Documented Safety Analysis

FUNCTIONAL AREA GOAL: A document that provides an adequate description of the hazards of a facility during its design, construction, operation, and eventual cleanup and the basis to prescribe operating and engineering controls through Technical Safety Requirements (TSR) or Administrative Controls (AC).

REQUIREMENTS:

- 10 CFR 830.204, Nuclear Safety Rule
- DOE-STD-1027-92, Hazard Categorization, 1992.
- DOE-STD-1104-96, Change Notice 1, Review and Approval of Nuclear Facility Safety Basis Documents (documented Safety Analyses and Technical Safety Requirements), dated May 2002.
- DOE-STD-3009-2002, Preparation Guide for U. S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses, Change Notice No. 2, April 2002.
- DOE-STD-3011-2002, Guidance for Preparation of Basis for Interim Operation (BIO) Documents, dated December 2002.
- DOE-STD-1120-2005, Integration of Environment, Safety, and Health into Facility Disposition Activities, 2005 (two volumes)
- DOE HDBK-3010-94, Airborne Release Fractions/Rates and Respirable Fractions for Nonreactor Nuclear Facilities, February 1996.
- DOE HDBK-1100-96, Chemical Process Hazard Analysis, 1996.
- DOE HDBK-1101-96, Process Safety Management for Highly Hazardous Chemicals, 1996
- DOE HDBK-1139/1-2000, Chemical Management, 2000

Performance Objective 1: Contractor Program Documentation

The documents should be clear, complete, consistent, and up-to-date.

Criteria

1. The DSA should accurately reflect current facility configurations, missions, hazards, scope of operations, and pertinent onsite and offsite conditions.

2. The DSA should be fully developed, approved, and implemented, and be consistent with the latest DOE requirements, unless the basis for deviating from these requirements can be fully justified.

3. The documents should be consistent, clearly presented, and reflected in facility directives and procedures.

4. The relationships between the DSA and other major safety management program documents (e.g., fire hazards analysis, criticality safety analysis, emergency response) should be defined and show consistencies.

5. The DSA should describe future facility life-cycle stages, missions, and operations, including deactivation and decommissioning, and explain the impact on the facility safety.

6. The hazards and controls documented in the facility DSA should be consistent with other environment, safety, and health documents for the overall protection of workers, public, and environment.

Suggested Lines of Inquiry

- Has contractor provided a documented safety analysis that can be reviewed and incorporated into the Safety Evaluation Report by the appropriate DOE Field Office?
- Does the hazard analysis process follow the guidance in DOE-STD-1027 and Chapter 3 of DOE-STD-3009-94? The reviewer is referred to the specific checklists for DOE-STD-3009-94.

- Are all processes and operations identified and clearly described?
- Have appropriate sources for criteria-based requirements, specifically DOE 420.1 and its associated implementation guides, been identified?
- Was a reasonable and complete set of criteria selected that encompasses applicable aspects of design and construction at an appropriate level?
- Is the extent and manner in which the selected criteria will be applied defined?
- Has the process by which design requirements will be developed and implemented from the selected criteria been defined?
- Are plant or process parameters that need to be monitored as part of the operation of safety systems identified and understood?
- Are required plant, process, and system responses that are required as part of the operation of safety systems identified and understood?
- Have the site characteristic assumptions common to the safety analysis that were used in prior environmental analyses and impact statements (if available) or the need to revise and update such assumptions used in facility environmental impact statements been identified or revised?
- Does the facility overview include a clear discussion of the facility's inputs, outputs, mission, scope of operations, life cycle stage, and history, including projected future uses if different?
- Is a description of the facility's structure and design basis or evaluation basis provided, including construction details, materials, dimensions, and layouts to the extent sufficient to support the hazards and accident analyses?
- Is a description of the facility's process systems and constituent components, instrumentation, controls, operating parameters, and relationships of the SSCs provided, along with a summary of the types and quantities of hazardous materials?
- Is a description of the facility's confinement systems provided?

Performance Objective 2: Contractor Program Implementation

2.1 Hazards to receptors: The hazards and risks to workers, public, and environment should be fully defined.

Criteria

1. All hazards that can have potential harm to the workers, public, and environment should be identified and analyzed, including chemical, nuclear, industrial, fire, explosion, electrical, and seismic hazards.

2. The hazard analysis should specify bounding facility hazards in terms of type, quantity, and form, and include a facility hazard classification.

3. The hazard and accident analyses should cover all activities for which approval is given and be consistent in approach with established industrial methodologies, identify preventive and mitigative features for the spectrum of events examined, and identify dominant accident scenarios.

Suggested Lines of Inquiry

- Is a recognized or agreed upon methodology used for the hazard analysis?
- Is the methodology used for the hazard analysis appropriate for the type of facility/operations and hazards present?
- Have all applicable types of hazards been addressed in the hazard analysis?
- Have all applicable release initiators been addressed?
- Have forms and quantities of all hazardous materials been identified?
- Have DBA's been identified and analyzed as appropriate?
- Are support and safety systems identified?

- Are accidents, situations, and/or modes for which a system's or structures safety function is required identified and linked to the safety analysis?
- Are both active and passive functions identified?
- Does the description clearly identify the location of the site, the location of the facility within the site, its proximity to the public and to other facilities, and identification of the point where the evaluation guideline is applied (i.e., the location of the maximally exposed off site individual)?
- Does the description clearly identify population sheltering, population location and density, and other aspects of the surrounding area to the site that relate to assessment of the protection of the health and safety of the public?
- Does the description provide the historical basis for site characteristics in meteorology, hydrology, geology, seismology, volcanology, and other natural phenomena to the extent needed for hazard and accident analyses?
- Have design basis or evaluation basis natural phenomena criteria been identified based on proven and accepted methods?
- Have sources of external accidents (e.g., nearby airports, railroads, or utilities such as natural gas lines) been clearly identified?
- Have nearby facilities impacting or impacted by the facility under evaluation been identified?
- Is the hazard identification methodology presented with regard to how the hazardous materials and energy sources were identified and inventoried, including the use of referenced information, if applicable?
- Is a summary table provided that systematically identifies the hazards by type, quantity, form, and location, including a brief summary of the major accidents or hazardous situations that have actually occurred at the facility? [Note: If classification issues preclude such specification in the main document, a classified Appendix must be provided.]
- Do the hazards and quantities identified cover all operations described in Chapter 2, Facility Description, including all modes of operation (startup, normal operation, shutdown, abnormal testing, or maintenance configurations, etc.)?
- Are the hazards and quantities identified consistent with the statements and assumptions made in the hazard and accident analysis chapter?
- Are the hazards and quantities identified consistent with the statements and assumptions made in the Fire Hazard Analysis for the facility?
- Are the hazards and quantities identified consistent with the statements and assumptions made in the Emergency Management Hazard Analysis for the facility?
- Are the quantities specified derived from credible bases (e.g., flowsheets, historical data, and operational limits) in a reasonably conservative manner?
- Are the initial and final hazard categories assigned for the hazards identified consistent with the methodology of DOE STD 1027 92, including segmentation, if employed?
- Is the hazard evaluation methodology (a) stated explicitly, (b) consistent with the safe harbor analysis methods chosen for this DSA, and (c) reasonably tailored to the type and complexity of the operations examined?
- Were facility operating personnel involved in the evaluation?
- Was available information used for the analysis (e.g., procedures, process and equipment descriptions, flowcharts) consistent with that reasonably available from the facility?
- Where holes existed in the available information, was supporting information generated (e.g., summary descriptions, drawings, and flowcharts) sufficient to provide a basic understanding of the significant operations, key parameters, and controls?
- Is a complete set of hazard evaluation worksheets/tables available to inspect? [Note: Completeness requires the following columns for each entry: a specific hazard, the accident type and cause, all associated preventive and mitigative controls, consequence and likelihood ranking estimates, and a field for comments or recommended action items.]
- Do the cumulative hazard evaluation worksheets address every hazard identified in the hazard identification summary table as well as each operation/activity described in the Facility Description Section of the DSA? Are initiating events also identified?
- Does the Fire Hazard Analysis appropriately flow forward into the DSA hazard analysis?

- Do all of the required worksheet entry columns appear to have been treated appropriately (i.e., there are no vague hazards or causes, no generic or incomplete control listings, and no comments or recommended action items)?
- Are the bases for consequence and likelihood binning qualitatively defined?
- Is the scenario binning technique applied consistently throughout the evaluation? Are consequences qualitatively assessed with and without the controls? [Note: The binning must clearly distinguish the largest consequence events to identify unique and representative scenarios for accident selection. Dismissal of physically plausible, internally initiated events due to risk or mitigated consequence criteria is inappropriate.]
- Are all of the significant aspects of the facility's operations known to the reviewer(s) and/or noted in the facility walkdowns covered by the hazard evaluation?
- Are the hazard analysis assumptions clearly presented and justified?
- Is there evidence, documented in the DSA or separately, that the hazard analysis generated action items and recommendations were assessed by facility and operations management?
- Are all of the pathways identified for uncontrolled release of large amounts of hazardous materials to the environment?
- Do the defense in depth measures identified provide reasonable and prudent prevention and mitigation for the potential environmental releases?
- Do the defense in depth measures identified provide reasonable and prudent prevention and mitigation for the potential environmental releases?
- In each accident scenario, is a basis explicitly identified for all major parameter values (e.g., values for the five factor formula defined in DOE HDBK 3010 94)?
- Is a basis explicitly identified for all major meteorological dispersion parameters?
- Are the general principles or references used for accident modeling, including any computer codes used, identified with sufficient amplifying information to clarify the bases for input and calculation?
- Is each scenario described in a clear, linear sequence (i.e., detailed, step by step explanatory text linked to any fault/event trees used)?
- Are the functions of preventive and mitigative features associated with each scenario clearly explained?
- Is documentation needed to support the scenario description (e.g., seismic damage) presented either in detail or as a summary of a cited reference?
- Is each complete scenario consistent with the hazard analysis and the rest of the DSA, and does it accurately reflect the findings of the separate studies referenced?
- Are the parameters used for calculation (a) supported by technical references and/or reasonable experience from relevant and reliable sources and (b) credible in the context of each overall scenario?
- Considered as a sum total, do the parameters used give confidence of a reasonably conservative answer?
- Is each final source term clearly specified?
- For each scenario, are unmitigated (or uncontrolled) consequences clearly identified and directly compared with the evaluation guideline to determine if the need for a safety class SSC designation exists?
- Has consideration been given to the need for an analysis of accidents beyond the design basis of the facility (see §830.204 and DOE STD 3009-94, Section 3.4.3) for outside the DSA cost benefit considerations if the consequences challenging the evaluation guideline are identified in the beyond design basis accident range? Are any such analyses sufficient to provide a perspective on potential facility vulnerabilities?
- Are the accident analysis assumptions clearly presented and justified?

Review Guidelines

- Walk down safety SSCs, checking for consistency with descriptions in the DSA.
- Check for dependence of safety systems on support systems and whether support system failure is addressed in the DSA.
- During walk-down, check for possible systems interaction during accidents. Determine the extent to which credit is taken for emergency response, and reasonableness of this response during all accident scenarios. Also determine if worker egress will invalidate assumptions about confinement and fire protection (e.g., if doors are left open).

2.2 Controls: The controls to prevent or mitigate hazards should be clearly identified.

Criteria

1. The Safety Structures, Systems, and Components (SSCs) should be identified and described consistent with the logic presented in the hazard and accident analyses.

2. Safety functions and associated design criteria for safety SSCs should be clearly defined and be consistent with the bases derived in the hazard and accident analyses.

3. Functional requirements and system evaluations should be derived from the safety functions and provide evidence that the safety functions can be performed.

4. Control of safety SSCs relevant to Technical Safety Requirements (TSR) development should be clearly identified.

5. The bases for deriving TSRs should be clearly identified in the SAR or equivalent safety documents and is consistent with the logic and assumptions presented in the hazard and safety analyses.

6. The bases for deriving safety limits, limiting control settings, limiting conditions for operation, surveillance requirements, and administrative controls should be provided.

7. Operating procedures and training should be based on the TSRs.

Suggested Lines of Inquiry

- Have appropriate safety SSC's been identified?
- Are safety functions defined for each safety structure and system?
- Have all functions required for facility safety been assigned to specific and uniquely identifiable systems or structures?
- Have the scope and boundaries of every safety system and structure been delineated?
- Have subsystems and components been associated with and defined as part of a specific safety system or structure?
- Have interfaces between safety SSC's and non-safety SSC's been identified and described?
- Has a set of functional requirements for each safety system and structure been defined?
- Are functional requirements referenced to the safety analysis?
- Do functional requirements support fulfillment of the system or structure's safety function?
- Is the identification of major controls in the defense in depth and worker safety discussions consistent with those identified in the hazard evaluation worksheets?
- Does the DSA demonstrate a coherent thought process leading to the selection of safety significant SSC and TSR commitments, and does that process focus on determining (a) the defense in depth items most important to avoiding uncontrolled releases of hazardous material, (b) those features most critical to avoiding worker fatalities or serious injuries or significant radiological or chemical exposures to workers, and (c) the associated TSRs most appropriate to ensure that these items and features are not seriously challenged and/or will likely maintain their functionality?
- Based on the defense in depth and worker safety information presented in the DSA, is the set of safety significant SSC designations and associated TSR commitments considered to be adequate?
- Does review of the basis for safety class designation indicate that all appropriate designations and associated TSR commitments have been made?
- Does each scenario whose unmitigated (or uncontrolled) consequences challenge the evaluation guideline document a coherent thought process for the selection of safety class SSCs from a candidate pool, as well as any additional TSR commitments?

Review Guidelines

- Walk down safety SSCs during facility visit, checking for consistency with descriptions in the DSA.
- Check for dependence of safety systems on support systems and whether support system failure is addressed in the DSA.
- During walk-down, check for possible systems interaction during accidents.
- Determine the extent to which credit is taken for emergency response, and reasonableness of this response during all accident scenarios. Also determine if worker egress will invalidate assumptions about confinement and fire protection (e.g., if doors are left open).
- Check for consistencies between Chapters 3, 4, and 5 of the DSA and the TSR.
- Check selected procedures against limiting conditions for operation. Does the decision on whether manual and/or automatic controls are provided reflect the results of the safety analysis?
- Have criteria based requirements been refined and successive tiers of referenced criteria?

Performance Objective 3: DOE Line Management Oversight

Line management should be committed to manage and maintain authorization basis per DOE directives.

Criteria

1. Line management should have appropriate plans and resources for developing, updating, reviewing, approving, and implementing facility authorization bases, including SER, USQ review, Operational Readiness Review, readiness review, and self-assessments.

2. DOE line management should follow responsibilities as set by DOE Order 411.1, "Safety Management Functions, Responsibilities and Authorities."

3. Line management should update DSA per DOE requirements.

4. Line management should have and maintain an authorization agreement that contains key terms and conditions under which the contractor is authorized to perform the work.

Suggested Lines of Inquiry

- Was available information used for the analysis (e.g., procedures, process and equipment descriptions, flowcharts) consistent with that reasonably available from the facility?
- Where holes existed in the available information, was supporting information generated (e.g., summary descriptions, drawings, and flowcharts) sufficient to provide a basic understanding of the significant operations, key parameters, and controls?
- Where issues require further study, a significant concern cannot be fully addressed at present, or major upgrades are planned, have appropriate interim operational control commitments been made?
- Is it clear in the authorization agreement, SER, and other AB documents annual updates will be completed?

Review Guidelines

- Review site and Headquarters funding and staffing plans relevant to developing, and updating DSA.
- Review the SER process for approving DSA and TSRs to determine the extent of the DOE staff independent review and its impact on the final documents.
- Review the annual update process for DSAs.
- Review plans for future mission changes to see how DSA updates will be addressed.