LA-UR- 98-2246

Approved for public release; distribution is unlimited.

Title: IDENTIFICATION OF PROCESS CONTROLS FOR NUCLEAR EXPLOSIVE OPERATIONS

CONF-980616--

Author(s): Stewart R. Fischer, LANL
Herbert Konkel, LANL
Kay Houghton, LANL
Michael Wilson, LANL

Submitted to: 1998 Safety Analysis Workshop
June 15-19, 1998
Park City, UT

Los Alamos
NATIONAL LABORATORY

DISCLAIMER

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

Identification of Process Controls for Nuclear Explosive Operations

Stewart R. Fischer, Herbert Konkel, Kay Houghton, and Michael Wilson
Los Alamos National Laboratory
Los Alamos, New Mexico

Introduction

Nuclear explosive assembly/disassembly operations that are carried out under United States Department of Energy (DOE) purview are characterized by activities that primarily involve manual tasks. These process activities are governed by procedural and administrative controls that traditionally have been developed without a formal link to process hazards. This work, which was based on hazard assessment (HA) activities conducted as part of the W69 Integrated Safety Process (ISP), specifies an approach to identifying formal safety controls for controlling (i.e., preventing or mitigating) hazards associated with nuclear explosive operations. Safety analysis methods are used to identify controls, which then are integrated into a safety management framework to provide assurance to the DOE that hazardous activities are managed properly.

DOE Nuclear Explosive Safety Order 452.2A requires HAs to be conducted for proposed nuclear explosive operations. In addition, the DOE has implemented an ISP to evaluate the need to redesign tooling and procedures for disassembly, inspection, and assembly activities associated with nuclear explosives. As part of this effort, it is essential that appropriate safety measures or controls be implemented to provide assurance to the USDOE that the proposed activities can be conducted safely without undue risk to the public or workers. As part of the recent W69 ISP dismantlement effort, various types of process safety controls were identified in an effort to improve safety. Process controls for nuclear explosive operations focus on preventing accidents, facility controls generally focus on mitigating the consequences of a release. Nuclear explosive operations typically have few engineered safety features and are dominated by administrative controls. For the W69 dismantlement process, controls took the form of emphasizing hazardous and critical steps in governing procedures and identifying safety systems, structures, and components, as well as identifying specific administrative control requirements. Methods for identifying these types of controls differ from the traditional DOE-STD-3009-94 approach because of the lack of discriminators between accident scenarios. Nuclear explosive processes often have many very low likelihood accident scenarios all with the same undesirable consequence. The only real discriminator between these scenarios is likelihood, which is fraught with large uncertainty.

As a result of our work on the W69 ISP dismantlement effort, we have developed an approach to identify controls and safety measures to improve the safety of nuclear explosive operations. The methodology developed for the W69 dismantlement effort is being adapted to the W76 ISP effort. Considerable work is still ongoing to address issues such as the adequacy or effectiveness of controls.

DOE nuclear explosive safety orders and some historical insights are discussed briefly in this paper. The safety measure identification methodology developed as part of the W69 ISP dismantlement process then is summarized.

Historical Perspective

The currently approved orders governing the safety of DOE nuclear explosive operations include DOE Orders 452.1A and 452.2A. These orders replaced orders issued in 1990, which had required a Quantitative Risk Assessment (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, which 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-series orders replaced the QRA with a requirement for a HA similar to that required by the DOE for facility safety via DOE Order 5480.23 and its guidance document, DOE-STD-3009-94.

Nuclear explosive operations carried out by the DOE involve assembly, disassembly, testing, staging, storage, and transportation of nuclear explosives. These operations, which are conducted at the Pantex Plant or the Nevada Test Site, are relatively simple and involve manual tasks. The successful completion of these tasks depends on human performance. Few credible accident sequences involve complex, multiple-failure events. Process activities are governed by formal procedural and administrative controls and the use of energy sources within the process facilities that could interact with the nuclear explosive is severely restricted. 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.

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

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) on 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.

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." It is specified 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 likelihoods. For accident sequences resulting in high consequence [i.e., high explosive (HE) detonation, HE deflagration, nuclear detonation (ND), 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 systems, structures, and components (SSCs) and 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.

Historically, there has been limited documentation of the linkage between process hazards and controls. The DOE NESS group generally identifies extensive lists of positive measures as part of their focused nuclear explosive safety study. However, the NESS group makes no real attempt to identify if controls are in place, maintained, or implemented to ensure that positive measures were effective. Similarly, the NESSG makes no formal assessment of adequacy or sufficiency with respect to the set of positive measures mitigating or preventing a hazard. The NESS process does not ensure or determine if controls were linked to implementing documents on the shop floor. In addition, no effort traditionally has been made to ensure that the identified positive measures were included as part of a formal Unreviewed Safety Question (USQ) change control process. In conclusion, before recent DOE initiatives [i.e., ISP, target-level-of-controls (TLCs), etc.], existing safety processes provided little documented assurance to a regulator that a nuclear explosive operation was indeed safe.

Analysis of Safety Measures and Defense in Depth

Defense in depth is defined as the concept of multiple layers of defense (or protection) with successive barriers to prevent the release of hazardous material or energy. To compensate for potential human and equipment or tooling failures, barriers include hardware as well as administrative controls and operator actions. Consistent with the graded approach, no minimum number of layers of defense is required for specific nuclear explosive operations. However, there are typically multiple layers of defense in depth for nuclear explosive operations. The inner layer relies on a high level of design quality to ensure that the tooling and equipment perform as designed. Additional layers include requirements for competent and well-trained personnel, thorough and comprehensive procedures, and effective maintenance (preventive and predictive). Safety management programs such as conduct of operations, radiation protection, and industrial safety help to ensure well-structured activities with minimal hazards and distractions. The outermost layer of defense is provided by the facility (bay or cell) safety-class systems, which act to mitigate the consequences of an accident and protect the public.

One of the primary purposes of the HA is to identify process-specific controls that can be relied on to ensure that the proposed nuclear explosive operation is within the SAR safety basis. The relationship between the SAR safety basis and the process-specific HAR requires some explanation. The SAR assumes that an accident occurs and focuses on minimizing offsite consequences, whereas the HAR focuses on preventing the accident. The facility SAR identifies specific administrative controls (ACs), facility design features (DFs), and safety-class and safety-significant SSCs required to protect the public from off-site release of radioactive materials. For these specific ACs, DFs, and SSCs, the SAR may require implementation of specific Technical Safety Requirements (TSRs) to ensure the operability of these systems or that certain administrative controls are followed and in place. The HAR focuses on identifying potential accident sequences involving worker and nuclear explosive safety and on developing appropriate process safety requirements to protect the worker and prevent or reduce the likelihood of a potential accident. For the nuclear explosive process, these requirements may take the form of ACs, DFs, nuclear explosive safety rules (NESRs), operational safety controls (OSCs), or other process-specific requirements.

For the W69 ISP dismantlement process, the safety assurance objective was accomplished by focusing on three areas as documented in the HAR. First, the HA was used to identify "critical" and "hazardous" procedure steps and "critical" tooling in the Nuclear Explosive Operating Procedures (NEOPs). The purpose of this activity is to ensure that the production technicians are made aware of potential hazards during the particular nuclear explosive activity. These

critical/hazardous steps are emphasized during the training program and identified appropriately in the NEOP. Second, to support the NESS group, the HA process was used to identify positive measures for which the HA takes credit in preventing or reducing the likelihood of HED/D, ND, or fire 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 HA process, in conjunction with the identification of positive measures, is used to identify specific functional control requirements that may be required to ensure functionality or operability of positive measures relied on to prevent or reduce the likelihood of particular accident sequences. The types of controls developed include the identification of safety SSCs, NESRs, or OSCs as well the identification of less formal, specific process control requirements. In this context, similar to the guidance provided in DOE-STD-3009-94, we want to take credit for specific aspects of existing plant safety management programs and hence we identify specific programmatic requirements required to ensure the operability of various tooling and equipment and related positive measures.

Identification of Hazardous and Critical Procedure Steps and Critical Tooling

One of the primary objectives of the SS-21 HA conducted for the bay and cell activities was to identify safety-critical operating steps in the NEOPs. In the memorandum from S. J. Guidice (December 13, 1993)[1] initiating the B61 SS-21 Demonstration Project, safety-critical operating steps were defined to be those in which the Technical Safety Objectives governing operations to be performed on nuclear weapons could be compromised. These Technical Safety Objectives include the following.

- Prevent the application of unauthorized and unanalyzed energy from sources external to the nuclear weapon, or any component of the nuclear weapon, so as to prevent the release of energy from sources internal to the nuclear weapon.
- Allow no single-point failure in an operation that could cause:
  a. energy sources within the weapon, including self-contained energy sources, to be activated or released,
  b. abnormal radioactive contamination, i.e., contamination above thresholds set in the operating procedures, and
  c. serious injury to personnel, i.e., lost workday injuries.
- Mitigate personnel exposure to radiation and hazardous substances to "As Low As Reasonably Achievable" (ALARA) levels that are less than 500 mrem (neutron quality factor of 20) per worker-year as a goal, but in any case, not to exceed OSHA limits.

Based on this guidance, the following HA-specific definitions of safety-critical operating steps and safety-critical tooling were adopted for the W69. Safety-critical operating steps identified in the HA are termed either a "Hazardous Step" or HS or a "Critical Step" or CS.

In the HA, we use the term "Critical Step" to denote a procedure step that, if skipped or performed incorrectly, will increase the likelihood of a dominant HED/D, ND, or fire event or worker disability/death at some later step in the procedure and a "Hazardous Step" as a procedure step that, if performed incorrectly, has a potential to immediately result in a dominant HED/D, ND, or fire accident sequence or worker disability/death as identified by the HA. The HS is intended to address hazards associated with technician technique such as with the use of tooling or during installation and removal of tooling (e.g., dropping of tooling).

In a similar fashion, the HAR defines safety-critical tooling as any tooling whose failure (excluding catastrophic failure) could significantly contribute to an identified accident scenario resulting in an HED/D or fire or a significant facility contamination or worker injury or exposure. In addition,

critical tooling was defined as tooling that would significantly increase the likelihood of an HED/D or fire if used in a degraded condition. To support the identification of safety-critical tooling and hazardous/critical steps, selection criteria were developed based on a likelihood and consequence matrix similar to the example provided in DOE-STD-3009-94.

Identified hazardous and critical procedure steps and safety-critical tooling should be incorporated into USQ change control processes. The intent is to link dominant accident scenarios with procedure steps so that future process/procedure changes could be evaluated in conjunction with change control processes to determine if new accidents had been introduced or if the consequence or likelihood of existing activities had been increased. This process links the procedure steps with process hazards and identified hazardous/critical procedure steps and safety-critical tooling. Tables could be developed and used by review personnel to ensure that changes properly consider hazards.

Identification of Positive Measures

One of the goals of the ISP is to implement a nuclear explosive operation that is as safe as possible. As part of the HA for the W69 bay and cell operations, positive measures and associated functional control requirements were identified for each potential accident sequence regardless of likelihood. DOE Order 452.2A defines positive measures as "design features, safety rules, procedures, or other controls used individually or collectively to provide nuclear explosive surety. Positive measures are intended to ensure a safe response in applicable operations and to be controllable. Some examples of positive measures are strong-link switches; other safety devices; administrative procedures and controls; general and specific nuclear explosive safety rules; design control of electrical equipment and mechanical tooling; and physical, electrical, and mechanical restraints incorporated in facilities and transport equipment."

Consistent with this requirement for positive measures to be controllable, the identification of positive measures and associated controls for the Bay and Cell activities begins in the early stages of the ISP process. During the HA, three basic questions are asked.

- What can happen?
- How likely is it to happen?
- What is the consequence if it does happen?

The identification of positive measures and associated controls includes asking three additional related questions.

- What will keep the event from happening?
- What will reduce the frequency of the event?
- What will limit or eliminate the consequence if the event does happen?

The identification of positive measures is an integral part of the entire HA process and is performed at each step of the HA. An important element of the ISP and the HA is an evaluation of existing potential positive measures and identification of additional positive measures that may either mitigate or prevent hazard scenarios.

One of the challenging aspects of the identification process is to decide which positive measures should be included for an identified accident sequence. The criteria for the selection are directly related to DOE ORDER O 452.1, "Nuclear Explosive and Weapons Surety Program," which states:

"There shall be positive measures to:

1. minimize the possibility of accidents, inadvertent acts, or authorized activities that could lead to fire, high explosive deflagration, or unintended high explosive detonation;
2. minimize the possibility of fire, high explosive deflagration, or high explosive detonation, given accidents or inadvertent acts;
3. minimize the possibility of deliberate unauthorized acts that could lead to high explosive deflagration or high explosive detonation;
4. ensure adequate security of nuclear explosives;
5. minimize the possibility of or delay unauthorized nuclear detonation."

Thus, the positive measures and their implementing controls are viewed as contributing directly to nuclear explosive surety. In addition, in the W69 HA, other positive measures that aid in the reduction of risk to the worker (for example, personnel protective equipment) also were included.

Identification of Process-Specific Safety SSCs, OSCs, and NESRs

As discussed above, one of the primary purposes of the HAR is to identify the process-specific controls necessary to ensure that the proposed nuclear explosive operation is bounded by the facility SAR safety envelope. Consistent with DOE-STD-3009-94, "safety-class" typically is reserved for SSCs needed to ensure protection of the public, whereas "safety-significant" is reserved for those required for defense in depth or worker safety. Safety-significant category SSCs are provided to ensure that important SSCs will be given adequate attention in the SAR and facility operations programs. DOE-STD-3009-94 recognized that when the graded approach is used, the majority of engineered features in an operation will not be identified as safety-class or safety-significant even though they perform safety functions. Therefore, all aspects of defense in depth identified for a specific process must be covered within relevant safety management programs committed to in the SAR. This last statement could be interpreted to mean that all aspects of defense in depth for a specific nuclear explosive operation (i.e., the W69 dismantlement), which includes administrative requirements (ACs) as well as positive measures as specific DFs, must be addressed in relevant safety management programs. This implies that additional controls should be implemented to address deficiencies that are uncovered during a review of the operations or as a result of the HA. These additional controls may take the form of NESRs, OSCs, or other process-specific requirements.

NESRs are defined in DOE Order SD AL 452.2 to be "Operating limits, surveillance requirements, safety boundaries, and management and administrative controls that significantly contribute to minimizing the possibility of nuclear detonation, or high explosive detonation/deflagration, in nuclear explosive operations." OSCs are defined to be "Operating limits, surveillance requirements, safety boundaries, and management and administrative controls that significantly contribute to protecting workers, the public, and the environment from hazards other than nuclear detonation and high explosive detonation/deflagration for specific nuclear explosive operations and associated activities." Safety-class SSCs are defined by DOE Order 6430.1A to be "Systems, structures, or components including primary environmental monitors and features of nuclear explosive operations and associated activities and facilities whose failure could adversely affect the environment or safety and health of the public as defined by safety analyses." DOE-STD-XXXX-96 interprets the term "adversely affect" to mean that Evaluation Guidelines are exceeded. Safety-significant SSCs are defined by DOE-STD-3009-94 to be "SSCs not designated as safety-class SSCs, but whose preventive or mitigative function is a major contributor to defense-in-depth and/or worker safety as determined from hazard analysis." The order further states that "safety-significant SSCs based on worker safety are those SSCs whose failure is estimated to result in an

acute worker fatality or serious injury." The orders further imply that safety SSCs require the development of NESRs or OSCs to ensure operability. To ensure the operability of non-safety-designated SSCs, additional process-specific control requirements were identified to address the need to ensure that all aspects of defense in depth were covered by relevant safety management programs.

An 11-step process was used for the W69 bay and cell activities to identify necessary controls to ensure that the dismantlement process fell within the SAR safety envelope. This process begins with a comprehensive review of the NEOP and the HA accident sequences and associated positive measures. For each accident sequence, the tooling and equipment are identified, and pertinent safety functions and operational or safety features are determined. Positive measures in place to ensure the operability/functionality of each piece of tooling or equipment are identified, as are safety management program commitments that provide assurance that the identified controls/measures are in place. Programmatic deficiencies are candidates for administrative control NESRs/OSCs; tooling and equipment considered to contribute more to safety may be identified as safety SSCs.

Conclusions

The W69 efforts address some of the shortcomings identified in prior safety reviews and provide the needed assurance to regulators that the nuclear explosive process is indeed safe. Efforts undertaken as part of the W69 ISP included the conduct of a detailed HA, which was used as the basis to identify positive measures and associated functional control requirements. Formal TSR-like controls then were developed and documented in an Activity Based Control Document (ABCD). This ABCD is maintained under formal change control. The HAs and control identification processes, similar to that conducted for the W69 dismantlement process, tend to be qualitative in nature; that is, limited formal quantification of scenario likelihoods is undertaken.

The advantages of this ISP HA process is that controls are identified that the contractor and the DOE are relying on to prevent accidents. The process is probably over-conservative because controls essentially are developed without specific regard to likelihood for all identified scenarios. Even though the qualitative nature of the HA process results in implied screening of accident scenarios based on the expertise and knowledge of the HA team, experience has shown that the HA process results in formalizing many currently existing controls and linking them to hazards. This HA process allows the contractor and regulator to better understand process hazards and the associated controls.

A possible disadvantage is that the ISP HA process may be too conservative and place an undue burden on the contractor through the formalization of large numbers of controls (i.e., TSR-level controls). In addition, the use of qualitative likelihood assessments may lead to a less-than-adequate understanding of accident progression and controls being identified incorrectly. In addition, improper likelihood judgments may lead to a focus on the wrong set of controls.

The role or use of the HA process to enhance the safety of nuclear explosive operations has evolved considerably over the past few years. The B61 SS-21 effort demonstrated the viability and usefulness of the conduct of a concurrent HA to support risk reduction. During the conduct of the W69 HA, efforts were made to identify safety SSCs, hazardous/critical procedure steps, and control requirements. At the conclusion of the W69 study, efforts were made to formally document the controls relied on to ensure nuclear explosive safety in an ABCD. DOE, recognizing the regulatory value of the ABCD document, has initiated an effort to provide a hierarchical ranking of controls based on their contribution to perceived safety. The hierarchical ranking process, which addresses the perceived adequacy or effectiveness of controls to mitigate or prevent an accident scenario, evolved into an effort called "Target Level of Controls" (TLC). During the past

year, efforts have been undertaken to apply the TLC philosophy to various nuclear explosive operations, including the W69, W76, W79, transportation activities, and the dynamic balancer. Current efforts are in progress within the DOE weapons complex to develop common guidance for application of the TLC philosophy. In addition, efforts are under way to shed light on qualitative judgments made to assess the adequacy, effectiveness, and sufficiency of controls.

References

1. S. J. Guidice, "Stockpile Stewardship Demonstration Project (SS-21)," DOE/ALO memorandum to J. D. Immele et al. (December 13, 1993).