

LESSONS LEARNED IN DEFINING THE ROLE OF SAFETY BASIS IN THE CONCEPTUAL DESIGN OF NEW DOE NUCLEAR FACILITIES

Scott T. Rogers, P.E.
Navarro Research and Engineering, Inc.
200 Union Blvd, Suite 215
Lakewood, CO 80228
(303) 420-3150
rogers@navarro-inc.com

Terry L. Foppe, P.E., CSP
Foppe & Associates, Inc.
9088 Hoyt Street
Westminster, CO 80021
(303) 915-8353
terryfoppe@comcast.net

Craig A. Sprain
Lookout Risk Management
PO Box 10000, PMB 203
Silverthorne, CO 80498
(303) 882-0922
csprain@aol.com

Abstract

This paper communicates some salient experience associated with the development of a Preliminary Hazards Analyses (PHA) during early conceptual design and its evolution as design progresses to support the critical decisions (CDs) of the DOE acquisition process. It also addresses the paradox between expectations for detailed control development and corresponding, appropriate degrees of design maturity. The paper directly supports the Integration of Safety and Design workshop topic, but is also relevant to Lessons Learned from the Safety Analysis Process.

The authors have been directly and indirectly involved in development of safety basis document preparation in support or conjunction with new nuclear facility conceptual design at multiple sites across the DOE complex. The authors have also informally canvassed other organizations involved in similar efforts. The work under consideration attempts to characterize some of the experience to date in meeting the expectations of appropriate integration of safety into the design process as described in DOE O 413.3, *Program and Project Management for the Acquisition of Capital Assets*. It also addresses how the PHA needs to evolve as the design matures to support development of the Preliminary Documented Safety Analysis (PDSA).

Based on experience with multiple projects and DOE sites, the authors have observed that interpretation of the DOE requirements is not uniformly understood or instituted, and consequently, the level of experience in effective implementation of safety integration in design is limited. This presents a challenge to new planned or in-design-stage facilities, particularly as the DOE attempts to develop a new DOE Technical Standard on this subject.

Organizations preparing for or engaged in new facility design processes should find the information beneficial in optimizing their efforts to provide effective support to their respective design and project management organizations and processes, and in coordinating with their DOE safety basis counterparts.

INTRODUCTION

Across the complex, we are seeing efforts to develop the next generation of nuclear facilities, as well as major modifications to existing facilities, to carry out the wide-ranging mission of the Department of Energy (DOE) and National Nuclear Security Administration (NNSA). These new facilities, which are in various stages of development include among others:

- NNSA's Pit Disassembly & Conversions Facility (PDCF), Mixed Oxide Fuel Fabrication (MOX) Facility, and Chemical & Metallurgical Research Replacement (CMRR) Laboratory
- Environmental Management's Hanford Waste Treatment Plan (WTP) and Hanford K Basins Sludge Treatment Process
- Office of Science's Physical Sciences Facility at PNNL, and
- Nuclear Energy's Advance Fuel Cycle Facility (AFCF).

In each case we desire a safety basis development process that is consistent with the regulations established under the Price Anderson Amendments Act (PAAA) as codified in 10CFR830 Subpart B. In particular, facility design criteria and identification and classification of safety systems structures and components (SSCs) must be established by the contractor and approved by DOE per the applicable requirements before major procurements and start of construction activities. However, in some cases, these determinations are needed much earlier in the design process. For new facilities, pre-approved design criteria can be found in DOE O 420.1B¹, *Facility Safety*, and its implementation guides and other relevant DOE Standards. However, during the conceptual phase, confidence in the appropriate identification and classification of SSCs is tempered with the understanding that design details, and in some cases mission details, is limited. These limitations, that make the design phase conceptual, also work against the safety basis developer who desires a clear understanding of hazards and potential consequences as early as possible in the life of the project.

This paper addresses the varying expectations for safety basis development in the early stages of a new nuclear facility. Emphasis is placed on issues associated with the development of the preliminary hazards analysis (PHA) since this analysis is typically the first documented safety basis for a new nuclear facility. The paper also addresses similar experiences with Preliminary Documented Safety Analysis (PDSA) development. We will also discuss DOE guidance on the subject as well as common and uncommon

¹ or DOE Order O 420.1A, whichever is in the DOE contract

understandings that have affected the development of these types of safety basis documents.

The safety basis experience and lessons learned discussed in this paper are based on our experience with the development of a Preliminary Hazards Analyses (PHA) for new Hazard Category (HC) 2 and 3 laboratories, PDSAs developed for major process design modifications, and canvassing individuals at a variety of DOE sites and organizations.

BACKGROUND ON DOE REGULATIONS, ORDERS AND STANDARDS

While 10CFR830, Subpart B provides the regulatory requirements for safety basis development, DOE Order 413.3, *Program and Project Management for the Acquisition of Capital Assets*, provides the requirements for the management of projects of \$20M or more. The experiences and lessons learned described in this paper are based on the application of the original version of the order from 2000 (as well as Change 1 from 2005) and implementing guidance found in the supporting DOE Manual 413.3-1, *Project Management for the Acquisition of Capital Assets*.

Note: Although DOE Order 413.3A was approved in July of 2006, this update is not yet in effect. Implementation of the updated Order is pending the issuance of DOE-STD-1189, *Integration of Safety into the Design Process*, which is currently in the DOE standards development process.

Figure 1 illustrates the DOE Acquisition Management System for major projects showing design phases and Critical Decision (CD) points. A CD is a formal determination made by DOE at a specific point in a project's development that allows the project to proceed to the next phase or CD.

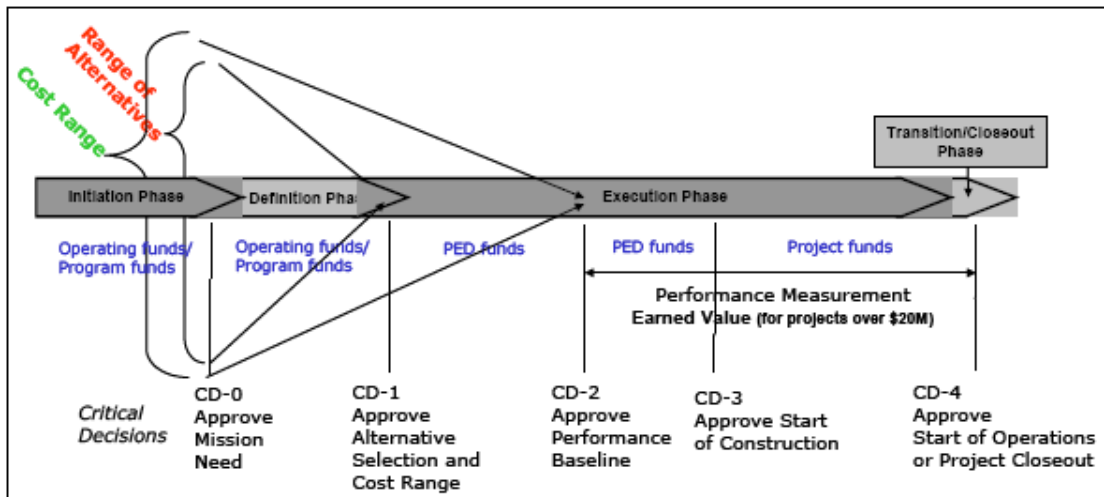


Figure 1 - DOE Acquisition Management System (from DOE M 413.3-1)

The initiation phase starts with pre-conceptual planning activities including development of the acquisition strategy and ends with DOE approval of the mission need at CD-0. The

initial phase is followed by the project definition phase where a conceptual design is developed based on consideration of a range of alternatives that would meet the approved mission need. During this phase, a preliminary hazards assessment (PHA) is also developed. While an initial cost and schedule estimate is also typically prepared at this time to support CD-1, there is still significant uncertainty in project cost at CD-1 as reflected in the Cost Range “wedge” in Figure 1.

Detailed project engineering and design (PED) starts after CD-1 approval and continues to mature through CD-3 at which point DOE approves construction. During this phase, design criteria are established and the PDSA is developed and approved such that procurement of materials and components can proceed on schedule.

The Order and Manual also describe ES&H documentation development for the various phases and CDs. For nuclear facilities, some of the safety-related specific documentation required to support CD-1 includes:

- Preliminary inventory of radioactive materials and hazardous chemicals
- Preliminary hazard categorization of the facility
- Analysis of primary facility hazards and design basis accidents (DBAs)
- Initial determination of likely Safety Class and Safety Significant SSCs

DOE regulations (10CFR830, Subpart B) also prescribe methodologies in DOE-STD-3009, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*. This standard, along with the additional guidance in DOE Guide G 421.1-2, *Implementation Guide For Use in Developing Documented Safety Analyses to Meet Subpart B of 10CFR 830*, also describes the role of the PHA in the context of PDSA and final DSA development.

Specific guidance is also provided in 10CFR830 and DOE-STD-3009 regarding the safety basis development for hazard category 3 (HC 3) facilities that allows for a “graded approach”. This approach can be summarized as:

- Basic description of the facility including SSCs
- A qualitative hazards analysis and possibly no quantitative accident analysis depending on the specific hazards and type and characteristics of radioactive and chemical inventories, and
- Hazard controls consisting at a minimum of inventory limits and safety management programs (SMPs) that are covered by Technical Safety Requirements (TSRs). No safety class SSCs are normally expected, and the need for safety significant SSCs or TSR Specific Administrative Controls (SACs) depend on the results of the hazards analysis.

Over the last twenty years and especially since the 2001, the DOE complex has put much effort into upgrading safety basis documentation for existing facilities; therefore expectations for HC 3 and HC 2 nuclear facility safety basis documents are fairly well understood. However, the expectations for safety basis development for new design projects have not been well established for the phases of a project, especially the early

phases. Therefore, the DOE has engaged in development of a new standard specific to integration of safety basis development into facility design (e.g., DOE-STD-1189) that is expected to fill this need.

Our discussion on this subject would not be complete without a brief summary of DOE guidelines on Safety Evaluation Report (SER) preparation. In the case of PDSA review and approval, there is acknowledgement of the possibility of design information being lacking at this stage of a project. The following excerpt from DOE G 421.1-2 provides guidance under these circumstances:

...it is recommended that the DOE PDSA reviewers prepare the PDSA SER based on one of the following PDSA findings/evaluations:

1. the proposed design item/system/activity is completely reviewed and found acceptable (subject to any DOE-imposed changes);
2. the proposed design item/system/activity is based on preliminary information and is accepted based on commitments to fully meet specific safety criteria in the final DSA (such as separation, redundancy, maintainability access, etc.); and,
3. the design item/system/activity is based on evolving research and/or information gathering and/or is accepted based on the preliminary information and the requirement to complete specific research before the DSA is finalized, to provide the final data in the DSA.

While it is most desirable for the DOE PDSA reviewers to make the first finding, DOE reviewers need to acknowledge the possibility and the acceptability of the other two PDSA SER findings.

While not specifically mentioned in the guide, it would appear that this approach to PDSA review and approval could also be applied to PHA development.

FROM PHA TO PDSA DEVELOPMENT

Facility hazard categorization (HC) has a significant impact on the safety basis development process. This notion is well understood by safety basis developers and project managers alike since safety basis development is viewed as one of the key factors in the ultimate cost and schedule of a nuclear facility project.

For an HC 3 facility, safety basis development can be greatly simplified relative to a complete DOE-STD-3009 DSA, as would be required for an HC 2 facility. In general, an HC 2 facility will have more safety significant and safety class SSCs based on the accident analysis results and site characteristics (e.g., site boundary, dispersion, etc.). Consequently, a lot of attention and effort is applied to the facility hazard categorization process to ensure its integrity and consistency with DOE-STD-1027-92, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports* (another standard that is prescribed by 10CFR830, Subpart B).

The hazard categorization process begins with hazard identification which is largely based on anticipated radiological and chemical inventories (a.k.a. Material-at-Risk or “MAR” values) that are consistent with the mission of the facility while also considering other hazards and energy sources that may be present that affect the rates of release of radiological and chemical materials under associated accident conditions. However when the specific details of the facility’s activities or processes are further developed in the later phases of the project, the safety analysis and hazard categorization should be re-visited to ensure appropriate control development and SSC designations.

In addition to providing a framework for the critical decisions that accompany the phases of project development, Integrated Safety Management (ISM) should be applied throughout all project phases. Especially during the early project phases, the project team has the opportunity to eliminate or minimize hazards and incorporate cost-effective accident prevention and mitigation features or strategies. In particular, DOE M 413.3-1 states that:

A fundamental premise of ISM is that accidents are preventable through early and close attention to safety, design, and operation... Safety through design is not just meeting the specified safety requirements in the design; it is the project team taking specific proactive measures regarding safety. This includes making design changes to eliminate hazards, minimize hazards, mitigate consequences, and preclude events that could release the hazard. Addressing hazards with a safety-through-design approach does not always require that systems, structures, or components be added that will prevent or mitigate the releases. Rather, it may involve removing or moving systems or changing design approaches that result in a safer facility and improved operations. It may also result in fewer safety class and safety significant controls being required in the final design.

Based on our experience, preliminary ES&H deliverables are typically documented in a facility-level PHA, which is submitted along with all other CD-1 project documentation, to DOE for approval at the conceptual development phase of the project. For the first time in the life of the new project, there is a preliminary safety basis for the facility which is based on a preliminary inventory of radioactive materials and hazardous chemicals.

The PHA and facility conceptual design at CD-1 provide the foundation for the next phase of development which includes a process-level hazards analysis and accident analysis that which support later development of the PDSA. In parallel, there are additional safety analysis documents that may need to be developed to support CD-2 and CD-3 including fire hazards analyses, emergency preparedness hazards analyses (EPHAs), security plans that address public access, siting plans that identify the nearest site boundary, and natural phenomenon hazard assessments that support SSC performance categories (PC).

As the design progresses from conceptual design through the finalization of design and PDSA, the entire project team of designers, engineers, architects, procurement personnel, and safety support personnel must collaborate and exchange information in an iterative

process so that the safety basis can be developed in a manner consistent with the CD process and to support design decisions and/or recommend viable alternatives.

A PARADOX IN THE DEVELOPMENT PROCESS

We are, therefore, left with a safety analysis development process that establishes initial and preliminary assumptions thereby defining the boundaries of the analysis that are later confirmed or revised. Although this process is well documented in DOE regulation, orders, standards and manuals, our experience has shown that certain information is often desired (yet not available) to provide conclusive safety basis determinations such as SSC designations early in the design process. While a conclusive determination is naturally desired as early as possible, the level of project definition and design in the early phases most often cannot support this. So there is a paradox between the desire for early, conclusive analysis results and the lack of specific project design information to support this analysis. Some examples of our experiences with this paradox are described in the following paragraphs:

- A hazard profile is often requested to support PHA development, which should include maximum radiological and hazardous chemical inventories (MAR) by form and location as well as energy sources, to support PHA development. This profile is critical to the initial and final hazard categorizations, and demonstration of DOE-STD-1027 compliance. The paradox in this case is that the PED phase has not started and layout of the facility has often not been established such that providing a precise location or locations for MAR can be established.
- During conceptual design, critical decisions on public access and control may not have been made for alternatives being evaluated. This is often the case when facility siting has not yet been determined due to pending NEPA decisions. Without an understanding of access and a distance to the facility site boundary, on-site and offsite consequences can not be analyzed in a precise manner. A conservative approach to PHA development in this case may result in the assumption of a short site boundary distance that translates into the apparent need for safety class SSCs. This would be the case for HC 2 facilities as well as HC 3 when there is a potential for “challenging” the 25 rem offsite Evaluation Guideline from DOE-STD-3009 due primarily to the differences in dispersion assumptions between hazard categorization methodology and safety class SSC determination methods.
- During conceptual design development leading up to CD-1, applicable industry codes and standards are often not identified. Since this determination can have a significant impact on cost and schedule of the project, and the DOE complex has many older facilities that are not compliant with newer codes and standards, there is typically significant interest in having a complete listing as early as possible. The paradox in this case is that by providing a detailed listing before the PED process, we appear to have made presumptions regarding the final design that can become expectations at later CD points. Consequently, we are at risk of having a

list of codes and standards that drive the PED process (rather than PED determining codes and standards based on the ISM and safety analysis process). This approach can also lead to conflict with ISM in that the project team does not seek reduction or elimination of hazards as the project progresses. Rather the project team ends up evaluating unrealistically high MAR quantities that then appear to require more safety SSCs.

- Another similar challenge that is essentially omnipresent is balancing the need for a preliminary NPH performance categorization with the conceptual maturity of design at CD-1. From the design authority perspective, early identification of the facility's seismic performance category and corresponding safety designation provides obvious and distinct advantages. These determinations are most often delegated to the safety basis experts. Making those determinations and assignments during the "Definition Phase" of design development from the safety basis perspective in most cases must be tentative. At this stage of design development, there is generally no specificity in many areas of the design such as the layout of the facility and parameters regarding magnitude and distribution of many of the operational hazards have not matured to the extent that a definitive determination for performance category or safety SSCs is possible.
- During the early project phases, there is also lack of design information important to PDSA development especially the specificity necessary to understand and document safety functions and how safety class and safety significant SSC functional requirements will be met. Safety SSC evaluations, which document how the functional requirements are met, provide the assurance that the safety functions will be provided under all credible accident conditions when they have been assumed to be functional with respect to specific performance criteria and standards. However, it may not be until the final design, and after PDSA approval, that assurance is provided that safety SSCs will meet the functional requirements. Since it is possible that the final design may establish new or revised operational requirements that affect the performance of safety SSCs, it is important to maintain a cohesive project team to ensure the necessary iterations between the safety basis development and project design even after PDSA approval and procurement of components and materials has begun.
- While much attention is paid to internal project specifics including facility hazard categorization, consideration also should be given to other concurrent activities and associated hazards that are not within the scope of the project. For a one-time, limited-life process, one approach is to establish an "initial condition" that there will be no concurrent facility processing operations and associated nuclear material inventories that are not evaluated in the project's safety basis. This assumption is critical and needs to be supported by a planned TSR level administrative control (SAC) to prohibit concurrent nuclear operations. Alternatively, concurrent activities could be evaluated by revising the hazard identification, hazard evaluation, accident analysis, and control allocations of the existing facility safety basis, considering interactive accident scenarios and identification of any additional controls, and address the interfaces between the project and existing facility safety basis documents.

- The design of a new facility (and in some cases a major modification to an existing) should specifically address existing site-wide or facility specific-exemptions to DOE Orders as well as industry codes and standards. Even though not considered as part of the project scope, re-visiting existing exemptions during the PED phase is important to timely determination whether upgrading may be required to comply with the current requirement and standards. This consideration also applies to consent orders or agreements with other regulatory agencies that affect the project.
- Another often ignored consideration is to specifically identify "Equipment Important to Safety" that are not safety class or safety significant SSCs at the appropriate design phase. This category of equipment is of interest to properly evaluate proposed changes through the Unreviewed Safety Question program. ITS equipment are non-safety class and non-safety significant SSCs that are generally those identified on the qualitative hazard evaluation tables for the PDSA/DSA identified to prevent or mitigate hazardous conditions that may have more than negligible or minor consequences, or are specifically identified in a DOE SER. The usual expectation is that this will be accomplished during the final DSA development.
- While many DOE sites already have mature 10CFR830 safety basis programs, these programs are largely based on experience with facilities that existed prior to 2000. For a new facility design, however, existing hazard analysis, accident analysis and control development methods may not be adequate. In particular, the design basis accidents (DBAs) for a new facility are evaluated for the primary purpose of precluding (by design) significant onsite or offsite consequences. This process results in the identification of safety SSCs that would prevent single-point failures, provide for redundancy and reliability, and establish adequate separation distance.

It is clear that safety basis development in the design process represents a number of challenges that are not immediately evident. Even for senior safety analysts who have substantial experience in developing, reviewing and implementation of 10CFR830 compliant DSAs for existing facilities, new nuclear facilities (and major process modifications) represent opportunity for optimization of safety in the development of their design. By capitalizing on this opportunity, we can ensure sound choices and designations of safety related equipment are made with the added benefit of minimizing operational limitations that can result from cumbersome administrative controls while reducing operational costs. Clearly there should be a recognition of the value that a mutual and collaborative effort between design and safety basis considerations, not only in terms of cost, but also in terms of efficiency and utility of the new facility or modification.

CONCLUSION

In both our first-hand experience and in discussions with others responsible for safety basis development, it is apparent that there is not yet a consensus on how to effectively integrate the safety basis development process into new facility designs in a manner that minimizes the risk to the public, non-involved workers, and the environment that also meets the project management goals of minimizing cost and schedule while fully carrying out the mission need. From our perspective, we anxiously await the outcome of DOE-STD-1189 development for any clarification it may provide in further defining this process. We also encourage safety analysts, design authorities, and other design project support personnel to enthusiastically participate in the DOE review process for the DOE-STD-1189.