a protective action provide component position feedback to the MPS. Component feedback is essential in confirming that protective actions have been initiated and completed. Valve position, for example, is shown on SDIS displays and allows an operator to identify safety valves in motion or in the safety position. Due to the simplified design of the NPM, actuation device status is limited to valve or breaker positions.

7.2.14.2 Plant Protection System

A component of human interface with the PPS is the MWS. The MWS is located close to the PPS equipment to facilitate troubleshooting activities. Diagnostics data for the PPS, as well as sensor and equipment status information, are accessible via the MWS.

The PPS provides status information for sensors and equipment to the SDIS and the PCS for indication and alarms. The PPS status information provided to the operator is of four types:

- ~~parameter~~process variable values and setpoints
- logic status
- equipment status
- actuation device status

The alarms and status information provided for PPS are used to confirm that the required PPS actions have been actuated, and remain actuated, as required, and that plant conditions have stabilized. Alarms and status information may be used for manual initiation of the required PPS actions; however, there are no manual PPS actions for which automatic action does not exist. Alarms associated with PPS are designed to alert the operator of abnormal plant conditions, equipment actuation, inoperable division-level components, or malfunctions that require maintenance.

~~Parameter~~Process Variable Values and Setpoints

Variables monitored by PPS, including setpoints, are provided for display to the operator via the PCS and the SDIS. Accident monitoring variables are available through the SDIS. The display instrumentation provides accurate, complete, and timely information which improves operator awareness and assists in making appropriate decisions.

Logic Status

PPS utilizes two fully redundant divisions to perform required functions. When process logic determines that a protective function actuation is required (e.g., control room habitability system actuation), an alarm is provided at the division level for the required PPS protective function actuation. There are no connections between divisions. In terms of human factors, this ensures that the source of the alarm can be readily determined.

Equipment Status

With continuous self-diagnostics, system modules generate a trouble alarm if there are equipment errors or inoperable channels or divisions. Detailed information regarding the trouble alarm is available from the MWS. This aids in determining the course of action to correct any problems.

The PPS allows periodic testing during normal operation. The affected channel can be placed in bypass in accordance with applicable technical specification limits. Any channel in bypass generates an alarm for that particular function. These notifications allow operators to remain aware of system status during the performance of maintenance or testing.

Actuation Device Status

Status feedback is provided for the execute features relied on by the PPS to accomplish a required action.

Periodic surveillance testing (e.g., actuation of device) is used to verify operability, in accordance with any applicable technical specification limits, see Section 7.2.15. Additional self-diagnostics are implemented in PPS to provide device status rapidly in the event of a component issue. The results of this testing are provided to the operators and maintenance personnel through the MCR status displays and the MWS local to the PPS equipment.

Component feedback is essential in confirming that the required actions have been initiated and completed. Valve position, for example, is shown on MCR displays and allows an operator to identify valves in motion or in their actuated position. Due to the simplistic design of the NuScale Power Plant, actuation device status in the PPS is limited to valve or damper positions.

7.2.14.3 Safety Display and Indication System

The SDIS is designed to meet the requirements of IEEE Standard 1023-1988. The HFE Program Management Plan (Reference 18.1-1) outlines how human factors are incorporated into the design of systems such as the SDIS.

The SDIS provides the following information to the operator:

- MPS and PPS post-accident monitoring parameter values
- MPS, PPS, and SDIS equipment status
- MPS and PPS actuation device status

The operator uses the SDIS for validation that a protective action has gone to completion and that the NPMs are being maintained in a safe condition. Because the SDIS does not perform actions, the operators use the SDIS to aid in decision making regarding plant operations.

Variables monitored by the MPS and PPS identified for PAM (Table 7.1-7) are available on the SDIS displays for the operator in an accurate, complete and timely manner. ~~Parameters~~Process variables are displayed such that when they exceed set limits, they are easily noticeable by the operator.

The SDIS displays the availability of the equipment of the MPS, PPS and SDIS. With continuous self-diagnostics in the systems, the SDIS is able to immediately alert the operator when equipment is no longer available.

Alarms associated directly with the SDIS are for failures of a communication module or a display. If an alarm occurs, the identified piece of equipment must be removed and replaced. The SDIS displays the status of the actuation devices controlled by MPS and PPS. The operators use this information to verify the completion of protective actions during DBEs requiring actuation of devices through the MPS or PPS.

Module Control System and Plant Control System

The MPS provides the capability to bypass an NMS channel to support NMS system calibration.

7.2.15.2 I&C system testing

The MPS is designed to support testing as specified in IEEE Standard 338-1987 as endorsed and modified by RG 1.118, Revision 3, and IEEE Standard 603-1991 (Reference 7.2-11) with supplemental guidance in RG 1.22, Revision 0, and RG 1.47, Revision 1.

The MPS and NMS allow SSCs to be tested while retaining the capability to accomplish required safety functions. The MPS uses modules from the HIPS platform which are designed to eliminate non-detectable failures through a combination of built-in self-testing and periodic surveillance testing.

Testing from the sensor inputs of the MPS through to the actuated equipment is accomplished through a series of overlapping sequential tests, and the majority of the tests may be performed with the NPM at power. Where testing final equipment at power has the potential to upset plant operation or damage equipment, provisions are made to test the equipment when the NPM is shut down.

Periodic surveillance testing also verifies the continual self-testing functions. Performance of periodic surveillance testing does not involve disconnecting wires or installation of jumpers for at-power testing. The self-test features maintain separation group and division independence by being performed at within the separation group or within the division.

The part of MPS that cannot be tested at power is the actuation priority logic circuit on the EIM. This includes the manual MCR switches and the nonsafety-related control that provide inputs to the actuation priority logic. The actuation priority logic consists of discrete components and directly causes actuation of field components that cause the reactor to shutdown or adversely affect operation. The actuation priority logic is a very simple circuit and has acceptable reliability to be tested when the reactor is shut down.

The manual trip and actuate switches in the MCR cannot be tested at power and require an outage. These switches are standby, low demand components such that testing every refueling outage is acceptable to maintain sufficient system reliability.

The SDIS supports MPS and PPS by providing the displays for Type B, Type C and Type D post-accident monitoring variables. Post-accident monitoring instrument channels have testing capability to verify, on a periodic basis, functional requirements to support calibration of the channels.

Continuous self-tests within the SDIS will detect and annunciate communication failures.

~~The design requirements of PPS and SDIS do not require they meet the single failure criterion during channel maintenance, test, or calibration provided the duration of such testing satisfies the applicable plant technical specifications (see Section 16.1) according to IEEE Standard 497-2002. The time interval required for a test or calibration~~

~~operation is so short that it would have an insignificant effect on overall availability of the PAM variable display provided by the SDIS. The allowable test intervals are identified in the plant technical specifications.~~The SDIS and PPS are designed to support periodic testing, calibration and maintenance. Either division of SDIS and PPS can fully accomplish their required functions, such that if a single division removed from service for testing, maintenance or calibration the other division remains available to perform the required functions. SDIS and PPS are not required to meet the single failure criterion during maintenance, test or calibration activities consistent with the guidance contained in IEEE Standard 497-2002. The time periods during which SDIS and PPS may be bypassed or removed from service is administratively controlled.

While the MPS is in normal operation, self-tests run without affecting the performance of the safety function, including its response time.

MPS data communications are designed with error detection to enhance data integrity. The protocol features ensure communications are robust and reliable with the ability to detect transmission faults. Similar data integrity features are used to transfer diagnostics data.

The MPS provides a means for checking the operational availability of the sense and command feature input sensors relied upon for a safety function during reactor operation.

This capability is provided by one of the following methods:

- perturbing the monitored variable
- cross-checking between channels that have a known relationship (i.e., channel check)
- introducing and varying a substitute input to the sensor

7.2.15.3 Fault detection and self-diagnostics

The MPS platform incorporates failure detection and isolation techniques. Fault detection and indication occurs at the module level, which enables plant personnel to identify the module that needs to be replaced.

Diagnostic data for the separation group and division of the MPS are provided to the MWS for the division. The MWS is located close to the equipment to facilitate troubleshooting activities. The interface between the MPS gateway and the MWS is an optically-isolated, one-way diagnostic interface. Diagnostics data are communicated via the MIB which is a physically separate communications path from the safety data path, ensuring the diagnostics functionality is independent of the safety functionality. Further discussion on how the MWS does not prevent or have adverse influence on the MPS performing safety functions can be found in Section 7.1.2.

The operation of the MPS is deterministic in nature and allows the systems to monitor themselves in order to validate functional performance. The self-test features provide a comprehensive diagnostic system ensuring system status is continually monitored. Detectable failures are alarmed to the operator in the MCR, and an indication of the

7.2-11 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE 603-1991, Piscataway, N.J.

7.2-12 Institute of Electrical and Electronics Engineers, "IEEE Guide for Generating Station Grounding," IEEE 665-1995 (R2001), Piscataway, N.J.

7.2-13 Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," IEEE 7-4.3.2-2003, Piscataway, N.J.

7.2-14 Institute of Electrical and Electronics Engineers, "IEEE Standard for Software Quality Assurance Plans," IEEE 730-2002, Piscataway, N.J.

7.2-15 Institute of Electrical and Electronics Engineers, "IEEE Standard for Software Configuration Management Plans," IEEE 828-2005, Piscataway, N.J.

7.2-16 Institute of Electrical and Electronics Engineers, "IEEE Standard for Software and System Test Documentation," IEEE 829-2008, Piscataway, N.J.

7.2-17 Institute of Electrical and Electronics Engineers, "IEEE Recommended Practice for Software Requirements Specifications," IEEE 830-1998, Piscataway, N.J.

7.2-18 Institute of Electrical and Electronics Engineers, "IEEE Standard for Software Unit Testing," IEEE 1008-1987 (R2009), Piscataway, N.J.

7.2-19 Institute of Electrical and Electronics Engineers, "IEEE Standard for Software Verification and Validation," IEEE 1012-2004, Piscataway, N.J.

7.2-20 Institute of Electrical and Electronics Engineers, "IEEE Standard for Software Reviews and Audits," IEEE 1028-2008, Piscataway, N.J.

7.2-21 Institute of Electrical and Electronics Engineers, "IEEE Guide for Instrumentation Control Equipment Grounding in Generating Stations," IEEE 1050-1996, Piscataway, N.J.

7.2-22 Institute of Electrical and Electronics Engineers, "IEEE Standard for Developing a Software Project Life Cycle Process," IEEE 1074-2006, Piscataway, N.J.

7.2-23 International Society of Automation, "Setpoints for Nuclear Safety-Related Instrumentation," ISA-S67.04-1994, Research Triangle Park, North Carolina.

7.2-24 American National Standards Institute/International Society of Automation, "Instrument Sensing Line Piping and Tubing Standards for Use in Nuclear Power Plants," ANSI/ISA 67.02.01-1999, Research Triangle Park, North Carolina.

7.2-25 NuScale Power, LLC, "Design of the Highly Integrated Protection System Platform Topical Report," TR-1015-18653, Revision 2~~1~~.

7.2-26 NuScale Power, LLC, "Nuclear Steam Supply Systems Advanced Sensor Technical Report," TR-0316-22048, Revision 0.

7.2-27 NuScale Power, LLC, "NuScale Instrument Setpoint Methodology Technical Report," TR-616-49121, Revision ~~0~~1.

7.2-28 Institute of Electrical and Electronics Engineers, "Standard for Flame-Propagation Testing of Wire & Cable," IEEE 1202-2006, Piscataway, N.J.

7.2-29 International Society of Automation, "Setpoints for Nuclear Safety-Related Instrumentation," ISA-67.04.01-2006, Research Triangle Park, North Carolina.

Enclosure 5:

Summary of NRC Staff Questions and NuScale Responses with references to applicable changes

Tier 1, Section 2.5.2, “Module Protection System”			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
T1-1	4/11/2017	**Status:** **Resolved/Closed**	No changes.
T1-2	4/11/2017	**Status:** **Resolved/Closed**	No changes.
T1-3	4/11/2017	**Status:** **Resolved/Closed**	No changes.
T1-4	4/11/2017	**Status:** **Resolved/Closed**	No changes.
T1-5	4/11/2017	**Status:** **Resolved/Closed**	No changes.
T1-6	4/11/2017	**Status:** **Resolved/Closed**	No changes.
T1-7	4/11/2017	**Status:** **Resolved/Closed**	No changes.
T1-8	4/11/2017	**Status:** **Resolved/Closed**	No changes.
T1-9	4/11/2017	**Status:** **Resolved/Closed**	No changes.

Tier 2, Section 7.0, "Instrumentation and Controls - Introduction and Overview"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.0-1	4/11/2017	**Status: Resolved / Confirmatory Item**	FSAR Figures 7.0-4, 7.0-5, and 7.0-13 were revised to show the trip/bypass switches in a defined position, instead of an intermediate position consistent with the design of the MPS. Additional changes were made after further review. Added 24-Hour Timers as an input to MPS Gateway in Figure 7.0-4 and 7.0-5. Removed intermediate position on switches that did not have such a position on Figure 7.0-5 and 7.0-13. Added MCR Isolation input for ESFAS HWM in Figure 7.0-5. Changed wording in Figure 7.0-5 from Operational Bypass to Operating Bypass. Changed wording in Figure 7.0-5 from Nonsafety Enable to Enable NS.
7.0-2	4/11/2017	**Status: Resolved / Confirmatory Item**	FSAR section 7.2.3.3 was revised to add information to describe in more detail the function of the actuation priority logic circuit, and the prioritization between the three inputs consistent with the MPS logic diagram figures in Section 7.1
7.0-3	4/11/2017	**Status: Resolved/Closed**	No changes.
7.0-5	4/11/2017	**Status: Resolved/Closed**	No changes.
7.0-6	4/11/2017	**Status: Resolved / Confirmatory Item**	FSAR Section 7.0.4.5.1 was revised to state that automatic control rod withdrawal may not be performed when thermal reactor power is between 0 and 15 percent.

Tier 2, Section 7.0, "Instrumentation and Controls - Introduction and Overview"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.0-7	4/11/2017	**Status: Resolved/Closed**	No changes.
7.0-8	4/11/2017	**Status: Resolved/Closed**	No changes.
7.0-9	4/11/2017	**Status: Resolved/Closed**	No changes.
7.0-10	4/11/2017	**Status: Resolved / Confirmatory Item**	FSAR Figure 7.0-10 was revised to remove the fourth input sub-module as it is not used in this application for the 24-hr timer inputs to the safety function module. Additionally, NuScale changed the communication port used for the Gateway from the SDB to the MIB.
7.0-11	5/11/2017	**Status: Resolved / Confirmatory Item**	FSAR Table 7.1-4 was updated in response to item (1) to include notes describing the reference for the elevation values for the RPV level and CNV level analytical limits. Additional notes and editorial changes were added to provide clarity and consistency with Table 15.0-7.

Tier 2, Section 7.1.1, "Design Bases and Additional Design Considerations"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.1.1-1	4/18/2017	**Status: Resolved/Closed**	No changes.
7.1.1-2	4/18/2017	**Status: Resolved / Confirmatory Item**	FSAR Table 7.1-18 was revised to add Note 2 to the Category 4 summary of design basis events.
7.1.1-2	5/11/2017	**Status: Resolved/Closed**	No changes.

Tier 2, Section 7.1.2, "Independence"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.1.2-1	5/11/2017	**Status: Resolved / Confirmatory Item**	FSAR section 7.1.2 was revised to correctly reflect that the Class 1E isolation is provided by the MIB communication module via isolated, one way fiber optic data links.
7.1.2-2	5/11/2017	**Status: Open**	This item is not addressed as part of this transmittal.

Tier 2, Section 7.1.5, "Diversity and Defense-in-Depth"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.1.5-1	4/11/2017	**Status: Resolved/Closed**	No changes.
7.1.5-2	4/11/2017	**Status: Resolved/Closed**	No changes.
7.1.5-3	4/11/2017	**Status: Resolved/Closed**	No changes.
7.1.5-4	4/11/2017	**Status: Resolved / Confirmatory Item**	No changes.
7.1.5-5	4/11/2017	**Status: Resolved / Confirmatory Item**	FSAR section 7.1.5.1.6 was revised to provide a pointer to FSAR section 13.5 regarding the operating and maintenance procedural administrative controls.
7.1.5-6	4/11/2017	**Status: Resolved / Confirmatory Item**	FSAR section 7.1.5.1.6 was revised to provide a pointer to FSAR section 13.5 regarding the operating and maintenance procedural administrative controls.
7.1.5-7	4/11/2017	**Status: Resolved/Closed**	No changes.

Tier 2, Section 7.1.5, "Diversity and Defense-in-Depth"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.1.5-8	4/11/2017	**Status: Resolved / Confirmatory Item**	No changes.
7.1.5-9	4/11/2017	**Status: Resolved / Confirmatory Item**	FSAR section 7.1.5.2.2 was revised to remove the level sensor from the Diversity and Defense-in-Depth Coping Analysis results.
7.1.5-10	4/11/2017	**Status: Resolved/Closed**	No changes.

Tier 2, Section 7.1.8, "Hazard Analysis"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.1.8-1	4/11/2017	**Status: Resolved / Confirmatory Item**	FSAR section 7.1.8.2 was revised to add a statement that the MPS and NMS Hazards Analyses were performed for all modes of system operation.
7.1.8-2	4/11/2017	**Status: Open**	This item is not addressed as part of this transmittal.

Tier 2, Section 7.2.1, "Quality"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.2.1-1	4/17/2017	**Status: Resolved/Closed**	No changes.
7.2.1-2	5/11/2017	**Status: Resolved / Confirmatory Item**	FSAR Section 7.2.1 was revised to add clarification that consistent with Regulatory Guide 1.170, exceptions to the documentation requirements for the NuScale Digital I&C Software Quality Assurance Program may be taken, and that in all cases the NuScale Quality Assurance Program takes precedence as described in section 17.5.
7.2.1-3	5/11/2017	**Status: Open**	FSAR section 7.2.1.6 was revised to add descriptive information on the activities performed as part of the security analysis verification to prevent unauthorized or undocumented code in digital safety systems, consistent with Regulatory Guide 1.1.52, revision 3.
7.2.1-4	5/11/2017	**Status: Open**	FSAR Section 7.2.1.6 was revised to provide additional information regarding the secure development and operating environmental aspects of previously developed and commercial off-the-shelf software including requirements placed on vendors consistent with Regulatory Guide 1.152, revision 3.

Tier 2, Section 7.2.2, "Equipment Qualification" AND Technical Report, "NuScale Instrument Setpoint Methodology"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.2.2-1	4/11/2017	**Status: Resolved / Confirmatory Item**	FSAR section 7.2.2.1 was revised to state that the MPS and NMS do not rely on environmental controls to function during design basis events. The MPS and NMS are designed to operate in the environmental conditions that may exist during design basis events.
7.2.2-2	4/11/2017	**Status: Resolved/Closed**	No changes.

Tier 2, Section 7.2.4, "Operating and Maintenance Bypasses"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.2.4-1	4/11/2017	**Status: Resolved/Closed**	No changes.

Tier 2, Section 7.2.5, "Interlocks"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.2.5-1	5/11/2017	**Status: Resolved / Confirmatory Item**	FSAR section 7.2.5.2 was revised to provide an explicit statement that no other safety-related mechanical system interlocks exists to prevent completion of an automatic function.

Tier 2, Section 7.2.7, "Setpoints" AND Technical Report, "NuScale Instrument Setpoint Methodology"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.2.7-1	4/11/2017	**Status: Resolved/Closed**	No changes.
7.2.7-2	4/11/2017	**Status: Resolved / Confirmatory Item**	FSAR Table 1.9-2 was revised to explain partial conformance with Regulatory Guide 1.105, revision 3 with respect to the use of ISA-67.04.01-2006.
7.2.7-3	4/11/2017	**Status: Resolved/Closed**	No changes.
7.2.7-4	4/11/2017	**Status: Resolved / Confirmatory Item**	NuScale Instrument Setpoint Methodology Technical Report Section 3.2.3 was revised to remove the last sentence regarding the assumption regarding M&TE uncertainties.
7.2.7-5	4/11/2017	**Status: Resolved/Closed**	No changes.
7.2.7-6	4/11/2017	**Status: Resolved / Confirmatory Item**	NuScale Instrument Setpoint Methodology Technical Report Section 4.1.4 and Figure 4-2 were updated to state that the margin applied in determining the nominal trip setpoint must be greater than or equal to the As-Found Tolerance.
7.2.7-7	4/11/2017	**Status: Resolved/Closed**	No changes.

Tier 2, Section 7.2.7, “Setpoints” AND Technical Report, “NuScale Instrument Setpoint Methodology”			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.2.7-8	4/11/2017	**Status: Resolved / Confirmatory Item**	NuScale Instrument Setpoint Methodology Technical Report Section 5.0, "Assumptions" was revised to state which assumptions apply generically to the Setpoint Methodology, and which assumptions are made due to the lack of final sensor uncertainty data.
7.2.7-9	4/11/2017	**Status: Resolved/Closed**	No changes.
7.2.7-10	4/11/2017	**Status: Resolved / Confirmatory Item**	NuScale Instrument Setpoint Methodology Technical Report Figure 6-1 was revised to add a final step to document the results of the setpoint calculations.
7.2.7-11	4/11/2017	**Status: Open**	This item is not addressed as part of this transmittal.
7.2.7-12	4/11/2017	**Status: Open**	Items one and two were not addressed as part of this transmittal. For item 3, Chapter 7 of the FSAR was reviewed and several editorial revisions were made to ensure consistency in terminology and use of "parameter" and "variable".
7.2.7-13	4/11/2017	**Status: Resolved / Confirmatory Item**	NuScale Instrument Setpoint Methodology Technical Report Revision 0 Section 5.8 (draft Revision 1’s Section 5.9) was revised to add a pointer to Table 5-1.
7.2.7-14	4/11/2017	**Status: Resolved / Confirmatory Item**	FSAR section 7.2.7 was revised to state the NuScale Instrument Setpoint Methodology provides calculated setpoints based on assumptions made for instrument uncertainty and accuracy data.

Tier 2, Section 7.2.7, "Setpoints" AND Technical Report, "NuScale Instrument Setpoint Methodology"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.2.7-15	5/11/2017	**Status: Resolved / Confirmatory Item**	FSAR section 7.2.7 was updated to state that the setpoint methodology provides calculated setpoints based on assumptions for instrument uncertainties, and that the setpoints may be updated based on plant-specific instrument uncertainty and accuracy data.

Tier 2, Section 7.2.8, "Auxiliary Features"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.2.8-1	5/11/2017	**Status: Resolved / Confirmatory Item**	FSAR section 7.2.8 was revised to remove the reference to 10 CFR 50.34(f)(2)(xxiii).

Tier 2, Section 7.2.9, "Control of Access, Identification and Repair"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.2.9-1	5/11/2017	**Status: Resolved / Confirmatory Item**	FSAR section 7.1.1.2.3 was revised to remove the pointer to section 7.2.9 regarding administrative controls for access to the remote shutdown station.
7.2.9-2	5/11/2017	**Status: Resolved / Confirmatory Item**	FSAR section 7.2.9.2 was revised to add information related to the markings of cable raceways for Class 1E systems.

Tier 2, Section 7.2.10, "Interaction Between Sense and Command Features and Other Systems"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.2.10-1	4/11/2017	**Status: Resolved/Closed**	No changes.
7.2.10-2	4/11/2017	**Status: Resolved/Closed**	No changes.
7.2.10-3	4/11/2017	**Status: Resolved/Closed**	No changes.
7.2.10-4	4/11/2017	**Status: Resolved/Closed**	No changes.
7.2.10-5	4/11/2017	**Status: Resolved/Closed**	No changes.
7.2.10-5	5/17/2017	**Status: Open**	This item is not addressed as part of this transmittal.

Tier 2, Section 7.2.12, "Automatic and Manual Control"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.2.12-1	4/11/2017	**Status:** **Resolved/Closed**	No changes.
7.2.12-2	4/11/2017	**Status:** **Resolved/Closed**	No changes.

Tier 2, Section 7.2.14, "Human Factors Considerations"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.2.14-1	4/11/2017	**Status:** **Resolved/Closed**	No changes.

Tier 2, Section 7.2.15, "Capability for Test and Calibration"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.2.10-5	5/17/2017	**Status: Resolved / Confirmatory Item**	FSAR section 7.2.15.2 was revised to remove references to plant technical specifications regarding testing of the SDIS and PPS.

Technical Report: Nuclear Steam Supply System Advanced Sensor			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
TR-AS-1	4/11/2017	**Status: Resolved / Confirmatory Item**	This item was addressed as part of item 7.2.7-4.
TR-AS-2	4/11/2017	**Status: Resolved/Closed**	No changes.
TR-AS-3	4/11/2017	**Status: Resolved / Confirmatory Item**	This item is not addressed as part of this transmittal, however NuScale will address this item in a future transmittal.
TR-AS-4	4/11/2017	**Status: Resolved/Closed**	No changes.
TR-AS-5	4/11/2017	**Status: Resolved/Closed**	No changes.
TR-AS-6	4/11/2017	**Status: Resolved / Confirmatory Item**	This item is not addressed as part of this transmittal.
TR-AS-7	5/11/2017	**Status: Resolved/Closed**	No changes.
TR-AS-8	5/11/2017	**Status: Resolved/Closed**	No changes.

Technical Report: Nuclear Steam Supply System Advanced Sensor			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
TR-AS-9	5/11/2017	**Status: Resolved/Closed**	No changes.
TR-AS-10	5/11/2017	**Status: Resolved/Closed**	No changes.
TR-AS-11	5/11/2017	**Status: Resolved/Closed**	No changes.

Part 4, "Generic Technical Specifications"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
7.2.7-12	5/11/2017	**Status: Resolved / Confirmatory Item**	Items one and two were not addressed as part of this transmittal. For item 3, Chapter 7 of the FSAR was reviewed and several editorial revisions were made to ensure consistency in terminology and use of "parameter" and "variable".
GTS-1	5/11/2017	**Status: Open**	This item is not addressed as part of this transmittal.
GTS-2	5/11/2017	**Status: Open**	This item is not addressed as part of this transmittal.
GTS-3	5/11/2017	**Status: Open**	This item is not addressed as part of this transmittal.
GTS-4	5/11/2017	**Status: Open**	This item is not addressed as part of this transmittal.
GTS-5	5/11/2017	**Status: Open**	This item is not addressed as part of this transmittal.
GTS-6	5/11/2017	**Status: Open**	This item is not addressed as part of this transmittal.
GTS-7	5/11/2017	**Status: Open**	This item is not addressed as part of this transmittal.
GTS-8	5/11/2017	**Status: Open**	This item is not addressed as part of this transmittal.
GTS-9	5/11/2017	**Status: Open**	This item is not addressed as part of this transmittal.

Part 4, "Generic Technical Specifications"			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
GTS-10	5/11/2017	**Status: Open**	This item is not addressed as part of this transmittal.
GTS-11	5/11/2017	**Status: Open**	This item is not addressed as part of this transmittal.
GTS-12	5/11/2017	**Status: Open**	This item is not addressed as part of this transmittal.

Category: Editorial Items			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
E-1	4/11/2017	**Status: Resolved / Confirmatory Item**	This item is not addressed as part of this transmittal; however NuScale will address this item in a future transmittal.
E-2	4/11/2017	**Status: Resolved / Confirmatory Item**	FSAR section 7.1.1.2.1 has been revised to point to the correct Figures for the RXB drawings using the location of the MPS and NMS equipment (Figures 1.2-14 and 1.2-15, respectively).
E-3	4/11/2017	**Status: Resolved / Confirmatory Item**	FSAR section 7.2.2.1 has been revised to point to the correct Figures for the RXB drawings using the location of the MPS and NMS equipment (Figures 1.2-14 and 1.2-15, respectively).
E-4	4/18/2017	**Status: Resolved / Confirmatory Item**	FSAR sections 7.0.4.1.3 and 7.0.4.1.4 have been revised to add information regarding the power source of the Shunt Trip Coil circuit for the Reactor Trip Breakers and Pressurizer Heater Trip Breakers.

Category: Editorial Items			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
E-5	4/18/2017	**Status: Resolved / Confirmatory Item**	FSAR section 7.2.13.3 has been revised to state an alarm is annunciated in the main control room when the MCR switches are isolated in the remote shutdown station.
E-6	4/18/2017	**Status: Resolved / Confirmatory Item**	FSAR Table 7.1-1 was updated to correctly refer to the "Increase in Feedwater Flow" transient which is described in Section 15.1.2.2
E-7	4/18/2017	**Status: Resolved / Confirmatory Item**	FSAR Figure 7.0-1 was revised to add notes regarding information conveyed in the figure to add clarity, including denoting the MPS Gateway and Maintenance Workstation are nonsafety-related components.
E-8	4/18/2017	**Status: Resolved / Confirmatory Item**	FSAR Figure 7.0-1 was revised to add notes describing the bidirectional communication interfaces on the MPS backplane connections.
E-9	4/18/2017	**Status: Resolved / Confirmatory Item**	FSAR Table 7.1-13 was revised to remove wide range containment pressure from the table as it is a nonsafety-related sensor.
E-10	4/18/2017	**Status: Resolved / Confirmatory Item**	FSAR Figure 7.0-10 was revised to remove the fourth input submodule shown for the safety function module.

Category: Editorial Items			
No.	**Date**	**Status**	**NuScale Changes to Address Staff Comments**
E-11	4/18/2017	**Status: Resolved / Confirmatory Item**	FSAR Figure 7.0-5 was revised to correct the text shown on the RTS M/I CM to read "RTS MIB CM".
E-12	4/18/2017	**Status: Resolved / Confirmatory Item**	ITAAC No. 1 in Tier 1, Section 2.5, Table 2.5-7 was revised to change "software lifecycle phases" to "system design lifecycle phases".
E-13	4/18/2017	**Status: Resolved / Confirmatory Item**	This item is not addressed as part of this transmittal; however NuScale will address this item in a future transmittal.

Category: Additional Changes to FSAR		
Revision 0 Page Number	**Section**	**Description of Change**
2.5-8	Tier 1, Table 2.5-2	Table 2.5-2 was revised to ensure correctness and consistency with Table 7.1-4 for the RCS Flow Interlock, F-1.
2.5-10	Tier 1, Table 2.5-4	Table 2.5-4 was revised to ensure correctness and consistency with Table 7.1-4 for the RCS Flow Interlock, F-1.
7.1-99, 7.1-109	Figure 7.1-1c and 7.1m	Removed duplicate DWSI actuation logic
7.1-111 through 7.1-122	Figures 7.1-1o through 7.1-1z	Editorial changes to rename abbreviation for enable nonsafety control switch from "NS ENABLE" or "NS DISABLE" to "ENABLE NS" or "DISABLE NS"

Category: Additional Changes to FSAR		
Revision 0 Page Number	**Section**	**Description of Change**
7.1-123 through 7.1-136	Figures 7.1-1aa through 7.1-1an	Updated reset coil logic for the ECCS valves and the close coil logic for the reactor trip and pressurizer heater trip breakers.
7.1-138	Figure 7.1-2	Revised figure to add clarifying information (Note 3) regarding EDSS power supplies to the MPS and PPS and to remove the duplicate figure titles.
7.1-115, 7.1-117, 7.1-118, 7.1-135, and 7.1-136	Figure 7.1-1s, Figure 7.1-1u, Figure 7.1-1v, Figure 7.1-1am, and Figure 7.1-1an	Editorial change to update figure titles.
7.1-5, 7.1-20, and 7.1-21	7.1.1.2.1 and 7.1.4	Editorial revisions to the MPS response time description were made to add clarity regarding the response time allocated to the MPS.
7.1-40 through 7.1-43	7.1.5.2.1	Where appropriate, added spurious reactor trip or demineralized water system isolation to align with logic diagrams
7.0-28, 7.1-60, 7.2-65-7.2-66	7.0.5, 7.1.9, and 7.2.16	Editorial changes to reflect updated revision numbers in topical and technical report references.
7.0-53	Figure 7.0-17	Add a missing interface and function for the module-specific containment system.
7.1-4	7.1.1.1	Changed "Certain monitored variables are relied upon to execute protective actions if setpoints …" to " … protective actions when setpoints …"

Category: Additional Changes to FSAR		
Revision 0 Page Number	**Section**	**Description of Change**
7.1-76, 7.1-77	Table 7.1-9	Revised table to make certain clarifications and additions. Split pressurizer level and RPV riser level since RPV riser level is a Type B and Type C variable while pressurizer level is not. Removed FWIV, MSIV, and MS isolation bypass since it is covered as part of containment isolation valve positions. Corrected power range linear power to indicate "Y" for the "Type A, B, or C Pam Variable?" column. Added missing entries for NMS Supply Fault, NMS-Flood, NMS-Flood Fault, and CES Suction Pressure.
7.1-79	Table 7.1-11	Editorial change to remove ";" and to change "MSIV bypass valves" to "MS Isolation bypass valves"
7.2-56	7.2.13.6	Editorial change from 10 CFR 50.34(f)(2)(xvii)(c) to 10 CFR 50.34(f)(2)(xvii)(C). Provided additional discussion on how MCS and PCS are used to address Three Mile Island Action Items.

Category: Additional Changes to NuScale Instrument Setpoint Methodology Technical Report		
Revision 0 Page Number	**Section**	**Description of Change**
Throughout	Throughout	Editorial changes were made throughout the Instrument Methodology Setpoint Technical Report.
45 and 46	Table 6-2	Added ESFAS actuation signals to ensure consistency with FSAR Table 7.1-4.