

This document was prepared in conjunction with work accomplished under Contract No. DE-AC09-96SR18500 with the U.S. Department of Energy.

This work was prepared under an agreement with and funded by the U.S. Government. Neither the U. S. Government or its employees, nor any of its contractors, subcontractors or their employees, makes any express or implied: 1. warranty or assumes any legal liability for the accuracy, completeness, or for the use or results of such use of any information, product, or process disclosed; or 2. representation that such use or results of such use would not infringe privately owned rights; or 3. endorsement or recommendation of any specifically identified commercial product, process, or service. Any views and opinions of authors expressed in this work do not necessarily state or reflect those of the United States Government, or its contractors, or subcontractors.

Synthesis of Safety Analysis and Fire Hazard Analysis Methodologies

D. Allan Coutts, Ph.D., FSFPE
Andrew M. Vincent, III
Washington Group International, Savannah River Site
2131 S. Centennial Drive, Aiken, SC, 29803
(803) 502-9811, Fax (803) 502-2811
allan.coutts@wsms.com

Abstract

Successful implementation of both the nuclear safety program and fire protection program is best accomplished using a coordinated process that relies on sound technical approaches. When systematically prepared, the documented safety analysis (DSA) and fire hazard analysis (FHA) can present a consistent technical basis that streamlines implementation. If not coordinated, the DSA and FHA can present inconsistent conclusions, which can create unnecessary confusion and can promulgate a negative safety perception. This paper will compare the scope, purpose, and analysis techniques for DSAs and FHAs. It will also consolidate several lessons-learned papers on this topic, which were prepared in the 1990s.

Introduction

During the 1990s DOE nuclear facilities transitioned to DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analysis*,¹ compliant safety analyses. This transition helped DOE and its operating contractors to better understand the fire risk in Nuclear Facilities. This lesson was documented in a 1999 EFCOG paper² and a DOE Fire Protection Workshop presentation.³ As a follow-on to this work, the DOE community developed a white paper titled *Synthesis of SAR and FHA Methodologies*.⁴ This white paper addressed the perception that requirements for preparing Documented Safety Analysis Reports (DSAs) and Fire Hazards Analyses (FHAs) are inherently incompatible. Unfortunately, significant effort continues to be expended resolving confusion over seemingly conflicting methodologies, perceived redundant documentation, and supposedly contradictory conclusions between DSAs and FHAs.

Since the publication of the 1999 papers 10 CFR 830, *Nuclear Safety Management*⁵; and 10 CFR 851, *Worker Safety and Health Program*⁶; and DOE-HDBK-1163-2003, *Integration of Multiple Hazard Analysis Requirements and Activities*⁷, have been issued. This paper will review the requirements in 10 CFR 830 and 10 CFR 851, and the recommendations in the handbook. In addition, since most of the applicable orders, standards, and guides have been revised, this paper will review the updated requirements associated with FHAs and DSAs, suggest what

expectations should exist for document consistency, and suggest techniques to avoid actual inconsistencies.

Requirement Review

Regulation 10 CFR 830 applies to all DOE Hazard Category 1, 2, and 3 Nuclear Facilities. The basic requirement is work must be performed in accordance with a safety basis that includes “hazard controls that ensure adequate protection of workers, the public, and the environment.”⁵ DOE Order 420.1B, *Facility Safety*,⁸ clarifies that the DSA focus is on protection “from nuclear hazards.” The safety basis must:⁵

1. Define the scope of the work to be performed
2. Identify and analyze the hazards associated with the work
3. Categorize the facility consistent with DOE-STD-1027-92⁹
4. Document the safety analysis for the facility
5. Establish the hazard controls* upon which the contractor will rely to ensure adequate protection of workers, the public, and the environment

Regulation 10 CFR 851 applies to all DOE Facilities. The basic requirements are⁶:

(a) Contractors must implement a comprehensive fire safety and emergency response program to protect workers commensurate with the nature of the work that is performed. This includes appropriate facility and site-wide fire protection, fire alarm notification and egress features, and access to a fully staffed, trained, and equipped emergency response organization that is capable of responding in a timely and effective manner to site emergencies.

(b) An acceptable fire protection program must include those fire protection criteria and procedures, analyses, hardware and systems, apparatus and equipment, and personnel that would comprehensively ensure that the objective in paragraph (a) of this section is met. This includes meeting applicable building codes and National Fire Protection Association codes and standards.

The implementation guide for 10 CFR 851¹⁰ cites two DOE documents related to fire protection:[†]

DOE-STD-1066-1999, *Fire Protection Design Criteria*¹¹

* As used in this paper the term control is used in the most general sense. It indicates a feature, system, or program that will reduce risk. It does not imply that the feature, system or program is credited as part of a safety basis, unless used in conjunction with the terms SS, SC or credited.

† Updated to the most recent edition.

DOE G 440.1-5, *Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program*¹²

Standard DOE-STD-1066-1999 does not specify the required contents of an FHA, but rather provides permissive language permitting the FHA to clarify the minimum design criteria for a project or facility.

DOE Guide 440.1-5 indicates multiple items that are to be covered in an FHA. Key items that define the overall scope of the FHA are:

- “To comprehensively and qualitatively assess the risk from fire within individual fire areas in a DOE facility” and document if the DOE fire safety objectives are met.
- “The focus of the FHA should be the individual fire areas* that comprise the facility.”

The fire protection objectives referred to in DOE Guide 440.1-5 are documented in DOE Order 420.1B and DOE Order 440.1A, *Worker Protection Management for DOE Federal and Contractor Employees*.¹³ The 420.1B requirement is to minimize the potential for:

1. Occurrence of a fire or related event;
2. Fires that cause an unacceptable onsite or offsite release of hazardous or radiological material that could impact the health and safety of employees, the public, or the environment;
3. Unacceptable interruption of vital DOE programs as a result of fire and related hazards;
4. Property loss from fire exceeding limits established by DOE; and
5. Fire damage to critical process controls and safety class systems structures and components (as documented by appropriate safety analysis).

In addition to establishing the fire protection objectives, DOE Order 420.1B establishes facility and programmatic safety requirements for both fire and nuclear safety programs. This order requires that FHA conclusions be incorporated in the DSA and be considered in selecting the design basis and beyond design basis events. It also requires that the FHA must be revised when changed to the annual DSA update impact the contents of the FHA.

The 440.1A fire protection requirement is to establish “a comprehensive fire protection program with the objective of providing an acceptable level of safety from fire and related hazards for DOE contractor personnel and for the public.”

In FY2001, the joint DOE/EFCOG Chemical Safety Topical Committee (CSTC) formed a team to evaluate approaches to integrate hazard analysis activities with overlapping scopes. The effort

* For DOE facilities a fire area is defined as a location bounded by fire-rated construction, having a minimum fire resistance rating of 2 hours, with openings protected by equivalently-rated fire doors, dampers or penetration seals.

included preparation of DOE-HDBK-1163-2003.⁷ A key observation in this handbook is that “FHAs should be coordinated and integrated through teaming of fire safety personnel with hazard/accident analysts, and any conflicts related to FHAs and DSAs should be resolved prior to the approval of the DSA.”

Key considerations established in the DOE orders, guides and handbooks related to coordinating FHA and DSA content include:

- The FHA conclusions should be incorporated in the DSA accident analysis and integrated into design basis and beyond design basis accident conditions.^{8,12}
- The FHA should include an inventory of all safety class systems, coupled with an evaluation of fire-related failure modes.¹²
- FHAs and DSAs should be integrated to ensure consistency of assumptions, consequences, design considerations, and other controls.⁷

Comparison of the Nuclear Safety and Fire Protection Program Goals*

The Society of Fire Protection Engineers (SFPE) recently updated the *SFPE Engineering Guide to Performance-Based Fire Protection Analysis*.¹⁴ This guide provides a comprehensive methodology that allows project goals to be refined into stakeholder objectives, design objectives and quantified performance criteria. The concepts presented in this guide will be used to demonstrate that all of the goals addressed by the DSA are included in the FHA and that the FHA must address additional goals.

Table 1 presents the DOE objectives restated as goals for the nuclear safety and fire protection programs.[†] The second goal in the fire protection program is the same as the nuclear safety program goal. The first fire protection goal (minimize the potential for fire or related event) is consistent with the nuclear safety goal. Often the controls (e.g., hot work programs) instituted to implement this goal are credited in the DSA. When this occurs, some review mechanism must exist (e.g., a formal USQ process) to ensure that changes to the fire protection program will not compromise the DSA conclusions.

The fifth fire protection program goal is consistent with the nuclear safety program goal, however there can be instances where minimizing the potential for fire damage to safety class systems is in excess of the nuclear safety program goals. An example of this would be an interlock that is only required during a process upset event (i.e., a non-fire event). If the process-upset event and any fire accident were independent, then the DSA would not require the interlock be protected from fire. Fire protection goal 5 would require some level of fire protection. This level of protection should be graded to reflect the importance to safety, the cost of protection, and the cost of replacement. Thus, there will be cases where potential for fire.

* Much of this section is excerpted from the earlier paper⁴ with minor editorial updates.

† As used in DOE vernacular the term “objectives” is interchangeable with the SFPE vernacular for “goals”.

Table 1.—Comparison of Nuclear Safety and Fire Protection Goals, Objectives and Sample Performance Criteria.

Goal	Stakeholder Objective	Sample Design Objective	Sample Performance Criteria
Nuclear Safety Program			
DOE non-reactor nuclear facilities are to be “designed and constructed so as to assure adequate protection for the public, workers, and the environment from nuclear hazards.”	No significant release of hazardous or radiological material	Limit the off-site doses to avoid deaths	Off-site: 25 rem
Fire Protection Program			
(1) minimize the potential for the occurrence of a fire or related event;	Minimize the number of unwanted fires	Establish a comprehensive fire protection program that includes the controls of combustibles and ignitions sources	Establish a comprehensive fire protection program that includes the controls of combustibles and ignitions sources
(2) minimize the potential for a fire that causes an unacceptable on-site or off-site release of hazardous or radiological material that will threaten the health and safety of employees, the public or the environment	No significant release of hazardous or radiological material	Usually coordinated with DSA design objectives for radiological releases.	Usually coordinated with DSA design objectives for radiological releases.
(3) minimize the potential for vital DOE programs suffering unacceptable interruptions as a result of fire and related hazards	No vital programs shall suffer an interruption greater than 6 months	Customized for individual program.	Customized for individual program.
(4) minimize the potential for property losses from a fire and related events exceeding defined limits established by DOE	Limit most fire losses to \$1 million	Prevent flashover in the room of origin for any large structure.	Properties with greater than 5,000 sq. ft. shall have automatic suppression
	Limit the maximum possible fire loss to \$50 million	Properties with a fire loss potential greater than \$1 million shall have automatic suppression	Properties with a fire loss potential greater than \$1 million shall have automatic suppression
	Limit the maximum possible fire loss to \$150 million	Properties with a fire loss potential greater than \$50 million shall be subdivided with fire walls and provided automatic suppression.	Provide freestanding 3-hour fire walls to limit the MPFL to \$50 million and automatic suppression [DOE G 440.1-5 & DOE-STD-1066-99]
		Properties with a fire loss potential greater than \$150 million shall be subdivided with robust fire walls and provided automatic suppression.	Provide freestanding 3-hour fire walls to limit the MPFL to \$150 million and automatic suppression [DOE-STD-1066-99]
(5) minimize the potential for critical process controls and safety class systems being damaged as a result of a fire and related events.	Customized for individual program.	Customized for individual program.	Customized for individual program.

damage to safety class systems is deemed acceptable. In such cases both the FHA and DSA should reflect this decision. The two remaining fire protection goals (mission continuity and monetary loss protection) are separate from the nuclear safety goal. Often the fire protection features required to accomplish these goals will reduce the nuclear safety risk. When the fire protection features are identified in the DSA as Safety Class or Safety Significant (SC/SS), the fire protection and nuclear safety programs are perceived as consistent. When a feature is not designated as SC/SS, there is sometimes the mistaken impression that the DSA and FHA are inconsistent. Not every control that reduces the nuclear safety risk to the public need be safety class, nor every control protecting workers need be safety significant. SS/SC controls are those that are judged mandatory to reduce the nuclear safety risk to an acceptable level. In addition to SS/SC controls, DOE requires the identification of Defense in Depth (DiD) items, which are considered additional controls that further reduce the nuclear safety risk. Where the FHA identifies a need for protective controls that the DSA does not designate as SS/SC, those controls are good candidates for DiD items. If such an item is not DiD, then it can usually be attributed to the third or fourth fire protection goal.

Comparison of the DSA and FHA Methodologies*

DSAs are the cornerstone of the safety basis for most Hazard Category 2 and 3 Nuclear Facilities in the DOE complex.[†] New DSAs are prepared to meet 10 CFR 830 using the methods described in DOE-STD-3009-94 which are similar to overall process used in preparing an FHA. In preparing a 3009-style DSA a multi-step analytical process is commonly used. The steps in this process are:

- Hazard identification that defines inventories of hazardous material and assesses the Facility Hazard Classification,
- Hazard evaluation that comprehensively characterizes hazards, qualitatively evaluates hazards, and identifies important equipment and administrative controls, and
- Accident analysis that quantitatively analyzes accidents of significant concern.
- Functional classification that ranks the importance of engineered controls (i.e., Systems, Structures and Components), which maintain facility safety.
- Controls selection that establishes the operating limits and programmatic requirements, which maintain facility safety.

An FHA uses a similar logic and starts with hazard identification, however in most instances the remaining steps are accomplished by a demonstration that the facility (both engineered features and administrative programs) is in compliance with the applicable codes (typically the *National*

* Much of this section is excerpted from the earlier paper⁴ with minor editorial updates.

[†] The safe harbor standard for preparation of DOE Hazard Category 1 facilities is not DOE-STD-3009-94, thus to simplify the remainder of this paper, Hazard Category 1 facilities will not be discussed further.

Fire Codes®), the prescriptive portions of the DOE fire protection orders^{8,13}, guides¹², standards¹¹, and the DOE objectives^{8,13}. In some facilities the FHA has contained the accident analysis using the DSA methodology. When code compliance approach is used, the generic analysis and control selection process used by the technical committee preparing the code, is assumed to be applicable. The use of generic analysis and controls (e.g., *The National Fire Codes*®) often leads to the misconception that the DSA and FHA methodologies are incompatible. When this occurs, the analytical methods must be evaluated. Sometimes the generic methods introduce controls that are not applicable to the situations normally found in nuclear facilities. Also the DSA efforts could be neglecting objectives or hazards that the FHA must address.

Addressing Perceptions*

◆**Duplicate Effort** - Both DSAs and FHAs are required to describe a broad spectrum of facility attributes. Examples include; site characteristics, facility description, process equipment and operations, hazards, damage potential, safety features and emergency preparedness, among other facets. Doing so in both documents is unnecessarily redundant. DOE requirements and expectations could be met by a comprehensive description in one document, with a summary description in the other.

◆**Prescriptive Fire Protection Requirements** - There is a perception that the FHA criteria in DOE directives precludes the use of analytical approaches based on probabilistic methodologies, fire modeling, and other performance-based techniques. While it is true that DOE Guide 420-5 directs that the risks from fire be qualitatively assessed for each fire area, it does not proscribe (i.e., prohibit) the use of probability and statistics as well as validated fire models in the ranking or description of fire scenarios within given areas. However, these analytical tools are subject to widely varying results depending the nature of the underlying assumptions, and DOE has had limited success in using these approaches. Thus, the selection of the most appropriate fire protection for given fire area must based on established design criteria as tempered by the judgment and experience of qualified fire protection engineers.

◆**Conflicting Controls** - The conclusions of a DSA are often perceived to be at odds with those of the corresponding FHA. In fact, it is not uncommon for a DSA to conclude that fire protection features are not needed to mitigate the consequences of bounding fires. While, under the same circumstances, the FHA will conclude that the same fire protection features are required. The following paragraphs demonstrate several reasons why these discrepancies sometimes occur.

◆**Differing Paradigms** – As stated previously, the primary goal of the DSA is to identify and justify an adequate set of controls for nuclear safety. Thus, the nuclear safety analysts must ensure that the analysis and controls can be successfully implemented as Technical Safety Requirements (TSRs) and Operational Safety Requirements (OSRs). The formality in the use and implementation of these documents, sometimes limits the types of controls that can be successfully credited. The DOE fire protection program has historically been based on best

* This section was called Issues in the earlier paper⁴, items that came from the earlier paper are marked with the symbol ◆.

industrial and insurance practices (Highly Protected Risk). These practices have been developed over the past 100 years and have been demonstrated to achieve the desired reduction in fire risk. Unfortunately, the formality required of nuclear safety programs is sometimes lacking, and thus duplicate protective features, or differing assumptions can occur.

◆The Small Fire – The accidents that are explicitly analyzed in most DSAs are severe and most of the effort is focused on demonstrating that the potential consequences for the most severe events are acceptably low. In most facilities, the most severe fires will be at frequencies below $1.0E-03/\text{yr}$, often approaching $1.0E-06/\text{yr}$. Since an incipient fire frequency in most nuclear facilities ranges from 0.1 to $1/\text{yr}$, it is possible that the overall fire risk (worker, monetary, mission, etc.) is dominated by the high frequency fires, rather than the very severe fires that are typically presented in the DSA. Thus, the fire protection program may require additional controls, not needed to achieve the appropriate nuclear safety risk as defined by the evaluation criterion in DOE-STD-3009-94.

◆Independence – As with most engineering efforts there is considerable flexibility in selecting the “best” approach. The definition of “best” includes such non-technical realities as limited budget, tight schedules, and available resources (e.g., people). Thus, the DSA and FHA can develop alternate controls strictly because they selected alternate approaches. This promotes the misconception that the FHA and DSA are not compatible. The correct interpretation is that the two documents should be coordinated in their development and their update schedules.

Recommendations*

◆Prior to the development of a DSA and FHA for a given facility, the (DOE and contractor) stakeholders should be clearly defined and then meet to define mutually acceptable assumptions, methodologies, formatting, etc. and to establish a mechanism for the timely resolution of disputes.

◆The schedule for the development of the DSA and FHA should be mutually compatible such that the FHA can be treated as an input to the DSA.

◆The selection of controls to reduce nuclear safety and other fire risks should be coordinated to ensure that the most effective set of controls are selected. The DSA control selection process should utilize controls that are already implemented in the facility if possible.

◆The fire protection engineer who is responsible for the development of the FHA should be on the "team" which is developing the DSA.

The conclusions of the fire hazard analysis should be incorporated into the DSA.¹⁵

* Recommendations carried forward from the earlier paper⁴ are marked with the symbol ◆.

Works Cited

- 1 *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analysis*. 2002. Washington, DC: Department of Energy. (April) DOE STD-3009-94.
- 2 Coutts, D. A., M. E. Bowman, C. E. Shogren and M. J. Hitchler. 1999. "Fire Risk Implications in Safety Analysis Reports" in *EFCOG Safety Analysis Workshop, June 13-18, 1999. Portland, Oregon*.
- 3 Coutts, D. A., M. E. Bowman, C. E. Shogren and M. J. Hitchler. 1999. "Fire Risk Implications in Safety Analysis Reports" at the *DOE/Contractor Fire Protection Conference, 21 April 1999, Atlantic City, NJ*.
- 4 "Synthesis of SAR and FHA Methodologies" in *Comparative Evaluation of Hazard Analysis Requirements - Preliminary Draft*. 2001. Link Technologies. http://hss.energy.gov/HealthSafety/WSHP/chem_safety/ws2001/cmworkshop/HANDOUTS/GossHandout.PDF.
- 5 *Nuclear Safety Management* 2007. Washington, DC: National Archives and Records Administration. 10 CFR 830. http://www.access.gpo.gov/nara/cfr/waisidx_07/10cfr830_07.html.
- 6 *Worker Safety and Health Program*. 2007. Washington, DC: National Archives and Records Administration. 10 CFR 851. http://www.access.gpo.gov/nara/cfr/waisidx_07/10cfr851_07.html.
- 7 *Integration of Multiple Hazard Analysis Requirements and Activities*. 2003. Washington, DC: Department of Energy. DOE-HDBK-1163-2003.
- 8 *Facility Safety*. 2005. Washington, DC: Department of Energy. DOE Order 420.1B
- 9 Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports. 1997. Washington, DC: Department of Energy. DOE-STD-1027-92.
- 10 *Implementation Guide for use with 10 CFR Part 851 Worker Safety and Health Program*. 2006. Washington, DC: Department of Energy. DOE G 440.1-8.
- 11 *Fire Protection Design Criteria*. 1999. Washington, DC: Department of Energy. DOE-STD-1066-1999.
- 12 *Implementation Guide for use with DOE Orders 420.1 and 440.1 Fire Safety Program*. 1995. Washington, DC: Department of Energy. (30 September). DOE G 440.1-5 (also known as DOE G-420.1/B-0 & G-440.1/E-0).

- 13 *Worker Protection Management for DOE Federal and Contractor Employees*. 2000. Washington, DC: Department of Energy. DOE O 440.1A.
- 14 *SFPE Engineering Guide to Performance-Based Fire Protection Analysis, 2nd Ed.* 2007. Quincy, MA: National Fire Protection Association.
- 15 Collopy, M. T., M.S. and C. P. Christenson. 2003. “The Practical Implementation of Integrated Safety Management for Nuclear Safety Analysis and Fire Hazard Analysis Documentation” in *Integration of Multiple Hazard Analysis Requirements and Activities*. 2003. Washington, DC: Department of Energy. DOE-HDBK-1163-2003.