TITLE: A New Paradigm to Establish the Safety Basis for Nuclear Explosive Operations

AUTHOR(S): Stewart R. Fisher, Steven Clement, Desmond W. Stack

SUBMITTED TO: PSAM 4
September 13–18, 1998
New York, New York
DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.
DISCLAIMER

Portions of this document may be illegible electronic image products. Images are produced from the best available original document.
A New Paradigm to Establish the Safety Basis for Nuclear Explosive Operations

Stewart R. Fischer, Steven Clement, and Desmond W. Stack
Los Alamos National Laboratory, Group TSA-11
Los Alamos, New Mexico

Abstract

The U. S. Department of Energy (DOE) has recognized that safety assurance requires a balance of institutional and engineering approaches as part of an ongoing safety process. This recognition formed the basis for a new approach to nuclear explosive safety with a focus on the inherent value of the examination process, as opposed to an absolute justification of the nuclear explosive operation against some predefined acceptance criteria. This new approach to safety is reflected in recent DOE Orders and Standards in that there is no requirement that quantitative risk assessment or risk quantification be used in meeting requirements. Furthermore, there is no requirement to compare hazard and accident analysis results against numerical acceptance criteria. This paper discusses the evolution of the DOE nuclear explosive safety orders and compares those with facility safety requirements. The DOE nuclear explosive safety process is examined, and an example application is discussed with emphasis on identification of safety measures and controls.

Historical Perspective

The currently approved orders governing the safety of Department of Energy (DOE) nuclear explosive operations include DOE Orders 452.1A and 452.2A. These Orders replaced earlier orders issued in 1990 that had required a quantitative risk analysis (QRA) for nuclear explosive operations. Despite this requirement, the 1990 Order did not provide specific guidance on how to integrate this QRA into the overall safety process that relied on the Nuclear Explosive Safety Study (NESS) and associated readiness reviews. The 1990 Order was amended via Interim Guidance to require a transition to a full QRA for all safety studies by January 1, 1996. The current 452 Orders replaced the QRA with a requirement for a hazard assessment (HA) similar to that required by the DOE for facility safety via DOE Order 5480.23 and its guidance document DOE-STD-3009-94.

During the 1990 to 1993 timeframe, several factors combined to produce changes in the way the safety of nuclear explosive operations was performed. One factor was the realization by DOE and the weapons laboratories that there were large uncertainties in the knowledge associated with how high explosives (HE) respond to insults typical of those encountered during weapon assembly/disassembly environments. Another major factor was the Defense Nuclear Facility Safety Board’s (DNFSB) Recommendation 93-1 which requested DOE to maintain consistency between nuclear safety at facilities that produce and
process fissile materials, relative to those facilities that assemble, disassemble and test nuclear explosives.

Nuclear explosive operations carried out by the DOE involve assembly, disassembly, testing and transportation of nuclear explosives. Process activities, which are conducted at the Pantex Plant or the Nevada Test Site, are governed by formal procedural and administrative controls. As a result of the importance of human behavior in nuclear explosive operations, DOE orders require that considerable attention be paid to training, personnel assurance programs, procedure development and tooling design.

**DOE Nuclear Explosive Safety Requirements**

Conceptually the safety basis documents required to authorize a nuclear explosive operation are established in DOE Order 452.2A and include a facility safety basis document [i.e., a Safety Analysis Report (SAR) or Basis for Interim Operation (BIO)] and an operation specific safety basis document [i.e. a hazard Analysis Report or HAR). DOE-STD-XXXX-96 clarifies the requirements and provides guidance for the safety analysis applicable to nuclear explosive operations and associated activities.

The new approach to nuclear explosive safety is reflected in Order 452.2A, Order 5480.23, STD-XXXX-96 and STD-3009. These orders do not require the comparison of hazard and accident analysis against numerical acceptance criteria nor is risk quantification required to determine the safety of a facility or process. DOE's new approach for facility safety establishes a broadly defined "safety basis" with increased emphasis on conducting a comprehensive examination of all hazards and the identification of positive measures and controls. This approach has led to designating the HA as the principal safety tool for use in both HARs and SARs. The HA is performed to examine the complete spectrum of accidents, qualitatively determine frequency and consequence, and to identify preventive and mitigative features associated with each accident scenario.

SARs, as prepared for DOE nuclear facilities, have as their goal the documentation of the required nuclear facility safety basis under DOE Order 5480.23. The safety basis is a combination of information related to the control of hazards at a facility (including design, engineering analyses, and administrative controls) upon which DOE depends for its conclusion that activities at the facility can be conducted safely. Order 5480.23 is rather general in its guidance; DOE STD-3009 is more specific and provides guidance for SAR preparation for existing nonreactor nuclear facilities.

Important in Order 5480.23 and Order 452.2A is the fact that there is neither a requirement nor a recommendation that QRA or risk quantification be used in meeting safety requirements. Further, there is no requirement in Order 5480.23 to compare SAR hazard and accident analysis results to numerical risk acceptance criteria of any kind. STD-3009 does provide offsite evaluation guidelines based on the highest consequence scenarios for use in identifying and evaluating safety
class systems, structures and components (SSCs). These evaluation guidelines are not intended to be risk acceptance criteria.

DOE's approach to determining safety systems and safety controls as part of the safety basis is described in STD-3009, that is, by performing hazard and accident analysis. Safety-basis information is derived by evaluating a set of accidents identified in the HA to determine design, functional, and operational requirements for the facility, process, etc. There is no attempt to assess or quantify risk rigorously using this approach. Frequencies and consequences are estimated and the results are assigned to bins spanning orders of magnitudes. Although it is realized that uncertainties are inherent in portions of the deterministic analyses, i.e. data and phenomenological uncertainties, there is no attempt to quantify them. The focus of the SAR is not the assessment of risk but rather an assurance of a given level of safety through the use of safety systems and controls developed through the hazard and accident analysis process.

For nuclear explosive operations, the scope of the HA is defined in DOE Order 452.2A, DOE/AL Supplemental Directive AL452.2 and draft DOE-STD-XXXX-96, "Preparation Guide for the U.S. Department of Energy Hazard Analysis Reports for Nuclear Explosive Operations," and specifies that the HA must address all aspects of worker and public safety and environmental protection. The HA, which is based on traditional HA techniques must address all nuclear explosive operations and associated activities and must identify all hazards using a step-by-step review of the entire operation. Human reliability and human factors analyses are to be performed and used to help determine accident sequence likelihood's. For accident sequences resulting in high consequence (i.e. HE detonation, HE deflagration, nuclear detonation, and fire) a thorough and detailed analysis of accident sequences is performed. For these high-consequence accident sequences, sufficient analytic detail, including uncertainty analyses is to be included in the HA. The HA also identifies and categorizes safety SSCs as well as identifies operational safety controls.

The HA provides the basis for the HAR which is a companion report to the facility SAR. The HAR, which is submitted to the DOE NESS group to support their deliberations, provides a thoroughly documented safety basis for a specific nuclear explosive operation including the bases for identified process controls.

Identification of Process Safety Measures

Design goals for nuclear explosives have been promulgated in DOE Order 452.1A and apply to operational weapons for military use. These goals, however, are not applicable to DOE assembly/disassembly operations. Several approaches for addressing safety in DOE nuclear explosive operations are possible and have been attempted in recent years - one approach focuses on demonstrating that the likelihood of possible undesirable accidents fall below some acceptable level. Another approach has relied on a group of subject matter experts to collegially judge that a process is safe. The third approach, which reflects the current philosophy, focuses on comprehensively identifying all potential accident
sequences and then identifying engineered safety features or administrative controls being relied on to mitigate or prevent the hazard. This third approach focuses safety analyst effort on understanding of the hazard and the mitigative and preventive features and their effectiveness and adequacy. Current efforts are in progress to establish criteria for selecting certain controls that are elevated and maintained at the Technical Safety Requirement (TSR) level. Embodied in this safety control hierarchy is the philosophy that more rigorous and better quality controls are required for high consequence high likelihood scenarios.

One of the primary purposes of the HA is to identify process-specific controls that can be relied on to ensure that a nuclear explosive operation can be conducted safely. The relationship between the SAR facility safety basis and the process specific HAR requires some explanation. The SAR evaluates on a bounding basis, the type of potential accidents that can occur within the facility. The SAR, while addressing accident prevention generically, generally assumes that an accident occurs and focuses on minimizing offsite consequences. On the other hand, the HAR focuses on preventing the accident in the first place. For bounding accident types, the facility SAR identifies both preventive and mitigative measures, including specific administrative controls, facility design features and safety SSCs required to protect the public and workers from releases of radioactive materials. For these specific controls the SAR generally requires implementation of specific TSRs to ensure either the operability of these systems or that certain administrative controls are in place and followed. The HAR focuses on identifying potential accident sequences and on developing appropriate process safety requirements to protect the worker as well as to prevent or reduce the likelihood of a potential accident. For the nuclear explosive process these requirements may take the form of Nuclear Explosive Safety Rules (NESRs), Operational Safety Controls (OSCs) or other process-specific requirements.

The safety assurance objective for the nuclear explosive process is accomplished by focusing on four areas. First the HA is used to support the identification of safety critical operating steps in the Nuclear Explosive Operating Procedures (NEOPs). The purpose of this activity is to ensure that the Production Technicians (PTs) are made aware of potential hazards associated with the particular nuclear explosive activity. The safety critical steps are emphasized during the training program and are identified appropriately in the NEOP. Second, the HA process is used to identify positive measures and associated control requirements for which the HA takes credit in preventing or reducing the likelihood of HED/D, fire or ND accident sequences. In this context, a positive measure is defined as “design features, safety rules, procedures, or other controls used individually or collectively to provide nuclear surety”. Third, the hazard assessment process forms the basis for the selection of safety SSCs in conjunction with the identification of positive measures and a comprehensive review of process tooling and equipment. Finally, the HA process is used to recommend additional controls that may be required to prevent or reduce the likelihood of particular accident sequences. The types of controls developed
include the formal identification of TSR like controls, i.e. NESRs, OSCs, etc. as well as the identification of process-specific institutional program requirements.

**Example: Accident Scenario Spreadsheet Focusing on Identification of Controls**

Table 1 presents a HA spreadsheet showing three representative accident scenarios and identified controls. These examples are based on actual spreadsheets developed for vacuum bay operations at Pantex. For simplicity only the information relevant to assessing control requirements have been included. Table 2 provides a brief text description of the positive measures, defense-in-depth and control requirements listed in Table 1.

The first accident scenario listed in Table 1 results from a process hazard identified as a weapon or worker strike from the hoist and/or strongback while the PT performs the hoist pre-operational check. The underlying assumption is that the PT loses control of the hoist due to either mechanical failure or by simply not paying close enough attention while performing the activity. For this scenario the HA identifies six existing positive measures that act to either prevent or mitigate accidents of this type. These are listed in Table 1 along with recommended control requirements for each positive measure. The HA does not identify any additional positive measures indicating that the existing positive measures are judged sufficient to prevent or mitigate this accident if the control requirements listed are implemented or verified to be already in place.

The second and third scenario result from an analysis of natural phenomena hazards. The second accident scenario is a lightning strike to the facility that results in electrical energy reaching the nuclear explosive. For this accident scenario two existing positive measures were identified as well as one additional recommended positive measure. The third scenario is a seismic event that results in appurtenances falling from the ceiling and striking the unit. It is assumed that the appurtenance that strikes the unit weighs approximately 150 lbs. The HA does not identify any existing positive measures for this scenario, however one positive measure and its associated control requirement is recommended.

**Table 1. Sample Accident Scenarios from the Vacuum Bay HA Spreadsheets**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Strike</td>
<td>Hostile and Strongback swing and strike the unit or worker while the PT is performing the pre-operational check.</td>
<td>HED/D</td>
<td>Weapon assembly could be in the bay during setup activities. PT loses control of hoist and/or strongback. Weapon is in the FW configuration.</td>
<td>TD12</td>
<td>None</td>
<td>QC1</td>
<td>WD1</td>
<td>M2</td>
</tr>
<tr>
<td>2</td>
<td>Lightning</td>
<td>Lightning strike to facility results in electrical energy discharging through wall of facility equipment to the weapon assembly.</td>
<td>HED/D</td>
<td>Lightning protection system fails to perform its intended function because the facility is not properly bonded.</td>
<td>FD1</td>
<td>M1</td>
<td>GC17</td>
<td>WD6</td>
<td>M3</td>
</tr>
<tr>
<td>3</td>
<td>Seismic</td>
<td>Seismic event results</td>
<td>HED/D</td>
<td>Weapon is in the</td>
<td>FD12</td>
<td>M1</td>
<td>GC17</td>
<td>WD7</td>
<td>M3</td>
</tr>
</tbody>
</table>
Table 2. Description of Positive Measures and Control Requirements

<table>
<thead>
<tr>
<th>Facility Measures</th>
<th>Control Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Strike in duct-work, light fixtures, overhead conduit support, overhead piping, acoustic panels, etc.</td>
<td>PW configuration (i.e., full-up weapon), Apparatus that strikes the unit is 150 lbs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Facility</th>
<th>Positive Measures</th>
<th>Control Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>FD1</td>
<td>Facility designed to withstand natural phenomena</td>
<td>GC5: The facility design shall mitigate the effects (to the weapon assembly) of lightning strikes to the facility</td>
</tr>
<tr>
<td>FD2</td>
<td>Facility layout control</td>
<td>GC5: The building shall have a specific location where it is parked and functionally tested that is away from any weapon system</td>
</tr>
<tr>
<td>FD3</td>
<td>Tooling and equipment are supported by overhead piping, Apparatus that acoustic panel, etc. falling from ceiling 150 lbs. strikes the unit</td>
<td>GC6: Facility equipment shall be adequately mounted to meet design basis natural phenomena events</td>
</tr>
<tr>
<td>FD9</td>
<td>Facility lighting protection system mitigates excessive energy differentials in facility</td>
<td>GC8: The facility shall have a fully functional lighting protection system (including bonding of all facility penetrations) that mitigates the effects (to the weapon assembly) of lightning strikes to the facility</td>
</tr>
<tr>
<td>I5</td>
<td>Severe weather warning</td>
<td>GC10: Equipment that is not sufficiently electrically isolated shall be disconnected from the weapon during severe weather warnings</td>
</tr>
<tr>
<td>M1</td>
<td>Periodic testing and maintenance to ensure T&amp;E meet specifications</td>
<td>GC1: Periodic testing and maintenance shall be performed on the hoist and load path components, as well as the RAMS and EASA system</td>
</tr>
<tr>
<td>M4</td>
<td>Post maintenance functional testing</td>
<td>GC4: Post maintenance functional testing shall be performed on the hoist prior to use</td>
</tr>
<tr>
<td>P4</td>
<td>Workers trained in techniques that prevent or mitigate hazards</td>
<td>GC6: Workers shall be trained and qualified in hoist operations and understand the associated hazards</td>
</tr>
<tr>
<td>FD12</td>
<td>Equipment safety interlocks</td>
<td>GC1: The hoist shall have engineered safety features that preclude loss of control</td>
</tr>
<tr>
<td>FD13</td>
<td>System emergency stop button/switch</td>
<td>GC2: The hoist shall have an emergency shut-off button to preclude loss of control</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defence-in-Depth</th>
</tr>
</thead>
<tbody>
<tr>
<td>FP</td>
</tr>
<tr>
<td>MG</td>
</tr>
<tr>
<td>WD1</td>
</tr>
<tr>
<td>WD6</td>
</tr>
<tr>
<td>WD7</td>
</tr>
</tbody>
</table>

Conclusions

The DOE nuclear explosive safety process for assembly/disassembly operations is still evolving, however a comprehensive HA is recognized as forming the basis for the safety analysis process. This new safety paradigm focuses on the identification of process controls and their adequacy/effectiveness to prevent or mitigate hazards. The SAR/BIO establishes the facility safety basis while the HAR establishes the operational safety basis. Specific process controls are linked to each potential accident scenario and are formally identified and documented in the HAR.