



Luminant



MNES
A MITSUBISHI NUCLEAR ENERGY SYSTEMS INC.

Security for US-APWR and CPNPP 3 and 4

David Lange, Senior Licensing Manager

Koji Shinomiya, Engineer

Satoshi Hanada, Engineer

Hikaru Ogasawara, Engineer

Mitsubishi Nuclear Energy Systems, Inc.



Luminant



MNES
A MITSUBISHI NUCLEAR ENERGY SYSTEMS INC.

Security for US-APWR and CPNPP 3 and 4



Luminant



Overview of Security for US-APWR and CPNPP 3 and 4

- DCD Tier 1 "Security ITAAC" => as presented separately
- DCD Tier 2 Section 13.6
 - DCD – Physical security element review
- COLA FSAR Section 13.6
 - Standard paragraph on Physical Security Plan
- Security assessment reports (Voluntary Elements)
 - High assurance evaluation (DCD and IBR in COLA)
 - Mitigative measures evaluation (DCD and IBR in COLA)
 - Cyber assurance evaluation (DCD and IBR in COLA)
- Physical Security Plan (COLA)
- Beyond DBT aircraft crash assessment (DCD)



Luminant



DCD Tier 1 "Security ITAAC"

- Planned to be updated in DCD Rev. 1 (already discussed)
- COLA will incorporate by reference (similar to other COLAs)
- Will follow Industry and NRC security task force working groups and appropriately update security ITAACs



Luminant



DCD Tier 2, Section 13.6 - "Physical Security Element Review"

- Purposes:**
 - Identify vital equipment and areas to be protected
 - Provide other physical security information
- Report basis:**
 - 10 CFR 73.55
 - NUREG 1178 Vital Equipment/Area Guidelines Study: Vital Area Committee Report
- Status and plan for identifying vital equipment and areas:**
 - DCD Rev. 0, Technical Report identified major key components and equipment to achieve hot shutdown and to avoid damage of fuel and radiological releases to public
 - DCD Rev. 1, Technical Report will expand vital equipment and area list to include all important (major) components and equipment (including piping, valve, power supply etc.) in systems that support the safety functions.
 - Updated report to be submitted with DCD Rev.1



Luminant



DCD Tier 2, Section 13.6 - "Physical Security Element Review" (cont.)

- Status and plan for providing other Tier 2 physical security information**
 - DCD Rev. 0, Technical Report provided physical security information for design certification applications per Chapter 13.6 – SRP 13.6.2 required elements
 - DCD Rev. 1, Technical Report will be updated and may provide additional physical security information (may move from safeguards Technical Report and place in Tier 2, Section 13. 6 as security-related information)
- Will follow Industry and NRC security task force working groups and appropriately update DCD**



COLA FSAR Section 13.6

- Standard paragraph
 - Will reference Physical Security Plan submitted separately
 - Will note that Physical Security Plan during construction is consistent with NEI-03-12, Appendix F (under NRC review)

- Will follow Industry and NRC security task force working groups and appropriately update COLA



Security Reports – “High Assurance Evaluation” (Voluntary Elements)

- Purpose:
 - Identify and integrate security enhancements into the US-APWR standard design to protect against the Design Basis Threat (DBT)
 - Confirm sufficiency of the design to protect against the DBT

- Report basis:
 - SRP 13.6.4 High Assurance Evaluation (Draft)
 - NEI 03-11 Guidance for the Preparation and Conduct of Force-on-Force Exercises
 - “Nuclear Power Plant Security Assessment Format & Content Guide” (partial use)

- Plan:
 - Technical Report will be prepared for reference plant (CPNPP)
 - Subsequent plants will use report with adaptations as necessary
 - Report to be submitted in support of the DCD (referred in future revision)
 - IBR in COLA



“High Assurance Evaluation” (cont.)

- Evaluation approach
 - 1) Characterize facility and site for evaluation of plant security
 - 2) Identify target sets
 - 3) Develop DBT scenarios for use in evaluation
 - 4) Develop protective strategy for US-APWR standard design
 - 5) Identify adversary and protective force timelines and pathways for each scenario
 - 6) Conduct assessments for each scenario, including peer review of assessments
 - 7) Identify and make improvements based on assessments
 - 8) Confirm sufficiency of design to protect against the DBT
 - 9) Prepare High Assurance Evaluation Report



Security Reports – “Mitigative Measures Evaluation”

(Voluntary Elements)

- Purpose:
 - Assess capability of the US-APWR to mitigate the impact of an assumed loss of large areas of the plant due to explosions or fire
- Report basis:
 - NEI 06-12, “B.5.b Phase 2 & 3 Submittal Guideline”
 - “Nuclear Power Plant Security Assessment Format & Content Guide”
 - SRP 13.6.5 Mitigative Measures Evaluation (Draft)
 - Proposed security rulemaking, 10 CFR 50.54 (hh)
- Plan:
 - Technical Report will be prepared for reference plant (CPNPP)
 - Subsequent plants will use report with adaptations as necessary
 - Report to be submitted in support of the DCD (referred in future revision)
 - IBR in COLA



“Mitigative Measures Evaluation” (cont.)

- Planned evaluation approach**
 - 1) Perform evaluation of US-APWR design
 - 2) Evaluate and identify mitigative measures for US-APWR DCD plant design for spent fuel pools, reactor core and containment
 - 3) Evaluate and identify mitigative measures for reference plant design (CPNPP)
 - 4) Identify within the Mitigative Measures Evaluation, COL implementation responsibilities in accordance with NEI-06-12
 - 5) Prepare Mitigative Measures Evaluation Report

- Will follow Industry and NRC security task force working groups and appropriately update evaluation approach**



Security Reports – “Cyber Assurance Evaluation”

(Voluntary Elements)

- Purpose:**
 - Assess the protection capability of all Critical Digital Assets (CDAs) of the nuclear plant from cyber threats

- Report basis:**
 - RG 1.152, DI&C-ISG-01, BTP7-14, DG-5022 (under consideration)
 - NEI 04-04 Cyber Security Program for Power Reactors
 - “Nuclear Power Plant Security Assessment Format & Content Guide”
 - SRP 13.6.6 Cyber Assurance Evaluation (Draft)

- Plan:**
 - Technical Report of “US-APWR Cyber Security Program” is to be submitted as a part of DCD Rev 1 (planned in August 2008)
 - COLAs will incorporate by reference for use as basis for plant implementation of cyber security.
 - ITAAC confirm software and hardware life cycle for as-built class 1E safety systems



**“Cyber Assurance Evaluation” (cont.)
(1) “US-APWR Cyber Security Program”**

- Roles and responsibilities
- Policies and procedures
- Training and awareness
- Defensive strategy
- Configuration management
- Asset retirement
- Incident response and recovery
- Periodic audit and assessment



**“Cyber Assurance Evaluation” (cont.)
(2) “Cyber Security Defensive Strategy”**

- Defensive strategy is based on levels of layers or trust levels
- The strategy relies on a defense-in-depth concept to protect digital assets
- The trust levels are applicable during the plant operation phase
- Other aspects including physical security, insider threat mitigation, and external threat mitigation are considered



“Cyber Assurance Evaluation” (cont.) (3) “Security Policy for the Development Phase”

- Cyber security applied during the development of CDAs to ensure no unintended code and change are included in the software during the development phase.
- RG 1.152 and BTP 7-14 software life cycle principles used to develop US-APWR digital safety systems
- Software life cycle for US-APWR digital safety systems
 - MELTAC Platform Basic Software
 - Safety System Digital Platform - MELTAC - (MUAP-07005)
 - Safety Application Software
 - Safety I&C System Description and Design Process (MUAP-07004)
 - Software Program Manual (MUAP-07017)
- Good industry practices, such as NEI-04-04, are adopted for non-safety digital systems



“Physical Security Plan (PSP)”

- Purpose:
 - The PSP will be submitted to the NRC as a separate licensing document for the COLA to fulfill the requirements of 10 CFR 50.34
- Report basis:
 - NEI 03-12 template, Rev.4
- Plan:
 - The PSP will include the “Training and Qualification Plan” and “Safeguard Contingency Plan”
 - The PSP for CPNPP 3 and 4 will be separate from CPNPP 1 and 2
 - CPNPP 3 and 4 will have its own protected area and security officer force



“Beyond DBT Aircraft Crash Assessment”

- Purpose:
 - Assess capability to withstand and/or mitigate specified beyond DBT aircraft crash event.

- Report basis:
 - NEI 07-13 “Methodology for Performing Aircraft Impact Assessments for New Plant Designs” (Draft – Rev. 04) that is consistent with proposed 10 CFR 52.500
 - NEI 07-13 is in the final stage of NRC approval



“Beyond DBT Aircraft Crash Assessments” (cont.)

- Plan:
 - Technical Report “Evaluation of Beyond DBT Aircraft Crash” is to be submitted to the NRC (planned for late 2008/ early 2009)
 - Main contents of Technical Report:
 - 1) Aircraft Impact Assessment of Containment and Spent Fuel Pool
 - 2) Assessment of Impact on Heat Removal Capability



**“Beyond DBT Aircraft Crash Assessments” (cont.)
(1) “Aircraft Impact Assessment of Containment
and Spent Fuel Pool (1/2)”**

- A) Assessment for Containment and Spent Fuel Pool integrity**
- This assessment is based on detailed structural analysis of the containment and the spent fuel pool walls
 - A detailed finite element model of 180-degree full-height symmetry section of the containment is constructed
 - Local failure mode “perforation” and global failure mode “plastic collapse” are considered
 - In the global “plastic collapse” analysis, strike locations will be evaluated using SGI-controlled NRC-supplied Riera force-time history



**Beyond DBT Aircraft Crash Assessments (cont.)
(1) “Aircraft Impact Assessment of Containment
and Spent Fuel Pool (2/2)”**

- B) Assessment for elevated Spent Fuel Pool integrity**
- Because MHI design employs an elevated spent fuel pool, a review of supports and walls around the elevated spent fuel pool is conducted to determine whether a detailed analysis of this area is required
 - In the event the above review show insufficient margin against failure, dynamic analysis of the impact of an aircraft on the supports for the spent fuel pool is performed
 - use the finite element model of the aircraft which is compatible with the NRC-supplied Riera force-time history, in combination with a detailed finite element model of the spent fuel pool super structure and supports
 - Analysis will account for absorption of the impact energy, and the failure configuration will include crushing and loss of material
 - Failure consequences to the spent fuel pool will be directly determined by the analysis



Beyond DBT Aircraft Crash Assessments (cont.) (2) "Assessment of Impact on Heat Removal Capability"

- A) Assessment for physical, shock and fire damage to structures containing safe shutdown equipment
 - Containment, fuel handling building, reactor building and power source building are considered
 - Detail analysis of postulated damage footprints resulting from aircraft impact on the plant's ability to maintain core cooling capability of fuel in the vessel and spent fuel pool is performed
 - i. level by level assessment for reactor building, fuel handling building and power source building considering layout drawings for each elevation showing safe shutdown equipment locations; power and control cable routing, structural details including wall thickness and reinforcing bar ratios, and fire protection features
 - ii. shock damage assessment to components within the containment
 - iii. Fire damage assessment for the containment (If the results of assessment for containment show a breach of the containment)



Summary of Security for US-APWR and CPNPP

