DNFSB/TECH-15

OPERATIONAL FORMALITY FOR DEPARTMENT OF ENERGY NUCLEAR FACILITIES AND ACTIVITIES

Defense Nuclear Facilities Safety Board

Technical Report

March 1997

OPERATIONAL FORMALITY
FOR
DEPARTMENT OF ENERGY NUCLEAR FACILITIES AND ACTIVITIES

This technical report was prepared for the Defense Nuclear Facilities Safety Board by the following staff members:

Steve Krahn
Matthew Moury

with assistance from:

Wayne Andrews
Dan Burnfield
Don Owen
and outside expert John Drain

FOREWORD

The Board has emphasized that when performing work involving hazardous materials, it is important to plan the work carefully, and to develop the controls and implementing procedures necessary to provide reasonable assurance that the work will be conducted safely. While the exact nature of these practices will vary depending on the work being performed, certain operational practices have evolved that have been effective. These operational practices are treated in this report as a composite forming what is termed "formality of operations."

John T. Conway
Chairman

EXECUTIVE SUMMARY

Commercial manufacturing organizations of all sizes have developed policies and practices, termed "formality of operations," to be followed by employees to ensure safety in the workplace, establish norms of performance, and promote work practices fostering efficiency and uniform product quality. For small companies, these "good engineering (or shop) practices" are often passed on by example and by word of mouth from journeyman to apprentice. Larger organizations usually codify these concepts in policies, requirements, and procedural documents to achieve desired practices on the shop floor, and such practices become an integral part of new employee training. When these policies and procedures are reinforced by all managers, from upper-level management to first-line supervisors, formality of operations becomes second nature.

As one might expect, the more fully developed and well-defined documents establishing formality of operations are found in industries with hazardous processes, such as chemical, nuclear, or mechanical. The common elements are the need to create a work environment in which operators are knowledgeable about their work tasks and know what to expect of and from coworkers; operating personnel have a thorough understanding of work hazards and corresponding mitigators, controls, and response actions; equipment is maintained within required standards by trained technicians to perpetuate designed safety; and evolutions take place in accordance with technically accurate procedures by thoughtful, attentive operators. The integration of these factors results in a safety culture that combines recognition of the facility's hazards, evaluation of risk, design for safety, and operation by trained and qualified personnel within established operating limits.

This report provides a detailed description of the concept of formality of operations. It also provides additional guidance on how to tailor a formality of operations strategy to different defense activities in the Department of Energy's complex, commensurate with the degree of hazard, the operational tempo, and the planned mission and remaining life of the facility.

TABLE OF CONTENTS

TABLE OF CONTENTS (concluded)

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

1.1 PURPOSE OF THIS REPORT

Safety is best achieved when it is made an integral part of work planning and performance. The Department of Energy (DOE), in response to Defense Nuclear Facilities Safety Board (Board) Recommendation 95-2, has committed DOE to upgrading its safety program to improve this integration. A principal objective is to ensure that operational controls for hazardous work and other operational commitments identified through hazard analysis and related work-planning activities are reflected in operational procedures and that operating personnel are trained and qualified to perform accordingly.

The integrated safety management (ISM) program, advocated by the Board and DOE, is structured around five core management functions: (1) define the scope of work, (2) analyze hazards, (3) develop and implement controls, (4) perform work within controls, and (5) provide feedback and continuous improvement. In the context of this report, the term "operations" is synonymous with the development of implementing procedures and the performance of work.

The Board has undertaken the development of a series of guides for use by its staff in assessing the adequacy of safety programs developed by DOE and its contractors for performing radiologically hazardous work. These guides will be structured to address the above core safety management functions and indicate what the Board has determined to be acceptable associated practices. This report represents the first of these guides.

Certain recognized good operational practices relative to performing hazardous work have evolved over the years. These are commonly found in operations manuals under such headings as conduct of operations, maintenance, configuration management, and qualification and training. The systematic selection and implementation of such practices is advocated and discussed in this report as "formality of operations."

The elements of formality of operations discussed herein are based on well-developed governmental (national and international) and industrial operating practices. Experience has shown that improved efficiency, product quality, and safety result when complex, hazardous tasks are accomplished in a formal, deliberate fashion following reviewed and approved procedures that implement industry-accepted practices, tailored according to the hazards involved. A good system of formality of operations, understood and practiced by all employees, is especially important in complex operations dealing with hazardous materials in the defense nuclear activities of DOE. There is also a close connection between the safety and the reliability of a plant. Equipment failures or human errors that could lead to accidents and subsequent harm to workers or the public have shortcomings in common with those that lead to low productivity and poor quality. Conversely, measures that contribute to plant safety will frequently help achieve a good record of operation.

The Board advocates safety management tailored to the hazard and complexity of an operation. The more hazardous and the more complex an activity, the more rigorous its safety management must be. A complementary concept is that lesser hazards and greater simplicity reduce the rigor required for purposes of safety. This means good engineering judgment must be applied to tailoring the safety program. Nowhere is this more essential than with respect to formality of operations. The process of designing such a program is, therefore, very subjective. To clarify how the process works, this report illustrates its concepts through their application to programs that have strikingly different operations. It is hoped that these examples will be useful when the general analysis is applied.

Thus, it must be kept in mind that this report speaks of a complete formality of operations program that is in keeping with Board Recommendation 95-2. This program is appropriately applied in practice by extracting what is essential to the specific operation being addressed.

This report sets forth the principles of operational formality in a logical framework. Though it deals specifically with activities at DOE's defense nuclear sites it should also help promote the concept of a safety culture[1] marked by a dedication to doing work safely. The concepts presented are fully consistent with the requirements in the Occupational Safety and Health Administration's (OSHA) 29 Code of Federal Regulations (CFR) 1910.119, *Process Safety Management of Highly Hazardous Chemicals*, and the guiding principles set forth in the Implementation Plan for Recommendation 95-2. It is expected that application of the practices described in this document will not only contribute to achieving a high degree of safety, but also lead to more efficient and economical operations.

1.2 BACKGROUND: PREVIOUS BOARD COMMENTS ON FORMALITY OF OPERATIONS

The Board has been urging DOE to adopt a level of formality in its operations that is commensurate with the risks involved.

The Board's 1991 *Annual Report to Congress* makes the following observations regarding the essentially equivalent concept of "discipline of operations":

> Operations are conducted in a disciplined manner when facilities are constructed in full accordance with approved plans and instructions; when drawings accurately portray the facilities as they actually have been built; when approved procedures are available and are used for testing, operations, and maintenance; when training and qualification of operators are accomplished

[1] The term "safety culture" is defined in Section 3-1.

using these procedures; and when quality assurance activities provide independent confirmation that all the foregoing have been and are being accomplished (Defense Nuclear Facilities Safety Board, 1991).

In 1992, the Board issued Recommendation 92-5, calling for observance of a high level of "conduct of operations" at DOE's active defense nuclear facilities. Like formality of operations, the term "conduct of operations" is used broadly here, in effect being equated with the full range of operational practices followed to ensure safety (Defense Nuclear Facilities Safety Board, August 17, 1992).

In 1995, the Board issued Recommendation 95-2, calling for the institutionalization of recognized good practices for safely planning and performing DOE's radiologically hazardous activities. Among the commitments made in the Implementation Plan submitted by DOE in response is the preparation of a guide dealing with each of the core functions, including operational practices.

1.3 REPORT ORGANIZATION

Section 2 describes two important items that must be developed in conjunction with a formality of operations program: the basis for safe operations and the basis for performance standards. Section 3 sets forth several underlying concepts that are essential to the successful implementation of a formality of operations program. Section 4 gives an overview of the four key elements of formality of operations, while Section 5 addresses the tailoring of those elements and their subelements to meet the needs and circumstances of a specific facility or activity. Section 6 describes the elements and subelements in detail. Section 7 provides two examples of the implementation of a formality of operations program. Section 8 addresses the linkages among the formality of operations key elements and between those elements and other functional areas. Finally, Section 9 presents conclusions.

2. BASIS FOR OPERATIONS AND SELECTED STANDARDS

Principle: The work planning/safety planning process must be accomplished within a framework of policies, rules, and requirements (other than rules) that are established by DOE and/or are applicable good practices within the commercial industry.

DOE has defined the basic framework for nuclear safety management of its varied activities. Taken as a whole, this framework represents an expected mode of conduct by DOE and its contractors. The operational formality program described in this report could be considered a mature program. It is recognized that facilities or activities are currently at varying levels of maturity in the implementation of such a program.

Principle: The health and safety of the public and workers rest on a properly trained workforce accomplishing tasks in a formal, deliberate fashion in accordance with reviewed and approved requirements and procedures that are tailored to the hazards involved.

In conjunction with developing a formality of operations program for any site, facility, or activity, two important items must be developed, understood, and for DOE and its contractors, agreed upon. The first is the analysis and resulting controls that form the basis for ensuring safe operations. The second is the adoption of practices or safety program commitments to ensure that the work is performed to generally accepted safety standards.

In response to Board Recommendation 95-2, DOE has committed to an integral work planning/safety planning process for DOE defense nuclear facilities, resulting in the definition of derived safety controls that are conditions for performing work. The derived safety controls and commitments are implemented by procedures or other technical work documents and practices, and workers are trained to know and understand the safety controls and their purpose. A discussion of the necessity for and composition of these items can be found in two Board technical reports: *Fundamentals for Understanding Standards-based Safety Management of Department of Energy Defense Nuclear Facilities*, DNFSB/TECH-5 (DiNunno, May 31, 1995) and Safety Management and Conduct of Operations at the Department of Energy's Defense Nuclear Facilities, DNFSB/TECH-6 (Kouts and DiNunno, October 6, 1995). The process, based on the safety management functions defined in DOE's Implementation Plan for Recommendation 95-2, is discussed in detail in a Board staff paper on work planning and performance.

An overall objective of integral work planning/safety planning is to ensure that tailored controls and other safety-related commitments are identified and applied to a defined scope of work. In other words, work planning/safety planning involves efforts to analyze hazards, identify the controls and commitments that provide inherent safety in the performance of work, and

implement these controls. Work planning/safety planning occurs at multiple levels, including site-wide, individual building/facility, and activity-specific. Results come into focus at the activity level, for example, stabilization of plutonium residues.

3. UNDERLYING CONCEPTS

Three underlying concepts must be understood and accepted if an organization is to benefit from implementing formality of operations as described in this report: safety culture, defense in depth, and a framework of controls.

3.1 SAFETY CULTURE

Principle: An established safety culture is distinguished by both attitudes and accepted practices. It governs the actions and interactions of all individuals and organizations engaged in hazardous activities.

The International Nuclear Safety Advisory Group (1991:1) succinctly defines safety culture as " . . . that assembly of characteristics and attitude in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance." The concepts and principles described in the present report, while essential to safe operations, are not sufficient if applied mechanically. According to the International Nuclear Safety Advisory Group (1991:1), there is a ". . . requirement to go beyond the strict implementation of good practices so that all duties important to safety are carried out correctly, with alertness, due thought and full knowledge, sound judgment and a proper sense of accountability." This requirement includes adherence to safety limits and standards during all activities.

3.2 DEFENSE IN DEPTH

Principle: Defense in depth provides an overall strategy for safety measures and features. When properly applied, it ensures that no single human or mechanical failure would lead to injury, and even combinations of failures that are only remotely possible would lead to little or no injury.

Defense in depth is implemented primarily through a series of barriers that should in principle never be jeopardized, and must in turn be violated before harm can occur to people or the environment. The International Nuclear Safety Advisory Group Safety Series No. 75-INSAG-3 (International Nuclear Safety Advisory Group, 1988:64) provides a detailed discussion of defense in depth and its application to nuclear power plants. The principle is equally applicable to other radiologically hazardous activities.

3.3 FRAMEWORK OF CONTROLS

Principle: Operations are conducted within a framework of controls intended to preserve the designed-in capability of structures, systems, and components important to safety and protection of the environment.

The framework of controls is structured around conduct of operations, maintenance and surveillance, training and qualification, and configuration management. These same programs are the key elements of an operational formality approach and are described in the next section.

4. KEY ELEMENTS OF A FORMALITY OF OPERATIONS PROGRAM

The key elements of a program of formality of operations encompass the set of practices used to ensure safety in a facility and in the operations conducted therein. That program forms an integral part of the broader concept of a safety culture (see Section 3.1). These key elements, although perhaps defined differently for different facilities or activities, are necessary for any operation in which both product quality and safety are required, though cost-benefit considerations may lead to different degrees of application in grading for facilities with different levels of hazard. The "normal components of formality in an intensive program of conduct of operations" described in DNFSB/TECH-6 (Kouts and DiNunno, October 6, 1995:3–4) are captured under each of these key elements, as shown in the appendix. The guiding principles of the four key elements with respect to safety can be defined as follows:

Conduct of Operations

Principle: Safe conduct of operations generally requires application of both technical and administrative controls.

Maintenance and Surveillance[2]

Principle: Structures, systems, and components (SSCs) or equipment and tooling that perform safety-related functions, or systems and components that support these SSCs, must be periodically tested, serviced and maintained so that they are capable of performing their functions as intended throughout the life of the activity in the facility.

Training and Qualification

Principle: Properly trained and qualified personnel must understand their workplace hazards, safety programs, system and equipment operation and interrelationships, and procedures so they can perform their assigned work safely and efficiently. Training emphasizes the rationale behind the safety practices established, together with the consequences (for safety) of shortfalls in personal performance. Continuing training and periodic requalification ensure that personnel maintain and improve their technical knowledge and proficiency.

---

[2]DNFSB/TECH-5 (DiNunno, May 31, 1995) lists "test and surveillance" as a separate element. Since test and surveillance programs are largely maintenance functions, although requiring additional controls and formality, they are combined in this report with the maintenance program under the maintenance and surveillance element for purposes of clarity.

Configuration Management

Principle: SSCs that serve a safety-related function are identified, documented, and controlled. The fundamental objective of configuration management is to establish and maintain consistency among the facility design basis, physical configuration, and facility documentation for safety-related equipment and supporting systems.

Each of the above four elements must exist, to some degree, for all hazardous operations. Each comprises several subelements that are described in greater detail in subsequent sections. These elements and their subelements constitute the breadth and the manner of tailoring defines the depth of a formality of operations program. The subelements presented are intended to be illustrative and may not contain all the criteria that exist at DOE facilities.

These key elements do not exist as separate entities. They draw heavily on each other (and on other areas of an integrated safety management program, as discussed in DNFSB/ TECH-5 [DiNunno, May 31, 1995]), and when properly integrated create a strong and effective program of formality of operations.

5. TAILORING METHODOLOGY

Principle: In application, the breadth and depth, or tailoring, of a formality of operations program must be reviewed to ensure that each subelement within each key element is appropriate to the activity under consideration. Those subelements deemed applicable should be tailored to match the associated hazards that may be present or the degree of control required to protect workers, the public, and the environment. Those deemed inapplicable, inappropriate, or redundant should be eliminated.

For commercial manufacturing facilities, the depth to which each subelement is implemented depends on the hazards associated with the material being processed, the manufacturing complexity, the product quality requirements, the operational tempo or required manual activities, and the duration of the production run. Similarly at nuclear facilities, the depth to which each subelement is implemented depends on the hazards associated with the activity, the operational tempo, and the remaining life or mission of the facility or activity. For example, a high-hazard nuclear facility with ongoing operations and an extended mission life would have a much more complete formality of operations program than would a low-hazard facility or a manufacturing plant with low hazards and lack of complexity. Moreover, a short-duration or one-time activity can be accomplished with tailored controls. For example, the presence of experts and administrative controls can be used in lieu of fully engineered controls for some activities of limited duration.

This tailoring approach is similar to that used for establishing the breadth and depth of DOE's Operational Readiness Reviews (ORRs) (U.S. Department of Energy, October 26, 1995). Figure 1 shows some of the key elements and subelements of a formality of operations program, which are analogous to the core requirements for an ORR (see Section 6 for detailed descriptions). Each of the key elements and subelements should be addressed and the rationale understood for excluding any from a program. In accordance with the tailoring approach outlined above, if a subelement is needed to control a hazard, the degree of its implementation is tailored based on the hazard. Table 1 shows a possible scheme for rating the degree of formality of operations for the key elements and subelements based on the above criteria. The key elements and subelements shown in the table are not all-inclusive, but provided only to illustrate a possible approach.

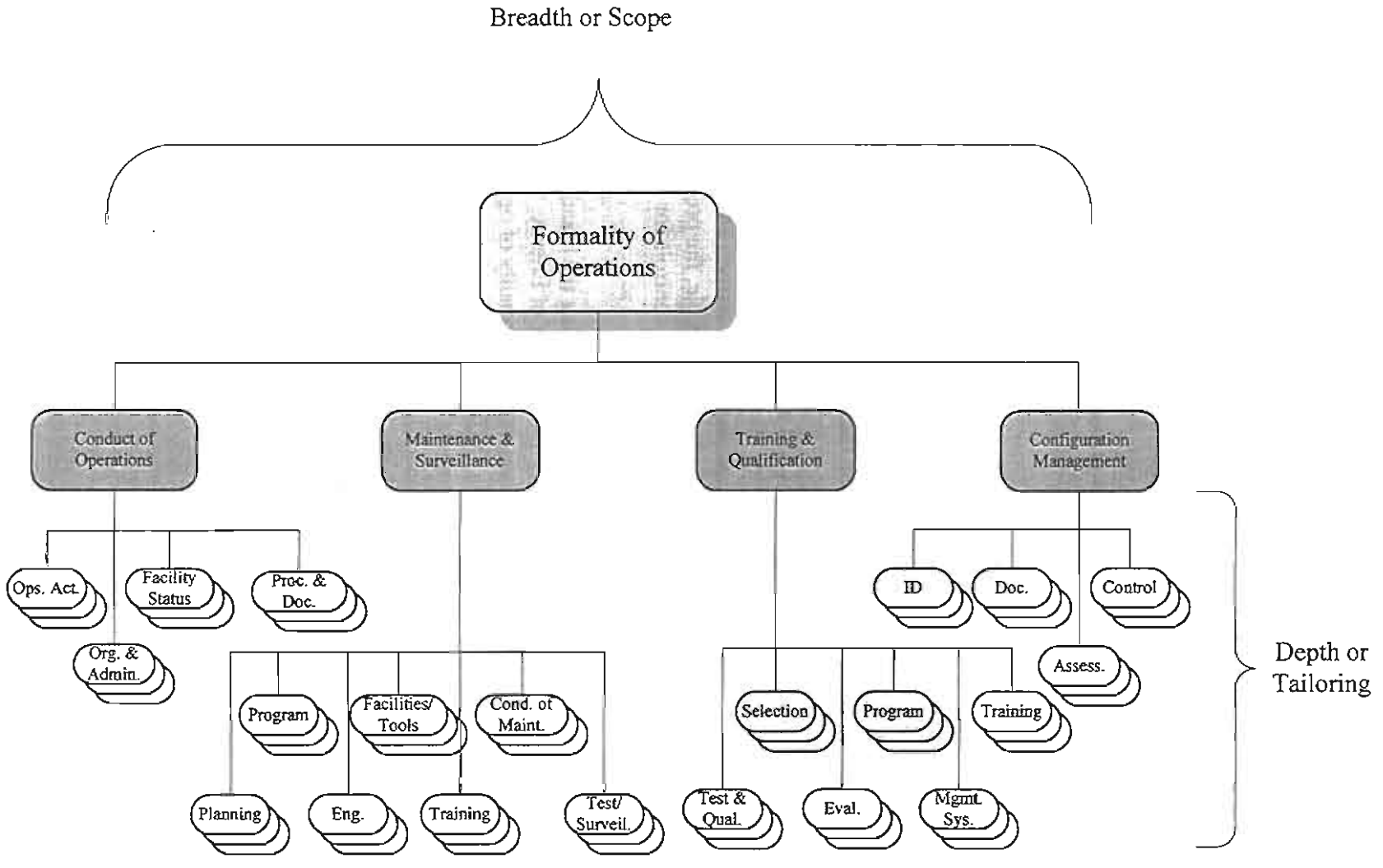

Figure 1. Formality of Operations: Breadth and Depth

Table 1. Example of Methodology for Tailoring Formality of Operations

Criteria	Sample of Formality of Operations Key Elements and Subelements						
	Conduct of Ops.	Facility Status Control	Maintenance	Maintenance Engineering	Surveillance	Training and Qualification	Configuration Management
High Hazard High Op. Tempo Ongoing Mission	A	A	A	A	A	A	A
Moderate Hazard Low Op. Tempo Ongoing Mission	B	A	A	B	A	B	B
Low Hazard Low Op. Tempo Short-Duration Mission	B	B	B	C	C	B	C

Typical Degree of Formality of Operations (Grade):
- **A - Full Implementation**
- **B - Partial Implementation**
- **C - Limited or No Implementation**

In the first case shown, all the elements are fully implemented because of the facility or activity's high hazards, high operational tempo, and long-term mission. In the second case, a lower operational tempo may allow for partial implementation of several elements not required to control a hazard, such as conduct of operations, maintenance engineering, training, and configuration management. For the last case, with limited hazards, a low operational tempo, and a short-term mission, many elements may not be required, such as facility status control or configuration management.

6. FORMALITY OF OPERATIONS ELEMENTS AND SUBELEMENTS: DETAILED DESCRIPTION

This section describes in detail the elements and subelements of a formality of operations program at industrial sites and defense nuclear facilities. These descriptions are intended to be comprehensive and to illustrate each element fully. However, programs would rarely contain all subelements. Therefore, to explain the concept of tailoring more fully, Section 7 provides case studies applying the formality of operations concept to depleted uranium hexafluoride (UF_6) cylinder storage and to assembly and disassembly of nuclear weapons.

6.1 CONDUCT OF OPERATIONS

Conduct of operations includes those management and administrative controls necessary to ensure that operations and maintenance are conducted safely and that the authorization basis for the facility or activity is preserved; it also encompasses the methodology for ensuring compliance with these controls. It is governed by four fundamental subelements: operational activities performed in a systematic manner that promotes safety; an organization with defined responsibilities and accountability, staffed by properly trained personnel; facility and equipment status known at all times, with changes in status being controlled by operations personnel; and activities governed by properly developed, approved, and controlled procedures and documentation. A detailed discussion of these four subelements follows (see also Figure 2):

- **Operational activities** are conducted in a way that ensures their safety and reliability. Operations are accomplished by deliberately complying with reviewed and approved procedures and using appropriate formality in communications, while still maintaining an inherently questioning attitude. Personnel are taught to understand and think about the results of each component/system control action before acting. When shift turnover is performed, incoming personnel receive an accurate picture of the overall status of the facility. The turnover is formal and includes a thorough review of appropriate documents describing important aspects of the status of the facility; it may also include a tour of the facility in sufficient detail to ensure that the status of facility systems is known. Plan-of-the-day/week meetings are conducted to facilitate coordination of activities in the facility between operations and support organizations.

- The operational **organization and administration** ensures effective implementation and control of operations activities. A clear chain of safety responsibility and communication is established and documented, and the resources and facilities and equipment necessary for the activity are put in place. Line management's responsibility for safety, quality, and staffing of the facility with adequate numbers of

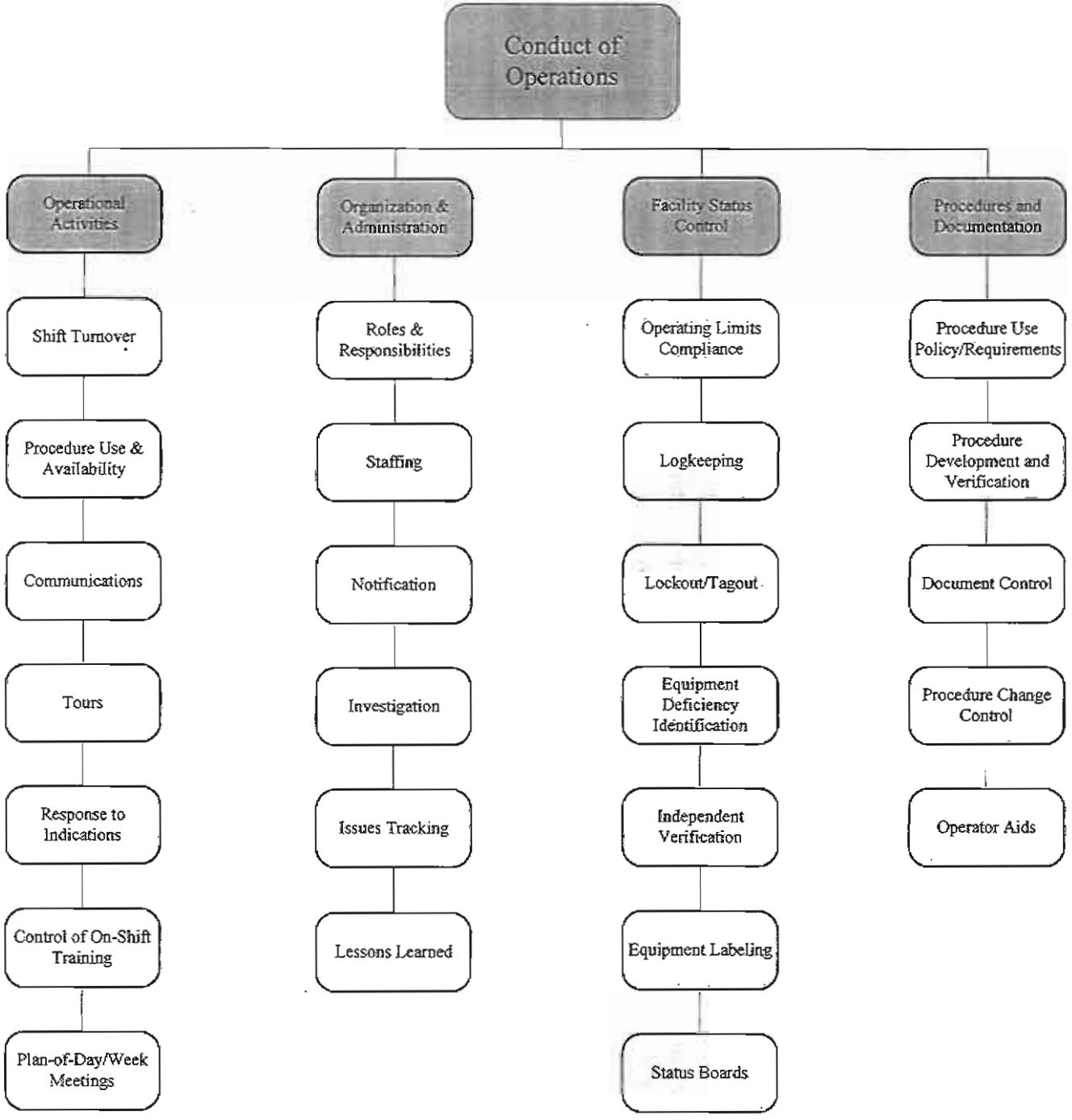

Figure 2. Conduct of Operations Subelements

trained personnel is clearly understood, and there is no confusion about the fact that line management is in charge. Line management establishes policy for adherence to safety requirements, as well as technically sound procedures for operation and safety control of the facility under all conditions (including maintenance and surveillance). Facility management institutes measures to ensure that events that could adversely affect safety are detected and evaluated for root cause, and that any necessary corrective measures are taken promptly.

- Operations personnel are aware of the **status of facility systems and equipment** under their control, and they ensure that those systems and equipment are used in ways that support safe and reliable operation. The facility is operated in compliance with operational limits and conditions approved in the authorization basis. The status of that compliance is verified at a frequency established to ensure that operations remain within those limits and conditions. System lineups on safety-related equipment are performed and verified following a state in which the facility or system has been shut down for a protracted period or has undergone maintenance. A program exists to protect personnel and equipment through proper control of the status, including independent verification of placement and removal of "do not operate" tags, caution tags, and warning tags. Timely, accurate, and sufficiently detailed records (round sheets or similar logs) of the values of important safety parameters exist to describe facility activities and status. An equipment labeling program also exists to ensure that operations and maintenance personnel can positively identify equipment operated or repaired. The use of color coding and labeling for pipes, valves, and components can also assist in proper equipment identification and avoidance of confusion.

- **Operations procedures and documentation** are clear, are technically accurate, and provide a level of detail appropriate for the activity, and authorization basis controls are properly implemented so equipment and systems can be operated safely. For more hazardous operations, line-by-line adherence to the procedures with check-off after each step may be necessary. Frequent performance of less-complex operations may require only that the procedure be available to be consulted at the workstation, depending on the maturity of the training and qualification program. Less-detailed procedures may be appropriate for lower-hazard operations or routine operations with highly skilled operators. Some operations by their very nature must remain flexible, and it might be possible to rely on the operators' "skill of the trade" to perform them with procedures that provide only safety limits for the activity. Examples might be most machining operations; low-complexity, repetitive operations; or certain research and development activities. Procedures are marked as to the level of use required to ensure safe operation. Actions to be taken by operators if a procedure cannot be followed as written are clearly defined. Methods for developing procedures, including procedure format, content, and operator involvement during procedure development, are defined. Procedures are developed for normal, abnormal, and emergency conditions. Approval of procedures by appropriate levels of management is required.

A formal process exists for review and approval of revisions to procedures, with changes receiving the same depth of review and level of approval as the initial versions. Both new and revised procedures are reviewed before issuance and at periodic intervals to ensure that the information and instructions are technically accurate and that appropriate human factors considerations have been included. An operator aid program is developed such that the aids are properly developed, approved, and posted, and contain information useful to operators in performing their duties.

6.2 MAINTENANCE AND SURVEILLANCE

Maintenance and surveillance (which is timely monitoring for performance degradation) includes all actions necessary for maintaining a system or product in or restoring it to a desired operational state. Structures, systems, and components (SSCs) or equipment and tooling that serve safety-related functions are the subject of a maintenance program tailored to their function and to operational requirements. This program ensures that such SSCs can perform their safety functions reliably throughout the life of the facility. It is based on a comprehensive understanding of system and equipment design and includes an appropriate mix of corrective, preventive, and predictive maintenance. This program also includes periodic functional testing and surveillance of safety-related systems to ensure that essential safety functions are fully operable. Administrative controls are applied that are appropriate for the work being performed and the skills of the personnel accomplishing it. The seven subelements of this key element are described in detail below (see also Figure 3):

- A **maintenance program** document is developed for the facility or activity, explicitly defining roles and responsibilities for maintenance and delineating required staffing levels and training. The responsibility of maintenance personnel for keeping operations staff aware of work in their facilities is explicitly defined. This document also describes the maintenance strategy, i.e., the mix of preventive, predictive, and corrective maintenance functions, including periodic inspections. Expectations for levels of procedural compliance are also addressed, along with a program for monitoring and improving maintenance effectiveness through evaluation of performance indicators, trend analysis, and program feedback.

- To accomplish maintenance evolutions effectively, adequate **facilities, equipment, and tools** are required, including controlled storage for equipment, tools, supplies, and parts. These items are necessary to support maintenance training and the ability of the maintenance organization to keep a facility in the desired operational state. A well-run program of tool and equipment control and calibration ensures that these items can perform their functions.

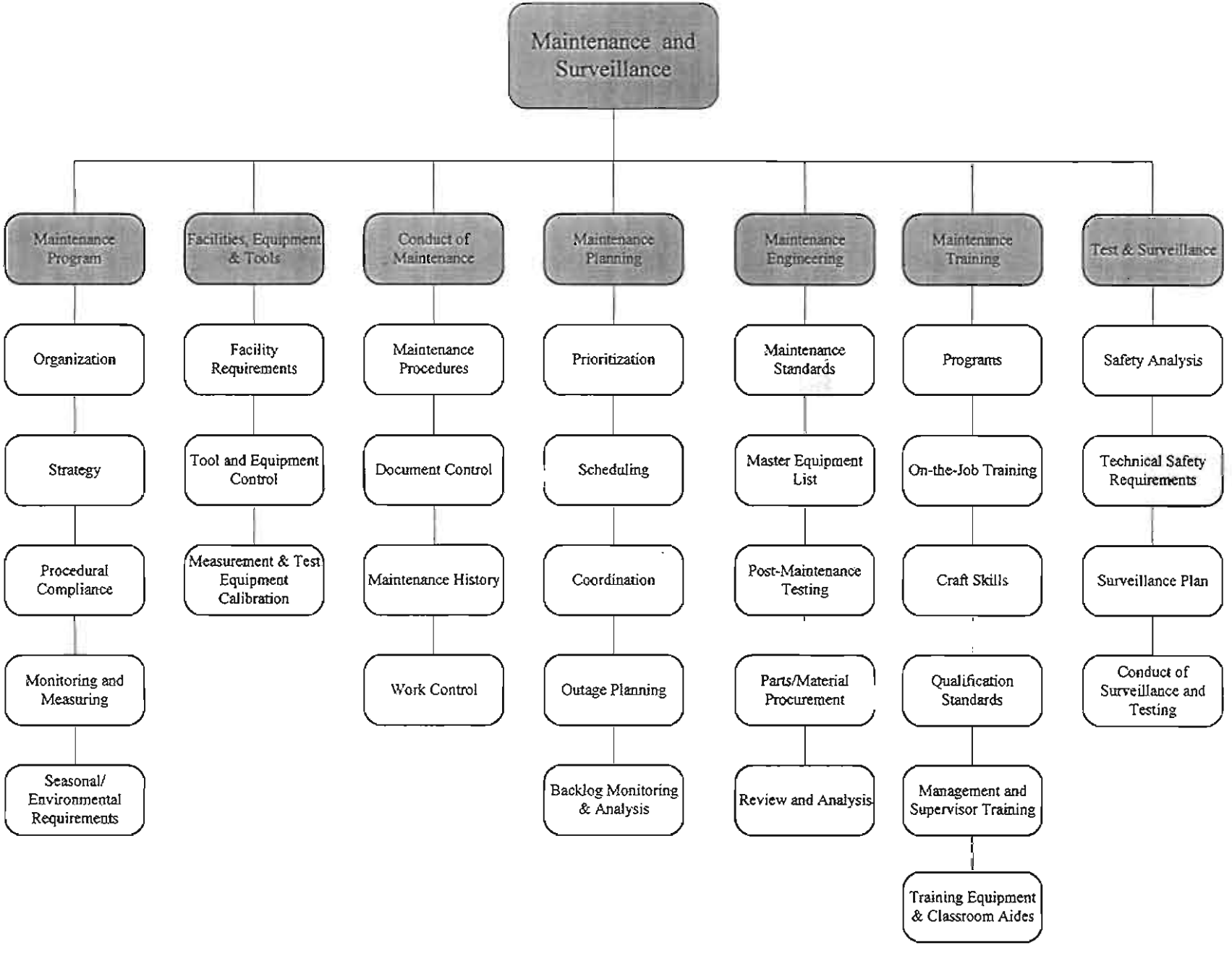

Figure 3. Maintenance and Surveillance Subelements

- Proper **conduct of maintenance** also plays a vital role in a good maintenance program. Of primary importance in conducting maintenance is an appropriately tailored work control program that includes guidance on subjects such as temporary repairs, troubleshooting, modifications, and performance of post-maintenance tests. Rigorous conduct of maintenance is grounded in adherence to appropriately scoped maintenance procedures that have been technically reviewed, particularly for safety aspects and impacts, and are subject to an adequate document control program. The record of completed evolutions is entered into the maintenance history of the equipment or system to ensure that trending information is readily available to maintenance engineers. This documentation contains sufficient detail to validate the use of approved procedures and properly qualified materials by trained technicians.

- **Maintenance planning** requires close coordination with operations personnel to ensure that maintenance does not compromise the safety of the facility or unintentionally disrupt the facility's mission. Additional considerations in planning maintenance include ensuring that scheduled maintenance (i.e., preventive and predictive maintenance and periodic inspections) is performed, incorporating as-low-as-reasonably-achievable (ALARA) methodology, minimizing risk to workers, and closely monitoring safety system availability so that corrective maintenance will be properly scheduled if required. As a part of maintenance planning, the backlog of maintenance actions is monitored closely and kept to a manageable level. Priority is given to returning safety-related equipment to operation.

- Several **engineering** functions are vital to the proper execution of maintenance tasks. These functions include developing maintenance standards; defining post-maintenance test criteria; determining the frequency, extent, and nature of surveillance testing; developing a master equipment list; and establishing requirements for replacement parts, equipment, and services. Also required are detailed engineering review and analysis of equipment failures and nonconforming materials, maintenance types and frequency, and root causes of systemic problems. With older equipment and systems, replacement parts may no longer be available from original sources. Engineering review to define requirements, maintain knowledge of qualified sources, and evaluate "like-for-like" or "equivalent" replacement may be required.

- **Training** for maintenance personnel is required in many areas. Foremost among these is the need for maintenance personnel to be constantly aware of the safety aspects of the tasks they are performing. This normally requires a combination of formal classroom training, on-the-job experience, and honing of craft skills. For personnel authorized to perform work on safety-related systems, special training is appropriate on system/component functions and interrelationships and on safety limits and conditions. Training equipment and classroom aides are used to facilitate understanding and retention of information acquired during training.

- **Test and surveillance** requirements are key to any facility's authorization basis. Surveillance is any regular monitoring for performance degradation. Surveillance requirements evolve from the safety analysis and are documented in the Technical Safety Requirements (TSRs). TSRs define the operating limits and surveillance requirements necessary to protect the health and safety of the public, and to reduce the risk to workers from any possible uncontrolled release of radioactive or other hazardous materials and from radiation exposure, such as that which could be due to inadvertent criticality. To ensure that the safe operation of the facility is maintained, these operating limits and surveillance requirements include testing, calibration, and inspection of the operability and quality of safety-related SSCs and associated support systems.

6.3 TRAINING AND QUALIFICATION

Training and qualification are necessary for hazardous operations whether at commercial manufacturing plants or at defense nuclear facilities. For a facility to be operated safely, management must institute a personnel selection, training, and qualification program that instills a culture whose goals are the achievement, maintenance, and advancement of qualification. This program includes continuing training to improve capabilities and maintain proficiency. The scope of this program is tailored to the hazards associated with the facility. The subelements of training and qualification are detailed below (see also Figure 4):

- The **selection of well-qualified personnel** is essential to facility safety. Operations supervisors are competent personnel knowledgeable about the results of the safety analysis and the operational limits of the facility or activity. The personnel selection process starts with a job and task analysis to identify the tasks required to accomplish that job, and the necessary skills, knowledge, or abilities for successful performance. This is followed by determination of criteria for education and experience (or equivalencies) to meet these requirements. Selection criteria are developed for individuals whose actions will be important to the safety of the facility, the public, other workers, or themselves. A process to ensure that selection standards are met is in place.

- **Training and qualification program analysis, design, and development** form the starting point for the establishment and conduct of a training and qualification program. This program trains and qualifies those individuals at all staff levels whose actions will affect the safety of operations. Training begins with training in hazard awareness for all personnel in the training program, and proceeds to development or enhancement of the skills and knowledge required by personnel to perform their work. This is followed by continuing training of personnel to maintain and enhance that knowledge and those skills. The training program is based on job and task analysis to determine the knowledge and skill levels appropriate for or required by the task(s)

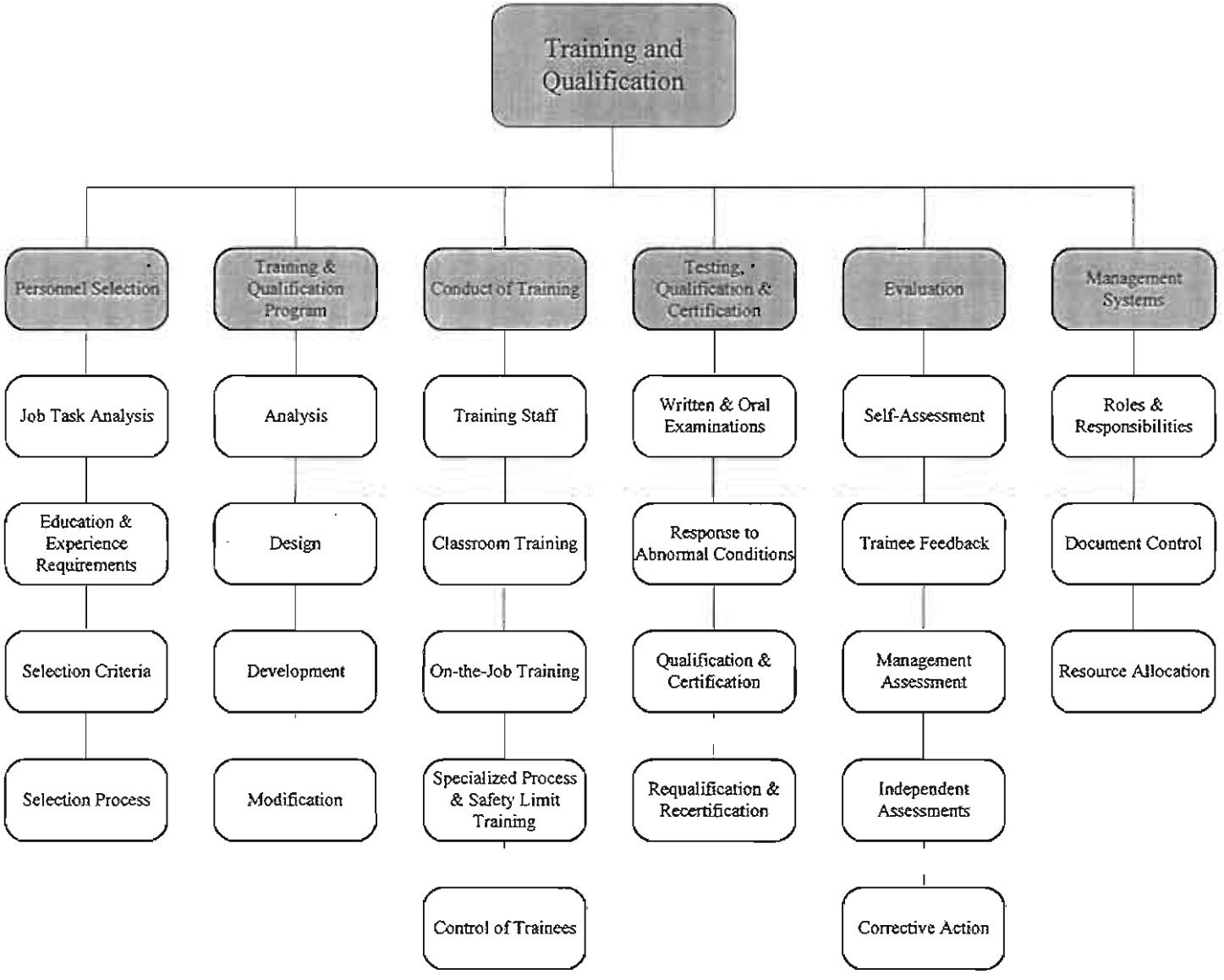

Figure 4. Training and Qualification Subelements

to be performed. It includes training in such fundamental areas as physics, chemistry, and math as appropriate to the general activities and processes performed. It also includes general topics such as radiological controls, technical support, the results of hazard analysis, operational safety limits, procedural adherence, and specific topics in process design and safety system design, as appropriate. The rigor of the training is commensurate with the associated hazards to the public, the workforce, and the environment.

- **Conduct of training** refers to the implementation of the training program discussed above. Elements of the implemented program include classroom instruction, on-the-job training, self-study, drills and emergency response exercises, and one-on-one discussion and performance evaluations. Retention of knowledge is evaluated periodically by oral and/or written examinations. Procedures are in place for designating personnel authorized to sign qualification records. The training organization ensures that trainers are properly qualified and that their performance is periodically evaluated. The process of evaluating on-the-job training is conducted by designated personnel knowledgeable in the operation being evaluated. During on-the-job training in the facility, the activities of the trainees are carefully monitored by qualified personnel to ensure that improper actions are not performed.

- **Testing, qualification, and certification** procedures include procedures for administering comprehensive final examinations, establishing criteria for evaluation, and if necessary, providing remediation. The use of written versus oral examinations is specified based on the hazard of the activity, with both types being used for higher-hazard activities involving more complex operations. A highly trained and formally qualified staff of operations, maintenance, and radiological control personnel is essential to safe plant operations. Oral examinations are conducted by boards and/or one-on-one by instructors during walkthroughs, which may include practical demonstrations. A process for periodic requalification and maintenance of proficiency exists. For positions more important to safety, formal certification of final qualification by line management is appropriate.

- **Evaluation** of the training and qualification program includes methods for determining the quality of the training and its applicability to the job tasks of trainees through periodic review and assessment. The evaluations are performed by the training staff, line managers, and independent assessment personnel. Evaluation of the training program is an ongoing process. The assessment program includes feedback from periodic evaluations of operations, drills and exercises, interviews, and audits of qualification records. Managers are responsible for providing feedback to the training manager on whether the training has been adequate to prepare workers for their assigned tasks.

- **Management systems** are needed to properly plan, manage, and oversee selection, training, qualification, and certification of personnel. Management is involved day-to-day in each of these functions. This involvement includes ensuring that training and qualification are accorded adequate resources, and that sufficient importance is placed on setting aside the time required for training and qualification/requalification.

6.4 CONFIGURATION MANAGEMENT

The configuration management program ensures that SSCs and equipment or tooling with a safety-related function are identified, documented, controlled, and periodically assessed. These are systems or equipment that provide defense in depth, or whose failure could adversely affect the environment or the safety and health of the public (see Section 3). The fundamental objective of configuration management is to establish and maintain consistency among the design, physical configuration, and documentation of the facility for those SSCs that are important to safe and reliable operation. Initial configuration management activities, whether conducted during design and construction or during reconstitution of the as-built design, are vital to establishing information as it is needed for the operational phase and the decontamination and decommissioning that will follow. An active configuration management program is also necessary during the operational phase of a facility's life. This program should help protect the integrity of the authorization basis for the facility by ensuring that proposed maintenance and/or modifications do not adversely impact the safety functions of SSCs. The program ensures that accurate drawings are available for system or equipment isolation during maintenance. The engineering organization is in charge of the configuration management program, and it provides support to other organizations in carrying out configuration management tasks. The four subelements of this key element are described in detail below (see also Figure 5):

- **Identification** of equipment and systems that serve a safety-related function, together with their design bases and functional requirements, is necessary to establish a baseline for configuration management. Criteria are developed for placing equipment in appropriate safety categories that will be used to determine the degree of change control to be exercised on activities associated with that equipment. All safety-related equipment, as identified in the authorization basis, is classified in accordance with these criteria.

- **Documentation** of configuration management activities includes drawings, system descriptions, databases, and other means used to document the design basis, functional requirements, and as-built configuration of safety-related SSCs. Facility design bases and functional requirements are developed for each piece of safety-related equipment, together with its safety category and associated drawings and system description documentation. Completion of approved changes is documented in a way that

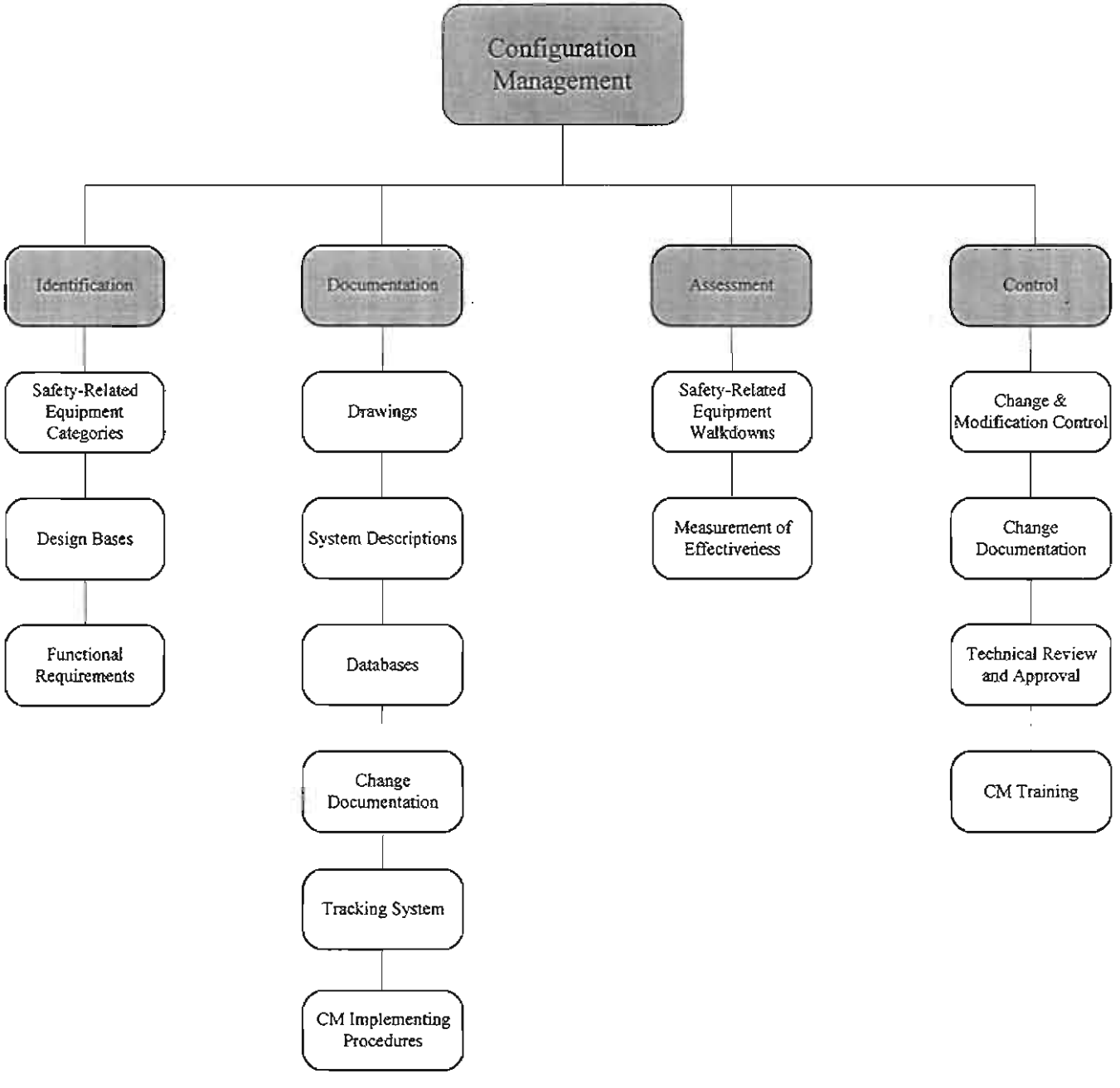

Figure 5. Configuration Management Subelements

allows tracing of all changes made since an initial configuration or design/as-built baseline. A tracking system is established to provide for each document the revision level, current status, document "owner," and any information regarding pending changes. This documentation is readily available to operations, engineering, maintenance, training, and other organizations needing such information. It may be appropriate to provide approved and up-to-date copies of safety-related system drawings in the Operations Control Center, if there is one.

- Line management conducts periodic **assessments**, including physical configuration assessments and walkdowns, to determine the agreement between the physical configuration and the configuration defined in the facility documentation, and to measure the overall effectiveness of the program of configuration management. Identified deficiencies within the program are corrected.

- **Control** of changes or modifications to approved design bases, functional requirements, and as-built configurations of safety-related equipment is necessary to ensure that safety functions are not inadvertently degraded. Proposed changes to design bases, functional requirements, or safety-related equipment should be reviewed and approved according to prescribed processes for the safety category assigned to the equipment. Change proposals identify impacts on the safety basis, as well as on the environment or mission; identify any testing needed after the change is made; and provide documentation of what has been done (e.g., proposed revisions to drawings, test procedures, or training materials) in sufficient detail to permit technical reviews and approvals. Review and approval are performed for each proposed change to verify that an adequate technical basis has been provided, that a complete change package exists, and that any needed external reviews and approvals have been obtained. Change proposals should also be reviewed for implications for safety of workers by means of job hazards analysis, process hazards reviews, and other "activity-based" reviews. Upon approval and implementation of changes, the documentation of change, records of the technical reviews and approvals, as-built information, and post-modification test results are provided to the organization responsible for maintaining current records on the configuration. Line management personnel with responsibilities for configuration management receive appropriate training.

7. IMPLEMENTATION EXAMPLES

This section illustrates the tailoring of formality of operations through two examples of implementation: storage and handling of depleted uranium hexafluoride (UF_6) cylinders and assembly and disassembly of nuclear weapons. The discussion is not intended to be all-inclusive, but rather to illustrate how the implementation of certain elements of formality of operations can be tailored to be commensurate with the level of hazard, the tempo of operations, and the projected duration of the activities. These two case studies were based on site reviews at the Pantex and Paducah plants and discussions with site personnel on the concepts in this report.

7.1 DESCRIPTION OF OPERATIONS

UF_6 Cylinder Storage and Handling. The hazards associated with UF_6 cylinder storage and handling are chiefly industrial safety issues related to hoisting and rigging, and the potential chemical hazards related to the breaching of a cylinder. UF_6 reacts readily with water to form the soluble reaction products uranyl fluoride (UO_2F_2) and hydrogen fluoride (HF), both of which are very toxic. Aqueous HF is also an extremely corrosive acid. If exposed to the atmosphere, UF_6 will react with humidity to form particulate fumes of UO_2F_2 and HF. The reaction is very fast, but is dependent on the availability of water/humidity. External contact with HF results in chemical burns of the skin, while exposure to airborne HF causes chemical burns/irritation of the eyes, nose, and throat. The radiological hazard associated with UF_6 is small. Each cylinder contains approximately 3 curies in a nominal 10 tons of the hexafluoride, depending on the assay. Cylinder storage and handling operations consist of moving cylinders to support inspection, yard construction, and other maintenance. Cylinders are stored at three sites (Portsmouth, Paducah, and Oak Ridge). DOE maintains records of material control and movement to track the quantities of uranium present in the cylinders.

DOE intends to continue storage of UF_6 cylinders for at least the next 15 to 25 years. During this time, handling of UF_6 cylinders for routine inspection, maintenance, and repair will continue. However, as is evident from the above description, cylinder handling is considered a low-risk, low-operational-tempo activity with a long-term mission.

Cylinder handling is performed during a single day shift, with a single team of cylinder handlers reporting to a supervisor. Inspection personnel perform periodic detailed visual inspections of cylinders to identify and monitor any degradation. Ultrasonic tests are used to evaluate a sampling of cylinders to detect trends in populations of cylinders. Certified boiler and pressure vessel code inspectors are used to evaluate nonconforming cylinders (e.g., bent stiffening rings, gouged cylinder walls) and any suspected breached cylinders. Health physics personnel evaluate the radiological aspects of cylinders and the cylinder yards. Workers remove old cradles and place new ones, and sweep and package cylinder rust from the concrete beds around the cylinders.

Weapons Operations. The potential hazards associated with weapons assembly and disassembly include a possibility of nuclear explosion (with subsequent plutonium and uranium dispersal), criticality hazards, chemical hazards, and radiological hazards. With ongoing reductions in the number of nuclear weapons in the stockpile (and continuing dismantlement), as well as support of the remaining stockpile, DOE will be required to continue these activities for the foreseeable future.

Although repetitive assembly or disassembly operations may be conducted over time, operations are commonly conducted on a single weapon for an extended period (i.e., days); therefore, they do not have the characteristics of work on an assembly line or a continuous process. The normal situation is for production work to be performed on a day-shift basis, 5 days per week. Therefore the operational tempo for the activities is high, the hazards are moderate to high, and the activities have a long-term mission.

Work is performed by Manufacturing Division Production Technicians (PTs), with one or more groups of PTs being under the supervision of an Operations Manager. The work areas (bays and cells) are under the operational control of a Facility Manager; that is, weapons operations are a tenant activity. The facilities and most of the support systems used by the PTs are operated and/or maintained by personnel from the Facility Operations Division. The Facility Manager is responsible for providing and maintaining the bays and cells, and for coordinating operations and maintenance to prevent mutual interference.

Three levels of systems/components are defined based on the safety significance of the system or component. The "critical safety systems" (CSSs) are those few systems identified whose failure could adversely affect the environment or the safety and health of the public. "Important" systems are those that are needed for operation, but are not significant to the safety of the CSSs. "Balance-of-plant" systems are those remaining. Limiting Conditions of Operation (LCOs) are derived from the Safety Analysis Report (SAR), the Technical Safety Requirements (TSRs), the Basis for Interim Operations (BIO), and the weapon-specific procedures.

7.2 DISCUSSION

This section illustrates the tailoring of the key elements and subelements of a formality of operations program to the above two examples of activities. Note that only a sampling of the tasks associated with the subelements is discussed for illustrative purposes.

7.2.1 Conduct of Operations

Operating Limits Compliance. For handling of UF_6 cylinders, there are a few operational controls (e.g., restricted access of refueling tanker trucks) that are easily implemented through training and procedures; there are no safety systems, per se, in the cylinder yards.

However, rigorous application of operating limits compliance is required for the work on nuclear weapons because numerous facility systems fulfill safety functions, and hazards must be controlled. Operating limits associated with safety systems and many others associated with the weapons are captured in facility and weapon procedures; these limits include those on the operability of systems, those associated with the weapons, and special limits associated with properties of the materials used in the weapons. Several limiting conditions are monitored by equipment providing audible or visible warning and automatic actions. Limiting conditions that would have less severe consequences if violated require recognition and response by personnel remote from the production operation. These parameters are monitored by roundsheet readings or by inputs into computer data storage. This level of monitoring provides adequate time to respond by ceasing the operation in progress and correcting the out-of-specification condition.

Logkeeping and Roundsheets. Logkeeping and roundsheets are required for both examples; however, the level of detail that is logged or recorded is significantly different. For activities with cylinders, logkeeping is required to maintain accountability and configuration control; there are no process parameters that require use of roundsheets. Records of cylinder movement are made whenever a cylinder is moved. General results of pre-move, post-lift, and post-relocation inspections of cylinders are recorded and maintained for each movement. The yard supervisor maintains a narrative log covering such items as major actions taken in the yards, potential breaches or other nonconforming characteristics identified by cylinder inspections, and numbers of cylinders moved and/or painted. In addition, a narrative log of activities by health physics technicians is maintained to record findings associated with cylinders, equipment, and material within the cylinder yard.

Logkeeping and roundsheet practices for weapons operations have been tailored to satisfy the unique requirements of the work being performed and the physical arrangements of the plant. Most of the indicators associated with systems or components of concern to operations within the bays/cells are located where they cannot be observed by the technicians. Parameter values that constitute LCOs are included on preoperational checklists. Since these systems/components are normally operated and/or maintained by Facility Operations technicians, these individuals are tasked with obtaining periodic readings and recording them on roundsheets. Notification of an out-of-specification condition is reported to the Facility Manager and relayed to Operations for action. Activities within the bay/cell are recorded in a narrative summary log; this log is intended to capture key events without becoming a redundant record of the information that must be recorded as part of the detailed procedures required for work on nuclear weapons. Many activities associated with assembly/disassembly are required by procedure to be recorded on

permanent records of weapon history. Transfer or disposition of special nuclear material or other designated components is reported by computer terminal for recording in a central computerized data file.

Lockout/Tagout Procedures. Consistent with regulatory requirements in 29 Code of Federal Regulations (CFR) 1910, the procedure for lockout/tagout is tailored by evaluation of the risk to personnel or equipment during the performance of work. There is no formal application of lockout/tagout for handling and storage of cylinders per se. Should handling equipment fail daily checks, it is reported to the immediate supervisor and then to maintenance for repair. Because of the low operational tempo, there is no requirement to lock or tag the equipment until maintenance is performed since only one crew member and one supervisor operate all handling equipment and perform the checks. If rotating crews were used, a more rigorous process of notification and control might be required to prevent inadvertent operation of deficient equipment.

For weapons activities, some tailoring can be applied. Low-risk work that poses no potential risk to personnel safety, has no potential for stored energy, has only one power source, and does not create hazards for other activities can be performed by an individual without a lockout/tagout. However, if the work continues beyond the end of the shift, lockout/tagout is required to prevent inadvertent operation of the equipment or system. Often, the lockout/tagout action is made an integral part of a work package developed by maintenance support personnel with the involvement of cognizant engineering personnel. Lockout/tagout actions that are not part of a work package are prepared by trained personnel and approved by a supervisor with specific training on lockout/tagout and the affected system.

Independent Verification. Independent verification is required for both cylinder handling and weapons operations, and it is imposed according to the risk associated with incorrect positioning of equipment or components. For handling of cylinders, the requirements for independent verification are limited. It is required for handling certain nonconforming cylinders or cylinders suspected of having been breached, whereupon a code inspector and the site cylinder program manager must determine the structural adequacy of the cylinders.

For facilities where weapons operations are conducted, restoration of CSSs requires independent verification to ensure that systems can perform their intended safety function if required. Given the critical nature of the work, procedures for assembly/disassembly of weapons frequently call for simultaneous independent verification of many steps in each procedure. In addition, independent verification of preoperational checks for facility systems and equipment/tooling used during the weapons operations is performed to mitigate the risk from improperly positioned components or use of unauthorized equipment or tooling.

Equipment Labeling. The priority for labeling of equipment is based on the risk associated with improper identification and operation of a component. Because the equipment used for handling of cylinders is limited to the dedicated, specially designed equipment for handling cylinders, there is no need for a formal labeling program. The cylinders are labeled to

support proper identification for periodic inspections. The lifting equipment is labeled individually with property numbers, and this is how it is identified on the lift plan for use by the supervisor. For facilities where operations are performed on weapons, there is no tailoring of the information required on the labels for equipment; all equipment used by the PTs during the operations must be labeled before use. However, since many facilities are old and their equipment is not labeled, the priority for accomplishing the labeling is driven by the safety significance of the equipment. Often the associated risk may be attached to the safety of maintenance workers. The highest priority is given to critical safety systems in the bays and cells, followed by support systems, and then equipment in the facilities where new dismantlement programs are being started.

7.2.2 Training and Qualification

Training Program Analysis and Design. The rigor of the specific training program should be tailored according to the risk associated with the job. Training requirements are based on a job and task analysis that defines the jobs and specific tasks required for successful performance.

Training Program Development. There are two categories of personnel involved in handling of cylinders, and their training is tailored according to the required skills and associated risks. Cylinder handlers are the operators who handle the UF_6, and their training is therefore the most rigorous, focusing on proper execution of the procedures for handling cylinders. The training is performed off line using empty cylinders. The mockup training is realistic enough to qualify operators without the need to provide controlled on-shift training. In addition, handlers receive training in fundamentals that includes physical and chemical characteristics of UF_6. Cylinder handlers, including those operators who drive fork lifts in the yards, are the only personnel, other than health physics technicians, that are qualified and subject to periodic requalification. The second category of personnel is inspectors—routine, ultrasonic test (UT), and boiler and pressure vessel (B&PV) code inspectors. Routine inspectors receive classroom and on-the-job training. UT inspectors receive classroom and on-the-job training and specific tests to qualify them as nondestructive testing (NDT) inspectors. The training for B&PV code inspectors is similar to that for the UT inspectors. However, they receive higher certification from the American Society of Mechanical Engineers because these inspections support maintenance of the integrity of the single boundary between radiological material and the environment, namely, the cylinder wall.

For weapons operations, the training requirements are also tailored to the risk associated with the work being performed. The PTs are in the position of highest risk. They receive extensive training on the hazards associated with weapons operations, including hazards from the materials they are handling, as well as the impact of their operations on the authorization basis and the potential for accidents to affect the environment and the public. The PTs also receive hands-on training on a trainer unit, written examinations, and performance demonstrations. They are then qualified to work on weapons under the supervision of a certified PT. Following satisfactory demonstration of on-the-job performance, line management certifies the PT. Certified personnel

have the additional requirement of maintaining proficiency by completing, typically, a minimum of 10 hours of hands-on work within a given 3-month period on those program elements in which they hold a certification. Biennial recertification of PTs is a formal process.

Facility Managers are key to the safety of operations because they are responsible for maintaining the facility in the condition required to provide necessary support to those operations and to provide safety systems that will function as required if needed. Therefore, the Facility Manager's training is rigorous, and focuses on the operational limits of the facility and the facility's authorization basis. The Facility Manager must also have training on the weapons operations that will take place in the facility in order to understand the risks associated with the work.

Training for Operations Managers is also rigorous because they supervise the actual weapons work. Training of Operations Managers focuses on the weapons operations since they are responsible for responding whenever the PTs have problems during operations. They must also receive training on the authorization basis of the facility as they are responsible for ensuring that the operational limits associated with the weapons operations are properly implemented and followed. Both the Facility Managers and the Operations Managers are qualified for their positions; however, since they are not conducting hands-on operations, they are not required to obtain line management certification.

7.2.3 Maintenance and Surveillance

For cylinder operations, the equipment most important to safety is that associated with lifting and handling. Handling of equipment is subject to a standard industrial preventive maintenance program that is tailored to the risk and complexity of the equipment. Higher-risk maintenance activities are subject to increased levels of control; for example, corrective maintenance for a breached or heavily corroded cylinder results in the development of a specific procedure and work package that are to be followed on a step-by-step basis during the repair or lifting process. A critical lift plan may have to be developed in these cases. Lower-risk maintenance, such as routine painting, is left to the skill of the crafts personnel. There are no further surveillance requirements for cylinder handling.

For weapons operations, maintenance procedures and surveillances are established from safety documentation, including the SAR, the Critical Systems Safety Manual, and the BIO. Surveillance requirements are also driven by national standards and codes, such as those of the National Fire Protection Association. The level of detail in the surveillance procedures is based on the complexity of the surveillance and the risks associated with the activity, including both traditional nuclear safety and worker protection (Occupational Safety and Health Administration) risks. Surveillance requirements for critical systems are developed by engineering personnel to ensure that a test adequately exercises the required safety function of the component. The periodicity of surveillance testing is based on analysis of failure rate data when available, and the manufacturer's recommendation and good engineering practice when such data are not available.

Details of procedures are based on risk, system complexity, and type of system. For example, maintenance on an important system posing significant worker electrical safety risks may be more detailed than a simple surveillance on a CCS.

7.2.4 Configuration Management

The configuration management program is tailored according to the safety significance of the component, system, or material.

For operations in the cylinder yards, the most important configuration item is the amount of uranium-235 in each cylinder; these data are maintained in a computer database. Whenever a cylinder is moved, that movement is recorded in the database so that material accountability is always maintained. Criticality safety is ensured by identifying cylinders that have greater than 0.7 percent uranium-235 and maintaining them in safe arrays. The next most important item for configuration is the lifting and handling equipment. Control of this equipment is maintained by permitting only a limited number of visually distinguishable designs on site, and having equipment identified on the lift plan and authorized by the supervisor; no additional controls are deemed necessary.

For weapons operations, nuclear material is strictly controlled and tracked for accountability purposes, as well as for criticality safety control. In addition, CSSs are subject to the strictest configuration management program because of their required safety function. Design information is established, organized, and controlled for such systems. Design changes, modifications, and component replacements for these systems receive independent review by the Change Control Board and reviews by all safety disciplines. Important systems and balance-of-plant systems are controlled with less rigor; however, adequate controls should be in place to ensure that the system configuration is maintained to permit safe, efficient maintenance and design changes.

8. INTEGRATION PHILOSOPHY

As previously discussed, the key elements of a formality of operations program are not isolated, but have direct interfaces with each other, as well as with other functional areas. Identifying those interfaces is critical to the successful implementation of a formality of operations program. However, recognizing that these interfaces exist is not sufficient; for a formality of operations program to be effective, a process is needed to define and control them. Roles and responsibilities on both sides of each interface should be established and documented.

The interfaces among the four key elements—conduct of operations, maintenance and surveillance, training and qualification, and configuration management—can best be illustrated by an everyday example, the processing of work orders.

8.1 ILLUSTRATIVE EXAMPLE: PROCESSING OF WORK ORDERS

Performing work normally includes processing a document that identifies the character of the work and assigns responsibility for its completion. For high-hazard activities, this process may also entail the development of a detailed work procedure, engineering review of the procedure to ensure technical adequacy and evaluation of impact on safety-related systems, and evaluation of the system status of the facility by the operations group to see whether the work can be performed safely. The structure discussed below is a comprehensive one. Grading criteria are addressed as the discussion proceeds.

Identification of the Work Requirement. The need for work can be identified in many ways: through observation of conditions during walkthrough of a facility, which is done as part of the conduct of operations program; through the completion of a preventive maintenance routine or surveillance as part of the maintenance and surveillance program; as part of an engineering program to update safety-related equipment; or simply through component or system failure. At this point, a work request is normally documented in some fashion and entered into a system for tracking purposes.

Assessment of Work. Once it has been determined that work must be performed, the task should be evaluated from a technical standpoint. Some jobs are easy; replacing a motor control switch on a control panel, for example, may simply require installing an available spare. Other work may require detailed technical assessment. The technical assessment may include determining a source of acceptable replacement materials, requiring a close interface with configuration management if the system is in the configuration management program; whether repair or replacement should be performed, with engineering support being called in to help with this decision; and what priority should be placed on the evolution (e.g., whether the component or system is important to the mission or safety of the facility). The assessment should include an evaluation of the effects on the safety envelope, and the potential for violating a safety limit if

maintenance is not completed within a specified time. The operations group should determine whether there are operational issues involved in removing a given system or component from use for maintenance.

Development of a Technical Work Document. The technical work document provides appropriately graded instructions for completion of the work. For the control switch replacement mentioned above, this might involve simply annotating the work request document. In the case of the complex work to be performed on a safety system, however, a detailed step-by-step procedure might be required, potentially written by the engineering support and maintenance organizations. The safety organization will review the job order for safety issues and provide technical assistance on environmental, safety, and health issues. Appropriate limits on conditions of the system may also be required from the operations group. In addition, specialty support groups may have to screen the action for safety precautions or special permits, such as for radiological protection and industrial hygiene. The approval level should be graded based on the safety significance of the work. As with all facility activities, the line organization still retains the ultimate responsibility for safety issues and decisions.

Scheduling of Work. Proper scheduling ensures that the appropriate priority is placed on resources being applied to the job and that all affected organizations are aware of the work. For the simple control switch replacement, one person within the maintenance organization using "skill-of-the-craft" knowledge might make the repairs, with no interaction with other organizations being required. Complex work might require scheduling of appropriately trained and qualified personnel and close coordination among the engineering, operations, and maintenance organizations.

Performance of Work. Conduct of operations subelements are used for controlling work. This function includes availability and use of procedures, formal communications and pre-evolution briefings and post-evolution notifications, lockout/tagouts with independent verification, and equipment labeling. The operations group configures the equipment or system for maintenance to be performed and then formally turns the equipment/system over to the maintenance organization for work. The members of the training organization should be aware of the required skills for each task and ensure that the appropriate level of training is provided. The configuration management program should ensure that as-built systems match the drawings used for planning the work and that lockout accurately isolates the system. For simple work such as the switch replacement, minimal controls might be required.

Closeout of Work Package. This function includes post-maintenance retest and turnover of the system to operations. For the control switch replacement, this might consist simply of verifying the operation of the new switch, informing operations that the work has been completed, signing the work order, and documenting the man-hours and materials used. For more complex work, it might entail complex retesting of systems using procedures established by the engineering organization, followed by documentation of the results and measures to ensure that changes are

captured by the configuration management program; formal turnover of the system to operations; formal closure of the work package; and filing for future reference.

8.2 KEY ELEMENT INTERFACES TO OTHER FUNCTIONAL AREAS

As noted above, besides the interfaces among the four key elements, each element also interfaces with various other functional areas, including engineering support; independent reviews; quality assurance; TSR, safety, and hazard analysis; and radiation protection. Table 2 describes each of these interfaces in general terms.

Table 2. Interfaces Between Formality of Operations Key Elements and Other Functional Areas

Functional Area	Formality of Operations Key Elements			
	Conduct of Operations	**Maintenance and Surveillance**	**Training and Qualification**	**Configuration Management**
Engineering Support	Engineering support ensures that operations are governed by technically correct limits, incorporated into procedures. Proposed changes to the facility/activity are reviewed and controlled to ensure that they do not inadvertently alter the design basis.	Engineering support ensures that test and surveillance procedures to be used are applicable to the appropriate safety-related equipment and that the test will correctly evaluate the requirement related to the safety-related function. Engineering support personnel review maintenance procedures to ensure that work and testing are adequate for repair and verification of operation of the components/systems. Preventive maintenance procedures and schedules are reviewed to ensure that system reliability is provided.	Engineering support personnel are properly trained to perform their assigned tasks. Engineering personnel provide technical material as required for the development of course material.	The configuration management program supports engineering by providing accurate design requirements and design basis information for safety-class systems. This is necessary to support SAR development and upgrades, and the evaluation of nonconformances and proposed changes. The engineering organization is in charge of the configuration management program.
Independent Reviews	An *independent* process, separate from facility operations, provides safety review on a continuing basis to verify that facility management establishes sound practices, and that the facility is operated in accordance with this direction. This review process receives top management attention.	Independent reviews of changes and modifications to safety-related equipment are performed, as are independent evaluations of the adequacy of the maintenance program.	Independent reviews identify any weakness in operations and performance of personnel that should be addressed in the training program. The training program provides training to independent assessment personnel.	Independent assessments may be made periodically to evaluate the physical configuration and to determine the agreement between the physical and documented configurations.

Table 2. (concluded)

Functional Area	Formality of Operations Key Elements			
	Conduct of Operations	**Maintenance and Surveillance**	**Training and Qualification**	**Configuration Management**
Quality Assurance	Quality assurance is applied to all activities as part of a comprehensive system designed to ensure with high confidence that all items developed and services and tasks provided meet specific requirements.	Maintenance activities, including documentation control, spare parts requisitioning, and post-maintenance testing, are conducted in accordance with the facility quality assurance program.	Training activities, including documentation control and management of training records, are conducted in accordance with the facility quality assurance program.	Design basis documents and configuration control are subject to control and verification by quality assurance procedures.
TSR, Safety, and Hazard Analysis	Proper control of the facility's safety basis is closely linked to the accuracy of design information, including TSRs, and to the proper identification and control of hazards. Conduct of operations ensures proper implementation of controls.	The test and surveillance program relies on accurate identification of surveillance requirements.	Training programs stress the importance of operational limits, the basis for those limits, and the consequences of violating them. Changes to the limits are incorporated into training materials.	Changes or modifications to approved design bases, functional requirements, and as-built configurations of safety-related equipment are controlled to ensure that safety functions are not inadvertently degraded or require modification.
Radiation Protection	Proper conduct of operations emphasizes the control of hazards, including radiation and contamination. An effective radiation protection program that supports this function is essential.	An input to the maintenance planning process is identification and analysis of the radiological hazards associated with the work. This allows appropriate planning to minimize personnel radiological exposures.	Training programs emphasize the importance of radiation protection and the concept of as low as reasonably achievable (ALARA).	The configuration management program ensures the control of equipment that protects workers from inadvertent, potentially fatal exposures to radiation (e.g., lockouts on X-ray machines, shielding).

9. CONCLUSIONS

As described in this report, the elements of formality of operations are not unique to the defense nuclear industry, but are based on well-developed industrial operating practices. There are no new requirements presented in this report, only a concept for tailoring existing ones to the work. The concepts presented here will help to achieve not only desired uniform product quality, but also safety, especially in highly technical fields dealing with hazardous material, a characterization that applies to many defense nuclear activities of DOE. Formality of operations ensures proper application of controls developed by integrated safety management systems and ensures that any material problems or changes are managed to maintain these controls or institute new ones as applicable.

As noted in the introduction to this report, safety is best achieved when it is intimately bound to the total process of work and is an essential part of all phases of work. Formality of operations will help to ensure that safety is integrated throughout a complex and hazardous work process. It is expected that the principles expounded in this report will contribute to achieving not only the necessary high degree of safety, but also more efficient and economical operations.

The tailoring of the key elements and subelements described are intended to be of assistance in establishing an appropriate level of operational formality at each of its nuclear facilities, a level that is commensurate with the hazards, the operational tempo, and the mission/remaining life of the facility.

These three major themes—using existing proven standards and requirements; linking the achievement of safety to the accomplishment of work; and tailoring to match the particular circumstances of a given site, facility, or activity—are important to the implementation of integrated safety management systems as envisioned by the Board in Recommendation 95-2. Properly structured operational formality is key to the safety functions "develop and implement hazard controls" and "perform work within controls" discussed by DOE in its Implementation Plan for Recommendation 95-2. It is believed that the further refinement of these safety management functions and the coherent philosophy provided by the concept of operational formality will be useful to DOE and its contractors as they develop their integrated safety management programs.

APPENDIX. CROSS-REFERENCE OF DNFSB/TECH-5 AND DNFSB/TECH-6

DNFSB/TECH-5 "Preserve System" Functional Areas	DNFSB/TECH-6 "Components of Formality of Operations" Bullet Numbers
Conduct of Operations	1, 2, 3, 4, 7, 8, 11, 12, 13
Maintenance and Surveillance	2, 6, 8, 10
Training and Qualification	5, 6, 12
Configuration Management	9, 13

The numbers in the table correspond to the following elements discussed in DNFSB/TECH-6 (Kouts and DiNunno, October 6, 1995):

1. Line management of operations, including a clear chain of safety responsibility.

2. Detailed procedures for operations and maintenance, including emergency procedures.

3. For more hazardous operations, line-by-line adherence to the procedures, with checkoff after each step.

4. A formal process for review and approval of changes to procedures.

5. Supervision by highly competent personnel who are knowledgeable about the results of the safety analysis and operating limits for the facility or activity.

6. A highly trained and formally qualified staff of operators and maintenance personnel.

7. An effective radiation protection program.

8. Adherence to a safety envelope comprising Technical Safety Requirements and Standards/Requirements Identification Documents.

9. A formal process for review and approval of structures, systems, and components important to safety and environmental protection.

10. A maintenance program that includes regularly scheduled preventive and predictive maintenance and timely corrective maintenance, conducted in accordance with approved procedures.

11. An orderly workplace.

12. A process that converts mistakes to lessons learned and uses these as a basis for improvement.

13. A process of independent safety review that includes close attention of top management.

LIST OF REFERENCES

REFERENCES CITED

Defense Nuclear Facilities Safety Board, *Annual Report to Congress*, Washington, D.C., 1991.

Defense Nuclear Facilities Safety Board, *Recommendation 92-5, Discipline of Operation in a Changing Defense Nuclear Facilities Complex*, Washington, D.C., August 17, 1992.

Defense Nuclear Facilities Safety Board, *Recommendation 95-2, Safety Management*, Washington, D.C., October 11, 1995.

DiNunno, Joseph J., *Fundamentals for Understanding Standards-based Safety Management of Department of Energy Defense Nuclear Facilities*, DNFSB/TECH-5, Defense Nuclear Facilities Safety Board, Washington, D.C., May 31, 1995.

International Nuclear Safety Advisory Group, *Safety Culture*, Safety Series No. 75-INSAG-4, Vienna, Austria, 1991.

International Nuclear Safety Advisory Group, *Basic Safety Principles for Nuclear Power Plants*, Safety Series No. 75-INSAG-3, Vienna, Austria, 1988.

Kouts, Herbert J. C. and Joseph J. DiNunno, *Safety Management and Conduct of Operations at the Department of Energy's Defense Nuclear Facilities*, DNFSB/TECH-6, Defense Nuclear Facilities Safety Board, Washington, D.C., October 6, 1995.

Title 29 Code of Federal Regulations Part 1910 (29 CFR 1910.119), Occupational Safety and Health Administration, *Process Safety Management of Highly Hazardous Chemicals*, OSHA Rule 29 CFR 1910.119, Washington, D.C., July 1, 1996.

U.S. Department of Energy, *Startup and Restart of Nuclear Facilities*, DOE Order 425.1, Washington, D.C., October 26, 1995.

REFERENCES ON FORMALITY OF OPERATIONS ELEMENTS

Conduct of Operations

International Nuclear Safety Advisory Group, *Basic Safety Principles for Nuclear Power Plants*, Safety Series No. 75-INSAG-3, Vienna, Austria, 1988.

International Nuclear Safety Advisory Group, *Safety Culture*, Safety Series No. 75-INSAG-4, Vienna, Austria, 1991.

U.S. Department of Energy, *Conduct of Operations Requirements for DOE Facilities*, DOE Order 5480.19, Washington, D.C., Chg. 1, May 18, 1992.

Maintenance and Surveillance

American Nuclear Society, *Administrative Controls and Quality Assurance for the Operational Phase of Nuclear Power Plants,* ANSI/ANS-3.2-1988, April 6, 1989.

U.S. Department of Energy, *Maintenance Management Program,* DOE Order 4330.4A, Washington, D.C., October 17, 1990.

U.S. Nuclear Regulatory Commission, *Proposed Methods for Regulating Major Materials Licensees*, NUREG-1324, Washington, D.C., February 1, 1992.

Training and Qualifications

American Nuclear Society, *Selection, Qualification and Training of Personnel for Nuclear Power Plant,* ANSI/ANS-3.1-1993, April 23, 1993.

Title 10 Code of Federal Regulations Part 55 (10 CFR 55), U.S. Nuclear Regulatory Commission, *Operators' Licenses*, NRC Rule 10 CFR 55, Washington, D.C., January 1, 1996.

U.S. Department of Energy, *Personnel Selection, Qualification, and Training Requirements for DOE Nuclear Facilities,* DOE Order 5480.20A, Washington, D.C., November 15, 1994.

Configuration Management

U.S. Department of Energy, *Guide for Operational Configuration Management Program*, DOE-STD-3006-93, Washington, D.C., September 9, 1993.