CH2M-36502-FP
Revision 0

An Enhanced Hazard Analysis Process for the Hanford Tank Farms

Prepared for the U.S. Department of Energy
Assistant Secretary for Environmental Management

Contractor for the U.S. Department of Energy
Office of River Protection under Contract DE-AC27-99RL14047

CH2MHILL
Hanford Group, Inc.

P.O. Box 1500
Richland, Washington

CH2M-36502-FP
Revision 0

An Enhanced Hazard Analysis Process for the Hanford Tank Farms

M. V. Shultz
CH2M HILL Hanford Group, Inc.

W. A. Grams
ELR Consulting Inc.

M. A. Knight
CH2M HILL Hanford Group, Inc.

Date Published
April 2008

To Be Presented at
The Nuclear Renaissance - Safety Analysis for the New Nuclear Age

Energy Facility Contractors Group (EFCOG)
Richland, WA

May 3-8, 2008

Published in
Proceedings of the 2008 Safety Analysis Workshop

Prepared for the U.S. Department of Energy
Assistant Secretary for Environmental Management

Contractor for the U.S. Department of Energy
Office of River Protection under Contract DE-AC27-99RL14047

CH2MHILL
Hanford Group, Inc.

P.O. Box 1500
Richland, Washington

Printed in the United States of America

An Enhanced Hazard Analysis Process for the Hanford Tank Farms

Milton V. Shultz
CH2M HILL Hanford Group, Inc.
P. O. Box 1500, MSN: S7-90
Richland, WA 99352
Phone: (509) 372-3740/Fax: (509) 372-2825
M_V_Jr_Milt_Shultz@rl.gov

Abstract

Key Words: Process Hazards Analysis, HAZOP, PrHA, Hazard Evaluation

CH2M HILL Hanford Group, Inc., has expanded the scope and increased the formality of process hazards analyses performed on new or modified Tank Farm facilities, designs, and processes. The CH2M HILL process hazard analysis emphasis has been altered to reflect its use as a fundamental part of the engineering and change control process instead of simply being a nuclear safety analysis tool. The scope has been expanded to include identification of accidents/events that impact the environment, or require emergency response, in addition to those with significant impact to the facility worker, the offsite, and the 100-meter receptor. Also, there is now an expectation that controls will be identified to address all types of consequences. To ensure that the process has an appropriate level of rigor and formality, a new engineering standard for process hazards analysis was created.

This paper discusses the role of process hazards analysis as an information source for not only nuclear safety, but also for the worker-safety safety management programs, emergency management, environmental programs. This paper also discusses the role of process hazards analysis in the change control process, including identifying when and how it should be applied to changes in design or process.

Introduction

CH2M HILL Hanford Group, Inc. (CH2M HILL) developed the Tank Farms Documented Safety Analysis (DSA) to comply with the requirements of 10 CFR 830, "Nuclear Safety Management"[1]. The DSA is structured according to the guidance contained in DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*[2]. When the DSA was approved it was thought that following its requirements would ensure that no events would occur with unacceptable consequences. Time has proved that we were both right and wrong. We have had no events that have exceeded DSA risk acceptance levels. What we have learned, however, is that unacceptable consequences and DSA risk acceptance levels are not one and the same. In learning this lesson, we have again discovered that with any endeavor the importance of addressing all the details.

This paper discusses the importance in addressing what is implied in the guidance for process hazards analysis contained in DOE-STD-3009-94 through reference to 29 CFR 1910.119, "Process Safety Management of Highly Hazardous Chemicals"[3]. The detail is imbedded in the Management of Change (MOC). This paper addresses how to structure process hazards analysis to support MOC within the context of a nonreactor nuclear facility.

In the Beginning

CH2M HILL developed the Tank Farms DSA, in accordance with DOE-STD-3009-94, by identifying and analyzing various hazards located in Tank Farm facilities and associated with Tank Farm processes. The hazard analysis was primarily focused on developing technical safety requirements- (TSR-) level controls to protect the public and the onsite worker. TSR level controls for the facility worker were also considered for hazards that could result in significant exposure to the effects of radiation, toxicity, fires, and explosions. This resulted in changes to designs and processes being evaluated with a focus on DSA accident levels of concern. However, this focus resulted in two problems:

- A tendency to treat each change in an isolated setting
- Limited identification of design and operational improvements that would provide additional protection for the facility worker and reduction of uncontrolled environmental releases.

The focus also resulted in limited development of information related to potentially higher frequency events with lower consequences that would be important to emergency response planning.

The Solution - CH2M HILL Process Hazards Analysis

Integrating MOC with hazard analysis requires a fundamental shift in thinking about where the process hazards analysis (PrHA) fits within the big picture of managing and performing work at Tank Farm Contractor (TFC) facilities. Instead of the hazard analysis process being a nuclear safety analysis tool that is used primarily to create and maintain a DOE-STD-3009-94 compliant DSA, the PrHA process is now part of the CH2M HILL engineering design process. The PrHA process does not replace other processes, but is instead intended to complement the design review process, job hazard analysis, as low as reasonably achievable (ALARA) work planning, as well as other existing safety management program owned processes.

The use of the term "PrHA" instead of "PHA" to denote "process hazards analysis" is taken from DOE-HDBK-1100-2004, *Chemical Process Hazards Analysis*[4]. Use of "PHA" for process hazards analysis tends to create confusion because the preliminary hazards analysis process described in MIL-STD-882, *Standard Practice for System Safety*[5], has historically been referred to as PHA.

The CH2M HILL PrHA process uses, as its basis, 29 CFR 1910.119. Two parts of this CFR are key: Process Hazards Analysis - Paragraph (e) which requires all covered facilities to have a documented PrHA that uses an approved method, and Management of Change - Paragraph (l) which requires a written program to manage changes to a facility/process, including changes to procedures. The approach to performing a PrHA is based on performance-oriented requirements so the type of analysis that best addresses a particular change may be chosen. In essence, 29 CFR 1910.119 requires ALL changes to undergo some level of review.

The CH2M HILL PrHA process is implemented through a PrHA procedure, a PrHA screening form, and a PrHA performance standard. The procedure defines the process used to determine when new, and changed TFC projects, processes, equipment, and documents requires a PrHA. In addition, when a PrHA is determined to be required, the procedure defines the standards to be used for performing the PrHA. The PrHA screening process is part of the procedure and is documented on a PrHA screening form. The form ensures implementation of key requirements of the MOC process that is similar to that defined in 29 CFR 1910.119. Guidance related to the specifics of PrHA technique selection and performance is provided in the standard. Figure 1 shows a graphical depiction of the process.

The CH2M HILL PrHA process is structured to be iterative because nearly all new projects/processes or modification of facilities/processes can be characterized in phases of activity that have progressively greater design and process detail. Changes/improvements identified during the PrHA are always best addressed as early as possible in the design/modification process. The PrHA procedure uses the following project-related terms to be consistent with DOE O 413.3A, *Program and Project Management for the Acquisition of Capital Assets*[6]:

1. Conceptual design
2. Preliminary design
3. Detailed design
4. Construction
5. Commissioning
6. Operations.

Changes in system design, process, or procedures can also have phases, but the phases are often condensed or abbreviated. In any case, the PrHA process is not considered complete until there are no further changes before startup.

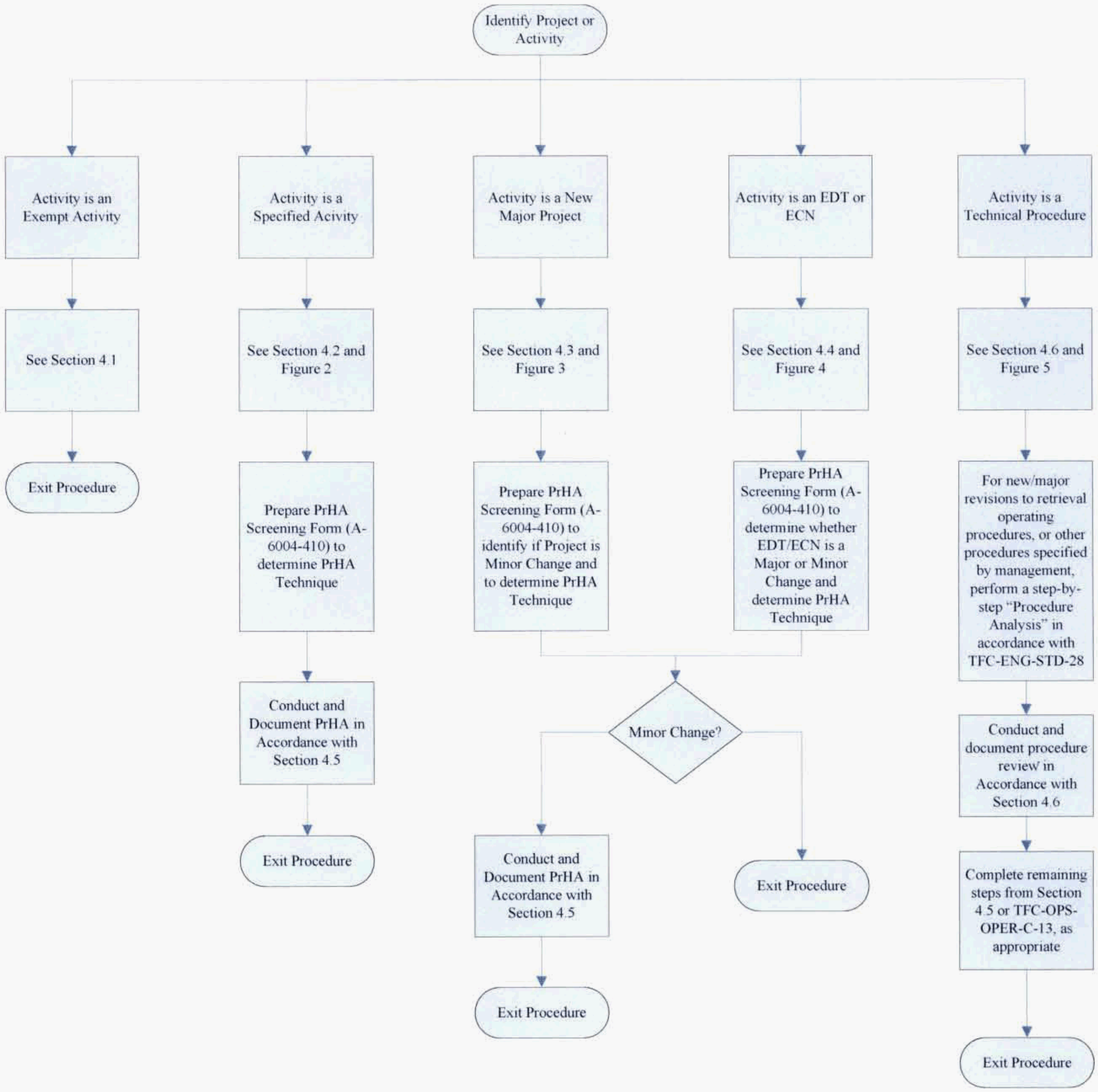

Figure 1. Overview Flowchart of Process Hazard Analysis Process.

Specifics of the PrHA Process

Hazard Identification

Information for all process chemicals, chemical reaction products, process materials, and operating conditions is required to be compiled before PrHA team meetings are held. The information is used during the team meetings to confirm or adjust assumptions about energy sources and hazardous or radioactive material. This information is also essential for the safety management programs to ensure that chemical, radiological, and industrial hazards are appropriately addressed for the protection of the facility worker and the environment.

Hazard Evaluation

The PrHA process requires a team approach to hazard analysis. The team approach is key to a successful PrHA. Furthermore, the CH2M HILL PrHA process requires that the team perform its deliberations in a meeting/workshop format. Three types of individuals are required to make up the team:

- A qualified leader
- A recorder (also referred to as a scribe or secretary)
- Subject matter experts.

All PrHA workshops are required to have a predefined quorum of individuals that must be present to ensure that the hazard evaluation process produces valid results. The quorum may include supplemental team members as deemed necessary by the PrHA Team leader and management.

The minimum quorum consists of a team leader, a recorder, and a core group of the following subject matter experts:

- Cognizant Nuclear Safety and Licensing safety analyst(s)

- Operations representative(s)

- Responsible engineer that is most knowledgeable of the design/system/activity being evaluated, for example:

  - Responsible project engineer (if a project)
  - Responsible system engineer (if what is being evaluated has one assigned)
  - Responsible process engineer

- Industrial safety/hygiene representative

- Radiation protection program representative.

The workshop meetings are structured to capture hazardous conditions representing a spectrum of accidents, as well as a spectrum of consequences and frequencies within each type of accident. The hazard evaluation team takes no credit with regard to the effects of preventive or mitigative controls such as equipment or component qualification, procedural actions, administrative requirements, or beneficial failure modes.

The evaluation team evaluates engineered protective design features that are included in the equipment or process being evaluated in two ways. Initially, the team identifies conditions taking no credit for this equipment being installed (e.g., secondary containment on a transfer line is not included in the evaluation). The team also considers the conditions of the actual design (e.g., secondary containment installed as designed) to identify the impacts of upsets based on the system as intended.

Hazard Evaluation Technique Selection

Physical Changes to Facilities/Systems/Processes

PrHAs are required to use structured and systematic approaches. Hazard evaluation techniques are selected based on the scale and phase of project or change under evaluation: The following are the categories into which CH2M HILL divides changes:

- Management Selected Projects/Modifications
- Projects
- Major Changes
- Minor Changes.

It should be noted that Minor Changes do not require a formal PrHA. However, this does not imply that no hazard analysis is performed because the normal processes that CH2M HILL uses to control work in the Tank Farms are still applied.

For new projects conducted in full accordance with DOE O 413.3A, evaluations are conducted at each stage of the project as follows.

- Conceptual Design Phase (once preliminary concept design established and process flow diagrams, process description, and waste inventory or flowsheet are available)
    - Preliminary Hazard and Operability Analysis (HAZOP)
    - What-If/Checklist
    - PHA
- Preliminary/Detailed Design Phase (once piping and instrumentation diagrams [P&ID] are developed, control logic is defined, and facility/equipment layout is established.)
    - Full HAZOP for tank waste processing, retrieval, and transfer systems
    - What-if Checklist – for simple well-defined changes, systems not suited to HAZOP, and procedures
    - Other techniques for specific systems (e.g., computer HAZOP, failure-mode effects analysis [FMEA], event tree)
- Detailed Design/Construction/Commissioning/Operations (in many cases a PrHA will have been conducted during preliminary and detailed design)

- Full HAZOP for major changes affecting multiple components/systems
- Delta HAZOP of less extensive changes (HAZOP of P&ID/drawings) focused mainly on changes and interfaces
- What-if Checklist – for simple well-defined changes, systems not suited to HAZOP, and procedures
- FMEA – for automated systems with limited human interaction

- Other techniques can be selected if the change is not appropriately evaluated by a HAZOP, What-if Checklist, or FMEA. However, approval of the technique by management is required and justification of the techniques selected is documented in the hazard evaluation report.

For new expense-funded projects and other smaller projects which do not include all the project stages specified in DOE O 413.3A, a PrHA is required before authorization of startup. However, it must be conducted sufficiently in advance to enable PrHA results to be incorporated into the process and equipment design.

- Like DOE O 413.3A-compliant projects, the exact technique to be used for new expense-funded projects and other smaller projects is established on the PrHA screening form. The normal techniques are the same:

  - Full HAZOP
  - Delta HAZOP
  - What-if Checklist
  - FMEA.

- Major changes made to new expense-funded projects and other smaller projects during construction or facility startup are also required to be evaluated.

- Other techniques for new expense-funded projects and other smaller projects may be selected if the change is not appropriately evaluated by the standard techniques. As with major projects, approval of the evaluation technique by management is required and justification of the techniques selected is documented in the PrHA report.

Changes to Procedures

It has been shown that component analysis identifies only a few human errors, whereas procedure analysis is able to reveal most human errors related to procedures, training, and ergonomics. Most significant accidents occur during non-routine operations. CH2M HILL evaluates changes to procedures through a process referred to as "Procedure Analysis." The process provides a systematic way to analyze procedures to identify potential sources of human error. Figure 2 presents a graphical depiction of the procedure analysis process.

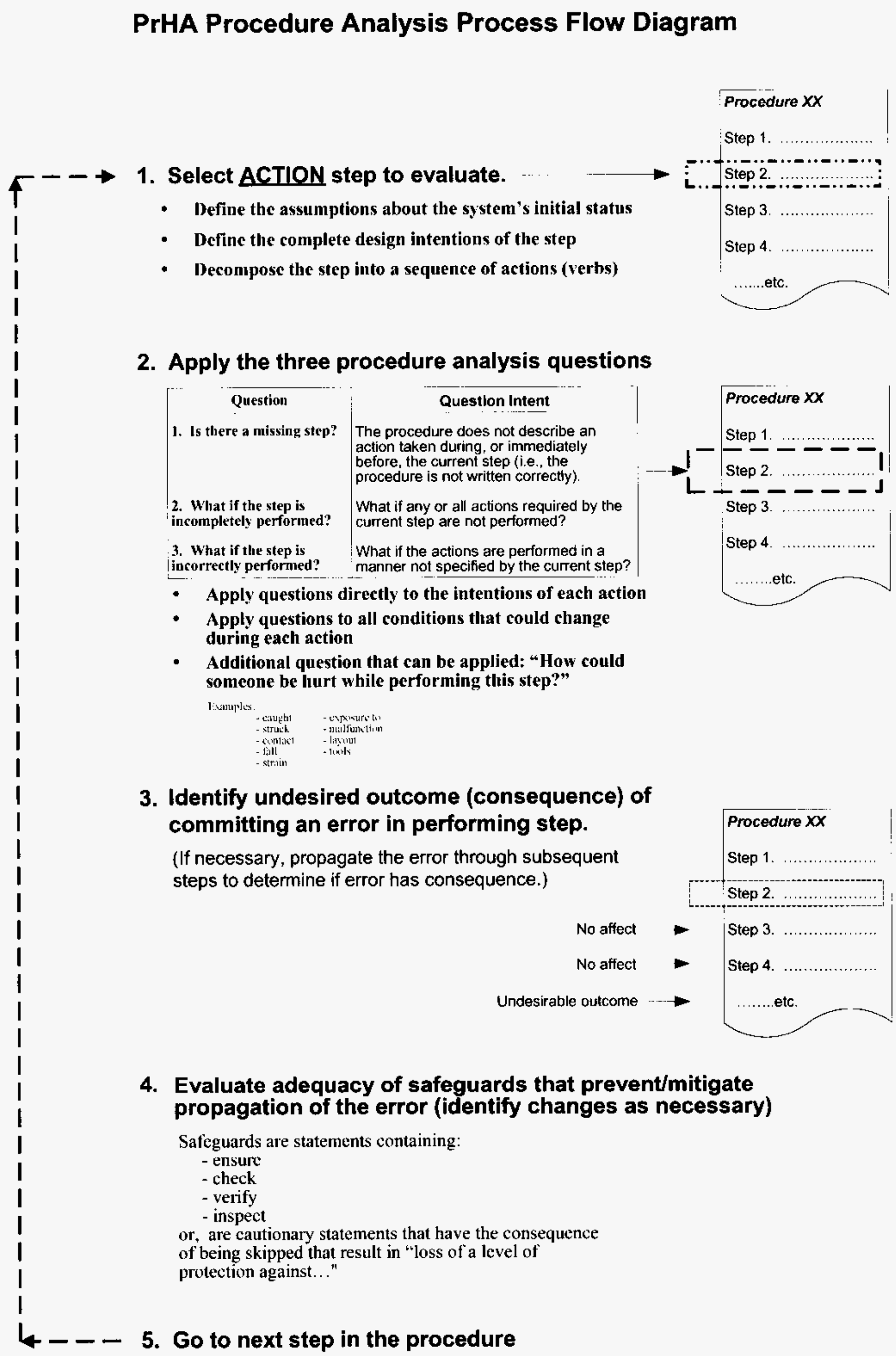

Figure 2. Procedure Analysis Process.

Procedure analysis is intended as a complement to the analysis of processes, systems, and components.

The procedure analysis process uses either guide words similar to HAZOP to review the procedure or the following What-if questions:

- Is anything missing from this step?
- What if this step (or any part of it) is not performed?
- What if the step is performed incorrectly?

The process requires minimal retraining, since it often uses the same team (or subset of the team). The technique is able to identify unique "causes" typically missed in a process PrHA, especially when humans are expected to perform special tasks only occasionally.

The process is currently focused on manual procedures such as:

- Startup and shutdown
- Emergency shutdown and restart (abnormal operating procedures)
- Commissioning/decommissioning equipment for maintenance
- Maintenance on active equipment
- Manual retrieval and transfer procedures.

Required PrHA Hazard Evaluation Study Information

The PrHA process is only as good as the design and/or process/operation information that is available to the hazard evaluation team. As noted earlier, the level of design maturity determines the availability of design, process, and operational information. The PrHA hazard analysis workshops are not held until the information has been collected. CH2M HILL requires the following the information according to different stages of a project:

- Conceptual Design

  Minimum study information:
  - Incident information related to similar equipment/systems/processes
  - Chemical/radiochemical inventory
  - Process or block flow diagram
  - Equipment performance requirements (flow, pressure, temperature, etc.)
  - Material Safety Data Sheets (MSDS) for process chemicals, working fluids
  - Process/system description (may be developed specifically for PrHA meeting)
  - Lists of existing structures, systems, and components (SSC) and TSRs.
  - Any preliminary hazard categorization or safety analysis results

- Preliminary/Detailed Design

  Minimum study information:
  - Results of prior PrHAs performed on the design

- Incident information related to similar equipment/systems/processes
- Chemical/radiochemical inventory
- P&IDs
- Equipment/facility general arrangement drawings or photographs
- Process/system description (formal description required for detailed design)
- Process Control Plan or Preliminary Control Plan (if one exists)
- Process flowsheet/material balance (if available)
- MSDS for process chemicals, working fluids
- Safety analysis results/controls and lists of existing SSCs and TSRs (if available)
- Normal process/system operating parameters
- Maximum performance specifications of procured equipment (flow, pressure, temperature, etc.)
- Valve and instrumentation data sheets (depending on design maturity)
- Preliminary/final operating procedures (if available)
- Applicable chemical reaction equations and stoichiometry for primary and important secondary or side reactions

- Design Changes

  The level of information necessary to evaluate a change to either a previously studied detail design or a proposed change to an existing/operating system is similar to the level of information required for the original full study of the system during preliminary/detail design. In addition, if a number of changes are outstanding against the key study drawings (P&IDs), it is necessary to make a preliminary update to the drawings to incorporate the changes so that representative drawing/s of the proposed system are available for study. If the outstanding changes are minor, they are marked up on the drawings prior to and during the study.

  The following information is required as a minimum:
  - Incident information related to similar equipment/systems/processes
  - Results of prior PrHAs performed on the system/equipment/process
  - Chemical/Radiochemical inventory
  - P&IDs – updated as necessary to reflect proposed final change configuration
  - Equipment/Facility General Arrangement drawings - updated as necessary to reflect proposed final change configuration
  - Normal and maximum equipment/system performance information (flow, pressure, temperature, etc.)
  - Available existing safety analysis/controls
  - Lists of existing SSCs and TSRs.
  - MSDSs for process chemicals, working fluids
  - Process Control Plan (if one exists)
  - Preliminary/final operating procedures (if available)

- Procedure Changes
  - Requires well-defined procedures
  - Requires a well-trained leader and experienced workers on the team.

Identification of Hazard Controls

A major responsibility of the PrHA hazard analysis workshop team is qualitatively identifying hazardous conditions as "acceptable" or "unacceptable." Of course, it is recognized that almost no hazardous conditions are acceptable without identification of some level of controls/safeguards.

The CH2M HILL PrHA process addresses hazard control in four ways:

1. Identification of changes in a design or process to eliminate or reduce the potential for events that impact safety or operation (including industrial accidents and environmental impacts).

2. Identification of various controls that eliminate or reduce the potential for events (existing or proposed hardware and procedures).

3. Identification of controls to protect the environment (existing or proposed hardware, procedures, and permit requirements).

4. Development of DSAs, TSRs, and preliminary documented safety analyses (requires additional evaluation and selection of controls by the Nuclear Safety and Licensing [NS&L] organization).

Actions and commitments related to existing DSA controls and non-TSR controls are required to be identified and agreed to during the hazard evaluation. Non-SSC/TSR controls developed during the hazard evaluation process are documented as they are identified, including information related to any alternatives discussed and rationale for selection and dismissal.

Control Selection Philosophy

Control selection to address radioactive and other hazardous material release events is based on the following strategy at all stages of design development:

1. Minimize hazardous material presence
2. Select SSCs over Administrative Controls
3. Select passive SSCs over active SSCs
4. Select preventative controls over mitigative controls
5. Select facility safety SSCs over personal protective equipment

6. Select controls closest to the hazard
7. Select controls that are effective for multiple hazards.

Hazard Mapping

The PrHA process does not end with the completion of the PrHA workshop meetings. The hazardous condition information developed during the meetings is evaluated to determine what impacts it has on the current hazard information contained in the DSA Hazard Analysis Database and in the Emergency Process Hazards Analysis (EPHA). This is accomplished by "mapping" each hazardous condition to a existing DSA hazardous condition and to an applicable EPHA analyzed condition. Hazardous conditions that do not "map" require further evaluation through the CH2M HILL NS&L and Emergency Management programs.

PrHA Review and Closeout Meetings

One or more PrHA review meetings are held after the initial PrHA study meetings in order to review progress of completing actions resulting from the PrHA workshop meetings and further analysis activities. Because the PrHA process tends to be iterative, more than one review meeting is often necessary.

In addition to the review meetings, a closeout meeting is required to be held before the design/process change is accepted for use. During this meeting all actions and commitments are verified as complete and closed or justification and continuing tracking is required.

Conclusion

Management of risk is necessary for a DOE contractor to meet the expectations of the customer. Developing and complying with the requirements of a DSA is only a part of what is necessary to accomplish this. CH2M HILL has implemented a process hazards analysis approach that supports the needs of all of the functions of the company that use hazard information. The needs of the DSA are met, but also the needs of environmental protection, emergency management, industrial and radiological safety, and operational excellence. The key to achieving this is twofold:

- Manage change by ensuring that ALL changes undergo the appropriate scrutiny

- Address the risks of changes through early and continuing identification of a broad spectrum of controls (design, hardware, and procedures) that address all of the consequences of concern.

References

[1]10 CFR 830, "Nuclear Safety Management," *Code of Federal Regulations*, as amended.

[2]DOE-STD-3009-94, 2006, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*, Change Notice No. 3, U.S. Department of Energy, Washington, D.C.

[3]29 CFR 1910.119, "Process Safety Management of Highly Hazardous Chemicals," *Code of Federal Regulations*, as amended.

[4]DOE-HDBK-1100-2004, 2004, *Chemical Process Hazards Analysis*, U.S. Department of Energy, Washington, D.C.

[5]MIL-STD-882, 2000, *Standard Practice for System Safety*, U.S. Department of Defense, Washington, D.C.

[6]DOE O 413.3A, 2006, *Program and Project Management for the Acquisition of Capital Assets*, U.S. Department of Energy, Washington, D.C.