

Integration of Criticality Safety and the DSA

EFCOG/SAWG

Mike Thieme, David G. Abbott, Ben Baranko & Art Geis

May 2007



Objective

- ◆ **Integrate the new criticality safety program into the new safety basis methodology, developed for the Idaho Cleanup Project (ICP)**

Background

- ◆ **The new DSA methodology and Criticality Safety Program**
 - Developed and approved for use on the ICP
 - Specifically designed to facilitate the cleanup project mission
 - While maintaining conformance with the approved “safe harbor”
- ◆ **The nuclear safety organization has an aggressive schedule to implement the new methodologies in support of the ICP life-cycle baseline**

Background (cont'd)

- ◆ **ICP operates spent nuclear fuel storage and handling facilities and must reliably implement a complex set of criticality safety controls**
- ◆ **Historically, these controls were derived in numerous CSEs and directly written into Chapter 6 of the facility Safety Analysis Report (SAR). Controlled lists were used to document the multitude of approved configurations for fuel storage and handling equipment**
- ◆ **All these documents received DOE-ID approval**

Challenge

- ◆ **The development and implementation of a new strategy and methodology for nuclear and criticality safety bases is one of the keys to achieving the ICP mission**
- ◆ **During the development of the new CSEs and DSAs for the fuel storage and handling facilities, it became evident that improved tools were needed to assure timely, effective development and implementation of the new methodologies**
- ◆ **A mapping document was developed to improve the timeliness and quality of the review and approval process, and assist operations personnel in identifying and integrating the CSE controls during the implementation of revised DSAs**

Develop mapping

- ◆ Documents were developed that mapped the criticality safety evaluation (CSE) and controls into the Documented Safety Analysis (DSA), Chapters 3, 4, 5, 6, and the technical safety requirements (TSR)
- ◆ The mapping document was used to demonstrate full, effective integration of the controls derived in the CSE (DOE-STD-3007) into the DSA (DOE-STD-3009), and provide a tool for use in facilitating technical review; U.S. Department of Energy, Idaho Operations Office (DOE-ID) approval; and development of an implementation matrix

Mapping process

- ◆ **Describe the criticality scenarios in DSA, Chapter 6**
 - CSE retains the detailed hazard evaluation per DOE-STD-3007
- ◆ **Summarize the CSE hazard evaluation in DSA, Chapter 3**
 - Provides the DOE-STD-3009 framework
- ◆ **Summarize the controls from the CSE in DSA, Chapter 6**
 - Engineered = safety-Structures, Systems and Components (SSCs)
 - Administrative = Specific Administrative Controls (SACs) or those defined by Criticality Safety Program functions

Mapping process (cont'd)

- ◆ **Detail the safety SSCs and SACs in DSA, Chapter 4 (3009)**
 - Safety function
 - System description
 - Functional requirements
 - Performance criteria and system evaluation
 - Controls
- ◆ **Derive the TSR-level controls in DSA, Chapter 5 (3009)**
- ◆ **Develop the TSR-level controls in the TSR document**

Mapping Process (cont'd)

(Insert the “Horizontal Slice”)

The ICP Goals

- ◆ **Take advantage of the graded-approach designed into the new methodologies**
 - Utilize the Safety Management Program (SMP) commitment to the Criticality Safety Program (CSP)
 - Consider controls for elevation to TSR-level, using DOE-STD-1186 and 3007
 - Improve the linkage and cross-walk of controls to implementing documents
 - Present an integrated control strategy for DOE-ID consideration in the DSA approval process

Features of the Graded Approach

- ◆ **Detailed performance criteria for fuel packages and fuel casks in “contractor-approved” controlled documents**
 - DSA, Chapter 4 performance criteria at a summary level that describe fundamentals vice specifics
- ◆ **All CSE, Section 7 controls presented in a “contractor-approved” controlled document**
 - Controls identified by each CSE
 - Annotated as “TSR-level” only if selected
 - All others subject to the CSP, and implemented by procedure

Features of the Graded Approach(cont'd)

- ◆ **Criticality Safety Evaluations (CSEs) are developed per applicable standards and requirements, and include:**
 - Identification and evaluation of contingent conditions
- ◆ **A cross-walk for scenarios is developed (contingency table):**
 - Describes assumptions, barriers, limits and controls
 - Maps to parameters and contingent conditions
 - Controls are evaluated for elevation to TSR-level controls in the DSA, using the principles described in DOE-STD-1186 and DOE-STD-3009
- ◆ **Determination of controls required – Section 7 of the CSE**
 - Described in the facility-specific Chapter 6
- ◆ **TSR-level controls may be:**
 - Engineered
 - Administrative – SAC in LCO or Directed-Action format
 - Design Features

Contingency Table SAR-114 (RPT-245 R1)

Criticality Scenario	Contingency	Parameter	Controls/Barriers
CASK RECEIVING AREA			
1. Criticality resulting from heavy object drop onto a fuel-loaded cask which causes fuel damage or loss of controlled cask configuration.	Movement of heavy object over fuel loaded cask.	Geometry (Fuel Configuration/ Integrity)	Control: Failure to comply with administrative control on load path prohibiting lifting heavy objects over or near fuel-loaded casks. Barrier: Low probability that a heavy object could result in cask damage worse than analyzed for cask drop. (Robust design of cask).
	Drop of a heavy object on or near a cask resulting in significant damage to cask and contents. Drop due to failure of lift equipment or load attachment points.	Geometry (Fuel Configuration/ Integrity) Moderation	Control: The Hoisting and Rigging SMP is credited with ensuring this failure is unlikely. Barrier: Damage from drop in the facility beyond analyzed cask accident is a very low probability event. Barrier: Criticality in this event would require moderation beyond the residual quantity remaining in a drained cask, in the absence of pulverization of a substantial quantity of fuel. Barrier: Loaded casks typically remain in the cask receipt area for a limited amount of time.

Contingency Table SAR-114 (RPT-245 R1) Cont

Criticality Scenario	Contingency	Parameter	Controls/Barriers
4.A – Criticality resulting from seismic failure of cask transfer car or cask transfer car insert resulting in drop of cask and spilling or damage to fuel.	Transfer of cask in cask transfer car without seismically qualified load-supporting equipment.	Geometry (Fuel Configuration/ Integrity)	Control: Failure to comply with administrative control that fissile material must be transferred in the cask transfer car only in combinations of load-supporting equipment that have been seismically qualified. Control: Cask transfer car and insert designs are passive design features.
	Occurrence of a seismic event when fuel is in cask transfer car resulting in drop of cask and spilling or damage to fuel.	Geometry (Fuel Configuration/ Integrity)	Barrier: Damage from drop in the facility beyond analyzed cask accident is a very low probability event. (Robust design of cask). Barrier: Criticality in this event would require moderation beyond the residual quantity remaining in a drained cask, in the absence of pulverization of a substantial quantity of fuel. Barrier: Low probability that a critical system results from a spill event, i.e. sufficient fuel breakage or spilling from an overturned cask along with significant moderator presence or ingress in a geometry conducive to criticality. Barrier: Loaded casks are typically in the CTP for a limited duration.

Criticality Scenario Logic Diagram

<p>Criticality Accident (Extremely Unlikely)</p> <p>{ Accident is still extremely unlikely if contingency 1 goes from unlikely to anticipated }</p>	<p>Contingency 1 (unlikely)</p> <p>{ loss of either control makes this contingency anticipated }</p> <p>Control #1 failure (anticipated)</p> <p>{ flag this control on CSCL as requiring DOE notification before changing }</p> <p>Control #2 failure (anticipated)</p> <p>{ flag this control on CSCL as requiring DOE notification before changing }</p>	<p>A loss of contingency 1, control #1 or #2 would make the likelihood of that contingency anticipated. However, because of the depth of controls for contingency 2 (extremely unlikely), the overall likelihood of a criticality accident is still extremely unlikely. Per STD-3007-2007, TSR level controls are not required; however, DOE would be notified of changes to the control set for contingency 1.</p>
	<p>Contingency 2 (extremely unlikely)</p> <p>Control #1 failure (unlikely)</p> <p>Control #2 failure (anticipated)</p> <p>Control #3 failure (unlikely)</p> <p>Control #4 failure (anticipated)</p>	

Criticality Safety Control List (CSCL)

- ◆ CSE's that support the facility safety basis are listed in the CSCL
- ◆ Key controls and assumptions from each CSE are listed in the CSCL
- ◆ CSCL (Section 4) serves as the bridging document between the CSE and the DSA (STD-3007-07 requirement)
- ◆ CSCL is a contractor approved list
- ◆ Controls in the CSCL that have not been elevated to TSR level, but whose failure could result in a single contingency will be annotated and DOE will be informed before such controls are changed. Note – a failure of one of these controls would still result in an over all extremely unlikely contingent condition.

Elevating Criticality Controls to the TSR Level

Criticality safety controls are credited features or controls that are considered for elevation to TSR level control either as SSC or SAC when one of the following conditions is met:

1. loss of the single control under consideration could directly result in a criticality accident
2. loss of the control set could result in a criticality accident scenario whose likelihood is qualitatively judged to be $>10^{-4}$
3. active controls requiring calibration to preclude loss of the control
4. identified as uniquely important and necessary to provide for increased reliability or protect from common mode failure, to ensure double contingency,
5. general references to control philosophy (e.g., mass control or spacing control or concentration control as an overall control strategy for the process without specific quantification of individual limits).
6. provide criticality accident alarm function to notify workers when a criticality accident has occurred. This is discussed in Section 6.6 of Chapter 6 of the facility-specific DSA.

Criticality Safety Program Control Strategy

◆ Strategy

Hazard Category	Facility Designation	Control Strategy
HC2	FMF	TSR - SAC in LCO format for double contingency TSR - SAC for Detection and Alarm, if required TSR - SAC for single contingent and/or single point, common mode failure
HC2	LCF Exempt D&D	TSR – facility-specific SAC for double contingency
HC2	LCF or Exempt D&D (form and distribution – criticality is not credible)	TSR – commitment to AC 5.100.6A (identified in Chapter 5, Table 5-1
HC3	LCF (form and distribution – criticality is not credible)	TSR – SAC for inventory control to protect the HC3 status
LTHC3	Exempt	No controls required for criticality safety The radioactive material inventory is controlled to protect the hazard categorization

Criticality Safety Program Control Strategy & Link to DSA

◆ Control Strategy

- CSE controls from Section 7 documented on CSCL
- Engineered, if required are either safety SSCs (Chapter 4) or EITS (defense in depth – managed by Configuration Management SMP)
- Administrative
 - Elevated to SAC, as required
 - Per PRD-112 and TSR 100 AC 5.100.6A, if not SAC
 - Implemented via procedures
- Validated by start up readiness assessment process

Benefits of the Approach

- ◆ Meets letter of the DOE Rule, Guides, and Standards
- ◆ Applies the graded-approach, using DOE standards, ANSI/ANS-8 standards, and guidance
- ◆ Enables an effective, efficient methodology to thoughtfully consider the appropriate control strategy
- ◆ Demands consistent implementation of a robust control set embracing defense-in-depth
- ◆ Encourages a balanced approach to maintaining effective controls as conditions change
- ◆ Allows conservative response to potential upset conditions
- ◆ Facilitates review and approval

Summary

- ◆ **Criticality Safety Evaluations developed per applicable standards and requirements**
- ◆ **Scenarios and controls developed to maintain double-contingency**
- ◆ **Mapping the CSE with the DSA demonstrates compliance with safe harbor methodology**
- ◆ **Linkage between CSE and DSA via CSCL**
- ◆ **Controls include Engineered and Administrative**
- ◆ **TSR-level controls considered and selected per applicable standards**
- ◆ **Mapping enhances the review and approval process**
- ◆ **Effective implementation verified using readiness determination process**