NRC Meeting on the Xe-100 Approach to Plant Control and Protection

Steve Vaughn, Licensing Engineer
Chris Crefeld, I&C Engineering Manager

February 16, 2022
Agenda

• Introductions
• Purpose and Objectives
• Xe-100 Plant Overview
• Xe-100 Required Safety Functions (RSFs)
• Overall Design Approach
  • Functional Design
    – Reactor Protection System (RPS)
    – Post Event Monitoring System (PEMS)
    – Investment Protection System (IPS)
    – Distributed Control System (DCS)
• Human System Interface
• Takeaways
Purpose and Objectives

• Purpose
  – Communicate the Xe-100 plant control and protection approach to the NRC staff prior to the formal licensing application to gather preliminary regulatory, licensing, and technical feedback.

• Objectives
  – Describe the Xe-100 Design and Required Safety Functions (RSFs)
  – Familiarize the NRC staff with the four major I&C systems and their associated functionality and interfaces
  – Discuss NEI 18-04 and the Design Review Guide (DRG) differences with DID

Note
The enclosed information is preliminary and is subject to change as the design progresses from the Preliminary through Final design phases. It is provided for planning and familiarization purposes in support of pre-application discussions.
Xe-100 Required Safety Functions (RSFs)

- The design of the Xe-100 plant follows a system engineering approach and leverages the risk-informed performance-based methodology from NEI 18-04 in developing the design and licensing bases.

Retain Radionuclides in Fuel Particles
- Control Reactivity
- Control Heat Removal
- Control Water/Steam Ingress
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 in developing the design and licensing bases.

• The Xe-100 plant Probabilistic Risk Assessment (PRA) model is used during each phase of the design process.

• The I&C design leverages the inherent stability and slow, self-regulating transient progression of the high temperature gas reactor (HTGR) core.

• Supplement the Xe-100 plant passive systems with an integrated I&C system so that no immediate operator actions are necessary to mitigate the progression of any licensing basis event (LBE).

• The Xe-100 plant design is comprised of the four major I&C integrated, yet independently functioning systems:

<table>
<thead>
<tr>
<th>System</th>
<th>Preliminary SSC Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed Control System (DCS)</td>
<td>Non-Safety Related</td>
</tr>
<tr>
<td>Investment Protection System (IPS)</td>
<td>Non-Safety Related</td>
</tr>
<tr>
<td>Post Event Monitoring System (PEMS)</td>
<td>Non-Safety Related</td>
</tr>
<tr>
<td>Reactor Protection System (RPS)</td>
<td>Safety Related</td>
</tr>
</tbody>
</table>
Plant Control & Data Acquisition System (PCDAS)

Main Control Room

DCS  IPS  RPS

PEMS

Matt Hertel
I&C Design Lead
Functional Design - RPS

- The RPS is a multichannel, isolated, safety related I&C system which monitors plant conditions and actuates protection mechanisms to prevent system transients which may result in damage to the reactor pressure boundary, the nuclear fuel, or any critical protective component which prevents radiological release.

- RPS consist of 4 channels that provide redundancy, independence, diversity, deterministic and failsafe outcomes

- The RPS is credited with mitigating DBAs and is classified as a Safety Related (SR) System.

- The RPS is a passive system by which it triggers an instant shutdown of the reactor module if two-out-of-four of the monitored parameter exceeds the allowable threshold based on the safety analysis.

- Additional RPS actions include the shutdown of the primary helium circulators, and/or closure of both the feedwater and main steam lines (isolation functions).

- The RPS utilizes an FPGA-based platform with an approved safety evaluation report (SER); does not use software or microprocessor during operation.
Reactor Protection System Architecture

Diagram showing the architecture of the Reactor Protection System with various components such as RPS Signal Conditioning, Trip Determination, RPS Voting, Priority Logic, and Actuated Equipment.
The 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.

Only data related to plant response and event analysis will be stored in the PEMS.

The PEMS has two configuration types, a module PEMS and a site PEMS. Each module PEMS is dedicated to monitoring critical parameters and protection system response status for that module.

All of the PEMS are networked together and provide monitoring plant status data through the DCS in the Main Control Room (MCR) and directly from PEMS to the Reserve Shutdown Room (RSR).

Although PEMS is considered a defense-in-depth system which provides insight into plant status and activity after an event, it is currently classified as a non-safety related with no special treatments (NST) system, based on regulatory guidance evaluated during the preliminary design phase.
Post Event Monitoring System (PEMS)

- Records plant parameters from the DCS, IPS, RPS, Radiation Monitoring System (RMS), & Seismic Monitoring System (SMS)
- Stores plant data for retrieval for post-event retrieval
- Acts as the "black box" for the plant
- Each module has its own PEMS in addition to a central Site PEMS
- Local display as well as remote display in MCR
Functional Design - IPS

- The IPS has two types of actions to correct plant transients:
  - Alarms and Runbacks (in conjunction with the DCS)
  - Component Trips (independent of the DCS; overrides any DCS actions)

- The design basis of the IPS is primarily to prevent damage to critical components during postulated transients.

- The IPS is not credited with mitigating DBAs and is classified as a non-safety-related system with no special treatment (NST).

- The IPS platform will utilize a hardened, off-the-shelf platform.
IPS Interfaces

Operational Concept: 2-Tier Graded Response

- **IPSC Alarm Setpoint + IPS Corrective Action**
  - DCS operating setpoints or configuration altered
  - DCS may recover if parameter returns to normal bounds

- **IPSC Trip Setpoint + IPS Trip Action**
  - DCS override by IPS via isolated actuator input
  - DCS must recover to lower operating state

<table>
<thead>
<tr>
<th>IPS Response Criteria</th>
<th>Nominal Setpoint</th>
<th>IPS Alarm Setpoint</th>
<th>IPS Corrective Action</th>
<th>IPS Trip Setpoint</th>
<th>IPS Trip Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPB Pressure</td>
<td>5.97 MPa</td>
<td>6.1 MPa</td>
<td>Reduce Reactor Power</td>
<td>6.2 MPa</td>
<td>Trip Circulators</td>
</tr>
<tr>
<td>Tube Bundle Outlet</td>
<td></td>
<td></td>
<td>Controlled Shutdown</td>
<td></td>
<td>Isolate FW</td>
</tr>
<tr>
<td>High</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Isolate HS</td>
</tr>
<tr>
<td>HPB Pressure</td>
<td>5.97 MPa</td>
<td>5.7 MPa</td>
<td>Reduce Reactor Power</td>
<td>5.5 MPa</td>
<td>Isolate HSS</td>
</tr>
<tr>
<td>Tube Bundle Outlet</td>
<td></td>
<td></td>
<td>Controlled Shutdown</td>
<td></td>
<td>Isolate FHS</td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Neutron Flux</td>
<td>100.0 %</td>
<td>105.0 %</td>
<td>Reduce Reactor Power</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Par. Range N.D.</td>
<td></td>
<td></td>
<td>Controlled Shutdown</td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• The DCS primary system-level operational functions include:
  – Intelligent Modular Automatic Control
    o Automatic Plant Startup Control
    o Automatic Shutdown Control
    o Automatic Medium (+/-10%) Load Step -w/o Turbine Trip
    o Automatic Large (+/-20%) Load Step -w/o Turbine Trip
  – Automatic Load Following
  – Automatic Grid-Frequency (Droop) Control
  – Load Rejection w/o Reactor or Turbine Trip
  – Recovery from a Turbine Trip w/o Reactor Trip

• The DCS will maintain the following plant process variables for desired plant operating conditions:
  – SG Inlet Temperature
  – Main Steam Pressure
  – Main Steam Temperature
  – Electrical Load

• The DCS will utilize a proven off-the-shelf Digital I&C Platform.
Human System Interface

- The Human System Interface (HSI) will consist of Operational Controls and/or Information Displays located in the MCR and RSR.

- Operator Resources in the Main Control Room are all NST:
  - Operator Display System
  - Operator Alarm System
  - Operator Procedure System
  - Hardwire Trip Panel (Reactor Scram, Helium Circulator Trip/SG isolation)

- Operator Resources in the Remote Shutdown Room including both NSR and SR systems:
  - Reactor Protection System & Displays
  - Post Event Monitoring System Displays
Defense-in-Depth: NEI 18-04 and I&C DRG

- NEI 18-04 DID Adequacy:
  - Plant Capability DID
    - Independence at each of the 5 layers of defense is sufficient
    - Risk margins against the Frequency Consequence (F-C) Target are sufficient
    - Evaluation of uncertainties
  - Programmatic DID
    - Reliability and Capability target are established
    - Special Treatments for all SR and NSRST is sufficient
  - Risk-informed Performance-based Evaluation of DID
    - Integrated Decision-making Process Panel (IDPP) actions

- Design Review Guide (DRG): I&C for Non-LWRs
  - Architecture assessment
  - Reliability
  - Robustness
Comparing NEI 18-04 and DRG I&C for Non-LWRs

Steve Vaughn
Licensing Engineer
Takeaways

• Classification of I&C systems/subsystems will continue to evolve as the PRA matures and Integrated Decision-making Process Panel (IDPP) convenes to identify I&C functions needed to provide required safety functions (RSFs) and PRA safety functions (PSFs) necessary for DID adequacy.

• The I&C architecture and platform qualification requirements will be adjusted to address PRA changes.

• Field instrumentation (e.g., sensors, actuators) will become better defined as system/component designs evolve and are finalized.

• The role of the operator during normal and transient conditions will better define operator interface requirements.

• Implementing NEI 18-04 risk-informed performance-based design and licensing concepts coincident with I&C system design and functionality will be challenging.

• The Xe-100 plant's resilient core design and unique passive safety features afford a simple, straightforward I&C design.
NEI 18-04 DID Framework


- 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

Deterministic Evaluation

- Risk insights and judgments to enhance plant capabilities
- Risk insights and judgments to enhance programmatic assurance

Plant Capability 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

Programmatic Defense-in-Depth

- 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