DOE G 452.2A-1A

1-17-97

IMPLEMENTATION GUIDE

for

DOE ORDER 452.2A,

SAFETY OF NUCLEAR EXPLOSIVE OPERATIONS

ASSISTANT SECRETARY FOR DEFENSE PROGRAMS

U.S. Department of Energy

DISTRIBUTION
All Department Elements

INITIATED BY:
Office of Defense Programs

CONTENTS

CONTENTS (continued)

1. INTRODUCTION.

a. Authorization and Applicability.

(1) This Department of Energy (DOE) Implementation Guide for use with DOE O 452.2A is approved by the Deputy Assistant Secretary for Military Application and Stockpile Management. It is applicable to DOE components and contractors responsible for nuclear explosive operations and associated activities and facilities.

(2) Implementation Guides are used to identify government and non-government standards for implementing the Department's requirements. Applicable DOE directives are included as a list following each section of this Guide. In addition, each section includes a list of references, which provide other sources of information.

(3) Beneficial comments (recommendations, additions, deletions) and any pertinent data that may improve this document should be sent to:

Deputy Assistant Secretary for Military Application
and Stockpile Management
Office of Weapons Surety
(DP-21, GTN)
U.S. Department of Energy
19901 Germantown Road
Germantown, MD 20874-1290
Phone: (301) 903-3463
Fax: (301) 903-8628

(4) DOE Implementation Guides are part of the DOE directives system and are issued to provide supplemental information regarding the Department's requirements as contained in Rules, Orders, Notices, and Regulatory Standards. Implementation Guides may also provide methods for implementing these requirements. Implementation Guides are not substitutes for requirements, nor do they replace Technical Standards that are used to describe established practices and procedures that implement requirements.

(5) This Implementation Guide addresses some of the safety programs discussed in DOE O 452.2A. Other programs are addressed in other DOE Orders, Standards, and Guides, as referenced in DOE O 452.2A. Except

as mandated by a regulation, contract, or administrative means, the provisions in this Implementation Guide are DOE's views concerning acceptable methods of program implementation and are not mandatory.

(6) Where appropriate, the scope and depth of the application of the methods and guidelines in this Guide are to be determined by the use of a graded approach. The level of rigor necessary to meet the requirements should be based on grading factors, such as the relative importance to safety and the magnitude of hazards involved. The graded approach shall not be used to obtain relief from requirements.

b. General Information.

(1) Many safety programs prescribed for DOE nuclear facilities have application to nuclear explosive operations and associated activities and facilities. For some of these programs, the existing standards and guidelines for nuclear facilities are sufficient; these documents are identified in DOE O 452.2A. For other programs, DOE standards specific to nuclear explosive operations provide the necessary standards and guidelines. This Guide does not duplicate any existing material, but provides additional guidance for implementing DOE O 452.2A.

(2) The following general hazard types may be present.

(a) Nuclear explosive.

(b) High explosive.

(c) Electro-explosive and pyrotechnic devices.

(d) High-pressure vessels, with and without radioactive gases.

(e) Criticality.

(f) Occupational hazards (industrial, radiological, and chemical).

(3) Implementation of requirements to prevent or mitigate one hazard shall ensure that the likelihood of a safety significant incident involving another hazard is not increased. If any such instance is identified, alternative methods should be investigated to attempt to implement the requirement without increasing the risk associated with other hazards. Requirements

that are not fully implemented because doing so would increase the overall risk of the operation will be identified and documented in the Safety Analysis Report (SAR) for the facility or the Hazard Analysis Report (HAR) for the operation.

(4) Guidelines, best management practices, or other implementation guidance that is not mandatory will be similarly treated, but justification for not incorporating non-mandatory guidance need not be documented in the SAR or HAR.

(5) Several references are being revised at this time. Until such time as all contractual documentation is adjusted to reflect changes in the DOE directives system, implementation plans should include the most current applicable directive(s) and an assessment of the possible impact of anticipated changes from the specific reference used. When the word "or" is used, several references may apply; when the word "and" is used, the intent is that all references apply.

2. PRINCIPLES AND PROCESSES.

a. Configuration Management.

(1) Introduction. DOE O 452.2A requires design laboratories and operating contractors to develop and implement a configuration management (CM) program for nuclear explosive operations and associated activities and facilities. The purpose of the CM program is to establish and maintain consistency among design requirements, physical configuration, processes, and documentation.

(2) CM Program Elements.

(a) The CM program for nuclear explosive operations and associated activities should be coordinated with the facility CM program. The facility CM program may address CM activities for nuclear explosive operations and associated activities rather than establish separate CM program plans. The CM program plan should serve as an integrating document, identifying where specific elements of the program are addressed. DOE-STD-1073-93, should be used in developing the CM program and in preparing the CM plans. As a minimum, the CM program plan should include the following elements.

1 Program management.

2 Design requirements.

3 Document control.

4 Change control.

5 Assessments.

(b) General CM program elements for nuclear explosive operations and associated activities and facilities should include measures to do the following.

1 Control the physical configuration of the equipment and systems so they are consistent with design requirements, documentation, and the safety basis.

2 Ensure that only proper, authorized equipment is used.

3 Review proposed changes to facilities, equipment, and operations in accordance with an approved change control process that identifies revisions in safety documentation.

4 Incorporate approved changes into all affected documents (such as design documents and procedures) and programs (such as the maintenance and training programs).

(c) DOE-STD-1073-93 provides acceptable methods and practices for implementing CM and also provides guidance on applying the graded approach.

(d) A unique consideration for nuclear explosive operations is to ensure that all proposed changes are reviewed for potential impact on nuclear explosive safety. In addition to changes to obvious items, such as tooling and the operating procedures, the change control process must also capture changes that are not obviously related to nuclear explosive safety but may have an adverse impact. Examples include changes to facility support systems, security procedures, and personnel training programs. CM program plans should specify responsibilities for reviewing proposed changes.

(e) CM controls for tooling and equipment should include the following.

1 Applicable controls specified by the criteria of paragraph (c) of 10 CFR Part 830.120.

2 Interfaces between CM controls for tooling and equipment and those for the facility.

3 Documentation and control of authorized tooling and equipment; a formal layout scheme can facilitate these controls.

4 Uniquely marked tooling and equipment.

5 Positive identification of tooling and equipment in a calibration/performance testing control program.

(3) Applicable Standards.

DOE-STD-1073-93, *Guide for Operational Configuration Management Program*, of 11/93.

(4) References.

(a) 10 CFR Part 830, *Nuclear Safety Management*, Section 120, "Quality Assurance Requirements."

(b) G-830.120, *Implementation Guide for use with 10 CFR Part 830.120, Quality Assurance*, of 4-15-94.

b. Issues Management.

(1) Introduction. DOE and DOE contractors shall develop and implement corrective action tracking and commitment tracking systems. These systems are key management tools to manage, plan, and assign work priorities, trend information to identify generic problems, and assess the effectiveness of safety programs. These objectives can be met with separate or combined tracking systems.

(2) Corrective Action and Commitment Tracking.

(a) A corrective action tracking system should monitor and track all safety-related corrective actions, including actions from Nuclear Explosive Safety Studies and Surveys; internal and external audits, appraisals, assessments, inspections, and reviews; and corrective actions resulting from reportable occurrences.

(b) Corrective actions should be based on root cause analyses to identify the underlying causes. Findings and corrective action data should be periodically reviewed to identify adverse trends or opportunities for improving safety.

(c) A corrective action tracking system should be formally established and implemented to ensure that all corrective actions are entered into the system and that their status is current. A formal system should have features that will do the following.

1 Identify the initiating source for the action, an assignment of a responsible organization or individual, and a scheduled completion date.

2 Identify significant or priority actions (e.g., actions that address prestart findings from a readiness review).

3 Report corrective action data to responsible managers in a manner that assists them in completing their assigned activities and also informs them of related actions being completed by other organizations.

4 Track corrective actions to closure, with follow-up verification.

(d) In addition to corrective actions, other commitments important to safety should be tracked. Examples are commitments to implement new requirements, upgrade programs, and incorporate new Technical Standards. A commitment tracking system should consider the applicable features listed above.

(3) Applicable Standards.

None

(4) References.

None

c. Occurrence Reporting.

(1) Introduction. DOE O 232.1 establishes a system for reporting operations information related to DOE-owned or -operated facilities and for processing that information to provide for appropriate corrective action. This section provides guidance for categorizing occurrences related to nuclear explosive safety.

(2) Emergency Occurrences. An emergency occurrence is the most serious type of occurrence and shall be reported immediately in accordance with DOE O 151.1. An emergency occurrence requires an increased alert status for onsite personnel and, in specific cases, for offsite authorities. In addition to the situations described in Chapter V, DOE O 151.1, the following are categorized as emergency occurrences.

(a) Unplanned nuclear or high-explosive detonation, or high-explosive deflagration.

(b) Dispersal of fissile material from a nuclear explosive.

(c) Seizure, theft, or loss of a nuclear explosive.

(d) Inadvertent or deliberate unauthorized arming of a nuclear explosive.

(e) Safeguards or security event, or a transportation accident, involving nuclear explosives that is a credible threat to DOE operations,

facilities, or personnel, and results or could result in significant effects on the public health and safety and/or national security.

(3) Unusual Occurrences. An unusual occurrence is a significant unplanned occurrence involving a nuclear explosive and shall be categorized and reported in accordance with the provisions of DOE M 232.1-1 for Group 9, Nuclear Explosive Safety. The following are categorized as unusual occurrences.

(a) The unauthorized introduction of electrical energy into a nuclear explosive.

(b) The unauthorized compromise of a nuclear explosive safety feature when installed on a nuclear explosive.

(c) Damage to a nuclear explosive that results in a credible threat to nuclear explosive safety.

(d) Inadvertent substitution of a nuclear explosive for a nuclear explosive-like assembly (NELA) or vice versa.

(e) A violation of a nuclear explosive safety rule (NESR).

(4) Off-Normal Occurrences. An off-normal occurrence is an abnormal or unplanned event or condition that adversely affects nuclear explosive safety but is not in the emergency or unusual occurrence category. It shall be categorized and reported in accordance with the provisions of DOE M 232.1-1 for Group 9, Nuclear Explosive Safety. The following are categorized as off-normal occurrences.

(a) A "near miss," a situation that could (but did not) result in a credible threat to nuclear explosive safety.

(b) A violation of the two-person concept of operations.

(c) Revocation of the Personnel Assurance Program (PAP) certification of an individual (for cause).

(d) Damage to a training unit during training operations indicative of a hazard to a nuclear explosive.

(e) The use of uncertified personnel or unauthorized equipment/tooling during a nuclear explosive operation.

(5) Applicable Orders.

(a) DOE O 151.1, COMPREHENSIVE EMERGENCY MANAGEMENT SYSTEM, dated 9-25-95.

(b) DOE O 232.1, OCCURRENCE REPORTING AND PROCESSING OF OPERATIONS INFORMATION, dated 9-25-95.

(c) DOE M 232.1-1, OCCURRENCE REPORTING AND PROCESSING OF OPERATIONS INFORMATION, dated 9-25-95.

(6) References.

None

d. Performance Indicators.

(1) Use of Performance Indicators. Contractors and laboratories are required to implement a Performance Indicator Program in accordance with DOE O 210.1 and the guidance of DOE-STD-1048-92. Operations Offices, contractors, and laboratories should develop nuclear explosive safety performance indicators tailored to the specific operations and unique site facilities and conditions. The following are examples of performance indicators for nuclear explosive operations and associated activities and facilities.

(a) PAP immediate removals.

(b) Two-person concept violations.

(c) NESR violations.

(d) Technical Safety Requirement (TSR) and Operational Safety Control (OSC) violations.

(e) Radiation dose to personnel.

(f) Occupational Safety and Health Administration recordable injuries.

(g) Nuclear explosive area reportable occurrences.

(2) Addition or Deletion of Performance Indicators. Based on a review of operations, appraisal results, and management assessments, performance indicators should be added or deleted as appropriate.

(3) Applicable Orders and Standards.

(a) DOE O 210.1, PERFORMANCE INDICATORS AND ANALYSIS OF OPERATIONS INFORMATION, dated 9-27-95.

(b) DOE-STD-1048-92, *DOE Performance Indicators Guidance Document*, dated 12-92.

(4) References.

None

e. Safety Analysis - Facility/Operations Interfaces.

(1) Introduction.

(a) DOE O 452.2A requires safety analyses of all nuclear explosive operations and associated activities and facilities. A facility safety analysis, documented in a SAR, generically addresses nuclear explosive operations that are expected to be performed in the facility. The HAR is a detailed hazards analysis involving a specific nuclear explosive operation. Taken together, the facility SAR and the operation HAR constitute the safety analysis for the nuclear explosive operation in a specific facility. The HAR documents the systematic evaluation of hazards to workers, the public, and the environment. The Nuclear Explosive Hazards Assessment (NEHA) is the portion of the HAR that contains a systematic evaluation of hazards that could lead to nuclear detonation, high-explosive detonation or deflagration, or fire. NESRs are those safety limits, operating limits, surveillance requirements, safety boundaries, and management and administrative controls that minimize the possibility of nuclear detonation, high-explosive detonation or deflagration, or fire, and are included in the NEHA for review and

consideration by the Nuclear Explosive Safety Study Group (NESSG). OSCs are safety limits, operating limits, surveillance requirements, safety boundaries, and management and administrative controls that protect workers, the public, and the environment from hazards other than nuclear detonation, high-explosive denotation and deflagration, and fire. OSCs are documented in the HAR and approved by the Operations Office manager. NESRs are documented in the NESSG report and must be approved by Headquarters.

(b) For facilities in which nuclear explosive operations are performed, SARs shall be prepared and processed in accordance with DOE 5480.23 and DOE-STD-3009-94. DOE 5480.23 specifies that a graded approach shall be used for analyzing, documenting, and providing for the safety of facilities. The rigor of the safety program should correspond to the level of the hazards. Section 2e(2), below, provides specific guidance for using DOE-STD-3009-94 to prepare SARs for facilities in which nuclear explosive operations and associated activities are performed.

(c) Facility TSRs shall be developed and implemented in accordance with DOE 5480.22. Similar operation-specific controls are specified in NESRs and OSCs. Section 2e(4), below, describes the roles and interrelationships of NESRs and OSCs, and provides guidance on developing, documenting, and implementing them.

(2) Facility SAR Content.

(a) DOE-STD-3009-94 should be used for preparing SARs. Each chapter contains a section titled, "Application of the Graded Approach." For some chapters, this guidance is keyed to a nuclear facility hazard category. For the purpose of preparing SARs for facilities in which nuclear explosive operations and associated activities are conducted, the graded approach guidance for a hazard category 2 nuclear facility should be used.

(b) Specific supplementary guidance for the referenced chapters of DOE-STD-3009-94 is provided in the following paragraphs.

1 Chapter 3, Hazard and Accident Analyses. DOE O 452.2A requires the facility SAR to describe the analysis of the full

spectrum of hazards involved in nuclear explosive operations and associated activities. The SAR should contain hazards analyses, in general, and an accident analysis for potential bounding hazards for each accident type. Definition of a bounding accident should be based on the expected worst-case nuclear explosive operation or associated activity characteristics associated with the accident type. The goal is to identify and analyze hazards that will bound future operations.

2 Chapter 5, Derivation of Technical Safety Requirements. TSR information is based on material detailed in Chapters 3 and 4 of the SAR and is developed and maintained in accordance with DOE 5480.22. TSRs address facility structures, systems, and components (SSCs) and administrative controls related to plant programs. NESRs and OSCs address operation-specific controls (see Section 2e(4), below). NESRs and OSCs should complement TSRs, not overlap them.

3 Chapter 6, Prevention of Inadvertent Criticality. Maximum inventory limits for fissile material shall be specified in the TSRs based on guidance contained in DOE O 420.1 or DOE 5480.24 and appropriate Joint DOE/Department of Defense Technical Publications (e.g., TP 20-7).

a The SAR addresses the criticality protection policy and program for the general handling and staging of single and multiple nuclear explosives and components. However, the SAR is not required to address the criticality safety of a specific nuclear explosive and its components since it is addressed in the design process, certified by the design laboratories, and documented in the HAR.

b The safety analysis in the SAR shall document bounding events to identify and describe control measures and limits.

4 Chapter 13, Human Factors. SARs should address human-to-machine interfaces that affect facility safety-class SSCs

and safety-significant SSCs. Human factor aspects of specific nuclear explosive operations and associated activities are addressed in HARs.

(3) Operation-Specific HAR Content. Refer to DOE-DP-STD-XXXX-96 for detailed requirements on operations-specific HAR content.

(4) Safety Measures.

(a) TSRs are facility limits and/or controls that apply to all operations. Facility safety limits, requirements, and controls contained in TSRs are derived from analyses in the SAR. NESRs and OSCs are derived in the HARs employing methods similar to those used to derive TSRs in the SAR. DOE 5480.22 and DOE 5480.23 provide an acceptable model for developing, documenting, and implementing NESRs and OSCs. The purpose of NESRs is to minimize the possibility of accidents involving nuclear detonation, high-explosive detonation or deflagration, and/or fire. OSCs are focused on worker health and safety and are directed toward minimizing the frequency and/or consequences of accidents not involving nuclear detonation, high-explosive detonation or deflagration, and/or fire. For example, in order to minimize personnel exposure from an uncontrolled tritium release, an OSC might be established for the operability of a gas exhaust system collector hose positioned directly over the nuclear explosive during tritium reservoir removal. This would provide a capability to collect and control the tritium gas that might be involved in an accidental tritium release.

(b) NESRs and OSCs consist of the following.

1 Safety Limits. Bounding process limits to prevent release of radioactivity or other hazardous material, or explosive detonation/deflagration. Safety limits are normally associated with safety-class SSCs and any controls associated with non safety class SSCs.

2 Operating Limits. Limiting Control Settings (LCSs) on safety systems are control process variables to prevent exceeding safety limits. Limiting Conditions for Operation (LCOs) are the lowest functional capability or performance

level of safety SSCs and their support systems required for normal safe conduct of operations. Such limits may include restricting the number of hazardous components present in a work area, the quantity of components or hazardous material present, or the temperature of a fluid system.

3 Surveillance or Status Verification Requirements. Test, calibration, inspection, or verification requirements that ensure operability and quality of safety-related systems or components, or the status of a safety feature.

4 Administrative Controls. Organization and management procedures, reviews, and other administrative elements that ensure safe operation.

(c) As appropriate, the operating contractor and/or the responsible design laboratory shall propose NESRs and OSCs, as derived from the safety analysis in the HAR/NEHA. Additional NESRs and OSCs may be proposed during preoperational safety reviews, such as the operation-specific readiness assessments or Nuclear Explosive Safety Studies. The Nuclear Explosive Safety Study includes review of all recommended NESRs and provides final recommended NESRs in the Nuclear Explosive Safety Study Report.

(d) NESRs and OSCs shall be recorded in controlled documents and maintained current. Revisions should be approved by the same authority that approved the original NESR or OSC. For ongoing operations, NESRs and OSCs should be reviewed annually, concurrent with the annual HAR review.

(e) NESR or OSC violations include the following.

1 Exceeding a safety limit.

2 Failing to take the actions required within the required time limit following: (1) exceeding an LCS, (2) failure to meet an LCO, or (3) failure to successfully meet a surveillance or status verification requirement.

3 Failing to perform a surveillance or status verification when required.

4 Failing to comply with an administrative control requirement.

(f) A violation of a NESR is an occurrence as listed in DOE M 232.1-1 and is subject to the reporting requirements of DOE O 232.1. Although not specifically listed, a violation of an OSC should be reported as an occurrence in accordance with DOE O 232.1.

(g) An acceptable format for specific NESRs and OSCs is depicted in Attachment 1 of DOE 5480.22. Other formats may be used, provided the required information is presented clearly.

(h) As stated in the guidelines of DOE 5480.22, TSRs are not based on maintaining some acceptable level of worker safety; rather, the risk to workers is controlled by reducing the likelihood and potential impact of a significant event (one that can cause serious personnel injury or an acute fatality). This is accomplished by developing TSRs for those systems and components that are barriers preventing uncontrolled release of radioactive or other hazardous materials, or that mitigate such releases.

(i) In a similar fashion, NESRs and OSCs should also establish barriers to prevent an uncontrolled release of radioactive or other hazardous material, or to mitigate the releases. Specific to nuclear explosive operations, NESRs and OSCs should also establish measures that prevent uncontrolled release of energy from explosives (i.e., main charge high-explosive or other explosive devices present in the nuclear explosive). The objective is for NESRs and OSCs to implement limits and controls that will reduce the likelihood or consequences of a significant event. Plant safety programs are relied on to contribute to the safety basis of the facility and its operation by providing worker safety for other events.

(5) Safety Basis.

(a) DOE 5480.23 defines the safety basis as the combination of information relating to controlling hazards at a nuclear facility, including design, engineering analyses, and administrative controls.

While the safety basis of a facility typically includes all operations performed in the facility, the nature of nuclear explosive operations and associated activities requires an operations-specific safety basis in addition to a general safety basis. A graphic depiction of the safety basis development for nuclear explosive operations and associated activities is shown in Figure 1.

(b) For facilities used for nuclear explosive operations and associated activities, the facility safety basis includes the Nuclear Explosive Safety Master Studies required by DOE-STD-3015-97, the generic accident analysis documented in the facility SAR, and the derivative TSRs. A generic accident is a synthesis of accident factors related to one or more nuclear explosive(s) that contain the largest quantity of explosives and nuclear materials expected to be resident in the facility. This enables the facility SAR to be developed for any nuclear explosive operation(s) likely to be performed in the facility. Specific nuclear explosive operations and technical details may (or may not) have been developed when the SAR is being produced. The facility safety basis also includes facility safety programs described in the SAR.

(c) The operation safety basis for nuclear explosive operations and associated activities includes the Nuclear Explosive Safety Studies required by DOE-STD-3015-96, the operation-specific hazard analysis documented in the HAR, and the derivative NESRs and OSCs. The safety basis for performing a specific nuclear explosive operation in a specific facility is the combination of the general facility safety basis and theoperation-specific safety basis. This is depicted in Figure 1.

(d) A nuclear explosive operation considered for introduction into a facility must be evaluated to ensure that the operation is within the facility safety basis. DOE-DP-STD-XXXX-96 specifies the process for evaluating whether the operation safety basis is within the facility safety basis.

(6) Applicable Orders and Standards.

(a) DOE O 232.1, OCCURRENCE REPORTING AND PROCESSING OF OPERATIONS INFORMATION, dated 9-25-95.

(b) DOE O 420.1, FACILITY SAFETY, dated 10-13-95.

(c) DOE 5480.22, TECHNICAL SAFETY REQUIREMENTS, dated 9-15-92.

(d) DOE 5480.23, NUCLEAR SAFETY ANALYSIS REPORTS, dated 3-10-94.

(e) DOE 5480.24, NUCLEAR CRITICALITY SAFETY, dated 8-12-92.

(f) DOE M 232.1-1, OCCURRENCE REPORTING AND PROCESSING OF OPERATIONS INFORMATION, dated 9-25-95.

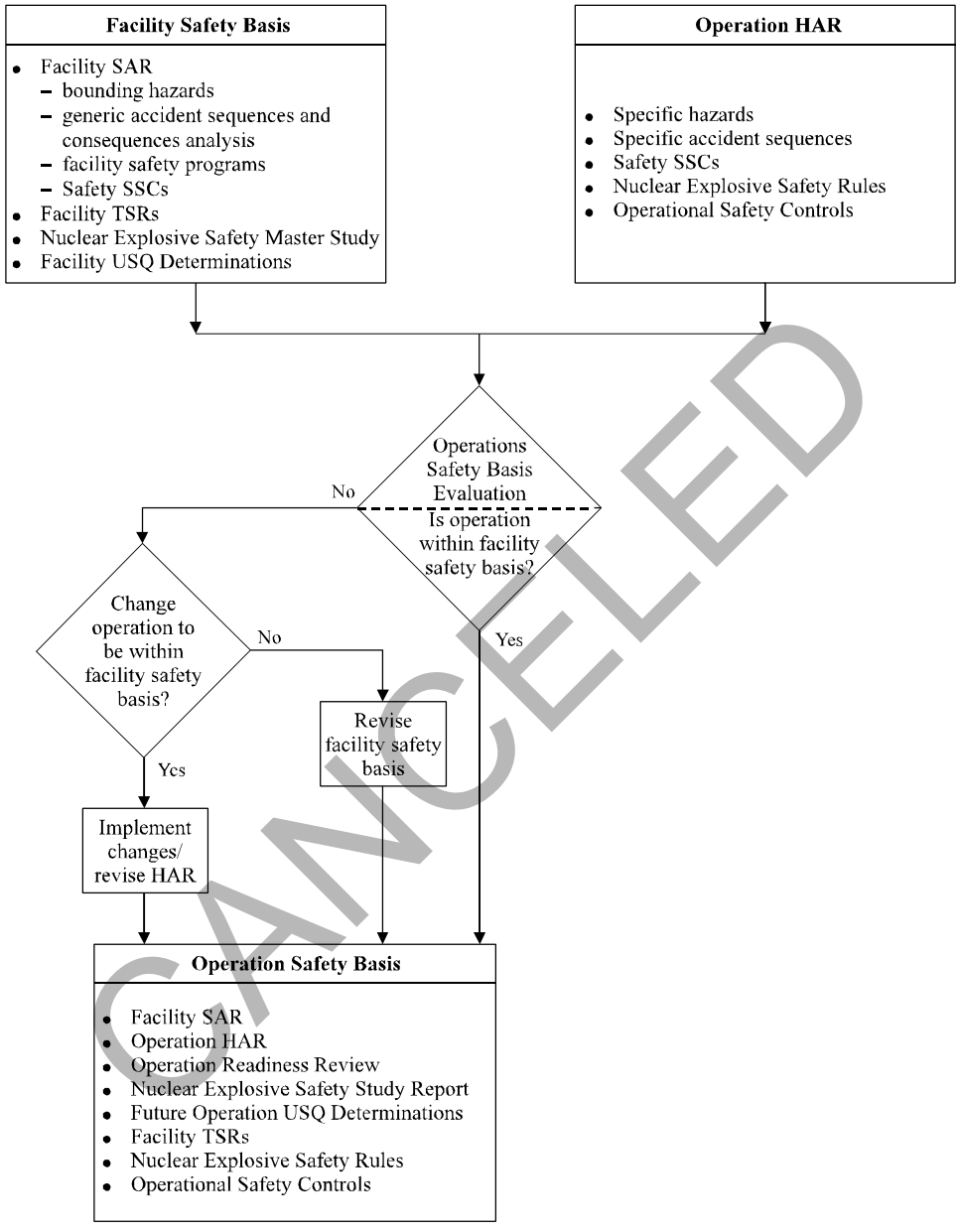

Figure 1. Safety Basis of a Nuclear Explosive Operation

(g) DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports*, dated 7-94.

(h) DOE-STD-3015-97, *Nuclear Explosive Safety Study Process*, dated 10-96.

(i) DOE-DP-STD-XXXX-96, *Preparation Guide for U.S. Department of Energy Hazard Analysis Reports for Nuclear Explosive Operations*, TBD.

(7) References.

TP 20-7, *Nuclear Safety Criteria*, dated 9-1-86.

f. Process Design.

(1) Introduction. Defense-in-depth is a safety management concept for process design that considers the synergistic effects of multiple layers of protection (e.g., equipment and facilities design, procedures, training), which collectively contribute to accident prevention and/or consequence mitigation. These layers of protection include equipment, people, facilities, and procedures.

(2) Tooling and Equipment.

(a) The following design criteria guidance applies.

1 Safety critical equipment should be designed to remain in a safe condition should a system or component fail.

2 Tooling, equipment, and layout should be designed and used in a manner that precludes introduction of unintended energy to nuclear explosives, including mechanical, thermal, electrical, radiation, and chemical energy.

3 Tooling and equipment should not include or otherwise introduce hazardous chemicals that could create hazardous or mixed (radioactive and hazardous) wastes.

4 The layout design should preclude the possibility of the tooling or equipment from making unintended contact with or striking the high explosive.

5 All tooling and equipment that apply energy to the nuclear explosive should have documented design criteria.

6 The tooling and equipment design process should incorporate human factors engineering to:

a minimize the likelihood of accident initiation from human interactions and to enhance worker safety;

b protect workers from serious injury caused by industrial or radiological accidents; and

c apply industry standards and guidelines, where appropriate, as early as practical in the tooling and equipment design process.

7 Safety-critical tooling and equipment should be designed to contain two or more independent physical safety features with no common mode of failure.

8 Tooling and equipment should be designed, fabricated, tested, approved, and available for credible contingencies and alternate processes.

9 Tooling, equipment, and layout should be designed to minimize exposure of personnel to hazards.

(b) Reliability measures provide a layer of defense against equipment failures that may have an adverse impact on safety. The following guidance applies.

1 Reliability of tooling and equipment should be optimized by applying appropriate standards to their design, fabrication, installation, testing, inspection, maintenance, storage, and use. The use of industry standards criteria should be based on their applicability to nuclear explosive operations.

2 Preventive and predictive maintenance programs should be established for tooling and equipment.

3 Post-maintenance testing procedures should be established for safety class and safety significant tooling and equipment.

(c) A checkout on a trainer with the actual tooling and equipment should be considered where possible to verify that potential human interactions with significant safety impact are not overlooked in the design process.

(3) People. Personnel selection, training, and qualification requirements provide a layer of defense that ensures that personnel performing nuclear explosive operations are reliable and adequately qualified to carry out operations. A system should be established to verify that personnel are qualified and, as appropriate, certified to perform their functions. The fitness for duty requirements of the PAP along with a personnel management system that can effectively process derogatory information and reach decisions concerning acceptability/removal of personnel assigned nuclear explosive duties are key factors to ensure personnel reliability.

(4) Facilities. The facility safety basis requirements provide a layer of defense that ensures the facilities are designed, built, modified, and maintained in a manner that recognizes and controls the hazards associated with expected operations. Safety envelope control requirements ensure that facilities are maintained and controlled in a manner consistent with the requirements of the SAR and TSRs. A formal program for tracking SAR/TSR surveillance requirements and status and a system for positive verification of compliance should be established.

(5) Procedures. A rigorous approach to preparing and adhering to procedures provides a layer of defense in conducting nuclear explosive operations and associated activities. Procedures should have the following attributes.

(a) Comply with design specifications and technical requirements.

(b) Clearly state cautions and warnings.

(c) Have design laboratory review and approval.

(d) Place proper emphasis on preventing an accident, detecting abnormal conditions, and protecting the worker, the public, and the environment.

(e) Identify appropriate points to safely interrupt work.

(f) Consider and incorporate waste minimization practices.

(g) Include sufficient information to perform the operation.

(h) Be organized so that operating personnel are not required to consult more than one document to accomplish a single process.

(6) Applicable Orders and Standards.

(a) DOE M 440.1-1, DOE EXPLOSIVES SAFETY MANUAL, dated 9-30-95.

(b) MIL-STD-1472D, *Human Engineering Design Criteria for Military Systems, Equipment and Facilities.*

(7) References.

None

g. Internal Safety Reviews.

(1) Internal Safety Review Program. As required by DOE O 452.2A, DOE contractors and laboratories must establish an internal, objective, and independent safety review program. The safety review program normally functions in an advisory capacity to line management. An internal safety review program should do the following.

(a) Be defined and delineated in writing (e.g., purposes, objectives, functions, authority, responsibility, composition, quorum, meeting frequency, and reporting requirements).

(b) Allow for the safety review function to report to a designated official at a sufficiently high level of management who will take necessary corrective action.

(c) Be recorded in sufficient detail to permit contractor management and DOE to evaluate the system's effectiveness.

(d) Be performed by personnel with technical discipline competence in the areas being reviewed.

(e) Be performed by independent personnel, i.e., those who did not perform or direct the work.

(f) Provide an opportunity for group discussions among safety reviewers.

(g) Serve as an independent determination of whether a proposed activity involves an unreviewed safety question (USQ), violation of a TSR/OSC/NESR, deviation from a safety analysis premise, or any other safety concern.

(h) Include the following.

1 Proposed modifications to facilities and equipment affecting safety;

2 Administrative, operating, maintenance, repair, testing, quality assurance (QA), immediate-action, and emergency procedures;

3 Training programs, qualification and certification requirements, and associated procedures;

4 Reports of occurrences, root cause analyses, and corrective action plans;

5 Safety analyses and evaluations;

6 Nuclear Explosive Safety Study input documents;

7 CM program plans and procedures;

8 QA program plan;

9 Maintenance implementation plan;

(i) Be reviewed for adequacy by management at least once every 3 years.

(2) Applicable Standards.

None

(3) References.

None

h. Readiness Reviews.

(1) Introduction.

(a) The essential attributes of DOE 5480.31 or DOE O 425.1 readiness reviews should be applied to nuclear explosive operations and associated activities to establish readiness review requirements for startup and restart of specific nuclear explosive operations. Some facility-based requirements do not apply to an operations-based activity. Also, there are additional requirements for readiness reviews that are specifically relevant to nuclear explosive operations.

(b) This section identifies the attributes of DOE 5480.31 or DOE O 425.1 readiness reviews that are considered essential and are expected to be included in the readiness review process for nuclear explosive operations. This section also provides examples of some features of nuclear explosive operations that require special consideration.

(2) Essential Attributes.

(a) Both the organization responsible for the operation and DOE perform independent readiness reviews.

(b) The readiness reviews provide independent reviews of readiness and will not be used as management tools to achieve readiness.

(c) The readiness review is formally documented in a manner equivalent to the specifications of DOE 5480.31 or DOE O 425.1

(plan-of-action, implementation plan, final report, and finding resolution).

(d) Contractor line management certification of readiness is a prerequisite for beginning the independent contractor readiness review.

(e) Certification of readiness by contractor management to DOE line management and by DOE line management to the operation approval authority is a prerequisite for beginning the DOE readiness review.

(f) Readiness reviews are conducted by qualified personnel with assessment expertise, who are independent of the operation being reviewed. Independent in this context means that personnel will not review their own work or work for which they were responsible. Senior members should not be from the line organization responsible for the operation; variance from this requirement may be granted by the appropriate approval authority.

(g) The breadth of readiness reviews includes applicable core requirements derived by the cognizant Operations Office from DOE 5480.31 or DOE O 425.1, plus any review areas unique to the operation.

(h) The readiness review team develops and documents the criteria and reviews approaches prior to beginning the review.

(i) DOE readiness review findings are categorized as prestart or post-start.

(j) All prestart findings are corrected prior to startup or restart of the operation and verified as closed by DOE.

(3) Additional Guidance. Refer to DOE 5480.31 or DOE O 425.1 and DOE-STD-3006-93 for additional guidance.

(4) Additional Considerations for Nuclear Explosive Operations.

(a) DOE 5480.31 or DOE O 425.1 requirements do not specifically address the startup or restart of an operation within an operating

facility. A comparable process for startup and restart of nuclear explosive operations is needed to fulfill DOE O 452.2A requirements. In addition, there are nuclear explosive safety requirements that must be satisfied prior to authorizing the operation.

(b) The following are some of the aspects of nuclear explosive operations that should be considered in the readiness review program for these operations.

1 DOE O 452.2A and Operations Office-specified criteria for when a readiness review is required.

2 Grading of readiness review requirements for startup or restart of operations where a full scope readiness review is not necessary (e.g., startup of an operation that is essentially the same as a fully reviewed and approved operation).

3 Interfaces between the operation and the facility, facility support systems, and facility environment, safety, and health programs.

4 A conditional startup authorization based on reviewing the operation conducted on a trainer, followed by a final authorization based on reviewing the operation conducted on a nuclear explosive.

5 Integrating the expertise of the design laboratories into the review process.

6 Additional nuclear explosive safety activities that are required prior to authorizing the operation (e.g., the Nuclear Explosive Safety Study).

(5) Applicable Orders and Standards.

(a) DOE 0 425.1, STARTUP AND RESTART OF NUCLEAR FACILITIES, dated 9-29-95.

(b) DOE 5480.31, STARTUP AND RESTART OF NUCLEAR FACILITIES, dated 9-15-93.

(c) DOE-STD-3006-93, *Planning and Conduct of Operational Readiness Reviews (ORRs)*, dated 11-93.

(6) References.

None