X Energy, LLC
801 Thompson Avenue
Rockville, MD 20852
+1 301.358.5600

3-Feb-2023

2023-XE-NRC-004

Project No. 99902071

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, DC 20555-0001

Submittal of X Energy, LLC (X-energy) White Paper: Xe-100 Plant Control and Data Acquisition System

The purpose of this letter is to submit Revision 2 of the subject white paper to the U.S. Nuclear Regulatory Commission (NRC) on behalf of X Energy, LLC (X-energy). The enclosed submission provides both proprietary and non-proprietary versions of the report. The report is provided for NRC review, for planning and familiarization purposes in support of pre-application discussions, and to obtain NRC feedback as indicated in the report. X-energy requests that the review focus on the following key design concepts: (1) functional design of the Plant Control and Data Acquisition System (PCDAS), which is comprised of multiple subsystems, (2) interfaces between control and protection, and (3) overall instrumentation and control architecture. The specific review schedule will continue to be developed with X-energy's NRC project manager.

This report contains commercially sensitive, proprietary information, and, as such, we are requesting that this information be withheld from public disclosure in accordance with 10 CFR 2.390, "Public inspections, exemptions, requests for withholding," paragraph (a)(4). Enclosure 1 is the Non-Public version of the report which contains nonredacted sensitive, proprietary information that is appropriately marked. Enclosure 2 provides an affidavit with the basis for this request. Enclosure 3 provides a redacted public version of the report that contains non-proprietary content.

This letter contains no commitments. If you have any questions or require additional information, please contact Wesley Steh at wsteh@x-energy.com or Ingrid Nordby at inordby@x-energy.com.

Sincerely,

DocuSigned by:
F053E736949E4C3...

Travis A. Chapman
Director, U.S. Licensing, Xe-100 Program
X Energy, LLC

cc:
X-energy, LLC
George Vanderheyden
Steve Miller
Martin van Staden

Nuclear Regulatory Commission
William Jessup
Stephanie Devlin-Gill
Michael Orenak

U.S. Department of Energy
Jeff Ciocco
Carl Friesen

ENCLOSURES:

1) Xe-100 White Paper, "Xe-100 Plant Control and Data Acquisition System, Revision 2" (Proprietary)

2) Affidavit Supporting Request for Withholding from Public Disclosure (10 CFR 2.390)

3) Xe-100 White Paper, "Xe-100 Plant Control and Data Acquisition System, Revision 2" (Non-Proprietary)

X Energy, LLC
801 Thompson Avenue
Rockville, MD 20852
+1 301.358.5600

Enclosure 1

X Energy, LLC
Xe-100 Plant Control and Data Acquisition System
White Paper, Revision 2
(Proprietary)

X Energy, LLC
801 Thompson Avenue
Rockville, MD 20852
+1 301.358.5600

Enclosure 2

Affidavit Supporting Request for Withholding from Public Disclosure

(10 CFR 2.390)

X Energy, LLC
801 Thompson Avenue
Rockville, MD 20852
+1 301.358.5600

Affidavit Supporting Request for Withholding from Public Disclosure (10 CFR 2.390)

I, Travis A. Chapman, Director, U.S. Licensing, Xe-100 Program, of X Energy, LLC (X-energy) do hereby affirm and state:

1. I am authorized to execute this affidavit on behalf of X-energy. I am further authorized to review information submitted to or discussed with the Nuclear Regulatory Commission (NRC) and apply for the withholding of information from disclosure. The purpose of this affidavit is to provide the information required by 10 CFR 2.390(b) in support of X-energy's request for proprietary treatment of certain commercial information submitted in Enclosure 1 to X-energy's letter XE-NRC-2023-004 from myself to the NRC which provides the X-energy white paper, "Xe-100 Plant Control and Data Acquisition System."

2. I have knowledge of the criteria used by X-energy in designating information as sensitive, proprietary, confidential, and export-controlled.

3. Pursuant to the provision of paragraph (b)(4) of 10 CFR 2.390, the following is furnished for consideration by the NRC in determining whether the information sought to be withheld from public disclosure should be withheld.

> a. The information sought to be withheld from public disclosure in Enclosure 1 is owned by X-energy. This information was prepared with the explicit understanding that the information itself would be treated as proprietary and confidential and has been held in confidence by X-energy.
>
> b. The information sought to be protected in Enclosure 1 is not available to the public.
>
> c. The information contained in Enclosure 1 is of the type that is customarily held in confidence by X-energy, and there is a rational basis for doing so. The information X-energy is requesting to be withheld from public disclosure includes technical information related to the design, analysis and operations associated with our Xe-100 high-temperature, gas-cooled, pebble bed advanced reactor design that directly impact our business development and commercialization efforts. X-energy limits access to this proprietary and confidential information in order to maintain confidentiality.
>
> d. Enclosure 1 contains information about the planned activities of X-energy related to the development of the Xe-100 design bases, TRISO-X fuel design bases, forecast design development timeframes, and relate to the commercialization strategy for our Xe-100 advanced reactor. Public disclosure of the information contained in Enclosure 1 would create substantial harm to X-energy because it would reveal valuable technical information regarding X-energy's design development, competitive expectations, assumptions, current position and strategy. Its use by a competitor could substantially improve the competitor's position in the design, manufacture, licensing, construction and operation of a similar competing product.

e. Additionally, Enclosure 1 was assessed for considered Export Controlled Information (ECI) under the provisions of 10 CFR 810 and was found to not contain ECI.

f. The Proprietary Information contained in Enclosure 1 is transmitted to the NRC in confidence and under the provisions of 10 CFR 2.390; it is to be received in confidence by the NRC. The information is properly marked.

I declare under the penalty of perjury that the foregoing is true and correct. Executed on February 3, 2023.

Sincerely,

DocuSigned by:
F053E736949E4C3...

Travis Chapman
Director, U.S. Licensing, Xe-100 Program
X Energy, LLC

X Energy, LLC
801 Thompson Avenue
Rockville, MD 20852
+1 301.358.5600

Enclosure 3

X Energy, LLC
Xe-100 Plant Control and Data Acquisition System
White Paper, Revision 2
(Non-Proprietary)

Xe-100
Plant Control and Data Acquisition System White Paper

Document ID Number	:	**006036**
Configuration Classification	:	**XE00-P-PCDA-GL-GL-GL-P**
Revision	:	**2**
Security Classification	:	**~~Proprietary~~**
Status	:	**Approved**
Date Created	:	31-Jan-2023
Project	:	**XE-100**

Preparer:
Electronically signed by Wesley Steh
01-Feb-2023 13:01

E-SIGNATURES

Reviewer:
Electronically signed by Matt Hertel
02-Feb-2023 15:56

Reviewer:
Electronically signed by Gregg Crannick
02-Feb-2023 15:56

Reviewer:
Electronically signed by Chris Crefeld
02-Feb-2023 15:56

Approver:
Electronically signed by Jon Facemire
03-Feb-2023 05:21

Document Approval Signees

Action	Designation	Name	Signature	Date
Preparer	Licensing Engineer	W. Steh		
Reviewer	I&C Deputy Eng. Manager	M. Hertel		
Reviewer	Plant Operations Manager	G. Crannick		
Reviewer	I&C Eng. Manager	C. Crefeld		
Approver	Licensing Manager	J. Facemire		

Copyright Notice

10 CFR 810 Export-Controlled Information Disclaimer

This document was reviewed by X-energy and determined not to contain information designated as export-controlled per Title 10 of the Code of Federal Regulations (CFR) Part 810 or 10 CFR 110.

Department of Energy Acknowledgement and Disclaimer

This material is based upon work supported by the Department of Energy under Award Number DE-NE0009040. This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

SYNOPSIS

X Energy, LLC (X-energy) is developing a Generation IV Advanced Reactor based on the High Temperature Gas-Cooled Reactor (HTGR) technology utilizing U.S.-developed uranium oxy-carbide (UCO) tri-structural isotropic (TRISO) coated-particle fuel embedded in spherical fuel elements, referred to as fuel pebbles. The reactor generates 200 MWt and produces high-quality, super-heated steam at 565°C and 16.5 MPa and is suitable for many different energy applications, including electricity, industrial process heat, district heating, desalination, wind/solar power augmentation, or a combination of these.

The Xe-100 plant is modular, with each unit containing a nuclear reactor and steam generator, or Nuclear Island (NI), coupled to a Conventional Island (CI). The NI remains consistent irrespective of the application and contains the safety related Structures, Systems, and Components (SSCs). The CI systems and components are commercially available and can be procured from multiple U.S. and Global vendors and optimally configured to suit the end user's requirements. A single reactor generates 200 MWt energy. A single reactor unit configured for electricity generation produces 80 MWe net power. The Xe-100 is designed to produce electrical power and/or process energy depending on the specific deployment application and the development of instrumentation and controls for the plant reflects this objective.

The Xe-100 Plant Control and Data Acquisition System (PCDAS), which is an integrated set of instrumentation and control (I&C) systems, is described herein. The purpose of this white paper is to provide to the NRC the following information: 1) the regulatory framework to which the PCDAS will align, 2) the regulatory guidance documents to be considered in the PCDAS design process, 3) the overall PCDAS architecture and overall PCDAS functional design, 4) the selected principal design criteria (PDC) to which the PCDAS will be designed to conform, and 5) the preliminary classification of PCDAS subsystems. This information is provided to augment descriptions of the Xe-100 I&C systems design provided in other white papers, technical and licensing topical reports (LTRs), and pre-application engagements with the NRC.

X-energy requests NRC feedback on the Xe-100 PCDAS architecture and system functional design, and NRC review of and comment on the following: 1) whether the I&C architecture is acceptable for further review and conforms to fundamental industry design principles and best practices, 2) whether functional design criteria have been established that will allow future review of the I&C systems for both safety-significant and non-safety-significant functions, 3) whether the I&C system classifications align with the philosophy of NRC Regulatory Guide (RG) 1.233 [5] and NEI 18-04 [7], 4) whether alignment of the I&C systems design to the regulatory framework of the NRC Design Review Guide (DRG): Instrumentation & Controls (I&C) for Non-Light Water Reactor (Non-LWR) Reviews [6] is acceptable, and 5) whether the regulatory guidance documents specified for consideration in the I&C design process are appropriate.

Note that the enclosed information is preliminary, pre-decisional, and is subject to change as the design progresses. It is provided for planning and familiarization purposes in support of pre-application discussions with and to request feedback from the NRC staff.

CONFIGURATION CONTROL/DOCUMENT CHANGE HISTORY

Document Change History

Rev.	Date	Preparer	Page/Section Revised	Description
A	21-Oct-2021	W. Catullo	Entirety	Initial Draft for Review
1	18-Nov-2022	M. Hertel	Entirety	Approval Release
2	31-Jan-2023	W. Steh	Entirety	Approval Release

Table of Contents

List of Tables

List of Figures

Abbreviations/Acronyms

Abbreviations/Acronyms

Short Form	Phrase
ANS	American Nuclear Society
ANS	Announcement and Notification System
ANSI	American National Standards Institute
AOO	Anticipated Operational Occurrence
APL	Application and Priority Logic
ASB	Access and Security Building
ASME	American Society of Mechanical Engineers
BDBE	Beyond Design Basis Event
BTP	Branch Technical Position
CACS	Central Analysis and Controls System
CAM	Continuous Air Monitor
CCDS	CI Condensate System
CCF	Common Cause Failure
CDA	Critical Digital Asset
CDCW	CI Condenser Cooling Water System
CDC	Complementary Design Criteria
CDS	Condenser System
CEB	Controls and Electrical Building

CFR	Code of Federal Regulations (USA)
CI	Conventional Island
CIE	CI Electrical System
CIFP	CI Fire Protection System
CIIA	CI Compressed & Instrument Air System
CILD	CI Liquid Drainage System
CIPW	CI Process Water System
CISS	Conventional Island Steam System
COMS	Plant Communications System
CPCW	CI Component Cooling Water System
CR	Control Rod
CRDC	Control Rod Drive Controller
CRDM	Control Rod Drive Mechanism
CS	Critical System
DACS	Data Acquisition and Control System
DBA	Design Basis Accident (an NEI 18-04-specific definition)
DBE	Design Basis Event (equivalent to Design Basis Accident (DBA) in Canadian terminology)
DCS	Distributed Control System
DDS	Digital Data System
DID	Defense-in-Depth
DIM	Display Interface Module

DMZ	Demilitarized Zone (Networking)
DRG	Design Review Guide
EIM	Equipment Interface Module
EP	Emergency Preparedness
ERDS	Emergency Response Data System
ESD	Event Sequence Diagram
FDAS	First-of-a-Kind Data Acquisition System
FHS	Fuel Handling System
FPGA	Field Programmable Gate Array
FW	Feedwater
GPS	Global Positioning System
HBCM	Hub Communications Module
HCS	Helium Circulator System
HFE	Human Factors Engineering
HIPS	Highly Integrated Protection System (i.e., self-testing)
HMI	Human-Machine Interface
HP	High Pressure
HPB	Helium Pressure Boundary
HSI	Human-System Interface
HSS	Helium Service System
HTGR	High Temperature Gas-Cooled Reactor

HV	Plant HVAC System
HVAC	Heating, Ventilation, and Air Conditioning
HW	Hardware
I&C	Instrumentation and Control
IAC	Intelligent Automatic Control
ICA	IPS Corrective Action
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IM	Interface Module
IO	Input/Output
IPA	IPS Protective Action
IPS	Investment Protection System
ISG	Interim Staff Guidance
LANS	Local Area Network System
LBE	Licensing Basis Event
LMP	Licensing Modernization Project
LOSP	Loss of Offsite Power
LTR	Licensing Topical Report
LVDT	Linear Variable Differential Transducer
MCLK	Master Clock System
MCR	Main Control Room

MDMS	Maintenance and Diagnostic Monitoring System
MHTGR-DC	Modular High Temperature Gas-Cooled Reactor Design Criteria
MICM	Monitoring and Indication Communication Module
MRS	Mobile Radio System
MS	Main Steam
MTVS	Multi-Media TV System
ND	Neutron Detector
NEI	Nuclear Energy Institute
NI	Nuclear Island
NIAB	Nuclear Island Auxiliary Building
NICW	Nuclear Island Cooling Water System
NIE	NI Electrical System
NIFP	NI Fire Protection System
NIFW	NI Feedwater System
NIHV	NI HVAC System
NIIA	NI Compressed & Instrument Air System
NILD	NI Liquid Drainage System
NILR	NI Liquid Radwaste System
NIPW	NI Process Water System
NIS	Nuclear Instrumentation System
NISS	Nuclear Island Steam System

Non-LWR	Non-Light Water Reactor
NRC	U.S. Nuclear Regulatory Commission
NSRST	Non-Safety-Related with Special Treatment
NST	Non-Safety-Related with No Special Treatment
NTP	Network Time Protocol
NUREG	Nuclear Regulatory Guide
OBE	Operating Basis Earthquake
OIS	Operator Interface System
OPC UA	Open Platform Communication Unified Architecture
PANS	Plant Area Network System
PCDAS	Plant Control and Data Acquisition System
PDC	Principal Design Criteria
PDCS	Plant-Wide Distributed Control System
PEMS	Post-Event Monitoring System
PFP	Plant Fire Protection System
PI	Plant Data Historian
PLC	Programmable Logic Controller
PLPRS	Primary Loop Pressure Relief System
POT	Potable Water System
PRA	Probabilistic Risk Assessment (same as Probabilistic Safety Assessment in Canadian terminology)

PSAR	Preliminary Safety Analysis Report
PSC	Plant Support Center
PSF	PRA Safety Function
PTT	Push-To-Talk
QA	Quality Assurance
RAM	Radiation Area Monitor
RAMTE	Rotary Absolute Multi-Turn Encoder
RB	Reactor Building
RCCS	Reactor Cavity Cooling System
RCS	Reactivity Control System
RCSS	Reactivity Control & Shutdown System
RFDC	Required Functional Design Criteria
RG	Regulatory Guide
RMS	Radiation Monitoring System
RPS	Reactor Protection System
RPI	Rod Position Indication
RSF	Required Safety Function
RSR	Reserve Shutdown Room
RSS	Reserve Shutdown System
RX	Reactor System
SCRAM	Safety Control Rod Axe Man (Reactor Shutdown)

SCS	Satellite Communications System
SEM	Seismic Event Monitor
SEW	Sewer System
SFISF	Spent Fuel Intermediate Storage Facility
SFSS	Spent Fuel Storage System
SG	Steam Generator System
SGDS	Steam Generator Dump System
SGPV	Steam Generator Pressure Vessel
SMS	Seismic Monitoring System
SR	Safety Related
SRM	Staff Requirements Memorandum
SSC	Structures, Systems, and Components
SSE	Safe Shutdown Earthquake
SSM	Solid State Storage Module
SSS	Start-Up and Shutdown System
STW	Storm Water System
SUR	Start-Up Rate (rate of change of power)
TBC	To be Confirmed
TELS	Telecommunications Systems
TG	Turbine Generator System
TI-RIPB	Technology-Inclusive, Risk-Informed, Performance-Based

TRISO	Tri-Structural Isotropic Coated-Particle Fuel
TTL	Transistor-Transistor Logic
UCO	Uranium Oxy-Carbide
WR	Wide Range
WTS	Water Treatment System
X-energy	X Energy, LLC

1. Introduction

1.1 Purpose

This document describes the overall approach to the design of the Xe-100 Plant Control and Data Acquisition System (PCDAS) supporting the Xe-100 technology-inclusive, risk-informed, performance-based (TI-RIPB) licensing basis. The PCDAS is comprised of multiple subsystems including the Distributed Control System (DCS), the Investment Protection System (IPS), the Reactor Protection System (RPS), the Post-Event Monitoring System (PEMS), the Radiation Monitoring System (RMS), and the Seismic Monitoring System (SMS). Additionally, this document describes the Reactivity Control and Shutdown System (RCSS), and other systems relevant to the I&C design to be developed as the Xe-100 design progresses. The enclosed information is preliminary, pre-decisional, and is subject to change as the design progresses from the Preliminary Design through Final Design phases.

1.2 Scope

The scope of this document includes the control, protection, and monitoring systems, their high-level functional designs and licensing basis development, the safety classifications of the included I&C systems, and the important interfaces between the various systems.

1.3 Document Layout

Section 2 provides definitions specific to the Xe-100 design. Section 3 discusses relevant regulatory requirements and guidance pertaining to I&C design both generically and for specific applications. Section 4 describes the systems engineering approach to control, protection, and monitoring system design, to include functional design, interactions between control and protection, human machine interface, and cyber security. Section 5 describes the architecture of each system (DCS, IPS, RPS, RCSS, PEMS, RMS, and SMS). Section 6 provides example of an anticipated operational occurrence (AOO) and design basis accident (DBA) to demonstrate how the I&C scheme functions. Section 7 describes the conclusions of this white paper and presents NRC review objectives requested by X-energy. Section 8 identifies references cited within this white paper.

2. Definitions

Definitions

Phrase	Definition
Plant	The Xe-100 plant is modular and consists of one or more units, with each unit containing a nuclear reactor and steam generator, or Nuclear Island (NI), coupled to a Conventional Island (CI).
Unit	The Xe-100 plant is modular and consists of one or more units, with each unit containing a nuclear reactor and steam generator, or Nuclear Island (NI), coupled to a Conventional Island (CI).
Plant Parameter	In the Xe-100 plant, a plant parameter can be any parameter within individual units, or a global parameter for all units.

3. Regulatory Analysis

3.1 Background

In the 2008 NRC Policy Statement on the Regulation of Advanced Reactors, (73 FR 60612; ADAMS Accession No. ML082750370), NRC set expectations for advanced reactors: "… the Commission expects that advanced reactors will provide enhanced margins of safety and/or use simplified, inherent, passive, or other innovative means to accomplish their safety and security functions."

NEI 18-04 [7], endorsed by the NRC in RG 1.233 [5], proposes a TI-RIPB approach with risk metrics more suitable for advanced non-LWRs. NEI 18-04 [7] provides a methodology for Licensing Basis Event (LBE) selection, SSC classification, and establishing adequacy of defense-in-depth (DID). In addition, NEI 18-04 [7] is focused on establishing guidance for advanced designs so license applicants can develop inputs that can be used to demonstrate compliance with applicable regulatory requirements, including the following:

- 10 CFR 50.34(a) [1]
- 10 CFR 50.55a [2]
- 10 CFR 52.47(a) [3]

Specifically, NEI 18-04 [7] establishes a risk informed methodology supporting compliance with:

- 10 CFR 50.34(a)(3) – Facility Design
- 10 CFR 50.34(a)(4) – Analysis and Evaluation of SSCs
- 10 CFR 50.34(a)(7) – Quality Assurance Program

NEI 21-07 [8] provides more clarity and establishes expected content of applications for an applicant following the NEI 18-04 [7] approach. Importantly, this document provides more clarity on how PDC should be defined for non-LWRs that follow the methodology of NEI 18-04 [7] and RG 1.233. X-energy expects to implement guidance from a future regulatory guide or interim staff guidance (ISG) that endorses NEI 21-07 [8], which is currently under development. The approach to instrumentation and controls design described herein will be revised as appropriate pending issuance of future regulatory guidance.

To modernize the NRC regulations, the Commission has provided direction to the NRC staff to promote, among other approaches, the use of Probabilistic Risk Assessment (PRA) technology in a manner that complements the NRC's deterministic approach and supports the NRC's traditional DID philosophy. In response to the Commission's direction, the NRC I&C staff developed a new I&C chapter of the NRC Design Review Guide (DRG) [6] that provides guidance for the NRC staff to use in reviewing the I&C portions of applications for advanced non-LWRs within the bounds of existing regulations: Instrumentation and Controls (I&C) for Non-LWR Reviews. This DRG chapter factors in the principles of RG 1.233 [5], which endorses the methodology in NEI 18-04 [7] with clarifications and points of emphasis. X-energy submitted a topical report [15] describing its commitments to the RG 1.233 [5] clarifications that received a positive safety evaluation in 2022 [14]; an accepted version has been processed affirming those commitments. Thus, the guidance presented in the NRC DRG is a proactive way to modernize the I&C safety review of advanced non-LWR applications by providing guidance for technology-inclusive, risk-informed, and performance-based reviews.

3.2 Applicable Code of Federal Regulations Requirements

X-energy identified the following requirements that govern the design of instrumentation and control systems to support the Xe-100 licensing basis.

3.2.1 10 CFR 50.34(a) – Contents of Applications; Technical Information

X-energy will develop portions of the Xe-100 licensing basis using the approach described in "Xe-100 Licensing Topical Report Risk-Informed Performance-Based Licensing Basis Development" [15]. This report describes how the risk-informed performance-based methodology developed in the Licensing Modernization Project (LMP) is being implemented by X-energy for design, analysis, and licensing of the Xe-100 reactor. As part of its first project, X-energy is developing application content based on a planned submittal under Title 10 of the CFR, Part 50. For a Construction Permit application, a Preliminary Safety Analysis Report (PSAR) presents the safety case for the plant. The approach X-energy is taking facilitates compliance with 10 CFR 50.34(a)(1), which states:

> *(a) Preliminary safety analysis report. Each application for a construction permit shall include a preliminary safety analysis report. The minimum information to be included shall consist of the following:*
>
> *(1) Stationary power reactor applicants for a construction permit who apply on or after January 10, 1997, shall comply with paragraph (a)(1)(ii) of this section. All other applicants for a construction permit shall comply with paragraph (a)(1)(i) of this section.*
>
> …
>
> *(ii) A description and safety assessment of the site and a safety assessment of the facility. It is expected that reactors will reflect through their design, construction and operation an extremely low probability for accidents that could result in the release of significant quantities of radioactive fission products. The following power reactor design characteristics and proposed operation will be taken into consideration by the Commission:*
>
> *(A) Intended use of the reactor including the proposed maximum power level and the nature and inventory of contained radioactive materials;*
>
> *(B) The extent to which generally accepted engineering standards are applied to the design of the reactor;*
>
> *(C) The extent to which the reactor incorporates unique, unusual or enhanced safety features having a significant bearing on the probability or consequences of accidental release of radioactive materials;*
>
> *(D) The safety features that are to be engineered into the facility and those barriers that must be breached as a result of an accident before a release of radioactive material to the environment can occur. Special attention must be directed to plant design features intended to mitigate the radiological consequences of accidents. In performing this assessment, an applicant shall assume a fission product release from the core into the containment assuming that the facility is operated at the ultimate power level contemplated. The applicant shall perform an evaluation and analysis of the postulated fission product release, using the expected demonstrable containment leak rate and any fission product cleanup systems intended to mitigate the consequences of the accidents, together with applicable site characteristics, including site meteorology, to evaluate the offsite*

> *radiological consequences. Site characteristics must comply with part 100 of this chapter. The evaluation must determine that:*
>
> *(1) An individual located at any point on the boundary of the exclusion area for any 2-hour period following the onset of the postulated fission product release, would not receive a radiation dose in excess of 25 rem total effective dose equivalent (TEDE).*
>
> *(2) An individual located at any point on the outer boundary of the low population zone, who is exposed to the radioactive cloud resulting from the postulated fission product release (during the entire period of its passage) would not receive a radiation dose in excess of 25 rem total effective dose equivalent (TEDE).*

By implementing the NEI 18-04 [7] approach as described in the "Xe-100 Licensing Topical Report Risk-Informed Performance-Based Licensing Basis Development" [15], X-energy will meet these regulations for the Xe-100. NEI 18-04 [7] offers "guidance for advanced designs so license applicants can develop inputs that can be used to demonstrate compliance with applicable regulatory requirements, including … 10 CFR 50.34(a), [which] describes the content required in the Preliminary Safety Analysis Report for a Construction Permit application." Specifically, the NEI 18-04 [7] approach will allow for identification and selection of LBEs, safety classification of SSCs and associated special treatments, and evaluation of DID adequacy.

3.2.2 10 CFR 50.55a – Codes and Standards

X-energy will develop the Xe-100 licensing basis using the approach described in the "Xe-100 Licensing Topical Report Risk-Informed Performance-Based Licensing Basis Development" [15]. This report describes how the risk-informed performance-based methodology developed in the LMP is being implemented for design, analysis, and licensing of the Xe-100 reactor. The approach facilitates compliance with 10 CFR 50.55a, which states:

> *(a) Documents approved for incorporation by reference. The standards listed in this paragraph (a) have been approved for incorporation by reference by the Director of the Federal Register pursuant to 5 U.S.C. 552(a) and 1 CFR part 51.*
>
> *…*
>
> *(2) Institute of Electrical and Electronics Engineers (IEEE)*
>
> *…*
>
> *(iii) IEEE standard 603–1991. (IEEE Std 603–1991), "Standard Criteria for Safety Systems for Nuclear Power Generating Stations (Approval Date: June 27, 1991), referenced in paragraphs (h)(2) and (h)(3) of this section. All other standards that are referenced in IEEE Std 603–1991 are not approved for incorporation by reference.*
>
> *(iv) IEEE standard 603–1991, correction sheet. (IEEE Std 603–1991 correction sheet), "Standard Criteria for Safety Systems for Nuclear Power Generating Stations, Correction Sheet, Issued January 30, 1995," referenced in paragraphs (h)(2) and (h)(3) of this section.*
>
> *…*

> *(h) Protection and safety systems. Protection systems of nuclear power reactors of all types must meet the requirements specified in this paragraph. Each combined license for a utilization facility is subject to the following conditions.*
>
> *…*
>
> *(3) Safety systems. Applications filed on or after May 13, 1999, for construction permits and operating licenses under this part, and for design approvals, design certifications, and combined licenses under part 52 of this chapter, must meet the requirements for safety systems in IEEE Std. 603–1991 and the correction sheet dated January 30, 1995.*
>
> *(i)–(y) [Reserved]*
>
> *(z) Alternatives to codes and standards requirements. Alternatives to the requirements of paragraphs (b) through (h) of this section or portions thereof may be used when authorized by the Director, Office of Nuclear Reactor Regulation. A proposed alternative must be submitted and authorized prior to implementation. The applicant or licensee must demonstrate that:*
>
> *(1) Acceptable level of quality and safety. The proposed alternative would provide an acceptable level of quality and safety; or*
>
> *(2) Hardship without a compensating increase in quality and safety. Compliance with the specified requirements of this section would result in hardship or unusual difficulty without a compensating increase in the level of quality and safety.*

By implementing the NEI 18-04 [7] approach as described in the “Xe-100 Licensing Topical Report Risk-Informed Performance-Based Licensing Basis Development” [15], X-energy will meet the intent of these regulations for the Xe-100 as applicable to the TI-RIPB process. NEI 18-04 [7] offers “guidance for advanced designs so license applicants can develop inputs that can be used to demonstrate compliance with applicable regulatory requirements, including … 10 Code of Federal Regulations (CFR) 50.55a, [which] describes the codes and standards approved for incorporation by reference.” Specifically, the NEI 18-04 [7] approach will allow for identification and selection of LBEs, safety classification of SSCs and associated special treatments, and evaluation of DID adequacy. Codes and Standards selected for I&C SSCs would be among the special treatments chosen under an NEI 18-04 [7] approach.

3.2.3 10 CFR 52.47(a) – Contents of Applications; Technical Information

X-energy will develop portions of the Xe-100 licensing basis using the approach described in the “Xe-100 Licensing Topical Report Risk-Informed Performance-Based Licensing Basis Development” [15]. This report describes how the risk-informed performance-based methodology developed in the LMP is being implemented for design, analysis, and licensing of the Xe-100 reactor. The approach facilitates compliance with 10 CFR 52.47(a) for future Part 52 applications (e.g., Design Approvals, Design Certifications, Combined Licenses), which states:

> *The application must contain a level of design information sufficient to enable the Commission to judge the applicant's proposed means of assuring that construction conforms to the design and to reach a final conclusion on all safety questions associated with the design before the certification is granted. The information submitted for a design certification must include performance requirements and design information sufficiently detailed to permit the preparation of acceptance*

and inspection requirements by the NRC, and procurement specifications and construction and installation specifications by an applicant. The Commission will require, before design certification, that information normally contained in certain procurement specifications and construction and installation specifications be completed and available for audit if the information is necessary for the Commission to make its safety determination.

(a) The application must contain a final safety analysis report (FSAR) that describes the facility, presents the design bases and the limits on its operation, and presents a safety analysis of the structures, systems, and components and of the facility as a whole, and must include the following information:

(1) The site parameters postulated for the design, and an analysis and evaluation of the design in terms of those site parameters;

(2) A description and analysis of the structures, systems, and components (SSCs) of the facility, with emphasis upon performance requirements, the bases, with technical justification therefor, upon which these requirements have been established, and the evaluations required to show that safety functions will be accomplished. It is expected that the standard plant will reflect through its design, construction, and operation an extremely low probability for accidents that could result in the release of significant quantities of radioactive fission products. The description shall be sufficient to permit understanding of the system designs and their relationship to the safety evaluations. Such items as the reactor core, reactor coolant system, instrumentation and control systems, electrical systems, containment system, other engineered safety features, auxiliary and emergency systems, power conversion systems, radioactive waste handling systems, and fuel handling systems shall be discussed insofar as they are pertinent. The following power reactor design characteristics will be taken into consideration by the Commission:

(i) Intended use of the reactor including the proposed maximum power level and the nature and inventory of contained radioactive materials;

(ii) The extent to which generally accepted engineering standards are applied to the design of the reactor;

(iii) The extent to which the reactor incorporates unique, unusual or enhanced safety features having a significant bearing on the probability or consequences of accidental release of radioactive materials; and

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

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

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

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

(3) The design of the facility including:

(i) The principal design criteria for the facility. Appendix A to 10 CFR part 50, general design criteria (GDC), establishes minimum requirements for the principal design criteria for water cooled nuclear power plants similar in design and location to plants for which construction permits have previously been issued by the Commission and provides guidance to applicants in establishing principal design criteria for other types of nuclear power units;

(ii) The design bases and the relation of the design bases to the principal design criteria;

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

(4) An analysis and evaluation of the design and performance of structures, systems, and components with the objective of assessing the risk to public health and safety resulting from operation of the facility and including determination of the margins of safety during normal operations and transient conditions anticipated during the life of the facility, and the adequacy of structures, systems, and components provided for the prevention of accidents and the mitigation of the consequences of accidents.

…

(11) Proposed technical specifications prepared in accordance with the requirements of §§ 50.36 and 50.36a of this chapter;

…

(13) The list of electric equipment important to safety that is required by 10 CFR 50.49(d);

…

(15) Information demonstrating how the applicant will comply with requirements for reduction of risk from anticipated transients without scram events in § 50.62;

…

(18) A description and analysis of the fire protection design features for the standard plant necessary to comply with 10 CFR part 50, appendix A, GDC 3, and § 50.48 of this chapter;

(19) A description of the quality assurance program applied to the design of the structures, systems, and components of the facility. Appendix B to 10 CFR part 50, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," sets forth the requirements for quality assurance programs for nuclear power plants. The description of the quality assurance program for a nuclear power plant shall include a discussion of how the applicable requirements of appendix B to 10 CFR part 50 were satisfied;

(20) The information necessary to demonstrate that the standard plant complies with the earthquake engineering criteria in 10 CFR part 50, appendix S.

By implementing the NEI 18-04 [7] approach as described in the “Xe-100 Licensing Topical Report Risk-Informed Performance-Based Licensing Basis Development” [15], X-energy will meet these regulations for the Xe-100. NEI 18-04 [7] offers “guidance for advanced designs so license applicants can develop inputs that can be used to demonstrate compliance with applicable regulatory requirements, including … 10 CFR 52.47, [which] describes the required information for a FSAR associated with a Standard Design Certification application.” Specifically, the NEI 18-04 [7] approach will allow for identification and selection of LBEs, safety classification of SSCs and associated special treatments, and evaluation of DID adequacy.

Regarding item (3)(i), the Principal Design Criteria for Xe-100 will be defined following the approach described in the Xe-100 Principal Design Criteria Licensing Topical Report [16].

3.3 Applicable Regulatory Guidance

X-energy identified the following regulatory guidance documents to be considered in the I&C design as applicable to the TI-RIPB process (as endorsed by NRC Regulatory Guides (RGs) 1.232 [4] and 1.233 [5]). Industry standards invoked by reference will also be considered in the I&C design as applicable to the TI-RIPB process.

Criteria	Title or Subject
Staff Requirements Memoranda (SRM)	
SRM to SECY 93-087 II.Q	Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems
SRM to SECY 93-087 II.T	Control Room Annunciator (Alarm) Reliability
SECY 22-0076	Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems
Regulatory Guides (RG)	
RG 1.12, Revision 3, 11/2017	Nuclear Power Plant Instrumentation for Earthquakes

Criteria	Title or Subject
RG 1.22, Revision 0, 02/1972 Reviewed 08/2012	Periodic Testing of Protection System Actuation Functions
RG 1.47, Revision 1, 02/2010	Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System
RG 1.53, Revision 2, 11/2003 Reviewed 12/2016	Application of the Single-Failure Criterion to Safety Systems
RG 1.62, Revision 1, 06/2010 Reviewed 10/2017	Manual Initiation of Protection Actions
RG 1.75, Revision 3, 02/2005 Reviewed 01/2016	Independence of Electrical Safety Systems
RG 1.89, Revision, 1 06/1984 Reviewed 12/2018	Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants
RG 1.97, Revision 5, 05/2019	Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants
RG 1.100, Revision 4, 05/2020	Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants
RG 1.105, Revision 4, 02/2021	Setpoints for Safety-Related Instrumentation
RG 1.118, Revision 3, 04/1995 Reviewed 08/2012	Periodic Testing of Electric Power and Protection Systems
RG 1.152, Revision 3, 07/2011 Reviewed 05/2019	Criteria for Use of Computers in Safety Systems of Nuclear Power Plants
RG 1.153, Revision 1, 06/1996 Reviewed 04/2017	Criteria for Safety Systems
RG 1.168, Revision 2, 07/2013	Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

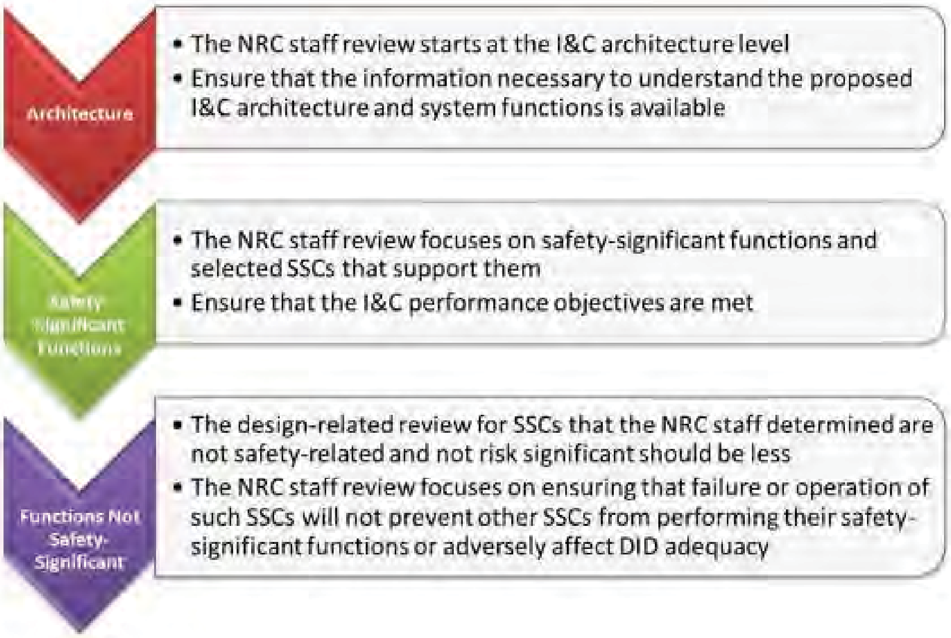
Criteria	Title or Subject
RG 1.169, Revision 1, 07/2013	Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
RG 1.170, Revision 1, 07/2013	Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
RG 1.171, Revision 1, 07/2013	Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
RG 1.172, Revision 1, 07/2013	Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
RG 1.173, Revision 1, 07/2013	Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
RG 1.180, Revision 2, 12/2019	Guidelines for Evaluating Electromagnetic and Radio- Frequency Interference in Safety-Related Instrumentation and Control Systems
RG 1.189, Revision 4, 05/2021	Fire Protection for Operating Nuclear Power Plants
RG 1.196, Revision 1, 01/2007 Reviewed 07/2013	Control Room Habitability at Light-Water Nuclear Power Reactors
RG 1.197, Revision 0, 05/2003 Reviewed 04/2015	Demonstrating Control Room Envelope Integrity at Nuclear Power Reactors
RG 1.209, Revision 0, 03/2007 Reviewed 06/2013	Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants
Branch Technical Positions (BTP)	
BTP 7-8	Guidance on Application of RG 1.22
BTP 7-10	Guidance on Application of RG 1.97

Criteria	Title or Subject
BTP 7-11	Guidance on Application and Qualification of Isolation Devices
BTP 7-12	Guidance on Establishing and Maintaining Instrument Setpoints
BTP 7-14	Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems
BTP 7-17	Guidance on Self-Test and Surveillance Test Provisions
BTP 7-18	Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems
BTP 7-19	Guidance on Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems
BTP 7-21	Guidance on Digital Computer Real-Time Performance

3.4 Regulatory Review Framework

The Xe-100 PCDAS will align to the NRC Design Review Guide (DRG): Instrumentation & Controls (I&C) for Non-Light Water Reactor (Non-LWR) Reviews [6] and NEI 21-07 [8] rather than the Nuclear Regulatory Guide (NUREG)-0800 Standard Review Plan, Chapter 7 [21].

NRC DRG: I&C for Non-LWR Reviews [6], issued in February 2021, outlines a regulatory review framework for I&C designs. Figure X-2 of the NRC DRG depicts the overall review approach, which consists of three tiers.


Architecture
Safety Significant Functions
Functions Not Safety-Significant

- The NRC staff review starts at the I&C architecture level
- Ensure that the information necessary to understand the proposed I&C architecture and system functions is available

- The NRC staff review focuses on safety-significant functions and selected SSCs that support them
- Ensure that the I&C performance objectives are met

- The design-related review for SSCs that the NRC staff determined are not safety-related and not risk significant should be less
- The NRC staff review focuses on ensuring that failure or operation of such SSCs will not prevent other SSCs from performing their safety-significant functions or adversely affect DID adequacy

Figure 1: Figure X-2. Overall I&C Review Approach

Section X.0.2 of the NRC DRG states that the first tier of this review approach should provide the NRC staff with an understanding of the proposed overall I&C architecture and I&C system functions. It is noted that such information could be made available by the applicant during the preapplication phase. The goal of this white paper is to provide to the NRC sufficient information to complete the first tier of the review process. Additional planning will be performed to scope whether a future revision of this paper will be resubmitted as a LTR or incorporated into a licensing application (i.e., Safety Analysis Report chapter content and technical bases).

3.5 Example of Alternative Approach to Regulatory Requirements

Section 50.55a, "Codes and Standards," of 10 CFR Part 50, requires in 10 CFR 50.55a(h) that safety systems for plants with construction permits issued after May 13, 1999, must meet the requirements of IEEE Std. 603-1991. A "safety system" is defined in IEEE Std. 603-1991 as "a system that is relied upon to remain functional during and following design basis events to ensure: (i) the integrity of the reactor coolant pressure boundary, (ii) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (iii) the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the 10 CFR Part 100 guidelines." A "safety function" is defined in IEEE Std. 603-1991 as "one of the processes or conditions (for example, emergency negative reactivity insertion, post-accident heat removal, emergency core cooling, post-accident radioactivity removal, and containment isolation) essential to maintain plant parameters within acceptable limits established for a design basis event."

Section 5.1 of IEEE Std 603-1991 states that the safety system must perform all safety functions required for a design basis event in the presence of (a) any single detectable failure within the safety systems concurrent with all identifiable but nondetectable failures, (b) all failures caused by the single failure, and (c) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. The single failure could occur prior to, or at any time during, the design basis event for which the safety system is required to function.

NRC RG 1.53, Rev. 2 [10] endorses IEEE Std. 379-2000, "Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," as a method acceptable to the NRC staff for satisfying the NRC's regulations with respect to the application of the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power plant safety systems.

However, NRC RG 1.233, Rev. 0 [5] endorses NEI 18-04 [7], which describes how the application of a single-failure criterion is not deemed necessary for reactor designs using the TI-RIPB methodology because advanced non-LWRs will employ a diverse combination of inherent, passive, and active design features to perform the required safety functions across layers of defense and will be subjected to an evaluation of DID adequacy. This endorsed process involves identifying Required Safety Functions and safety-significant PRA Safety Functions, then assigning associated reliability and capability targets, and selecting special treatments to assure that the reliability and capability targets will be met. For I&C systems, those special treatments will include consideration of Codes and Standards and the associated regulatory guidance and select a set of special treatments that align with the reliability and capability targets identified. Therefore, the Xe-100 plant licensing basis will not adopt IEEE Std. 379-2000 as endorsed by RG 1.53, Rev. 2. The design requirements of various I&C SSCs might include the single-failure criterion to support the PRA, however.

4. System Engineering Approach to Control and Protection System Design

4.1 Overall Design Approach

The design of the Xe-100 plant follows a system engineering approach and leverages the risk-informed performance-based methodology from NEI 18-04 [7] in developing the design and licensing bases as laid out in "L-2021-TOP-0019 - X-energy, LLC - Safety Evaluation of Xe-100 Topical Report: Risk-Informed Performance-Based Licensing Basis Development, Revision No. 2" [14]. As such, the Xe-100 plant Probabilistic Risk Assessment (PRA) model is used during each of the design phases; establishes a set of licensing basis events (LBEs) for the safety case; and supports system, structure, or component (SSC) classification, identification and selection of special treatments, and evaluation of defense-in-depth (DID) adequacy. Preliminary classification of SSCs as Safety Related (SR), Non-Safety Related with Special Treatment (NSRST) or Non-Safety Related with No Special Treatment (NST) has been completed in accordance with the NEI 18-04 [7] process at the system level during the conceptual design stage with Quality Assurance (QA) requirements applied in accordance with the guidance of NEI 18-04 [7], Table 4-1. As the design progresses, SSC classification will be refined at the sub-system and component levels with QA requirements applied accordingly. Selection of special treatments is under development in accordance with NRC RG 1.233 [5] and NEI 18-04 [7] and X-energy's internal implementing procedures.

The Xe-100 Principal Design Criteria (PDC) will be defined following the approach described in the Xe-100 Principal Design Criteria Licensing Topical Report [16]. As discussed in that LTR, the MHTGR-DC from RG 1.232 [4] cover PDC that would be considered Required Functional Design Criteria (RFDC), Complementary Design Criteria (CDC) and special treatments under a Licensing Modernization Project (LMP) framework. In alignment with the guidance in RG 1.233 [5], "A designer can use safety-analysis methods appropriate to early stages of design, such as failure modes and effects analyses and process hazard analyses. Designers may likewise use the design criteria from RG 1.232 [4] and confirm or refine them throughout the design process to develop the final PDC provided in an application." The intent of the MHTGR-DC will be met as described in the PDC LTR through identification of RFDC, CDC or special treatments that align with the MHTGR-DC as refined in the PDC LTR. The Xe-100 overall I&C design approach seeks to best utilize the inherent stability and slow transient progression of the HTGR core design by focusing on two areas of innovation: control automation and optimization of instrumentation. Both areas leverage parallel design and analysis workflows to simulate and evaluate I&C design as it affects the operation of the plant, the transient response of the plant, and the safe control of the plant in selected LBEs.

The Xe-100 control system utilizes automation to control plant operation during normal and abnormal events that minimizes human actions to transition between operating modes. This approach reduces the human workload and thus the potential for human error. The Xe-100 is ideally suited for automated control given its inherent safety and other design features that result in stable and predictable operation. Of primary importance is a strong negative temperature coefficient of reactivity over the entire operating range, resulting in the Xe-100 reactor self-moderating its power level whenever there is an imbalance such that less heat is removed from the core than is produced. This characteristic (inherently stable core during increased power or temperature conditions) combined with its low power density and large thermal inertia, ensures that the Xe-100 reactor maintains design parameters within the design basis of the helium pressure boundary (HPB) and the TRISO-X fuel design in the case of I&C system malfunctions. The design philosophy for I&C protection systems, which arises from the inherent stability of the Xe-100 design is that the protection systems generally enable normal operation of the plant with active signals.

If these signals are removed by component failure, protection system trips, or any other means, key components are designed to fail in a safe configuration. This results in a system which requires no human actions to mitigate progression of any design basis accident (DBA).

The Xe-100 instrumentation system is intended to provide the most efficient means of satisfying design requirements related to effective control of the plant, detection of abnormal operating conditions, characterization of performance indicators, and demonstrating regulatory compliance. The high degree of safety achieved by passive mechanisms results in a low number of safety-related instruments. The thermal feedback which self-regulates power transients also serves to greatly simplify the control architecture of the plant, reducing the required number of primary control instruments. These critical instruments are isolated to hardened networks while modern smart instrumentation is utilized for non-safety related applications, such as system diagnostic monitoring for predictive maintenance. This integrated approach results in an I&C architecture with a small number of highly controlled, critical instruments and control loops which are separated from a much larger adaptive network of non-critical instrumentation.

4.2 Functional Design of the Plant Control and Data Acquisition System (PCDAS)

The Plant Control and Data Acquisition System (PCDAS) utilizes an integrated set of instrumentation and control systems, each of which has a defined functional design to either take action to control plant operation during normal operation and transients or monitor key parameters. The Xe-100 instrumentation and control design is comprised of the following related but separately functioning systems, each with their own dedicated equipment (with minor exceptions to be discussed later):

- Distributed Control System (DCS)
- Investment Protection System (IPS)
- Reactor Protection System (RPS)
- Reactivity Control and Shutdown System (RCSS)
- Post-Event Monitoring System (PEMS)
- Radiation Monitoring System (RMS)
- Seismic Monitoring System (SMS)

Figure 2 shows a high-level functional design and interactions between the different Xe-100 I&C systems.

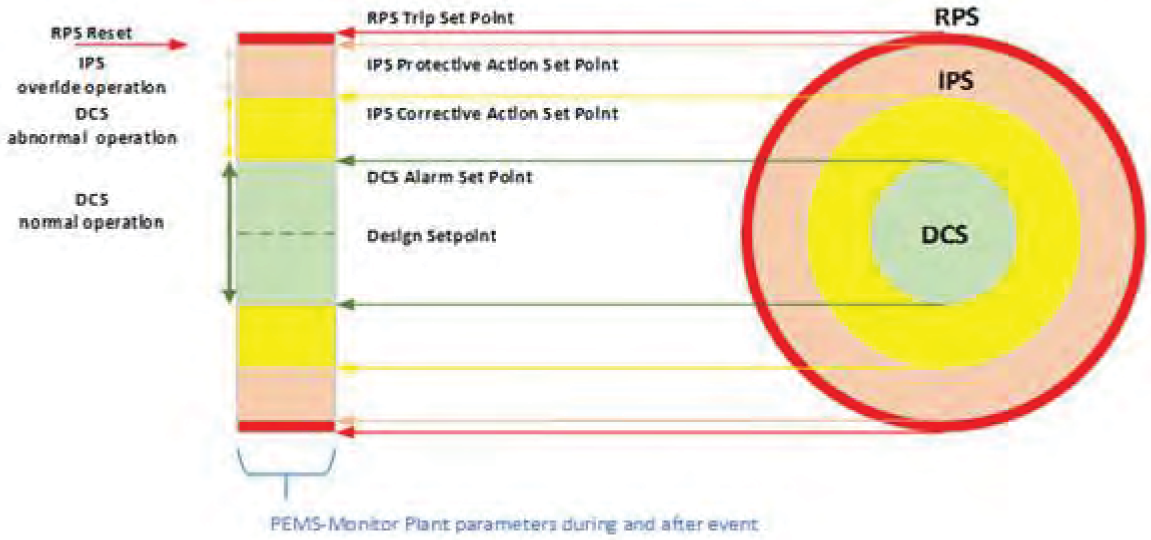


Figure 2: High Level Functional Design and Interactions between the Xe-100 Plant I&C Systems

The Xe-100 plant modes and states ([[ ]]^P) used in the integrated control philosophy, along with the actions taken by IPS and RPS and the status of key components in each state is shown in Figure 3. For the states contained in [[ ]]^P, an RPS Trip or IPS Protective Action results in a transition to the appropriate State in [[ ]]^P. For example, if the unit is in [[ ]]^P and an RPS Trip occurs, the mode will transition to [[ ]]^P. Additionally, there are IPS Corrective Actions that work in conjunction with the DCS to transition the plant as necessary. Examples of these actions include turbine runbacks and circulator runbacks.

[[ ]]^{P}

Figure 3: Normal Operation Modes & States Diagram

4.2.1 Functional Design of the Distributed Control System (DCS)

The Distributed Control System (DCS) refers to multiple levels of control architecture, from basic control loops for simple processes to complex sequence controls which transition the plant between specified operating states. The DCS is composed of several system-level process controllers which are intended to be modular in hardware (HW) design and operation. Control functions are typically contained in a single DCS process controller but may require input from other modules for more complex control actions or satisfaction of control system interlocks. Generally, the DCS should be capable of running each controller in a variety of defined operational states. This is accomplished by the DCS targeting an allowable range for process parameters. The DCS will provide control input to keep the system operating in the allowed range (assumed in the Chapter 3 accident analysis prior to the onset of an LBE), with specific setpoints assigned for alarms, interlocks, and automated transitions as needed to ensure safe and efficient operation of the plant.

As shown in Figure 2, the DCS bandwidth corresponds to the allowable bandwidth in which the DCS will control a given parameter during operation. When plant parameters move into the yellow area within the DCS control range, annunciators will be activated to alert the operators of the specific plant parameter that went into the yellow area. The yellow area is defined as an extended normal operation envelope and parameters in this range will not immediately result in damage to the plant but may have time limits associated with operation in this range. When the plant is operating in this range DCS will perform actions such as sending run-back or adjusted setpoints to attempt to bring the plant parameter back into the inner normal operation band. Procedures will be developed for each parameter that needs to be controlled and what actions should be taken by the operator when parameters remain in the yellow band. The purpose of the extended normal operation band is to limit the number of plant trips while highlighting to the operator that a parameter is not within the optimal operation range.

The DCS primary system-level operational functions include:

- Automatic Plant Startup Control
- Automatic Shutdown Control
- Automatic Load Following
- Automatic Grid-Frequency (Droop) Control
- Automatic Medium (+/-10%) Load Step w/o Turbine Trip
- Automatic Large (+/-20%) Load Step w/o Turbine Trip
- Load Rejection w/o Reactor or Turbine Trip
- Recovery from a Turbine Trip w/o Reactor Trip

Table 1 illustrates a high-level control approach for the Xe-100 plant involving a critical plant-controlled variable/parameter and the associated control system process (manipulated) variable for desired plant operating conditions. The primary energy conversion functional design consists of these four control loops that simplify the plant response to anticipated transients.

The DCS historian will record plant data, operator actions, alarms, and equipment failures on a data storage device.

Consistent with PDC 13 (“Instrumentation and control”), the DCS monitors variables and systems over their anticipated ranges and maintains these variables and systems within prescribed operating ranges during normal operation. The DCS is also part of the control room and is used to operate the Xe-100 plant safely under normal conditions, consistent with PDC 19 (“Control room”).

The DCS functionality is consistent with the first layer of DID established in NEI 18-04 [7], “Prevent off-normal operation and AOOs”. Per NEI 21-07 [8], design criteria related to this layer of DID should be met via Non-Safety-Related with No Special Treatment (NST) provisions to ensure owner-operator requirements are met. Therefore, DCS is preliminarily classified as NST. The functional, system, and component-level classification will continue to be reevaluated during the final design phase.

Table 1: High-Level Control Approach for the Xe-100 Plant

Controlled Variable	Set Point	Manipulated Variable
Steam Generator Inlet Temp.	750 °C	Control Rod Position
Main Steam Pressure	16.5 MPa	Helium Circulator Speed
Main Steam Temp.	565 °C	HP Feed Pump Speed
Electrical Load	40-100%	Turbine Throttle Valve Position

Note: The Electrical Load Set Point is based on the Turbine configuration currently being evaluated

4.2.2 Functional Design of the Investment Protection System (IPS)

The Investment Protection System (IPS) monitors and provides protective controls for variables essential to supporting response to AOOs and preventing damage to the Xe-100 plant. The IPS accomplishes this by detecting if parameters deviate from the allowed range for normal operation and triggering protective control actions which force a system to isolate or transition to a lower operating mode. The IPS only provides protective control functions if the DCS fails to maintain the selected plant parameters within the required limits.

As shown in Figure 2, the IPS bandwidth (demarcated with the orange band) corresponds to limits for the plant parameters which pose a risk to the plant investment. The IPS has two types of actions, as shown in Figure 2 and Table 2. The first type of IPS action is called an IPS Corrective Action (ICA), a command is sent from the IPS to the DCS to force the plant to a lower operating mode or to pause power ramp-up, these actions occur at the boundary between the orange and yellow regions of Figure 2. The second type of IPS action is called an IPS protective action (IPA), which is initiated by a direct or high priority connection to the relevant actuator or subsystem. These actions will be independent of the DCS function and will override any output from the DCS. These actions include control and shutdown rod insertion, helium circulator rundown (stop), steam generator isolation, steam generator water dump, and others. IPA occurs at the boundary between the orange and red regions of Figure 2.

For example, if a plant parameter enters the orange region of Figure 2, the IPS will initiate a corrective action via the DCS by forcing a change to a lower plant operating mode or reduced power, see Table 2. The IPS would prevent the DCS from returning to full power operation if the adverse parameter remained in the orange region and would permit continued operation at reduced power to allow the plant operators to find and respond to the root cause of the plant condition. If the parameter continues to deviate from the allowed range and crosses the orange/red boundary, the IPS would then initiate a protective action by overriding the DCS control and place the reactor in a shutdown state or any other direct action depending on the plant transient in question. See Table 2 for additional information.

These actions attempt to correct the plant transient via an optimal controlled response versus an RPS trip action, which results in an immediate shutdown/mitigating response. As such, the IPS reduces unnecessary RPS trips (if IPS action can safely control unit response without exceeding an RPS setpoint) and can prevent damage to high investment plant components/structures that could result in unplanned outages and extended down times. IPS does not initiate any of the safety functions associated with the safety-related SSCs.

Transient analysis of potential scenarios has been conducted to identify the optimal IPS control setpoints and required unit response. Criteria were established and used in this analysis. These criteria are primarily associated with preventing damage to critical components during postulated transients. A preliminary set of IPS alarm and trigger parameters, and associated corrective/protective actions is shown in Table 2.

The IPS is designed to support conformance with the following PDC: PDC 1 ("Quality standards and records"), PDC 2 ("Design bases for protection against natural phenomena"), PDC 3 ("Fire protection"), PDC 4 ("Environmental and dynamic effects design bases"), PDC 10 ("Reactor design"), PDC 13 ("Instrumentation and control"), PDC 15 ("Reactor helium pressure boundary design"), PDC 19 ("Control room"), PDC 20 ("Protection system functions"), PDC 26 ("Reactivity control systems"), PDC 28 ("Reactivity limits") and PDC 29 ("Protection against anticipated operational occurrences").

The IPS functionality is consistent with the second layer of DID established in NEI 18-04 [7], “Control abnormal operation, detect failures, and prevent DBEs”. Per NEI 21-07 [8], this layer of DID should function to “Minimize frequency of challenges to SR SSCs”. Since IPS performs this function, it is preliminarily classified as Non-Safety-Related with Special Treatment (NSRST) and is subject to special treatment as determined by the integrated decision-making process for evaluation of DID adequacy and for meeting reliability and capability targets. The functions in Table 2 are preliminarily identified as required and will be reviewed and updated as necessary as the design progresses. The functional, system and component-level classification will continue to be reevaluated during the final design phase.

Table 2: Preliminary IPS Response Matrix

IPS Response Criteria Parameter Name Location Parameter State	**Nominal Setpoint** 100% MCR	**IPS Corrective Action Setpoint**	**IPS Corrective Action**	**IPS Protective Action Setpoint**	**IPS Protective Action**
HPB Pressure Tube Bundle Outlet Plenum High	[[[redacted]]]^{P}	[[[redacted]]]^{P}	Reduce Reactor Power	[[[redacted]]]^{P}	[[[redacted]]]^{P}
HPB Pressure Tube Bundle Outlet Plenum Low	[[[redacted]]]^{P}	[[[redacted]]]^{P}	Reduce Reactor Power	[[[redacted]]]^{P}	[[[redacted]]]^{P}
Neutron Flux Pwr. Range N.D. High	[[[redacted]]]^{P}	[[[redacted]]]^{P}	Reduce Reactor Power	[[[redacted]]]^{P}	[[[redacted]]]^{P}
Pwr. Range SUR All N.D. Ranges High	[[[redacted]]]^{P}	[[[redacted]]]^{P}	Prevent control rod withdrawal	[[[redacted]]]^{P}	[[[redacted]]]^{P}
HPB Humidity SGPV Circ. Bypass High	[[[redacted]]]^{P}	[[[redacted]]]^{P}	Reduce Reactor Power	[[[redacted]]]^{P}	[[[redacted]]]^{P}
Hot Helium Temperature SG Inlet Plenum High	[[[redacted]]]^{P}	[[[redacted]]]^{P}	Reduce Reactor Power	[[[redacted]]]^{P}	[[[redacted]]]^{P}

IPS Response Criteria Parameter Name Location Parameter State	**Nominal Setpoint**	**IPS Corrective Action Setpoint**	**IPS Corrective Action**	**IPS Protective Action Setpoint**	**IPS Protective Action**
	100% MCR				
Main Steam Temperature Turbine Inlet High	[[[redacted]]]P	[[[redacted]]]P	Reduce Reactor Power	[[[redacted]]]P	[[[redacted]]]P
Main Steam Pressure Turbine Inlet High	[[[redacted]]]P	[[[redacted]]]P	Reduce Reactor Power	[[[redacted]]]P	[[[redacted]]]P
Feedwater Temperature FW Pump Outlet High	[[[redacted]]]P	[[[redacted]]]P	Reduce Reactor Power	[[[redacted]]]P	[[[redacted]]]P
Feedwater Temperature FW Pump Outlet Low	[[[redacted]]]P	[[[redacted]]]P	Reduce Reactor Power	[[[redacted]]]P	[[[redacted]]]P
Feedwater Pressure FW Pump Outlet High	[[[redacted]]]P	[[[redacted]]]P	Reduce Reactor Power	[[[redacted]]]P	[[[redacted]]]P

4.2.3 Functional Design of the Reactor Protection System (RPS)

The Reactor Protection System (RPS) is a multichannel, isolated, safety related (SR) I&C system which monitors plant conditions and actuates protection mechanisms to prevent damage to the reactor pressure boundary, the nuclear fuel, or any critical protective component which prevents fission product release. The RPS only has a single operating mode by which it triggers an immediate shutdown of the reactor unit if two-out-of-four channels of the monitored parameter exceed the allowable threshold based on the safety analysis limit (RPS setpoints are conservative with respect to actual safety analysis limits). The shutdown sequence always consists of the insertion of shutdown and control rod banks (via gravity) when an RPS trip is activated. Depending on plant conditions, additional RPS actions include the shutdown of the primary helium circulators (i.e., zero percent flow) and/or isolation of the Steam Generator System (SG). Isolation of the SG is accomplished by removing power to solenoids that allow the Feedwater and Main Steam Isolation Valves to be held open, thereby closing both sets of valves and isolating the SG from the feed and steam systems. These additional actions are triggered if the trip was in response to either an elevated moisture concentration in the primary system or elevated primary system pressure (both indications of a SG tube leak). In the event of High Cold Helium Temperature, depending on the High Mass Flow Ratio or if equivalent full rod insertion is not detected after an RPS trip within the required time limit, the helium circulators will be shut down without automatic isolation of the steam generator. The Main Control Room (MCR) operators have two manual hardwired actuation controls: one that drops the shutdown and control rods and a second one that isolates the SG and reduces helium circulation to 0% flow via the pumps variable speed drives. RPS manual trip/isolation functions are not credited in the DBA analysis and are not expected to be required to mitigate the consequences of DBEs within the F-C target or prevent the frequency of Beyond Design Basis Events (BDBEs) with consequences greater than the 10 CFR 50.34 dose limits from increasing into the DBE region, thus these switches are not currently classified as SR. The RPS monitored parameters, actuation setpoints, and protective actions are described in Table 3.

As shown in Figure 2, the RPS bandwidth (demarcated with the red band) limits the plant parameters that pose a potential risk to public or worker safety. When a plant parameter reaches the outside edge of the red band, the RPS will send trip signals to the main plant actuators per a pre-developed “hard-wired” trip matrix that will ensure the reactor trips (i.e., control and shutdown rod insertion) and isolation functions to ensure barriers to radionuclide release are maintained (primarily the fuel and its layers) by taking other protective actions (e.g., He circulator shutdown, SG isolation).

The RPS is a SR system designed to direct the completion of protective actions in the case of design basis accidents and other LBEs. The RPS will override all other control systems (by removing power to the final actuation device) to place the reactor unit in a shutdown state. The RPS is designed with self-testing that covers each module from sensor input to the automatic actuation output switching logic with the exception of the Application and Priority Logic (APL) circuitry on the Equipment Interface Module (EIM). The APL is constructed of discrete logic components and receives commands from the automatic actuation voting logic and the hardwired signal inputs. The individual self-tests on the different components of the RPS evaluate whether the platform is functioning correctly. For the APL (which contains discrete logic), periodic surveillance testing, as required in technical specifications, will be required to test if the APL is functioning correctly. The RPS modules check if each is functioning correctly, and the error checking on the communication buses verifies that the transfer of data is correct.

The RPS is designed to support conformance with the following PDC: PDC 1 ("Quality standards and records"), PDC 2 ("Design bases for protection against natural phenomena"), PDC 3 ("Fire protection"), PDC 4 ("Environmental and dynamic effects design bases"), PDC 10 ("Reactor design"), PDC 13 ("Instrumentation and control"), PDC 15 ("Reactor helium pressure boundary design"), PDC 19 ("Control room"), PDC 20 ("Protection system functions"), PDC 21 ("Protection system reliability and testability"), PDC 22 ("Protection system independence"), PDC 23 ("Protection system failure modes"), PDC 24 ("Separation of protection and control systems"), PDC 25 ("Protection system requirements for reactivity control malfunctions"), PDC 26 ("Reactivity control systems"), PDC 28 ("Reactivity limits") and PDC 29 ("Protection against anticipated operational occurrences").

The RPS performs Required Safety Functions (RSFs), as defined by NEI 18-04 [7]. Since the RPS performs RSFs, it is classified as SR and is therefore subject to special treatment and has defined required functional design criteria associated with its PDCs. The functions in Table 3 are preliminarily identified as required and will be reviewed and updated as necessary as the design progresses. The system is designed such that no single failure of any component will prevent the RPS from tripping the reactor. Although application of the single-failure criterion is not required per RG 1.233 [5], given the importance of RPS, application of the single-failure criterion is preliminarily considered an appropriate special treatment.

Table 3: Preliminary Xe-100 RPS Response Matrix

Trip Criteria Parameter Name Measurement Location Adverse Parameter State	**Nominal Setpoint** 100% MCR	**RPS Setpoint**	**RPS Immediate Actions**
HPB Pressure SG Tube Outlet High	[[[redacted]]]^{P}	[[[redacted]]]^{P}	[[[redacted]]]^{P}
HPB Pressure SG Tube Outlet Low	[[[redacted]]]^{P}	[[[redacted]]]^{P}	[[[redacted]]]^{P}
Neutron Flux External Wide Range N.D. High	[[[redacted]]]^{P}	[[[redacted]]]^{P}	[[[redacted]]]^{P}
Intermediate Range SUR External Wide Range N.D. High	[[[redacted]]]^{P}	[[[redacted]]]^{P}	[[[redacted]]]^{P}
HPB Humidity SGPV Circ. Inlet/Outlet Bypass High	[[[redacted]]]^{P}	[[[redacted]]]^{P}	[[[redacted]]]^{P}
Hot Helium Temperature Steam Generator Inlet High	[[[redacted]]]^{P}	[[[redacted]]]^{P}	[[[redacted]]]^{P}
Cold Helium Temperature Steam Generator Outlet High	[[[redacted]]]^{P}	[[[redacted]]]^{P}	[[[redacted]]]^{P}
Mass Flow Ratio (He/H_2O) CV and FW Pump Outlet – To be Confirmed (TBC) High	[[[redacted]]]^{P}	[[[redacted]]]^{P}	[[[redacted]]]^{P}
Manual Trip - RCSS MCR and RSR True	[[[redacted]]]^{P}	[[[redacted]]]^{P}	[[[redacted]]]^{P}
Manual Trip - Moisture Ingress MCR and RSR True	[[[redacted]]]^{P}	[[[redacted]]]^{P}	[[[redacted]]]^{P}

4.2.4 Functional Design of the Reactivity Control and Shutdown System (RCSS)

The Reactivity Control and Shutdown System (RCSS) consists of neutron absorber rods that are used as Reactivity Control and Shutdown Rods for the reactor. The RCSS system is comprised of the Reactivity Control System (RCS) and Reserve Shutdown System (RSS). The rods can be moved individually for testing or by bank. There are two rod banks: the RCS bank and the RSS bank.

The RCS is comprised of 9 control rods that control reactor power during normal operating conditions, including start-ups, shutdowns, and transients. The RCS control rods remain partially inserted and can be moved as required to maintain reactor outlet temperature, facilitate load following or to adjust reactivity during xenon transients. The DCS/IPS will provide a demand signal to the RCSS (Corrective Action) to insert, remove or hold each control rod during power operation mode ([[ ]]^{P}), or during Hot Startup mode ([[ ]]^{P}). During these two operating modes, the reactor will remain critical. When required, the DCS/IPS will provide a demand signal to the RCSS to fully insert the control rods and shutdown rods (Protective Action). This action will bring the reactor into a Safe Shutdown mode ([[ ]]^{P}), for which the reactor will become sub-critical.

The RSS is comprised of 9 shutdown rods with the capability to provide excess negative reactivity to keep the reactor subcritical at all temperature ranges with the most reactive rod stuck in the full out position. Under normal operating conditions the RSS rod bank is held in the fully withdrawn position. When required, an RPS trip or manual operator trip will fully insert the control rods and shutdown rods by removing power to the Control Rod Drive Mechanism (CRDM) motors via the CRDM power supplies, which will cause all rods to release into the core under the force of gravity. This action will place the reactor in a safe shutdown mode ([[ ]]^{P}).

The RCSS is designed to support conformance with the following PDC: PDC 1 ("Quality standards and records"), PDC 2 ("Design bases for protection against natural phenomena"), PDC 3 ("Fire protection"), PDC 4 ("Environmental and dynamic effects design bases"), PDC 10 ("Reactor design"), PDC 13 ("Instrumentation and control"), PDC 15 ("Reactor helium pressure boundary design"), PDC 19 ("Control room"), PDC 20 ("Protection system functions"), PDC 26 ("Reactivity control systems"), PDC 28 ("Reactivity limits") and PDC 29 ("Protection against anticipated operational occurrences").

The RCSS is comprised of equipment classified as SR and NSRST. All components that fail in a manner that could prevent a rod from dropping (i.e., Chain, Sprocket, Rod, etc.) are classified as SR. All components that contribute to rod positioning (i.e., Rotational Absolute Multi-Turn Encoder (RAMTE) or Linear Variable Differential Transducer (LVDT) Coils) are preliminarily classified as NSRST. The functional, system, and component-level classification will continue to be reevaluated during the final design phase. The system is designed such that no single failure of any component will prevent the RCSS from tripping the reactor. Although application of the single-failure criterion is not required per Regulatory Guide 1.233 [5], given the importance of RCSS, application of the single-failure criterion is preliminarily considered an appropriate special treatment. In the Xe-100 plant, there are two means of reactivity control. The primary means of reactivity control is the strong negative temperature coefficient of reactivity. The secondary means of reactivity control is the RCSS.

4.2.5 Functional Design of the Post-Event Monitoring System (PEMS)

The Post-Event Monitoring System (PEMS) provides insight into plant status and activity during and after an event (e.g., a seismic event) which may degrade other means of data recording in the DCS. The PEMS monitors key plant parameters and records plant signals passing through the green band, orange band, and red band (Figure 2). The primary function of the PEMS is data collection and storage. Only data related to plant response and event analysis will be stored in the PEMS.

The PEMS has two configuration types, a Unit PEMS and a Common PEMS. Each Unit PEMS is dedicated to monitoring critical parameters and protection system response status for that module. The Common PEMS is dedicated to monitoring information which is not associated with a specific unit. All the PEMS are networked together (Figure 20) and provide monitoring plant status data through the main displays in the MCR and through PEMS displays in the Reserve Shutdown Room (RSR).

Each PEMS is composed of two redundant chassis as shown in Figure 21 and Figure 22. Each chassis is comprised of five (5) types of HIPS module: Interface Modules (IM), Monitoring and Indication Communication Modules (MICM), Hub Communications Modules (HBCM), Display Interface Modules (DIM), and Solid-State Storage Modules (SSM). These modules utilize different Field Programmable Gate Array (FPGA) types between Chassis A and Chassis B, providing functional diversity. The Solid-State Storage Modules (SSM) act as the core of the PEMS, storing data under a wide range of adverse conditions to preserve records for physical recovery and offsite analysis. Each SSM provides for simple recovery by untrained personnel and preserves data integrity as a means of last resort in the case that an event disables the DCS historian.

The Interface Modules receive inputs from dedicated channels via interface with the other I&C systems and then conditions the data stream to meet input requirements to the PEMS components.

The Monitoring & Indication Communication Modules send and receive data to and from other plant PEMS, as well as allow communication to the Emergency Planning Network and to diverse offsite data collection (e.g., the Plant Support Center). The Hub Communications Modules provide data hubs which integrate the other modules together into a functional system.

The Display Interface Modules processor receives data for display locally on the PEMS panel (in the Reserve Shutdown Room (RSR)) as well as remotely in the MCR.

The electrical supply accepts power from two independent sources through the Reactor Building Uninterrupted Power Supply, which can provide battery backup power to its respective Unit PEMS for 72 hours.

Consistent with PDC 13 (“Instrumentation and control”), the PEMS monitors variables and systems over their anticipated ranges during and after licensing basis events. The PEMS is also designed to support conformance with the following PDC: PDC 1 ("Quality standards and records"), PDC 2 ("Design bases for protection against natural phenomena"), PDC 3 ("Fire protection") and PDC 4 ("Environmental and dynamic effects design bases").

The extent of applicability of RG1.97 [12] and any associated special treatments to the PEMS is being determined following the approach defined in RG 1.233 [5] and NEI 18-04 [7]. As there are no operator actions credited for Xe-100 safety functions, there are no Type A variables required for display to the operator to perform manual safety functions.

The PEMS is preliminarily classified as NSRST based on regulatory guidance evaluated during the preliminary design phase and is subject to special treatment as determined by the integrated decision-making process for evaluation of DID adequacy and for meeting reliability and capability targets. PEMS is considered a defense-in-depth system which provides insight into plant status and activity for a period of time surrounding events. The functional, system, and component-level classification will continue to be reevaluated during the final design phase as various analyses inform the licensing basis for the system.

4.2.6 Functional Design of the Radiation Monitoring System (RMS)

The Radiation Monitoring System (RMS) monitors and logs radiological parameters related to the operation of the Xe-100 plant. The RMS provides a stream of measurement data to the PEMS) as well as to the Plant Communications System (COMS). The RMS utilizes a central Data Acquisition and Control System (DACS) adjacent to the MCR which provides a means of actuating RMS control functions such as self-calibration, alarm testing, and detector pump, valve, and solenoid actuations. The RMS DACS is based on two redundant servers that collect data from each monitor and interface with the Common PEMS and COMS.

The RMS detector network is comprised of two primary types of radiation monitors: the Radiation Area Monitor (RAM) and Continuous Air Monitor (CAM). The RAMs measure gross gamma levels and the CAMs measure particulate, noble gas, or tritium concentrations. These monitors are deployed on skid mounted instrument racks and connected to local Human-Machine Interfaces (HMIs) in their respective plant areas. Each RAM and CAM has two RS485 outputs. One of these outputs is connected to a network which delivers monitoring data to the PEMS, and the second output connects it to the RMS DACS. This configuration ensures that data is always provided to the PEMS but allows for centralized display and control for the operators in the Controls and Electrical Building.

Consistent with PDC 13 (“Instrumentation and control”), PDC 63 (“Monitoring fuel and waste storage”) and PDC 64 (“Monitoring radioactivity releases”), the RMS monitors variables and systems over their anticipated ranges during normal operations and licensing basis events. The RMS is also designed to support conformance with the following PDC: PDC 1 ("Quality standards and records"), PDC 2 ("Design bases for protection against natural phenomena"), PDC 3 ("Fire protection") and PDC 4 ("Environmental and dynamic effects design bases").

The RMS is preliminarily classified as NSRST and is subject to special treatment as determined by the integrated decision-making process for evaluation of DID adequacy and for meeting reliability and capability targets. The functional, system, and component-level classification will continue to be reevaluated during the final design phase.

4.2.7 Functional Design of the Seismic Monitoring System (SMS)

The Seismic Monitoring System (SMS) is a data collection and alarming system that provides time history seismic data for structures related to safety functions in the case of a seismic event. Currently, the only Category 1 structures, or structures related to safety functions, are the Reactor Buildings (RBs). The SMS also monitors auxiliary and conventional structures deemed important to the Xe-100 design to comply with US and additional Canadian regulatory guidance. Currently, the selected structures are the Controls and Electrical Building (CEB), the Access and Security Building (ASB), and the first Spent Fuel Intermediate Storage Facility (SFISF), all of which are seismic Category 2 structures. The SMS does not perform any safety indication or control functions.

All Seismic Event Monitors (SEMs) triaxial accelerographs transmit data to the unit SMS Central Analysis and Controls System (CACS) located in the RSR of RB 1 for data storage. Each module SMS CACS transmits time history seismic data to the common DCS cabinet in each CEB to provide data storage redundancy. Additionally, the SMS CACS generates alarms sent to the Common PEMS via dry contacts and to the common DCS via MODBUS TCP. The common DCS and common PEMS subsequently provide alarms in the MCR. These alarms provide audio and visual indication when the operating basis earthquake (OBE) or safe shutdown earthquake (SSE) criteria are exceeded per 10 CFR 50 Appendix S. In the case of a seismic event, exceedance of these criteria would prompt an operator-initiated shutdown of the Xe-100 plant to assess any structural damages. The common DCS data link and common PEMS hardwired connection to the CEB are not seismically rated as the CEB is a Category 2 structure. However, in the case of any observed seismic event, operators will be required to obtain alarm statuses from the RSR where the seismically qualified module CACS will provide seismic alarm. In the case of a major seismic event (above OBE level), operators will shut down the entire plant, evacuate the MCR, and seismic annunciation will not be necessary to reach the MCR via a seismically qualified link. However, a history of seismic alarms and time history data will be stored in the seismically qualified SMS CACS in the RSR of RB 1 for post-accident analysis.

Consistent with PDC 13 (“Instrumentation and control”), the SMS monitors variables and systems over their anticipated ranges during normal operations and licensing basis events. The SMS is also designed to support conformance with the following PDC: PDC 1 ("Quality standards and records"), PDC 2 ("Design bases for protection against natural phenomena"), PDC 3 ("Fire protection") and PDC 4 ("Environmental and dynamic effects design bases").

The SMS is preliminarily classified as NST. The functional, system, and component-level classification will continue to be reevaluated during the final design phase.

4.3 Defense-In-Depth

Defense-in-Depth (DID) is a safety philosophy in which multiple lines of defense, safety margins, and compensatory measures are applied to the design, construction, operation, maintenance, and regulation of nuclear plants to prevent and to mitigate accidents and to assure adequate protection of public health and safety. The philosophy is also intended to deliver a design that is tolerant to uncertainties in the knowledge of plant behavior, component reliability, or human performance that might compromise safety. In the design and analysis process for the Xe-100 plant, the deterministic approach is integrated with a risk-informed evaluation methodology to ensure that selected design features provide the required level of safety and DID.

The three elements of a DID approach include:

- Plant Capability DID
- Programmatic DID
- Risk-Informed and Performance-Based Evaluation of DID

The detailed elements of the Xe-100 plant DID framework are illustrated in Figure 3.

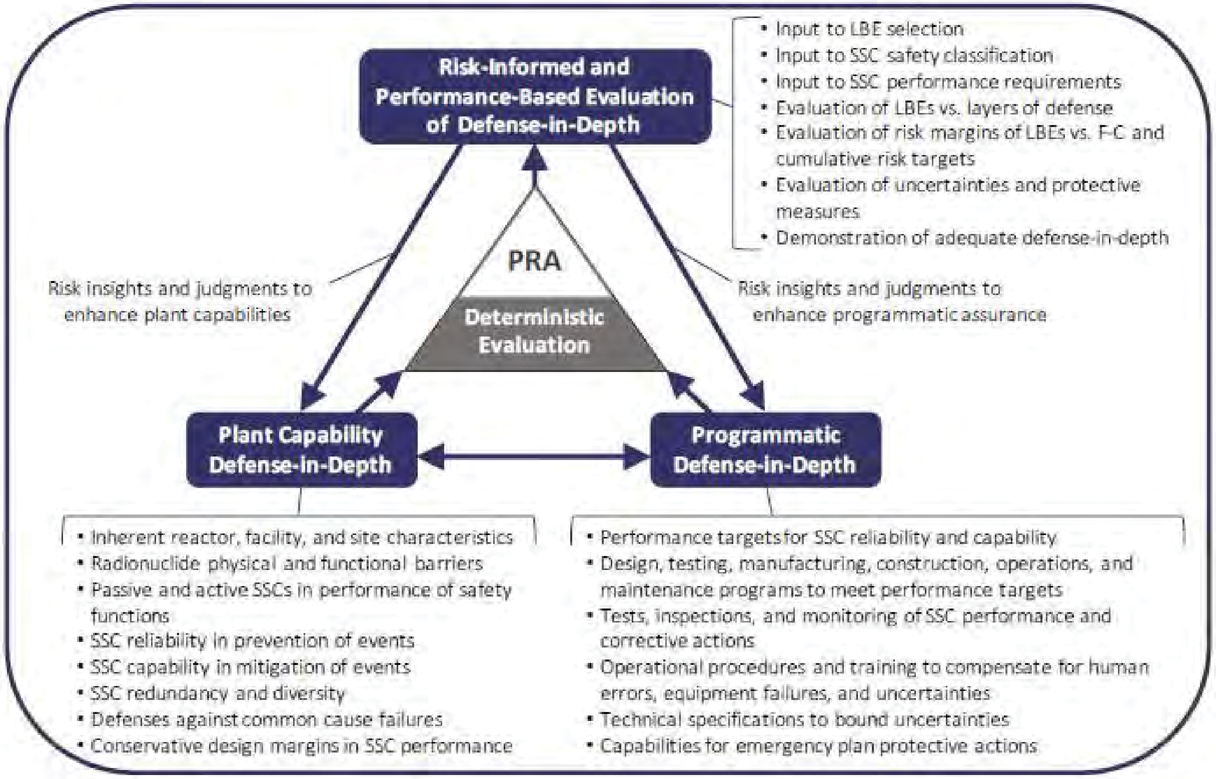

Risk-Informed and Performance-Based Evaluation of Defense-in-Depth
Input to LBE selection
Input to SSC safety classification
Input to SSC performance requirements
Evaluation of LBEs vs. layers of defense
Evaluation of risk margins of LBEs vs. F-C and cumulative risk targets
Evaluation of uncertainties and protective measures
Demonstration of adequate defense-in-depth
PRA
Deterministic Evaluation
Risk insights and judgments to enhance plant capabilities
Risk insights and judgments to enhance programmatic assurance
Plant Capability Defense-in-Depth
Programmatic Defense-in-Depth
Inherent reactor, facility, and site characteristics
Radionuclide physical and functional barriers
Passive and active SSCs in performance of safety functions
SSC reliability in prevention of events
SSC capability in mitigation of events
SSC redundancy and diversity
Defenses against common cause failures
Conservative design margins in SSC performance
Performance targets for SSC reliability and capability
Design, testing, manufacturing, construction, operations, and maintenance programs to meet performance targets
Tests, inspections, and monitoring of SSC performance and corrective actions
Operational procedures and training to compensate for human errors, equipment failures, and uncertainties
Technical specifications to bound uncertainties
Capabilities for emergency plan protective actions

Figure 4: Detailed Elements of Xe-100 Defense-in-Depth Framework

In particular, the Xe-100 plant I&C systems largely contribute to and support the following DID elements:

Plant Capability DID

- Active SSCs in performance of safety functions
- SSC reliability in prevention of events

- SSC capability in mitigation of events
- SSC redundancy and diversity
- Defenses against common cause failures

Programmatic DID

- Design, testing, manufacturing, operations, and maintenance programs to meet performance targets
- Tests, inspections, and monitoring of SSC performance and corrective actions
- Capabilities for emergency plan protective actions
- Selection of appropriate codes, standards and regulatory guidance

The Xe-100 safety design approach is used to provide inherent characteristics and passive/active SSCs that are sufficient to protect the public, as well as to provide the primary strategy for Plant Capability DID. An example of an inherent characteristic and passive/active SSCs available to support one of the Xe-100 plant safety functions involving I&C systems is provided in Table 4.

Table 4: Example of Design Features and SSCs Providing Plant Capability DID

Safety Function	Inherent Features and Passive SSCs	Active SSCs
Control Reactivity	Strong negative temperature coefficient of reactivity	Control and protection systems Distributed Control System Investment Protection System Reactor Protection System Reactivity control systems Reactivity Control System Reserve Shutdown System

An initial assessment of SSC classifications using insights from the PRA and deterministic safety analysis, and an initial assessment of plant capability DID has been completed. A systematic DID assessment in line with NEI 18-04 [7] will be established and provided in future submittals.

4.4 Interfaces Between Control and Protection

The RPS functions are independent of the DCS and IPS; however, the RPS sends both the status and the commands of the RPS system via a safety-related qualified signal isolation device so that a coordinated and integrated response is provided as detailed in Figure 4. That is, the overall I&C is designed around a hierarchy where RPS overrides IPS and DCS, and IPS overrides DCS to ensure that one system does not interfere in the demanded actions of the other.

The DCS is the lowest level of control, being subject to override by IPS and RPS actuation signals. In general, the IPS and DCS are supplied signals via their own dedicated field instrumentation. Due to space limitations and other considerations, some instrumentation is currently planned to be shared between the RPS and IPS/DCS. This includes the neutron flux detectors and flow instrumentation in the hot gas duct. As the design further matures, technical and regulatory justification will be established and will be included in the basis for the completed Xe-100 plant Preliminary Design (and in the PSAR submittal). Signals are shared via Class 1E isolation, consistent with PDC 24 ("Separation of protection and control systems).

[[

]]^{P}

Figure 5: Interface Between RPS and PEMS/DCS/IPS

4.4.1 Interface Between DCS and IPS

The IPS and DCS are both connected to the same automation bus. The IPS and DCS can send sensor values and calculated values between each other within certain rules. The IPAs will be executable without the DCS. Therefore, all actuators and sensors needed for the IPAs will be directly accessible by the IPS. See Figure 6 for example of IPS direct actuation. Sensors associated with the IPS are either being routed to the dedicated IPS controller before being forwarded to the DCS as shown in Figure 7, or the IPS and DCS can share sensors as shown in Figure 8. The IPS/DCS receives sensor data from the RPS, as shown in Figure 11, but the IPS will not rely on receiving data from the DCS as it has a higher safety rating (NSRST vs. NST). The wiring topology of how sensors and actuators will be connected depends on response time. If the DCS and IPS require responsive sensor data or fast actuation, then these will be directly wired to the applicable controller module. See Figure 6 for direct actuation and Figure 8 for direct signal connection examples.

The IPS utilizes two types of control output. The IPS will provide setpoint offsets to the DCS to maintain monitored system parameters in the dedicated operating range and will force the DCS to change states to a lower operating mode if a monitored parameter is outside the allowable range. These are called IPS corrective actions and are executed via the DCS, as shown in Figure 5.

Additionally, the IPS may actuate dedicated components to place a specific system or sub-system offline immediately, if the system meets a specific set of protection criteria. This mechanism is a final resort to protect the investments of the module or plant and will be precluded by an attempt to drive the system to a lower operation mode. All IPAs shall work independent of the DCS.

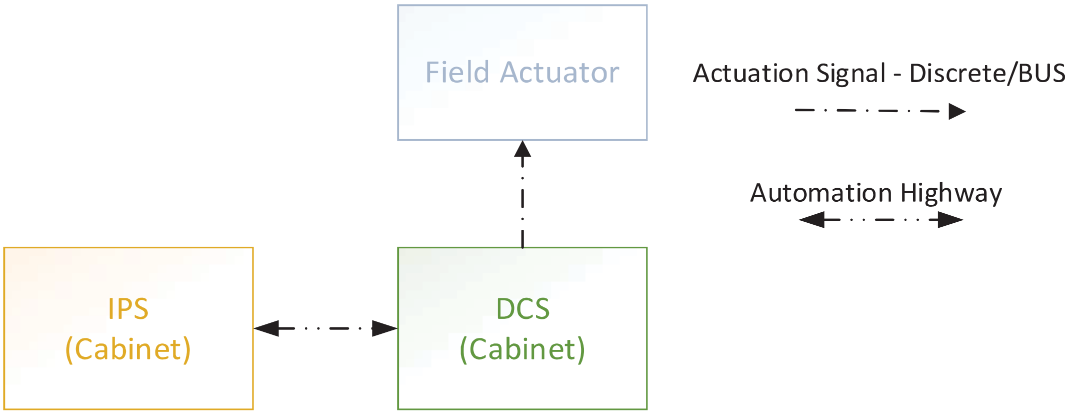


Figure 6: IPS forces DCS to a Lower Plant Mode (Corrective Action)

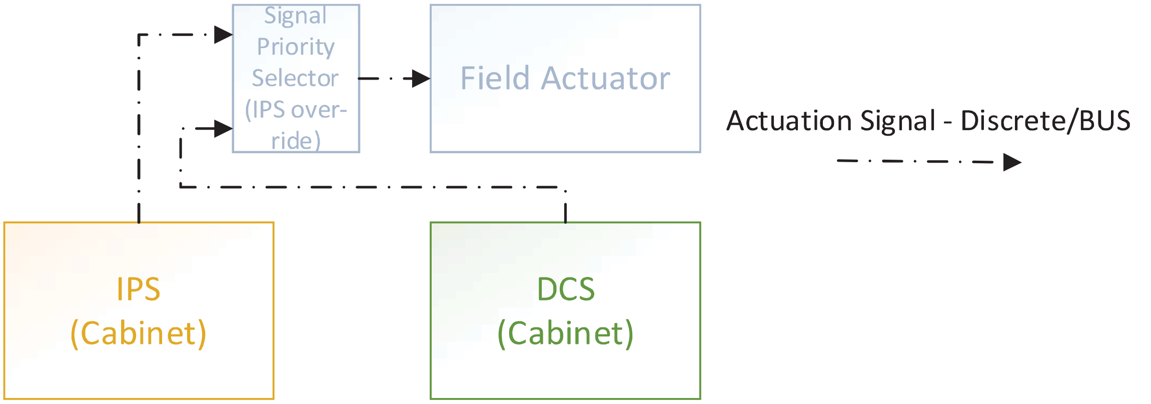

Signal Priority Selector (IPS over-ride)
Field Actuator
Actuation Signal - Discrete/BUS
IPS (Cabinet)
DCS (Cabinet)

Figure 7: IPS Actuation Prioritized Over DCS - With External HW (Protective Action)

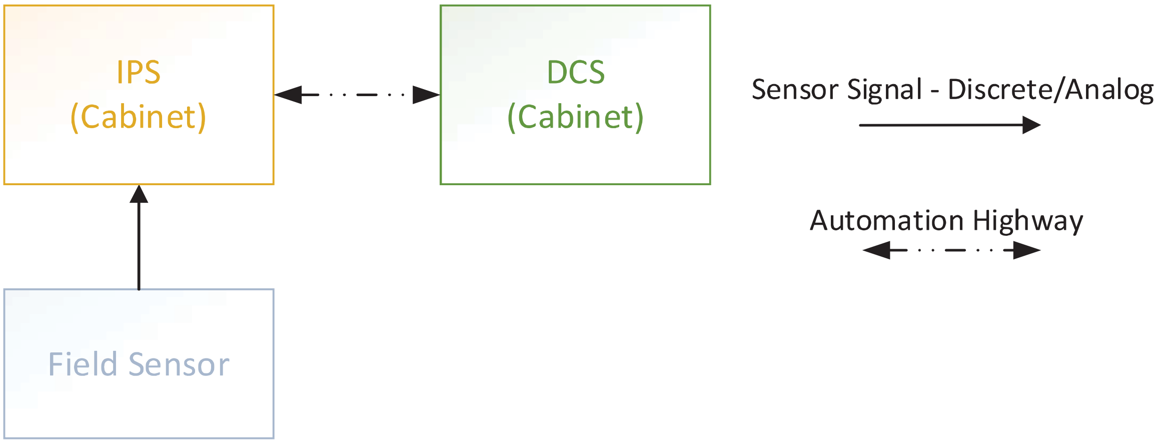


Figure 8: IPS Field Sensor Routed to DCS via the Automation Bus

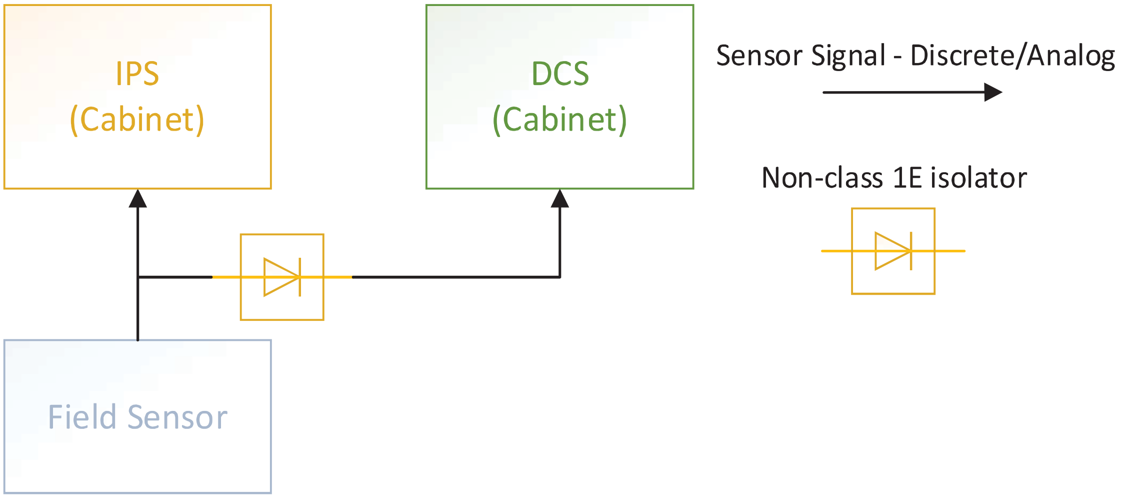


Figure 9: IPS and DCS Share Field Sensor

The DCS HMI will provide the operational IPS interface status indications, alarms, and a means of resetting IPS protective actions. The DCS can only reset IPS actions if the initiating plant state first returns to a normal operating condition.

4.4.2 Interface Between RPS and IPS/DCS

The RPS is installed in the RB and does not rely on any input from the IPS/DCS to ensure that Xe-100 PDC 22 is adhered to. However, the IPS/DCS will receive sensor data from the RPS. The IPS/DCS and RPS will share sensors via isolated signal/data lines as shown in Figure 4. The IPS will share RPS actuators via a completely independent interface, see Figure 9 and Figure 10. The RPS will always de-energize an actuator to a fail-to-safe mode. For example, the Steam Generator isolation valves will be designed to fail closed when the power or air supply is removed. This action is accomplished by the RPS to satisfy Xe-100 PDC 23. The IPS however, will control the valves to a shut position via a control signal.

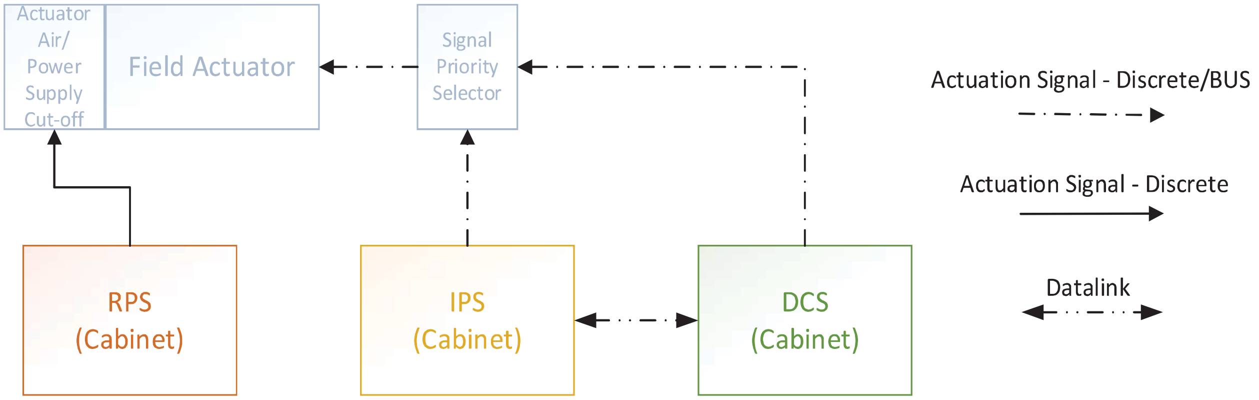

Actuator Air/ Power Supply Cut-off
Field Actuator
Signal Priority Selector
RPS (Cabinet)
IPS (Cabinet)
DCS (Cabinet)
Actuation Signal - Discrete/BUS
Actuation Signal - Discrete
Datalink

Figure 10: RPS Shared Actuator via External Signal Priority Selector

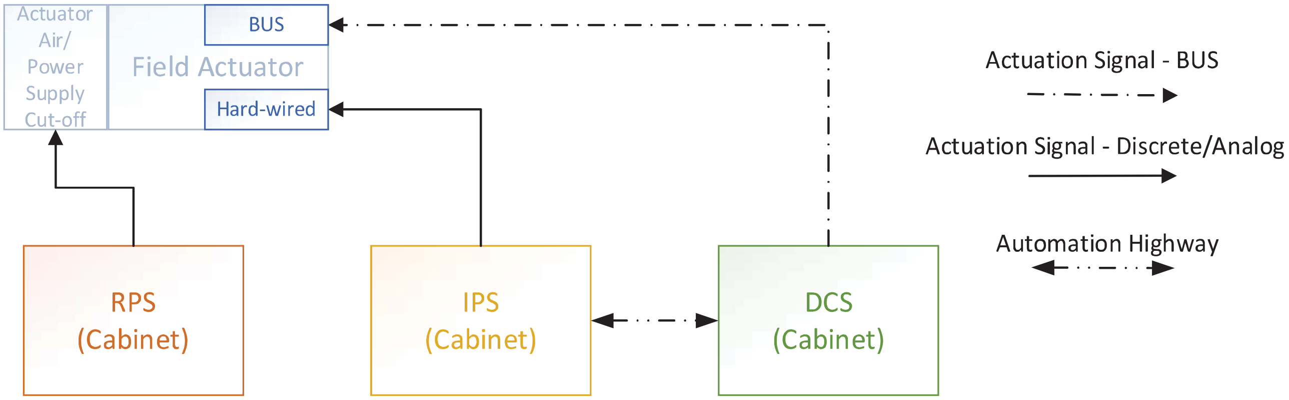


Figure 11: RPS Shared Actuator with Compatible Built-In Priority Selector

Sensors used by the RPS are sent to the IPS/DCS by one of the two methods shown in Figure 11. External Class 1E isolated repeaters are used in the field when fast response times are required for control. When a plant parameter response time is not critical the sensor data will be provided via the RPS isolated RS-485 outputs.

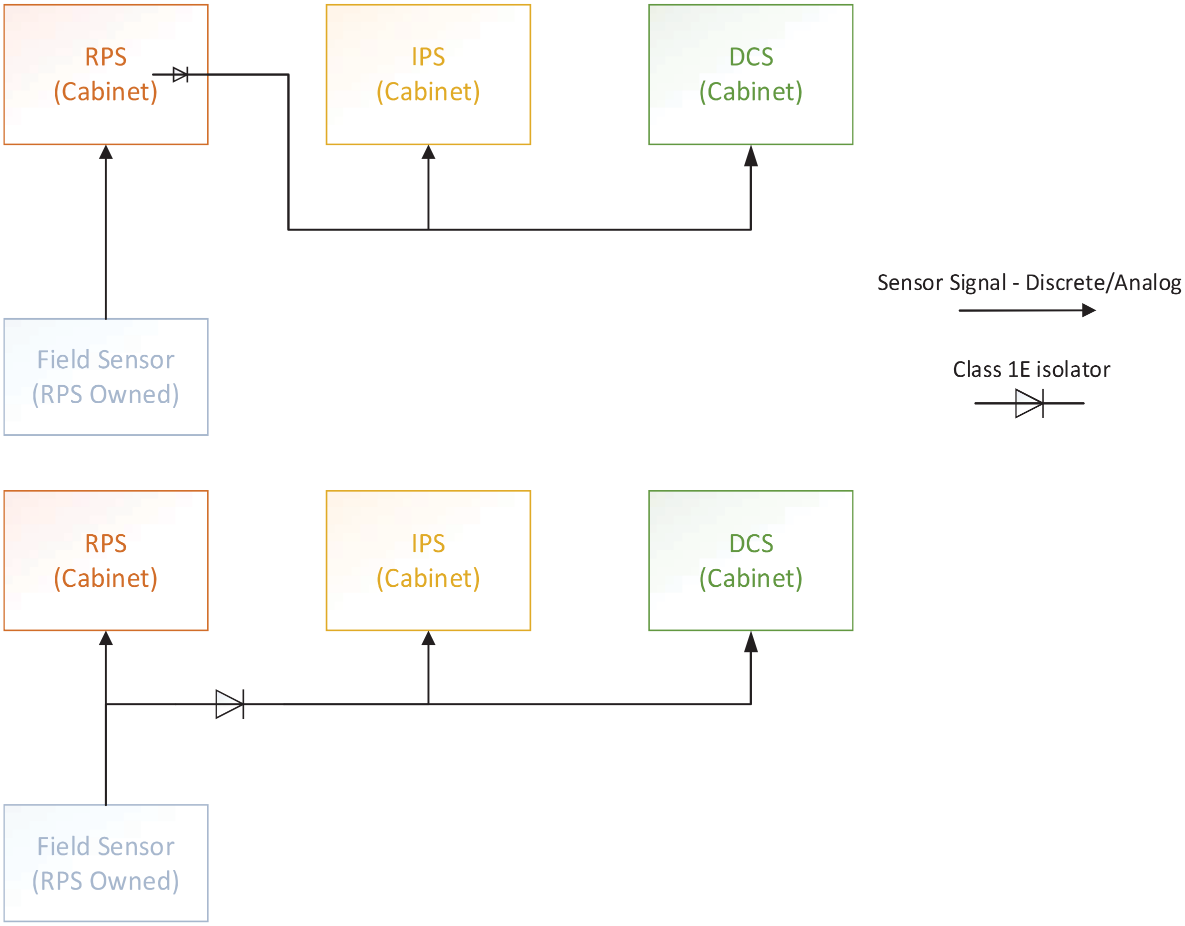


Figure 12: RPS Shared Sensor Arrangement

4.4.3 Interface Between RCSS and RPS /IPS/DCS

The RCSS control rod drive programmable logic controller (PLC) receives insert/withdraw and bank scram commands and permissives from the DCS/IPS via a datalink using Modbus protocol or hardwired signals. The RCSS PLC will provide the DCS with status information and rod position via a custom datalink.

4.4.4 Interface Between RPS and PEMS

The PEMS receives information from the RPS via a qualified unidirectional RS485 datalink from each RPS division as shown in Figure 21 . RPS Divisions A and B transmit data to one Interface Module (IM) within the Unit PEMS, and RPS Divisions C and D transmit to another. Given the diversity of the FPGAs utilized by the RPS Highly Integrated Protection System (i.e., self-testing) (HIPS) platform, this structure provides redundancy and diversity to PEMS monitoring of RPS parameters.

4.4.5 Interface Between DCS and PEMS

The Unit PEMS interfaces with the Module DCS via redundant unidirectional RS485 datalinks that connect to separate PEMS interface modules (Figure 20). The Common PEMS interfaces with the Common DCS via redundant unidirectional RS485 datalinks that connect to separate PEMS interface modules (Figure 21 and Figure 22). These links provide key DCS parameters that are used by operators and response personnel for plant/system diagnostics and recovery should an event occur.

4.4.6 Interface Between RMS and COMS

The RMS provides data to the COMS OPC Data Hub, which passes it on to the MCR HMI to alert the operator to potential radiological release. These alarms are accompanied by data to inform the operators of the type, location, and magnitude of the initiating event. The Data Hub also provides RMS data to the PI Historian, where it can be integrated with health physics data for an overall radiological assessment of the plant. Information is also available to the operators at the central RMS cabinet HMI in the equipment room adjacent to the MCR.

4.4.7 Interface Between RMS and PEMS

The PEMS monitors all RMS parameters through multiple redundant interfaces: The Common PEMS monitors data from the central RMS DACS as well as direct interface with site RMS detectors (such as perimeter monitors) that are not specific to a reactor module. The Unit PEMS monitors direct inputs from RMS detectors that are specific to the reactor modules. These interfaces are illustrated in Figure 20, Figure 21, and Figure 22.

4.4.8 Interface Between SMS and DCS

The SMS CACS Cabinet receives seismic data from all seismic instrumentation throughout the plant. The CACS sends alarm data through a dedicated MODBUS TCP interface to the common DCS in the CEB. The common DCS interfaces to the MCR to provide seismic alarm data to operators. The SMS to common DCS data interface is not seismically qualified as the CEB is not a Category 1 structure.

Additionally, the SMS CACS Cabinet transmits time-history seismic data to the common DCS via a TCP/IP datalink. This provides a redundant measure of data storage and the ability to send time-history seismic data to the plant historian and, through the historian, to the offsite plant support center for further storage and analysis.

4.4.9 Interface Between SMS and PEMS

The SMS CACS Cabinet receives seismic data from all seismic instrumentation throughout the plant. The CACS sends hardwired alarms via dry contacts to the common PEMS in the CEB. The common PEMS also provides alarm displays to the operators in the MCR as a defense in depth measure. The SMS to common PEMS data interface is not seismically qualified as the CEB is not a Category 1 structure.

4.5 Human System Interface (HSI)

The Human System Interface (HSI) will consist of Operational Controls and/or Information Displays located in the MCR, RSR, and any local control station installed remotely in the plant. The operator interfaces will consist of the following:

Display Graphics

- Operator Input Devices (e.g., touch screens, keyboard, mouse, push buttons)
- Audible and Visual Alarms
- Computerized Procedures System
- Wall Panel Displays

The Human-System Interface (HSI) Design is coordinated by the Human Factors Engineering (HFE) Design Team, in accordance with Xe-100 plant requirements, regulatory requirements such as NUREG-0700/0711, and HFE program related requirements.

Xe-100 plant control philosophy relies on a higher level of automation than traditional nuclear operating units. The initial Xe-100 concept of operations established a shift crew of three control room operators who will oversee multi-unit operations from a single control room, optimized at the conceptual design phase for four units.

The normal interface between the operator and the control systems can be defined as Intelligent Automatic Control (IAC). IAC consists of several modules for different equipment and functions fed by plant sensors. The module programming will send signals to various final actuation devices (e.g., pump motor starters, valve actuators) to achieve the desired actions to transition to other plant operating modes. The IAC interface permits the operator to initiate a certain maneuver (e.g., changing the reactor power, turbine power, mass flows, etc.), which the control system will then execute automatically within a pre-programmed operational envelope. The control system will allow the operator to observe the plant status, control actions, and to control any actuators manually, if required. However, during normal operations, it is not necessary for the operator to directly control any of the actuators.

Figure 12 shows a high-level example of the IAC control approach for the energy conversion function for the Xe-100 plant design.

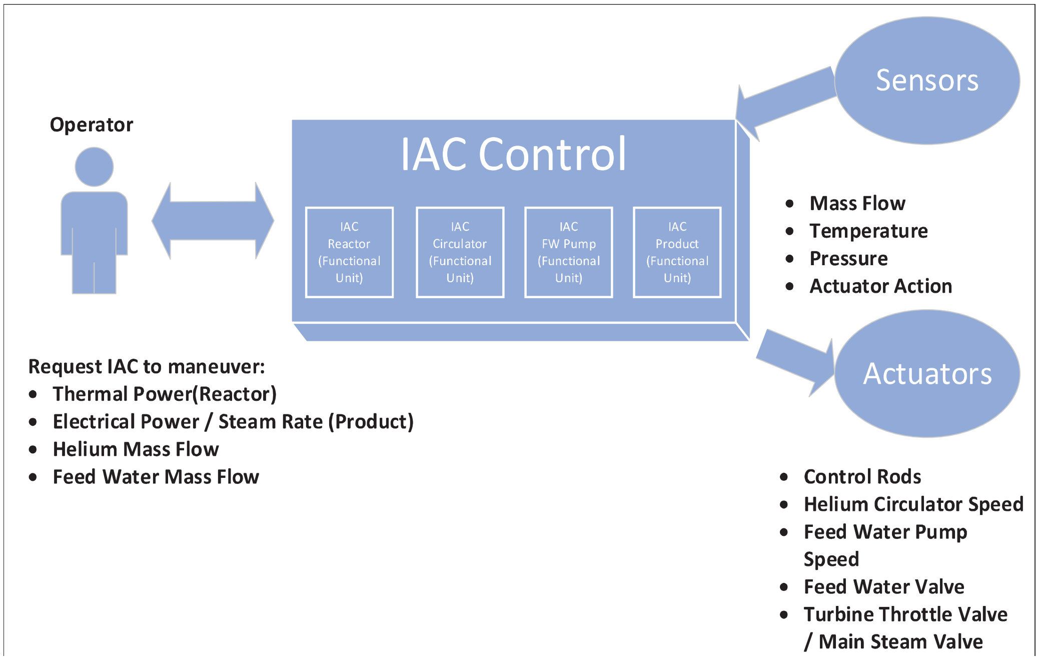


Figure 13: Example of the IAC Control Approach for the Xe-100 Plant Energy Conversion Function

The HSI design is being developed with a design goal to minimize human actions that safety functions do not require human actions, and that no human action will exacerbate the impact of off-normal events. In a layered defense, the Plant Control and Data Acquisition Systems are designed to detect and trip the plant automatically should any parameter exceed its allowable limits. This design provides the framework to significantly reduce operator cognitive and task load and, as a result, will require fewer operators to control the plant. Additionally, it allows for control of multiple units from a single control room.

The design of the HSI will take into consideration the Xe-100 plant control philosophy, and the concept of operation. The HSI will incorporate features that perform many of the system functions or operator tasks while enabling operators to better understand the automation's processes and increase their transparency. The Integrated Style Guide criteria establishes HSI features that allow the MCR operators to effectively monitor multiple displays and maintain the necessary level of situational awareness. The HSI design will also support the management of the workload for coordinating and controlling four reactor modules. Using data gathered from the Task Analysis, the necessary level of automation will be implemented to perform monitoring, control, and diagnostics of plant systems to support operator workload. To meet operational requirements of the Xe-100 plant and ensure graphical user interface design flexibility, advanced graphics software tools are being included for the implementation of the HSI. The HSI applications will be integrated with the DCS via a proven industry standard& platform-independent protocol such as Open Platform Communications Unified Architecture (OPC UA).

4.6 Communications Interface (COMS)

The Xe-100 Plant Communication System (COMS) provides a comprehensive and secure communications solution for Xe-100 plant operations, maintenance, and engineering. The COMS is separate from and does not include the communications associated with physical plant security. COMS consists of the nine subsystems below:

- Local Area Network System (LANS)
- Plant Area Network System (PANS)
- Digital Data System (DDS)
- Master Clock System (MCLK)
- Telecommunications System (TELS)
- Mobile Radio System (MRS)
- Announcement and Notification System (ANS)
- Multimedia TV System (MTVS)
- Satellite Communications System (SCS)

The plant communication system is an integrated but segmented solution that will provide high availability and secure communications for the Xe-100. The segmented design uses a combination of logical segmentation and physical segmentations to ensure:

- Failures in one segment will not impact other segments
- Communication between segments is limited and controlled
- Essential functions are given highest priority of resources
- Communication management functions are separate from data communications
- Communication between security zones/layers are restricted

Technology and design alone do not ensure security in communications. [[

-
-
-
-
-
-]]^{P}

4.6.1 Local Area Network System (LANS)

The Local Area Network System (LANS) is the data network supporting network communications for Non-Safety Related operations, control, and emergency preparedness. [[

-
-

-
-
-
-

]]^{P}

The LANS integrates and segments non-safety related networks such as:

- DCS
- Control Room
- Non-DCS systems requiring an interface with the DCS or the control room
- PEMS

4.6.2 Plant Area Network System (PANS)

[[

-
-

]]^{P}

4.6.3 Digital Data System (DDS)

The Digital Data System (DDS) is a datacenter system that supports the communications applications and other plant applications. The DDS provides a virtual computer environment for supporting applications such as:

- Plant Data (PI) Historian
- Active Directory
- Communications Applications

- Management Applications
- Maintenance Applications
- File Servers
- Cyber Security Applications

4.6.4 Master Clock System (MCS)

The Master Clock System (MCLK) is the stratum 1 Network Time Protocol (NTP) time source for the Xe-100 plant. The clock is synchronized via secure Global Positioning System (GPS) and will serve accurate time for digital components on the Xe-100 networks.

4.6.5 Telecommunications System (TELS)

The Telecommunications System (TELS) is the primary voice communication system for the Xe-100 plant. The TELS is a networked based solution that will provide telephone service throughout the Xe-100 plant.

4.6.6 Mobile Radio System (MRS)

The Mobile Radio System (MRS) is a wireless radio network for voice and data communications for the Xe-100 plant. The MRS will provide two-way voice and Push-To-Talk (PTT) capabilities for Emergency Preparedness (EP), operations, and maintenance. The MRS is a separate radio network from the physical security wireless radio network.

4.6.7 Announcement and Notification System (ANS)

The Announcement and Notification System (ANS) supports the public address system for the Xe-100 plant. The ANS will support announcements via a variety of methods for plant evolutions and emergencies.

4.6.8 Multimedia and Television System (MTVS)

The Multimedia and Television system (MTVS) will provide the operational, maintenance, and engineering cameras for the Xe-100 plant. Strategically placed cameras will aid plant personnel with the operation and maintenance of the Xe-100. The MTVS will also supply televisions with live television broadcasts and company digital signage.

4.6.9 Satellite Communications System (SCS)

The Satellite Communications System (SCS) is a secondary provider of voice and data communications for the Xe-100. The satellite will also serve as the voice and data provider in remote locations and initial constructions phases.

4.6.10 Conceptual Architecture

The COMS conceptual architecture in Figure 25 provides a visual representation of the network architecture across the cyber security levels. The figure depicts the various boundary devices and the divisions between the plant networks. Determination of specific technology for the protection between the boundary layers will be defined in the XE-100 cyber security plan and defensive architecture.

4.7 Cyber Security

The overall cyber security approach for the Xe-100 plant consists of (1) establishing, (2) implementing, and (3) maintaining compliance with the cyber security program required by the regulatory entities for the given region based on the physical location of the plant. The cyber security program protects the systems that ensure the safety of the plant and public while keeping a balance of operational and financial objectives. [[

-
-
-
-
-
-

-
-

-
-
-
-
-
-]]^{P}

The SSC classifications used for the Xe-100 plant include three categories:

- SR – corresponds with the NEI 08-09 classification of Safety Related (Direct)
- NSRST – corresponds to NEI 08-09 [22] and NEI 13-10 [23] Non-Safety Related critical digital assets (Indirect)
- NST – corresponds to NEI 08-09 [22] and NEI 13-10 [23] Non-Safety Related critical digital assets (Indirect)

There is significant overlap between the Xe-100 SSC classification and the NEI 08-09 CDA classification. The classifications of the Xe-100 Preliminary SSC Classification List [24] act as a starting point for digital asset classification, and ongoing assessments will be performed across the range of digital systems and assets as the design of the Xe-100 plant is finalized.

5. Overall Architecture

The Plant Control & Data Acquisition System (PCDAS) refers to all systems which are required for the operation and safety of the entire Xe-100 plant. Table 5 and Figure 17 show internal and external interfaces and boundaries of the PCDAS with other Xe-100 systems.

Each Unit Module has a separate automation bus. The automation buses (ethernet) of each of the Unit Modules are separate from each other and are linked to the common (plant-wide) application bus via a redundant Unit Module application server pair. The common system automation bus is also linked to the plant wide application bus via a separate application server pair.

Each Unit Module also has an independent, safety-related RPS. The RPS provides plant sensor and status indications to the IPS and PEMS via a qualified, Class 1E datalink or, in selected cases, an isolated analog signal (e.g., ex-core detectors) as shown in Figure 4. This sensor/status information is used by the IPS/DCS to control various plant processes, provide plant status and alarms to the plant operators in the MCR, and stored in both the PEMS and DCS Historian. Each module RPS also provides sensor/status information to its associated displays in the RSR.

The HSI (displays) connects to the automation bus via the application server. The automation bus connects to the process interface via the automation servers.

5.1 Distributed Control System (DCS)

The Distributed Control System (DCS) provides controls and indications for the systems associated with the direct function of energy production. There is a segmentation between the nuclear island and conventional island controllers and between each Unit Module. This segmentation allows each of the Xe-100 Modules to operate and function as a standalone system. The DCS is the lowest level of control, being subject to override by IPS corrective/protective actions and RPS trip signals. The DCS risk significance with regards to ongoing Xe-100 plant defense-in-depth (DID) analyses will inform the DCS design. Any modifications resulting from the DID analysis will be incorporated into the DCS system configuration, quality requirements, and/or interfaces within the I&C architecture.

5.2 Investment Protection System (IPS)

The Investment Protection System (IPS) function is to provide corrective and protective actions related to critical plant parameters for the protection of assets, and continuity of safe return to power production. Corrective actions at the IPS level are directed to the setpoint of lower-level controllers, implemented in the DCS. The DCS will have a bidirectional communication with the IPS to provide status and feedback information. Conversely, IPS protective actions of equipment that are initiated by the IPS for investment protection are accomplished by either direct actuation or a priority selector to allow IPS actuations with a higher priority than the DCS signals, see Figure 6. The IPS will utilize a 3-input sensor voting logic for non-safety related inputs. The IPS will use a 4-input voting logic configuration for signals shared from RPS as shown in Figure 13. The IPS can receive the RPS sensor values either via a digital communication bus or directly with an isolated signal repeater as shown in Figure 4 and Figure 11. The 3-input and 4-input voting logic will reduce nuisance trips and allow for online repair and maintenance. A conceptual Xe-100 plant IPS functional architecture is illustrated in Figure 18.

The IPS functionality and associated setpoints will continue to be reevaluated as preliminary and final design analyses inform the licensing basis for the system. Any modifications resulting from future risk-informed Xe-100 plant design changes/requirements will be incorporated into the IPS system configuration, quality requirements, and/or interfaces within the I&C architecture.

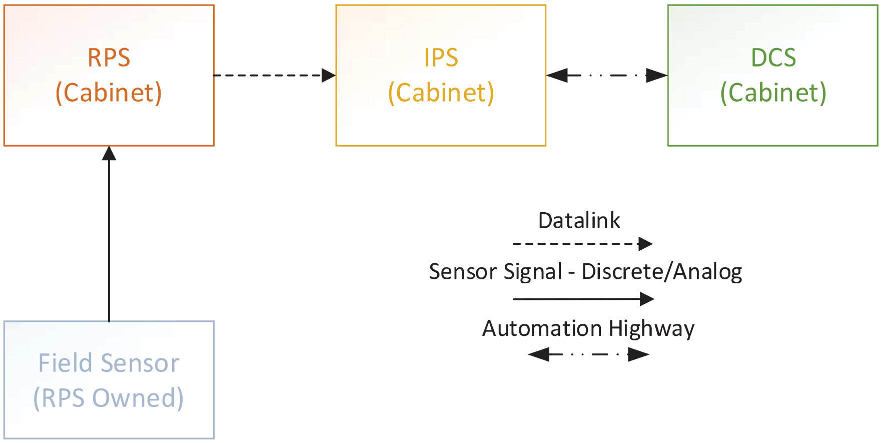


Figure 14: Shared Sensors from RPS

5.3 Reactor Protection System (RPS)

The Reactor Protection System (RPS) uses a four-channel configuration that satisfies physical and electrical independence and separation requirements. Due to the inherent safety of the Xe-100 plant and use of passive safety features, there are minimal safety related I&C components required to support the safety case.

- The RPS is based on the HIPS platform, which is a FPGA-based system. It is credited with mitigating DBAs and therefore is classified as SR.
- Electrical power, including CRDM and Helium Circulator power supplies are not required to be safety related. The basis for this classification is that electrical power is not required for safety-related SSCs to perform their respective Required Safety Functions.
- Additional HIPS platform technical details are available in the “Safety Evaluation by the Office of New Reactors Licensing Topical Report (TR) 1015-18653-NP, (Revision 2) “Design of the Highly Integrated Protection System Platform” (Docket: PROJ0769) [17].

The RPS is designed to ensure that the fulfillment of its safety functions is assured in the event an accident occurs simultaneously with a postulated failure or unavailability due to maintenance. The RPS is implemented such that a single failure of an RPS component will not render an RPS division incapable of performing its intended safety functions, performing isolation functions, or causing spurious trips. Two-out-of-four coincidence voting logic and online automatic self-testing is utilized to ensure PDC 21 ("Protection system reliability and testability"), PDC 22 ("Protection system independence"), and PDC 25 ("Protection system requirements for reactivity control malfunctions") are fulfilled.

- RPS reactor trip and isolation functions are achieved by removing power via the final actuation device. The final actuation device that removes power to the SG isolation valves, Circulators and CRDMs are the EIM outputs in the RPS.
- The isolation valves, control and shutdown rods are SR; however, the associated electrical and control connections are NSRST or NST.

The HIPS platform and the SR boundary is shown in Figure 14. The Feedwater and Main Steam Isolation Valves are normally closed and require the RPS to allow power to solenoids that hold each valve open.

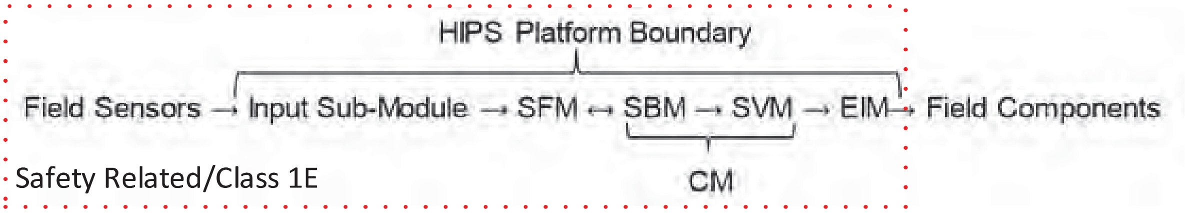


Figure 15: HIPS Platform and SR Boundary

In addition to temperature, pressure, humidity, and mass flow, the RPS incorporates four channels of flux monitoring (Figure 15) via four ex-core ND arrays placed adjacent to the Reactor Cavity Cooling System (RCCS) standpipes.

- Source range neutron monitoring is provided by two B-10 proportional counters (per channel). The source range signal is obtained via transistor-transistor logic (TTL) pulse, which are counted by the RPS.
- Wide range (WR) neutron monitoring is provided by three compensated B-10 ion chambers (per channel), which produce a 0-5Vdc logarithmic signal for intermediate range indication and a linear 0-5Vdc for power range indication.

The RPS calculates Start-up Rate (SUR) and source range count-rate based on these analog ND signals. The source range detectors are only used for indications and are not used for any reactor trip parameters. The wide range detectors monitor two decades of overlap with the source range startup detectors to provide high SUR protection. The startup detectors are used during reactor startups to ensure a controlled approach to criticality. Therefore, the startup detectors are considered NSRST. In addition to high SUR protection the wide range detectors provide a linear signal used for high reactor power trip and a logarithmic indication to 250% reactor power. Ongoing reactor analysis is being performed to determine if the inherent safety features of the core and TRISO fuel prevent excessive SUR and neutron flux levels from occurring. If it is shown that safety limits cannot be exceeded due to high SUR or neutron flux, the WR detectors would also be considered NSRST.

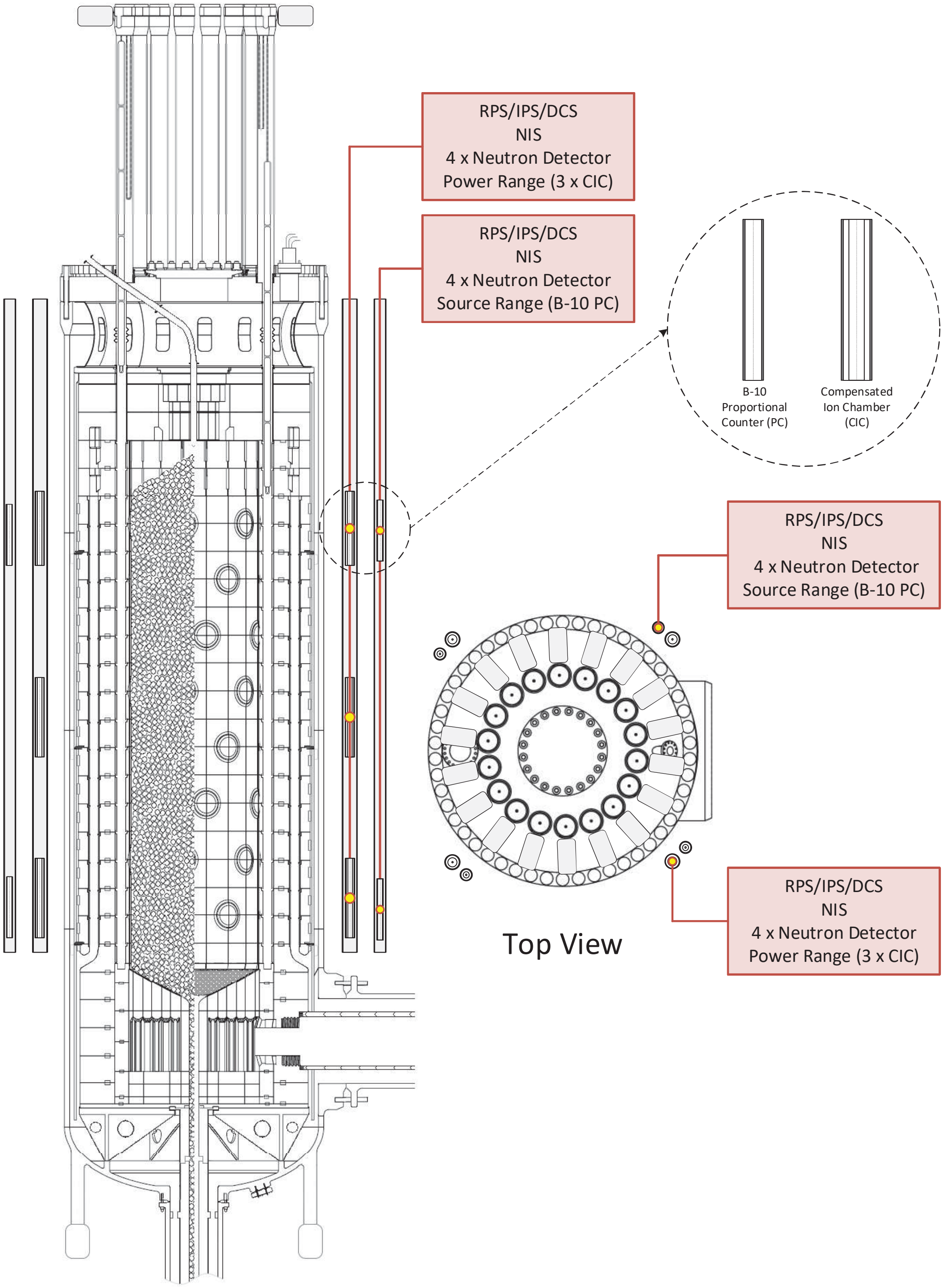


Figure 16: Neutron Detector Locations in the Xe-100 Reactor Pressure Vessel

The HIPS platform is designed such that a safety division functions independently of other safety divisions. The RPS uses two FPGA technology types that provide diversity to greatly reduce the likelihood of postulated digital common cause failures. One FPGA technology type is used in Channels A and C, and another FPGA technology type is used in Channels B and D. A conceptual Xe-100 plant RPS functional architecture is illustrated in Figure 19.

The MCR includes switches for manually actuating RPS protective functions (in support of DID against beyond DBEs) including: (1) a manual reactor trip which de-energizes the CRDMs and (2) a manual Steam Generator isolation and Helium Circulator trip.

Per procedure the operator will perform a reactor trip before isolating primary and secondary flow. These hardwired manual actuation buttons are not required to be safety rated because there are no manual operator actions credited in the Xe-100 plant safety analysis. For reactor trips that do not immediately secure the Helium Circulator, the RPS monitors for shutdown indications and will subsequently shutdown the Helium Circulator if confirmation of rod drops has not occurred within the required drop time.

5.4 Reactivity Control & Shutdown System (RCSS)

The Reactivity Control & Shutdown Systen (RCSS) system is comprised of the RCS and RSS. Both the RCS and RSS have nine (9) individual rods allocated to either RCS or RSS banks. The rods can be moved individually or by bank. The neutron absorber rods are moved by CRDMs which are located on the reactor pressure vessel lid attached to Standpipes (Tubes) and CRDM Housings (see Figure 16). A single Control Rod Drive Controller (CRDC) will control movement of the nine (9) RCS CRDMs and the nine (9) RSS CRDMs. The CRDMs are comprised of electrical motors, position sensors, and SCRAM deceleration devices with a chain and drive sprocket arrangement that permits the lifting and lowering of the neutron absorber rods into and out of the reactor core. The CRDM motors are powered and controlled by the RCSS motor drive controllers that receives rod position commands from the RCSS CRDC. The RCSS CRDC receives control rod drive insert/withdraw requests from the DCS/IPS based on operating plant conditions.

The design of the RCSS CRDMs and neutron absorber rod assemblies is essentially the same for both systems, other than a slight difference in chain length to provide a different fully inserted position for the rods. The CRDM for each RCS and RSS mechanism will be supported by individual power supplies and a control system that will adjust the vertical position of the neutron absorber rods in the reactor core.

The CRDM arrangement will include sensors to serve as a rod position indication (RPI) system. Several different types of instruments will be used to detect and report the vertical position of the control rods, including a RAMTE attached to the electric motor shaft, a LVDT located around the outer diameter of the standpipe that houses the CRDM, and mechanical or pressure detecting switches that can confirm the vertical position of the fully inserted rod within its guide tube.

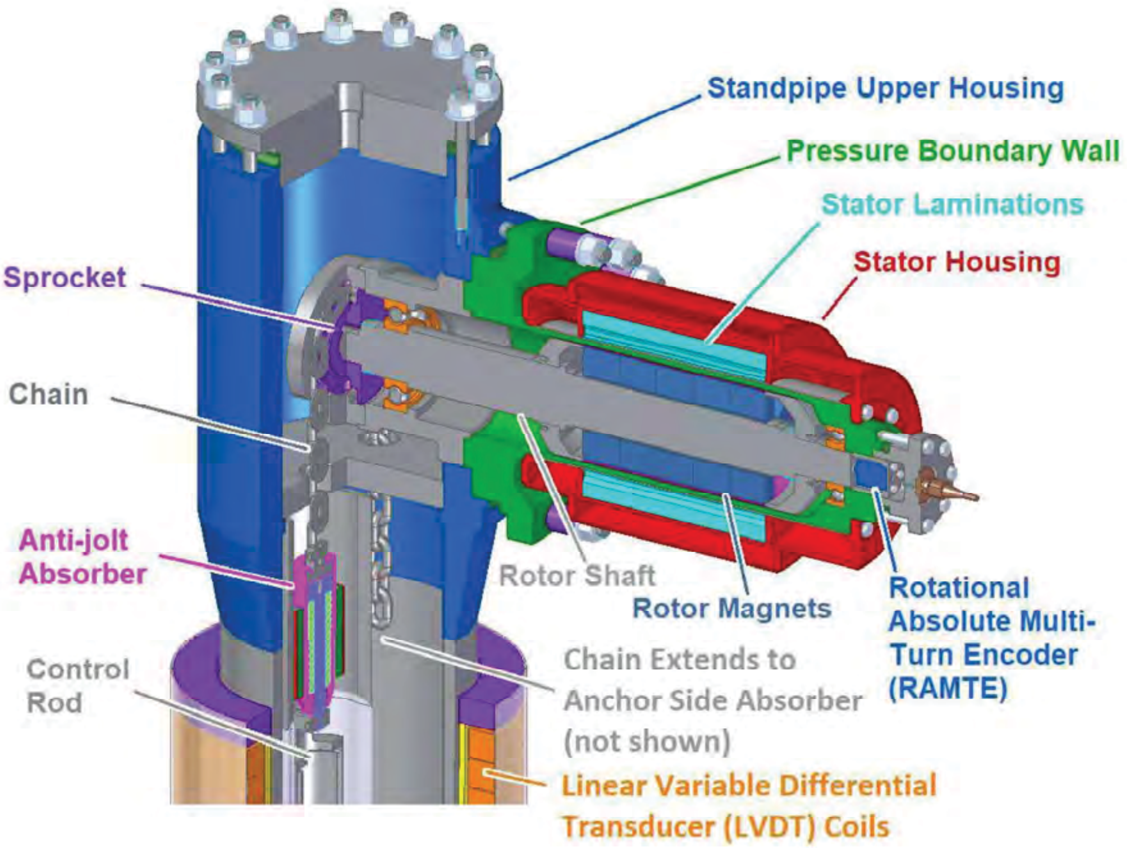

Standpipe Upper Housing
Pressure Boundary Wall
Stator Laminations
Stator Housing
Sprocket
Chain
Anti-jolt Absorber
Control Rod
Rotor Shaft
Rotor Magnets
Rotational Absolute Multi-Turn Encoder (RAMTE)
Chain Extends to Anchor Side Absorber (not shown)
Linear Variable Differential Transducer (LVDT) Coils

Figure 17: CRDM System Arrangement

5.5 Post-Event Monitoring System (PEMS)

The Post-Event Monitoring System (PEMS) provides monitoring functions that will record parameters that are important to assess the status of the plant after an event which may have rendered the DCS Historian incapable of recording critical parameters. The PEMS receives isolated information from the RPS and non-isolated information from the IPS, DCS, RMS, and SMS. The PEMS, like the RPS, is based on the HIPS platform, which is a FPGA-based system. A high level PEMS functional layout is shown in Figure 20. Functional architectures of the Module and Common PEMS are illustrated in Figure 21 and Figure 22, respectively. Each Unit PEMS monitors parameters that are associated with its corresponding reactor module, whereas the Common PEMS monitors general site parameters.

Unit PEMS Interfaces

- Reactor Protection System
- Investment Protection System
- Module Distributed Control System
- Module-specific Radiation Monitoring System detectors

- Reactor Cavity Cooling System
- Site Post-Event Monitoring System

Common PEMS Interfaces

- Common Distributed Control System
- Site Radiation Monitoring System detectors
- Offsite Plant Support Center & Digital Twin
- Seismic Monitoring System
- Module Post-Event Monitoring Systems

Every PEMS is divided into two (2) redundant chassis, each of which contains modules for data reception, storage, display, and transfer.

The extent of applicability of RG 1.97 [12] and any associated special treatments to the PEMS is being determined following the approach defined in RG 1.233 [5] and NEI 18-04 [7]. As there are no operator actions credited for Xe-100 safety functions, there are no Type A variables required for display to the operator to perform manual safety functions. Consistent with the guidance of NUREG-0700 [20], select variables are continuously provided to the operator at the PEMS displays in both the MCR and RSR.

The PEMS functionality will continue to be reevaluated as final design analyses informs the licensing basis for the system. Any modifications resulting from future risk-informed Xe-100 plant design changes/requirements will be incorporated into the PEMS system configuration, quality requirements, and/or interfaces within the I&C architecture.

5.6 Radiation Monitoring System (RMS)

The Radiation Monitoring System (RMS) monitors and logs radiological parameters related to the operation of the Xe-100 plant. The RMS accomplishes this by providing a range of radiation detectors at various locations to provide comprehensive coverage of the plant and by connecting all measurement HW to a central network for data logging. The RMS is intended to cover all effluent, particulate, liquid waste, and gross gamma monitoring for the plant; it does not cover solid waste streams, personal radiological protection such as dosimetry or portal monitoring, or radiological monitoring for processes which are internal to other plant systems. For example, the Helium Service System (HSS) contains radiation monitoring to determine the level of fission products in the primary loop and these instruments are not a part of the RMS.

The RMS provides measurement data to the PEMS as well as to the COMS, which passes alarms to the operator. The RMS utilizes a centralized DACS server to provide simple controls such as self-calibration, local alarm testing, and local pump, valve, and solenoid actuations to the operator in the CEB. This architecture is displayed Figure 23.

RMS instrumentation will be installed at the following locations:

- Controls & Electrical Building
  - DACS cabinet in the server room adjacent to the MCR

  - Gamma area monitors in the MCR
  - Stationary alpha-beta particulate air monitors in the MCR HVAC

- Reactor Buildings (RBs)
  - Gamma area monitors in the RSRs
  - Gamma area monitors in the Control Rod Drive & Steam Generator cavities
  - Gamma area monitors by the different stages of the FHS
  - Argon-41 monitors for the RCCS effluent ducts
  - Airborne particulate monitoring in the RB Heating, Ventilation, and Air Conditioning (HVAC)
- Nuclear Island Auxiliary Buildings (NAIBs)
  - Gamma area monitor in the HSS high radiation area
  - Noble gas, tritium, and alpha-beta particulate monitors in the HVAC system and effluent stack
- Fuel Handling Auxiliary Buildings
  - Gamma area monitors on the upper and lower floors
  - Airborne particulate monitoring on the upper and lower floors
- Spent Fuel Intermediate Storage Facilities
  - Gamma area monitors in the Spent Fuel Storage Room
- Radioactive Waste Treatment Building
  - Gamma area monitors on the upper and lower floors, drum and decontamination areas
  - Airborne particulate monitoring in the HVAC system
- Inter-Unit Access Tunnels
  - Airborne particulate monitoring in the Inter-Unit Access Tunnel HVAC stack effluent
- Plant Boundary
  - Gamma area perimeter monitoring system

5.7 Seismic Monitoring System (SMS)

The Seismic Monitoring System (SMS) provides monitoring and alarming functions for the Xe-100 plant to inform operators if a plant shutdown is necessary after a seismic event. The SMS has no control actions. 10 CFR 50 Appendix S, RG 1.12 [9] and ANS 2.2 – 2016 [19] require that all Category 1 structures of a nuclear power plant site be monitored for seismic response in the case of an earthquake. The only Category 1 structures in the Xe-100 design are the four, seismically independent, RBs.

SMS instrumentation will be installed at the following locations:

- [[
-
-

-
-
-
-
-
-
-

]]^{P}

The above SMS architecture is laid out in Figure 24. This system architecture allows for seismic data responses to be collected for all structures related to safety functions as well as a response for free field plant activity.

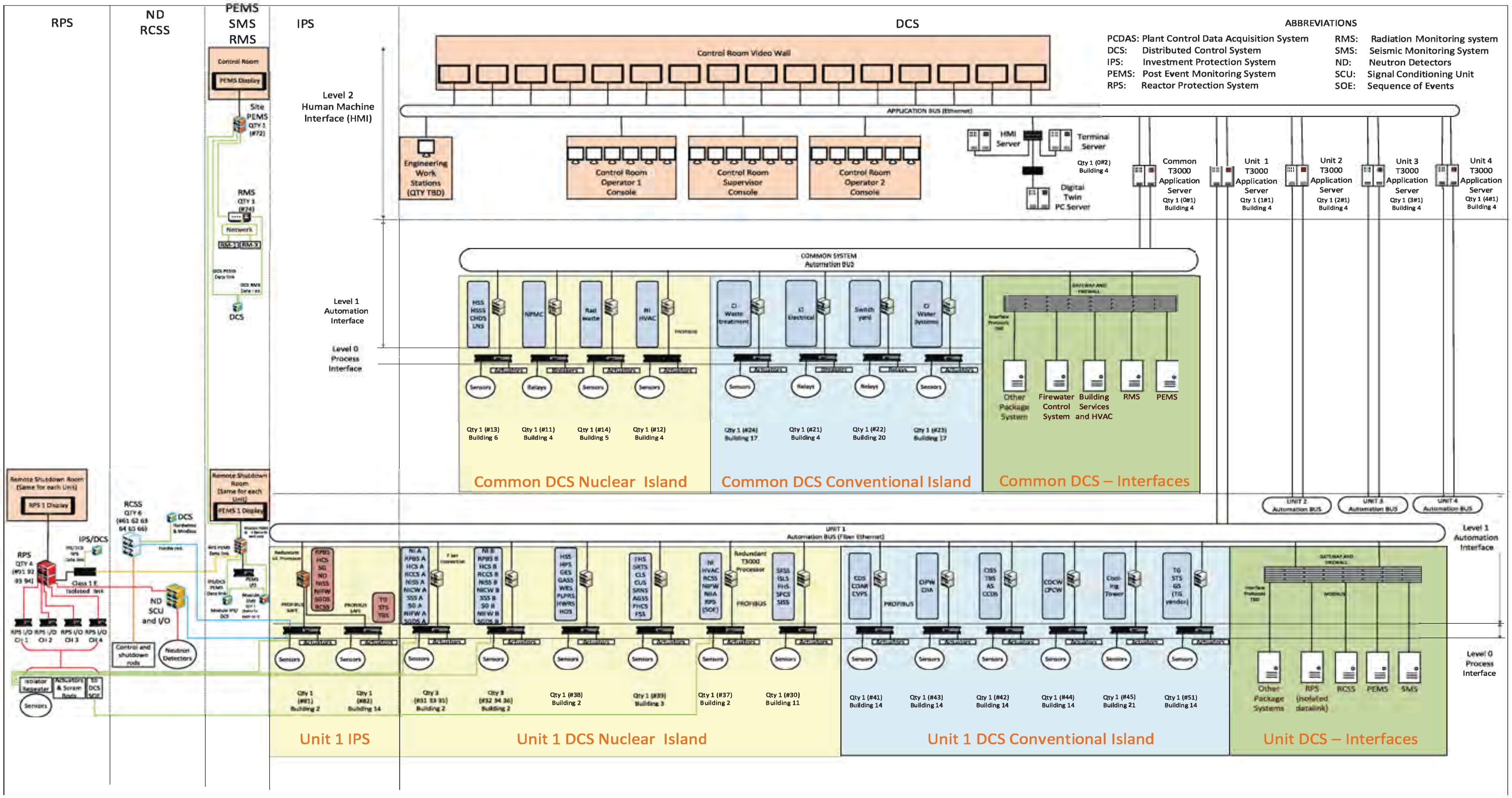


Figure 18: Conceptual Plant-Wide Distributed Control System (PDCS) Architecture

Table 5: Plant Systems Internal or External to the DCS

Abbreviation	System Name	Abbreviation	System Name	Abbreviation	System Name
IPS	Investment Protection System	RX	Reactor System	NILD	NI Liquid Drainage System
RPS	Reactor Protection System	SG	Steam Generator System	NILR	NI Liquid Radwaste System
PEMS	Post Event Monitoring System	HCS	Helium Circulator System	NIE	NI Electrical System
NIS	Nuclear Instrumentation System	FHS	Fuel Handling System	TG	Turbine Generator System
RMS	Radiation Monitoring System	SFSS	Spent Fuel Storage System	CDS	Condenser System
SMS	Seismic Monitoring System	RCCS	Reactor Cavity Cooling System	CISS	CI Steam System
MDMS	Maintenance & Diagnostic Monitoring System	HSS	Helium Service System	CCDS	CI Condensate System (CI Feedwater)
FDAS	First-of-a-Kind Data Acquisition System	SSS	Startup and Shutdown System	CDCW	CI Condenser Cooling Water System
OIS / MCR	Operator Interface System / Main Control Room	NISS	NI Steam System	CPCW	CI Component Cooling Water System
WTS	Water Treatment System	NIFW	NI Feedwater System	CIFP	CI Fire Protection System
PFP	Plant Fire Protection System	RWT	Radioactive Waste Treatment System	CIIA	CI Compressed & Instrument Air System
HV	Plant HVAC System	NICW	NI Cooling Water System	CIPW	CI Process Water System
STW	Storm Water System	NIFP	NI Fire Protection System	CILD	CI Liquid Drainage System
SER	Service Water System	NIHV	NI HVAC System	CIE	CI Electrical System
SEW	Sewer System	NIIA	NI Compressed & Instrument Air System		
POT	Potable Water System	SGDS	Steam Generator Dump System		
COMS	Plant Communications System	NIPW	NI Process Water System		

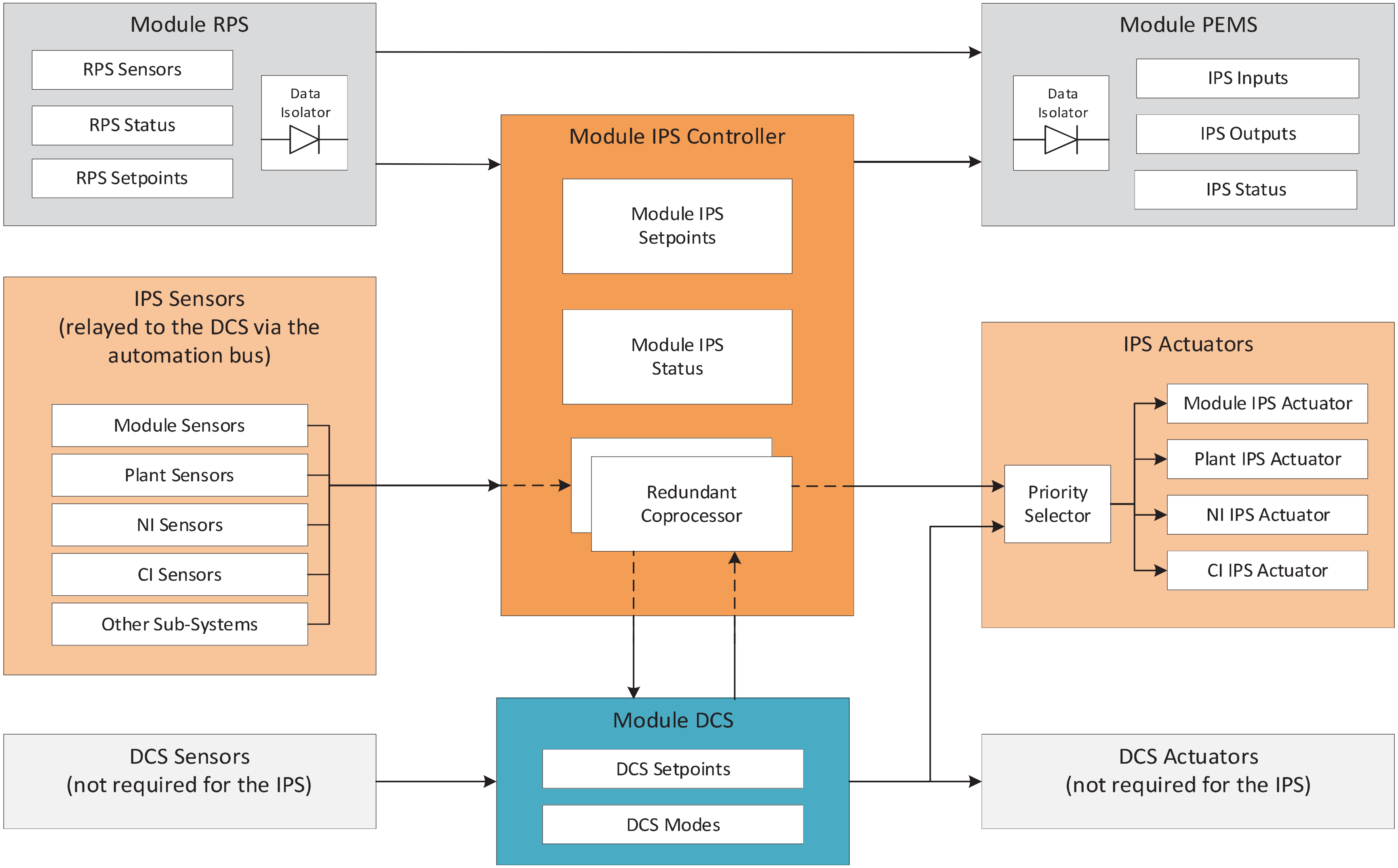
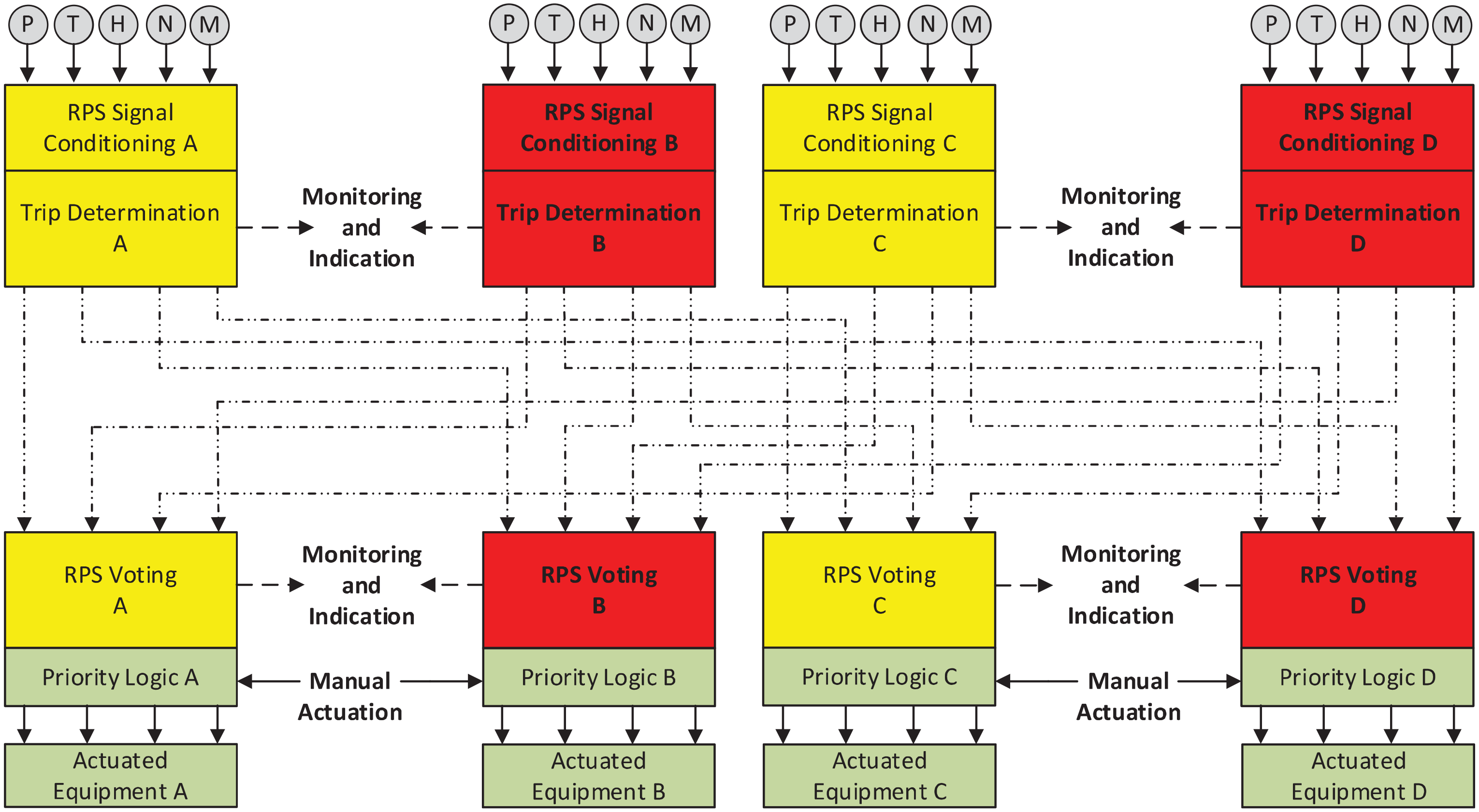


Figure 19: Conceptual IPS Functional Architecture



LEGEND

RPS	**Reactor Protection System**
———	**Hard-wired Signal**
— — —	**One-way Serial Connection**
— · —	**Triple Modular Redundant One-Way Serial Data Connection**
🟨	**FPGA Technology Type 1**
🟥	**FPGA Technology Type 2**

Figure 20: Conceptual RPS Functional Architecture

[[

]]^{P}

Figure 21: Post-Event Monitoring System Network Layout

[[ ]]^P

Figure 22: Unit PEMS Architecture

[[ ]]P

Figure 23: Common PEMS Architecture

[[ ]]^{P}

Figure 24: RMS Architecture

[[

]]^{P}

Figure 25: SMS Architecture

[[ ]]^{P}

Figure 26: Conceptual COMS Architecture

6. Control and Protection System Response to Plant Transients

The purpose of this section is to illustrate the interactions of various I&C systems in response to plant transients. The LBEs identified below are from the Phase 1 PRA. As the design matures, the PRA will be updated and the LBEs will be analyzed in accordance with the iterative NEI 18-04 [7] design process.

6.1 Transients Event Sequence Analysis

The Xe-100 I&C systems are designed to respond to different plant initiating events and bring the plant to a stable operating state. Phase 1 PRA details these specific initiating events using the approach defined in NEI 18-04 [7] and the ASME/ANS Advanced Non-Light Water Reactor PRA Standard [18]. The initiating events considered in the preliminary design are listed below and are followed by Table 6 which specifies the I&C system responses to each initiating event.

- Turbine Trip
- Reactor Trip
- Single Circulator Shutdown
- Loss of Both Circulators
- Loss of Steam Generator Feedwater Flow
- Loss of Offsite Power
- Control Rod Withdrawal
- Small HPB Breach
- Medium HPB Breach
- Large HPB Breach
- Steam Generator Tube Rupture
- Loss of Nuclear Island Cooling Water System
- Feedwater and Steam Line Breaks

Two initiating events, the Turbine Trip and the Control Rod Withdrawal, are further detailed below to demonstrate how I&C systems will perform in response to these events.

Table 6: Xe-100 Plant I&C System Response to Plant Transients

Design Basis Events (DBEs) (Event Sequence, Phase 1 PRA)								Trip Criteria	IPS				RPS		
DBE 1, 2, 6 Turbine/Reactor Trip	DBE 3, 4, 12 Circulator(s) Shutdown	DBE 5 Loss of Feedwater	DBE 7 Rod Withdrawal	DBE 8, 9, 10 Small, Med, Large HPB Leak	DBE 11 SG Tube Rupture	DBE 13a Steam Line Break	DBE 13b Feedwater Line Break	Parameter Name Parameter State	FW + MS Isolation with SG Dump	Turbine Bypass	Circulator Run Down	Power Reduction & Controlled SD	Control Rod Trip	Circulator Shutdown	FW + MS Isolation
		X			X		X	HPB Helium Pressure High	X		X	X	X	X	X
	X			X				HPB Helium Pressure Low	X (iso only)			X	X		
			X			X		Neutron Flux High				X	X		
			X					Reactor SUR High				X	X		
				X	X			Primary System Humidity High	X		X	X	X	X	X
			X			X		Hot (SG Inlet) He Temp. High				X	X		
		X					X	Cold (SG Outlet) He Temp. High			X	X	X	X	
		X				X	X	Mass Flow Ratio (He/H_2O) High			X	X	X	X	
X								Main Breaker Open		X		X			
X								Turbine Speed High		X		X			
X								Auxiliary Bus Frequency High / Low		X		X			

6.2 AOO Example – Turbine Trip

The turbine trip anticipated operational occurrence assumes a trip of the turbine generator on one and only one unit. Possible causes include loss of condenser vacuum, excessive shaft vibration, loss of generator load or various faults and actions of the turbine generator controls and its support systems. The plant control and protection systems (DCS, IPS and RPS) are designed so that a turbine trip on one reactor-turbine unit does not disturb or adversely affect operation of the remaining reactor-turbine units. The PEMS continuously monitors and records the parameters associated with the actions of the control and protection systems.

The event sequences for this event for the Xe-100 plant will be designed to implement the following event mitigation strategy (Reference Table 7 and Figure 26):

Sequence Number 1

The DCS will be employed to reduce reactor power to the load that the bypass valves to the condenser can handle, to compensate for the loss of turbine load and maintain the reactor at reduced power until the cause of the turbine trip is corrected. The IPS will continue to monitor the plant variables for a deviation beyond the IPS setpoints as shown in Table 2. No active function will be performed by the IPS during a turbine trip when all the plant variables are within their setpoints (i.e., feedwater pressure or temperature out of bound, helium temperature or pressure out of bound).

The DCS will ensure that the reactor power, helium circulator speed, reactor outlet temperature and SG FW flow are in proper balance during this plant transient. Main loop forced cooling will be maintained via steam bypass to the condenser and recirculation of condensate and main feedwater to the steam generator and using both or either one of the two helium circulators.

Sequence Number 2

If the normal DCS control to reduce reactor power is unsuccessful the MS temperature would rise due to the loss of turbine load, then IPS will attempt a corrective action by forcing the DCS to go to a lower plant mode. If that plant runback to reduce reactor power is also unsuccessful, the IPS will shutdown the reactor by lowering the control and shutdown rods. If the IPS does not manage to keep the plant within the RPS setpoints, the RPS system will independently trip the reactor to a shutdown state. These actions will achieve a subcritical reactor via sufficient control/shutdown rod insertion.

Following a successful reactor shutdown or trip, core heat removal will be accomplished by the circulators, main feedwater and steam systems using the turbine bypass with heat removal via the condenser. The DCS will ensure that helium circulator speed, SG feedwater flow, and steam dump demand (using the turbine bypass to the condenser) are in proper balance during this plant transient to control and maintain reactor core heat removal.

The pressure transient resulting from a Turbine Trip at full power does not reach the HPB pressure setpoint that initiates the actuation of the Primary Loop Pressure Relief System (PLPRS) safety valves; therefore, the HPB remains intact.

[[

]]^{P}

Figure 27: Turbine Trip Event Tree (AOO)

Table 7: Turbine Trip Functional Success Criteria (AOO)

ESD Pivotal Event (Event Tree Top Event)	Functional Success Criteria
[[ ]]^{P}	[[ ]]^{P}
[[ ]]^{P}	[[ ]]^{P}
[[ ]]^{P}	[[ ]]^{P}
[[ ]]^{P}	[[ ]]^{P}

ESD Pivotal Event (Event Tree Top Event)	Functional Success Criteria
[[ ]]^{P}	[[ ]]^{P}
[[ ]]^{P}	[[ ]]^{P}

Sequence Number

1 —
2 —

6.3 DBE/BDBE Example – Control Rod Withdrawal

The control rod withdraw DBE assumes a withdrawal of at least one control rod (RCS) or shutdown rod (RSS), or rod bank, on one and only one reactor plant unit that is operating at full power at the time of the initiating event. Causes include spurious rod withdrawal signals from the DCS, or human error. The plant control and protection systems (DCS, IPS and RPS) are designed so that a rod withdrawal on one reactor unit does not disturb or adversely affect operation of the remaining reactor units. The PEMS continuously monitors and records the parameters associated with the actions of the control and protection systems.

The event sequences for this event for the Xe-100 plant will be designed to implement the following event mitigation strategy (Reference Table 8 and Figure 27).

Sequence Number 1

Following a control rod withdrawal DBE during full power an increase in the Neutron Flux and/or the Hot Helium Temperature is expected.

The expected plant response to a control rod withdrawal initiating event is to:

- Achieve a reactor shutdown and subcritical reactor via sufficient control rod and/or shutdown rod insertion via the IPS (with independent control rod insertion interface from the DCS), or
- Achieve subcritical reactor via sufficient control rod and/or shutdown rod insertion via RPS (by removing power to the control rod and shutdown rod motors), or
- Manual reactor trip by an operator.

The DCS will ensure that helium circulator speed, and steam generator feedwater/steam mass flow are in proper balance during this plant transient. Specifically, core heat removal will be achieved by maintaining loop forced cooling by:

- Controlling speed in one or both helium circulators, and
- Balancing main feedwater flow and steam dump flow (using the turbine bypass to the condenser).

Sequence Number 2

For this sequence, a reactor shutdown/trip was achieved via the IPS, RPS or by operator action (in response to indications of increased reactivity, reactor power and/or hot helium temperature), however heat removal via the FW and steam system was not able to be maintained. In response, the DCS will activate the Startup/Shutdown System (SSS) to provide feed water to the steam generator for heat removal.

The IPS will continue to monitor the HPB setpoints as well as the MS flowrate to determine if sufficient flow is provided to the steam generator.

Sequence Number 3

If the SSS and/or the FW pumps do not provide sufficient flow, the IPS will perform a protective action by running down the Helium circulators and/or isolating the SG. These actions will prevent thermal shock to the steam generator and protect plant investment. During a steam generator isolation, the reactor would rely on the RCCS to remove the reactor power decay heat.

The pressure transient resulting from control rod withdrawal does not reach the Helium Pressure Boundary pressure setpoint that initiates the actuation of the PLPRS safety valves; therefore, the HPB remains intact.

[[

]]^{P}

Figure 28: Control Rod Withdraw Event Tree (DBE)

Table 8: Control Rod Withdraw Functional Success Criteria (DBE)

ESD Pivotal Event (Event Tree Top Event)	Functional Success Criteria
[[ ]]^{P}	[[ ]]^{P}
[[ ]]^{P}	[[ ]]^{P}
[[ ]]^{P}	[[ ]]^{P}
[[ ]]^{P}	[[

ESD Pivotal Event (Event Tree Top Event)	Functional Success Criteria
	]]^{P}
[[ ]]^{P}	[[ ]]^{P}

Sequence Number

1	🟨
2	🟥
3	🟪

7. Conclusions and Review Objectives

7.1 Conclusions

X energy intends to license the Xe-100 design for construction and operation using a risk-informed and performance-based approach, and has developed PDC to support both the design and licensing process and compliance with pertinent regulatory requirements of Title 10 of the CFR Parts 50 and 52. The PDC described in this report were developed using the guidance in RG 1.232, "Guidance for Developing Principal Design Criteria for Non-Light Water Reactors" [4], Regulatory Guide (RG) 1.233, "Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light Water Reactors [5]," NEI 18-04, "Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development [7]," NEI 21-07, "Technology Inclusive Guidance for Non-Light Water Reactors Safety Analysis Report: Content for Applicants Using the NEI 18-04 Methodology [8]," and Xe-100-specific PRA Safety Functions (PSFs) and design features.

X-energy has developed PDC to support the Xe-100 plant and licensing process. The Xe-100 PDC will be defined following the approach described in the Xe-100 Principal Design Criteria Licensing Topical Report [16]. The PDC listed below are specifically addressed by the Instrumentation and Controls design:

- PDC 21: Protection System Reliability and Testability
- PDC 22: Protection System Independence
- PDC 23: Protection System Failure Modes
- PDC 24: Separation of Protection & Control Systems
- PDC 25: Protection System Requirements for Reactivity Control Malfunctions

The PDC listed below (as they relate to I&C systems) will be addressed by safety analysis and further design:

- PDC 1: Quality Standards and Records
- PDC 2: Design Bases for Protection against Natural Phenomena
- PDC 3: Fire Protection
- PDC 4: Environmental and Dynamic Effects Design Bases
- PDC 10: Reactor Design
- PDC 13: Instrumentation and Controls
- PDC 15: Reactor Helium Pressure Boundary Design
- PDC 19: Control Room
- PDC 20: Protection System Functions
- PDC 26: Reactivity Control Systems
- PDC 28: Reactivity Limits
- PDC 29: Protection Against Anticipated Operational Occurrences
- PDC 63: Monitoring Fuel and Waste Storage
- PDC 64: Monitoring Radioactivity Releases

In Table 9 below, PDC 21 through 25 are addressed with specific Instrumentation and Control functions.

Table 9: I&C Design in Support of Conformance with PDC

Principal Design Criteria	Instrumentation and Controls Compliance
PDC 21 ("Protection system reliability and testability"): The protection system shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.	The RPS includes redundancy in sensor inputs, power, module, communication, equipment interface, and platform. This ensures that no single failure results in loss of the protection function, and removal from service of any component or channel does not result in loss of the required minimum redundancy. Each input module contains built-in self-test features to detect single-point failures in each channel, the FPGA logic circuits, memory configuration, and the power management logic. Use of two-out-of-four voting logic is used so that a single failure of a trip signal will not prevent an equipment actuation from occurring when required while also having one division of equipment out of service for maintenance.
PDC 22 ("Protection system independence"): The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and design basis accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.	The RPS includes four separate and redundant channels configured in such a way as to satisfy physical and electrical independence and separation requirements. The four divisions of the RPS cabinets are split between two levels in the Reactor Building, which is a Safety Rated structure that precludes natural phenomena from failing the RPS. The HW will not experience failures due to abnormal services conditions as required by RG 1.89 [11], RG 1.209 [13], and IEEE Std. 323. The RPS platform includes a level of diversity such that there are always two or more redundant components that will be able to perform Required Safety Functions, and the different components will have different attributes to sufficiently reduce the likelihood of a common cause failure (CCF). This design includes built-in equipment diversity to address potential digital CCF concerns.
PDC 23 ("Protection system failure modes"):	The RPS is a passive system that fails into a safe state upon loss of electrical power or detection of

Principal Design Criteria	Instrumentation and Controls Compliance
The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced.	adverse environmental conditions. Due to this passive design, the RPS only removes enable signals. In order for the RPS outputs to be enabled, the system requires electrical power with process inputs active, connected and within predetermined parameters, and no trip signals present that would satisfy trip logic. If internal temperatures in the RPS exceed 100C, the system will automatically trip all outputs.
PDC 24 ("Separation of protection and control systems"): The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.	The RPS is functionally independent from the control systems. The input and output cables of the RPS are routed separately from other plant cables, and no more than two channels are routed in the same conduit. Analog senor inputs to the RPS are repeated via Class 1E isolation devices from either a dedicated field component, the input of the RPS or as an RS-485 signal from the RPS communication module.
PDC 25 ("Protection system requirements for reactivity control malfunctions"): The protection system shall be designed to ensure that specified acceptable system radionuclide release design limits are not exceeded during any anticipated operational occurrence, accounting for a single malfunction of the reactivity control systems.	The RPS monitors neutron flux, helium temperature, pressure, humidity and mass flow with redundant sensors. Neutron flux and helium temperature and mass flow are important indications of reactor power. If any parameter exceeds the predefined setpoints (with respect to coincidence voting), both the shutdown and control rods are dropped into the core, including in the event of a single failure of the reactivity control system.

7.2 Review Objectives

X-energy requests review and comment on the contents of this white paper, most notably the following: 1) whether the I&C architecture is acceptable for further review and conforms to fundamental industry design principles and best practices, 2) whether functional design criteria have been established that will allow future review of the I&C systems for both safety-significant and non-safety-significant functions, 3) whether the I&C system classifications align with the philosophy of NRC RG 1.233 [5] and NEI 18-04 [7], 4) whether alignment of the I&C systems design to the regulatory framework of the NRC Design Review Guide (DRG): Instrumentation & Controls (I&C) for Non-Light Water Reactor (Non-LWR) Reviews [6] is acceptable, and 5) whether the regulatory guidance documents specified for consideration in the I&C design process are appropriate.

8. Cross References and References

8.1 Cross References and References

	Document Title Cross References: X-energy documents that may impact the content of this document. References: X-energy or other documents that will not impact the content of this document	**Document No.**	**Rev./ Date of Issuance**	**Cross Reference/ Reference**
[1]	10 CFR 50.34(a) – Contents of Applications; Technical Information	N/A	August 19, 2019	Reference
[2]	10 CFR 50.55a – Codes and Standards	N/A	October 27, 2022	Reference
[3]	10 CFR 52.47(a) – Contents of Applications; Technical Information	N/A	June 12, 2009	Reference
[4]	NRC Regulatory Guide 1.232, Developing Principal Design Criteria for Non-Light Water Reactors	N/A	0	Reference
[5]	NRC Regulatory Guide 1.233, Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light Water Reactors	N/A	0	Reference
[6]	NRC Design Review Guide (DRG): Instrumentation and Controls for Non-Light Water Reactor (Non-LWR) Reviews	N/A	February 26, 2021	Reference
[7]	NEI 18-04, Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development	N/A	1	Reference
[8]	NEI 21-07, Technology Inclusive Guidance for Non-Light Water Reactors Safety Analysis Report Content for Applicants Using the NEI 18-04 Methodology	N/A	1	Reference
[9]	NRC Regulatory Guide 1.12, Nuclear Power Plant Instrumentation for Earthquakes	N/A	3	Reference
[10]	NRC Regulatory Guide 1.53, Application of the Single-Failure Criterion to Safety Systems	N/A	2	Reference
[11]	NRC Regulatory Guide 1.89, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants	N/A	1	Reference
[12]	NRC Regulatory Guide 1.97, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants	N/A	5	Reference

[13]	NRC Regulatory Guide 1.209, Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants	N/A	0	Reference
[14]	L-2021-TOP-0019 - X-energy, LLC - Safety Evaluation of Xe-100 Topical Report: Risk-Informed Performance-Based Licensing Basis Development	ML22187A 271	2	Reference
[15]	Xe-100 Licensing Topical Report Risk-Informed Performance-Based Licensing Basis Development	001522	2	Cross Reference
[16]	Xe-100 Principal Design Criteria Licensing Topical Report	004799	1	Cross Reference
[17]	Safety Evaluation by the Office of New Reactors Licensing Topical Report (TR) 1015-18653-P (Revision 2) "Design of the Highly Integrated Protection System Platform"	ML17111A 596	2	Reference
[18]	ASME/ANS RA-S-1.4-2021, Probabilistic Risk Assessment Standard for Advanced Non-Light Water Reactor Nuclear Power Plants	N/A	2021	Reference
[19]	ANSI/ANS 2.2-2016, Earthquake Instrumentation Criteria for Nuclear Power Plants	N/A	2020	Reference
[20]	NUREG-0700, Human-System Interface Design Review Guidelines	N/A	3	Reference
[21]	NUREG-0800, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition	N/A	N/A	Reference
[22]	NEI 08-09, Cyber Security Plan for Nuclear Power Reactors	N/A	6	Reference
[23]	NEI 13-10, Cyber Security Control Assessments	N/A	7	Reference
[24]	Xe-100 Preliminary SSC Classification List	001067	3	Cross Reference