ORNL/M-2490

CMWG-2

ORNL/M--2490

DE93 003888

Configuration Management

OVERVIEW AND PHASE I IMPLEMENTATION GUIDANCE

November 1992

Issued By:

Configuration Management Working Group

MARTIN MARIETTA ENERGY SYSTEMS, INC.
Oak Ridge, Tennessee

Prepared for the U.S. Department of Energy
under U.S. Government Contracts
DE-AC05-84OR21400 and DE-AC05-76OR00001

CONTENTS

LIST OF FIGURES

ACRONYMS

CI	Configuration items
CM	Configuration Management
CMWG	Configuration Management Working Group
CSA	Criticality Safety Approval
DOE	Department of Energy
DOE-OR	Department of Energy Field Office, Oak Ridge
HFIR	High Flux Isotope Reactor
NPDES	National Pollution Discharge Elimination System
OSR	Operational Safety Requirements
RCRA	Resource Conservation Recovery Act
SAR	Safety Analysis Report
TS	Technical Specifications
TSR	Technical Safety Requirements
USQD	Unreviewed Safety Question Determinations

EXECUTIVE SUMMARY

Configuration management (CM) is a process for ensuring that the complex and diverse operations managed by Martin Marietta Energy Systems, Inc., accomplish their objectives while satisfying necessary constraints.

The basic concepts of configuration management - identifying important items, knowing their requirements, controlling changes, and keeping accurate documentation--are not new to Energy Systems employees. What is new is the integration of these concepts into a management system that is selectively applied where it will achieve the greatest benefit.

Within Energy Systems and the Department of Energy (DOE) complex, configuration management is generally thought of in terms of five elements: change control, requirements, document control, assessments, and organization and administration. These elements are already largely in place in operational areas such as the High Flux Isotope Reactor (HFIR), criticality alarm systems, and the weapons production process. Some of the elements are also being applied to activities such as the control of company policies; contracts; award fee milestones; and the scope, cost, and schedule aspects of selected line item construction projects.

The first element of configuration management is **change control**. Proposed physical or administrative changes are evaluated and accepted or rejected based on their anticipated effects. If the effects are determined to be acceptable, the change is then implemented. The concept of change control is familiar to most people; it exists in virtually all operations. In most cases a proposed change is informally evaluated through discussions or through an individual thought process. In selected other cases, a formal, rigorous, and documented process is employed.

A decision to accept or reject a proposed change requires an understanding of its effects. A key to this understanding is knowledge of what the current configuration is and why it is so. Whether the configuration was a deliberate creation or simply "grew," its creators were working within known constraints to satisfy specific objectives. These constraints and objectives are the **requirements** of the current configuration. A change that violates these requirements could lead to unintended, perhaps unacceptable, consequences. This knowledge and understanding of requirements is the second element of configuration management.

An important aid to understanding is accurate and consistent documentation. Documents describe the current configuration and record its requirements. They communicate operational limitations and procedural steps. As a result, documents used for important decisions must be kept current with the physical/functional configuration and with requirements. **Document control** is, therefore, the third configuration management element.

Many facilities and activities currently managed by Energy Systems have evolved over years of less formal change and document controls. As a result, the current configuration, its intended purpose, and its constraints may not be fully understood and existing management controls may not be adequate by today's standards. This leads to the fourth element of configuration management: **assessment**. The assessment process compares the current configuration with applicable requirements (some of which may need to be reconstructed, if no longer available). It also examines current change and document control practices to see if they meet today's standards.

The fifth configuration management element is the **organization and administration** of the other elements. This element is the management process that makes the other elements work correctly.

Configuration management can be graphically represented as shown in Fig. 1. The desired results are summarized by the triangle. One point of the triangle is the requirements, another is the existing physical/functional configuration, and the third is documentation. Change control and document control keep the points of triangle consistent. The assessment element and the organization and administration element encompass the process.

An integrated configuration management process is necessary to adequately manage operations with the potential for significant health, safety, or environmental effects. It is also needed for those operations with the potential to violate laws, regulations, or permits; breech safeguards or security; or cause significant damage to production or research capability. However, it does not apply to all things equally. The application of configuration management is **graded** so that controls and documentation are proportional to the importance of the item being controlled. For example, a safety class 1 component--one whose failure could lead to harm to the public--may require very rigid controls whereas other components in the same facility might need little or no control because the effects of uncontrolled changes can only be inconsequential. Grading may also reflect the remaining lifetime of the facility, activity, process, or experiment.

The gap between today's expectations and the current status of some facilities is such that a **phased** approach to implementing configuration management is necessary. Phasing basically refers to the progressive implementation of the key elements. An example phased approach and implementation schedule are shown in Fig. 2. The phases can be simplistically thought of as taking control of the most important items (Phase I), improving understanding and practices (Phase II), and gaining complete understanding and integrating the overall process (Phase III). Although configuration management generally applies to many facilities, activities, processes, and experiments, Phase I is specifically directed toward those that have been designated as high or moderate hazard (by the Facility Safety Department) or that possess an environmental permit.

The phased and graded concepts are combined such that resources are systematically allocated to items of greatest importance first. The importance of an item to concerns such as health and safety determines both the timing and the depth and rigor of configuration management implementation. Items of greater importance are treated first and more aggressively than less important items.

The implementation of CM is a line organization responsibility. It is an integral part of the Total Quality Management process, not a "program." To assist the plant sites and other organizations in this process, the Configuration Management Working Group (CMWG) was formed with representatives (configuration management coordinators) from the sites and other major organizations and with a Department of Energy (DOE) observer. The near-term purpose of this group has been to use its diverse cross section of specialties to devise a suitable configuration management definition and general implementation scheme for Energy Systems. The group is also developing a set of suitable tools (guidance documents) to reduce duplication of work at the sites.

This is the first of a series of guidance documents developed by the Configuration Management Working Group. Chapter 1 describes the overall configuration management concept and model. Chapter 2 discusses the phased approach to implementation. Chapter 3 provides more detailed guidance for Phase I activities, including the identification and control of the configuration items of greatest importance.

Energy Systems' configuration management requirements are stated in draft policy ES-CM-100, "Configuration Management," (ref. 1) and in standard ESS-CM-101, "Configuration Management." (ref. 2) Elements of configuration management are required in DOE Orders such as 4700.1, *Project Management System,* (ref. 3) 5480.5, *Safety of Nuclear Facilities,* (ref. 4) and 5480.19, *Conduct of Operations Requirements for DOE Facilities* (ref. 5). An Order specifically on configuration management is also being drafted by DOE.

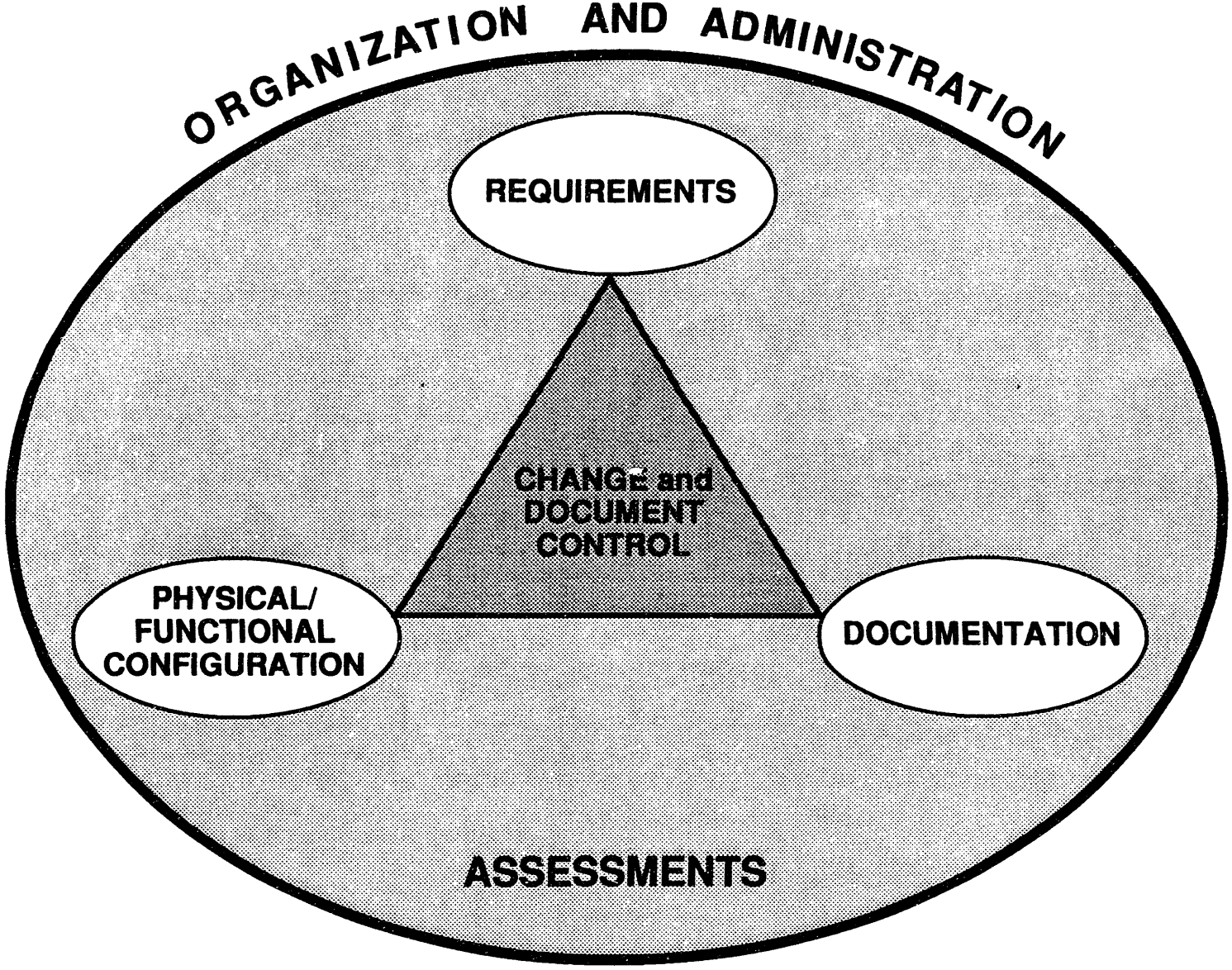

Figure 1

BASIC CONFIGURATION MANAGEMENT RELATIONSHIPS

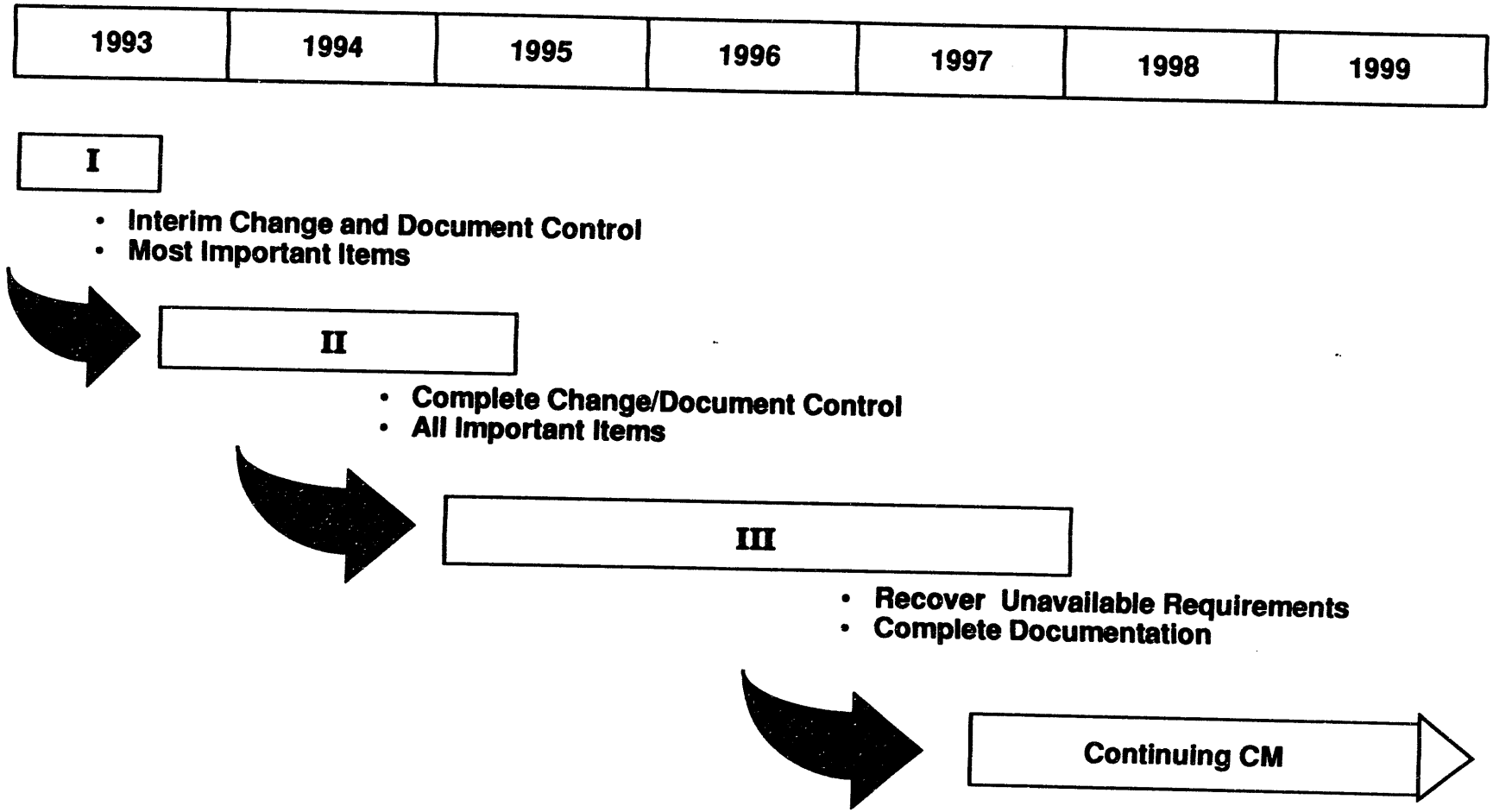

Figure 2

PHASED APPROACH TO THE IMPLEMENTATION OF CONFIGURATION MANAGEMENT

1.0 CONFIGURATION MANAGEMENT OVERVIEW

1.1 INTRODUCTION

The facilities, activities, processes, and experiments managed by Martin Marietta Energy Systems, Inc., often involve materials and processes that are hazardous, sensitive, or costly. The risk that may be inherent in these operations is made acceptable by ensuring that they satisfy requirements established by law and regulation, good design, and good operating practices. Configuration management (CM) is an management process intended to ensure that these operations conform to these requirements.

The configuration management concept was developed primarily in the aerospace and nuclear power industries in response to events caused when equipment was not kept in the configuration its designers intended. Some of the events resulted in significant environmental disasters. Investigators found that the events were often caused by breakdowns of management controls. These breakdowns allowed improper changes that left equipment unable to perform as required or as documents indicated it would. The configuration management concept was developed to systematically address these breakdowns.

Energy Systems and the Department of Energy (DOE) have generally recognized the need for effective configuration management. Health and safety can be better protected; environmental permits, laws, regulations, and orders can be more consistently complied with; and investments in equipment and special programs, such as safety analyses or "as-built" documentation, can be preserved.

Configuration management is not a new concept at Energy Systems. Several facilities and processes currently have configuration management programs and practices that benefit safety and quality. A company-wide program begun in 1990 boosted configuration management in other facilities. In addition, existing procedures (e.g., records management) and programs (e.g., Safety Analysis Report Update Program) provide a basis for successful configuration management in many organizations.

Due to the gap that may exist between todays configuration management standards and the current status of many facilities, activities, processes, and experiments, effective configuration management is best implemented using a "phased and graded" approach. This approach focuses resources first where they will do the most good. The phased and graded approach and the key concepts and configuration management elements are discussed in the following section and in Chap. 2.

1.2 KEY CONCEPTS

Although the elements of configuration management exist in some form in most operations, their objectives and importance are often not understood. As a result, they are often not well integrated or fully effective. This section summarizes some of the key concepts that are the foundation for configuration management.

1.2.1 Configuration Management

Configuration management is an integrated management process that ensures that the physical and functional arrangement of configuration items -- hardware, software, procedures, or other physical or administrative items whose failure could lead to unacceptable consequences -- meet requirements throughout the life of the facility, activity, process, or experiment. It also

ensures that key documentation such as procedures or drawings that may influence conformance with requirements is accurate.

Configuration management may be viewed (Fig. 1) as a triangle binding the physical/functional configuration of configuration items with design and administrative requirements and with documentation. If configuration management is effective, the three points of the triangle are always in agreement.

Configuration management is a way of doing business, not a program that begins and ends. It begins at the inception of a new project and ends only when the operation is shut down and the site is restored. Configuration management is the responsibility of line managers and personnel because they are the people who control the configuration items -- that is, who can cause or prevent change. It is best accomplished through adequate standard operating procedures and information systems incorporating configuration management concepts rather than through separate, special configuration management procedures and data bases.

1.2.2 Configuration Item (CI)

Configuration items are structures, systems, components, computer hardware or software, instructions or procedures, or other physical or administrative items whose failure can lead to unacceptable (or undesirable) consequences. The consequences of concern here are loss of life or health, significant environmental impact, noncompliance with laws, breaches of security or safeguards, or major damage to key facilities. Thus configuration items are the objects of any description that we wish to ensure function correctly.

Configuration items will often be a small subset of the total number of items involved in a facility, activity, process, or experiment. They should be only those items whose failure leads to consequences that we are unwilling to accept. For example, a criticality monitoring system may be identified as a configuration item because its failure to alarm a high radiation condition could endanger workers. On the other hand, a water cooler's motor is generally not a configuration item because its failure is typically inconsequential. In another example, an administrative procedure that is used to ensure a safe arrangement for stored radioactive materials may be a configuration item because an error in it might lead to an unsafe arrangement.

Configuration items are identified by evaluating their vital functions and the constraints they must meet to avoid failure. These functions and constraints make up the requirements of the items.

1.2.3 Requirements

Requirements are the functions, or objectives, that a configuration item must achieve, plus the constraints it must function within. For example, the function of a fire protection system might be to spray a specified amount of water in a particular area when a fire occurs. The system's constraints might be that it have a very high reliability to work when needed and that it not spray when there is no fire.

Knowledge of the requirements of each configuration item is essential for decision making. For example, the minimum acceptable flow rate of a pump should be known before the pump is modified in a way that reduces its output. The same knowledge would be needed to adequately test the pump or to throttle its flow by closing down a valve. Failure to meet the minimum flow requirement could result in destruction of the pump or in its failure to perform a safety function. Similarly, knowledge of the environmental permit levels on a stack would be required prior to venting a room used for cleaning equipment with solvents.

There are two principal forms of requirements: design and administrative. **Administrative requirements** are non-physical constraints established to produce an essential result or prevent an unacceptable one. For example, an administrative requirement might specify the spacing of stored drums of radioactive materials or the maximum concentration of a hazardous substance that can be discharged to the environment.

Design requirements apply to physical structures, systems, and components. (The design may have been the deliberate action of engineers or it may have been a series of actions by others that resulted in a new or modified structure, system, or component.) Design requirements specify the function of an item and the limits, or parameters, within which the designer understands the item will work correctly; exceeding these limits may lead to failure. For example, the design requirements for a computer may specify that the room temperature not exceed 30°C. Exceeding this temperature may lead to undependable operation or destruction.

Closely associated with design requirements are **design bases**. A design basis is the *why* behind the design requirement's *what*. For example, the design requirement for a heat removal pump may be that it deliver 200 liters per minute. The design basis for this requirement may be an analysis showing 165 liters per minute are needed, plus a conservative margin of 35 liters per minute due to uncertainty in the calculation. Knowledge of this design basis would allow a new analysis (with less uncertainty) to support continued use of the pump if its flow rate were reduced to 190 liters per minute.

Another concept related to knowledge of requirements is the **design authority**. The design authority is a person(s) or organization responsible for (1) knowing and understanding the design requirements and design basis and (2) evaluating the acceptability of proposed changes to the design of a system, structure, or component. The design authority is also generally responsible for design control and technical adequacy.

1.2.4 Requirements/Design Basis Recovery

Many of the facilities, activities, processes, and experiments managed by Energy Systems have long existed without change control and documentation processes that meet current standards. As a result, the requirements applicable to configuration items are often no longer available. Recovery and documentation of these requirements is essential to ensure that important configuration items are identified and controlled.

Administrative requirements are generally found in technical safety requirements (TSRs), regulations, permits, procedures, and correspondence. Recovery of these requirements may entail identifying and reviewing applicable documentation.

Design requirements and design bases are found in engineering drawings, calculations, safety analysis reports, vendor manuals, and similar sources. However, these sources sometimes cannot be located, have not been kept current with physical and functional changes, or are not consistent or reliable. When this occurs, the design requirements and design bases may need to be recovered or "reconstituted."

Unavailable design requirements and design bases can be re-established by analysis, testing, consultation with past and present personnel knowledgeable of the item or by other means. Although often a resource-intensive effort, the recovery of design requirements and bases is needed at least as far as required to support safe operation, significant environmental compliance, and change control.

1.2.5 Configuration Item Documentation

Configuration item documentation includes the technical documents (e.g., drawings, procedures, safety analyses, descriptions) and records that describe the item's design and administrative requirements, design bases, operational controls, performance results, and other key attributes. This documentation must be controlled to ensure it is consistent with the actual configuration of the item because inaccuracies or inconsistencies could lead to incorrect assumptions by people operating, maintaining, or modifying the item.

1.2.6 Grading

Configuration management is not applied with equal rigor to all features of all facilities, activities, processes, and experiments. Some features, such as a reactivity control system on an experimental reactor, may require a through understanding of requirements and bases, an extensive review and approval system for proposed changes, detailed documentation, and frequent tests. The majority of other features, such as office equipment or personnel procedures, usually require little or no control. Between these two extremes, configuration management should be applied in proportion to the importance of the controlled item. This concept of making configuration management efforts commensurate with relative importance is called grading.

In addition to importance, grading may consider factors such as remaining facility life and operational status. Thus the configuration management effort applied to items in a facility that is scheduled for shutdown in five years would not be as extensive as one with a long remaining life. Also, a facility in standby would be expected to receive less rigorous configuration management than a similar one in full operation.

1.2.7 Phasing

Effective configuration management cannot be instantly imposed on existing operations. As a result, a phased implementation approach is used to provide an orderly timing and sequencing of new activities. Configuration management is first applied to the most important configuration items, those whose failure could endanger health and safety or cause significant environmental non-compliance. This phase would be followed by others, both expanding the configuration management effort on the most important items and expanding the effort to other items on a basis of decreasing importance.

The Energy Systems approach to phased implementation is discussed further in Chap. 2. The approach used by each organization should follow this general pattern, although details may vary according to needs and resources.

1.3 CONFIGURATION MANAGEMENT MODEL

As shown in Fig. 1, the objective of configuration management is to maintain the relationship between requirements, physical/functional configuration, and documentation. The five elements of configuration management must be in place and functioning for this to occur. They can together be thought of as the "model" of configuration management. The five elements are change control, requirements, document control, assessments, and administration and organization. They are shown graphically in Fig. 3. The following is a discussion of these elements, their attributes, and their interrelationships.

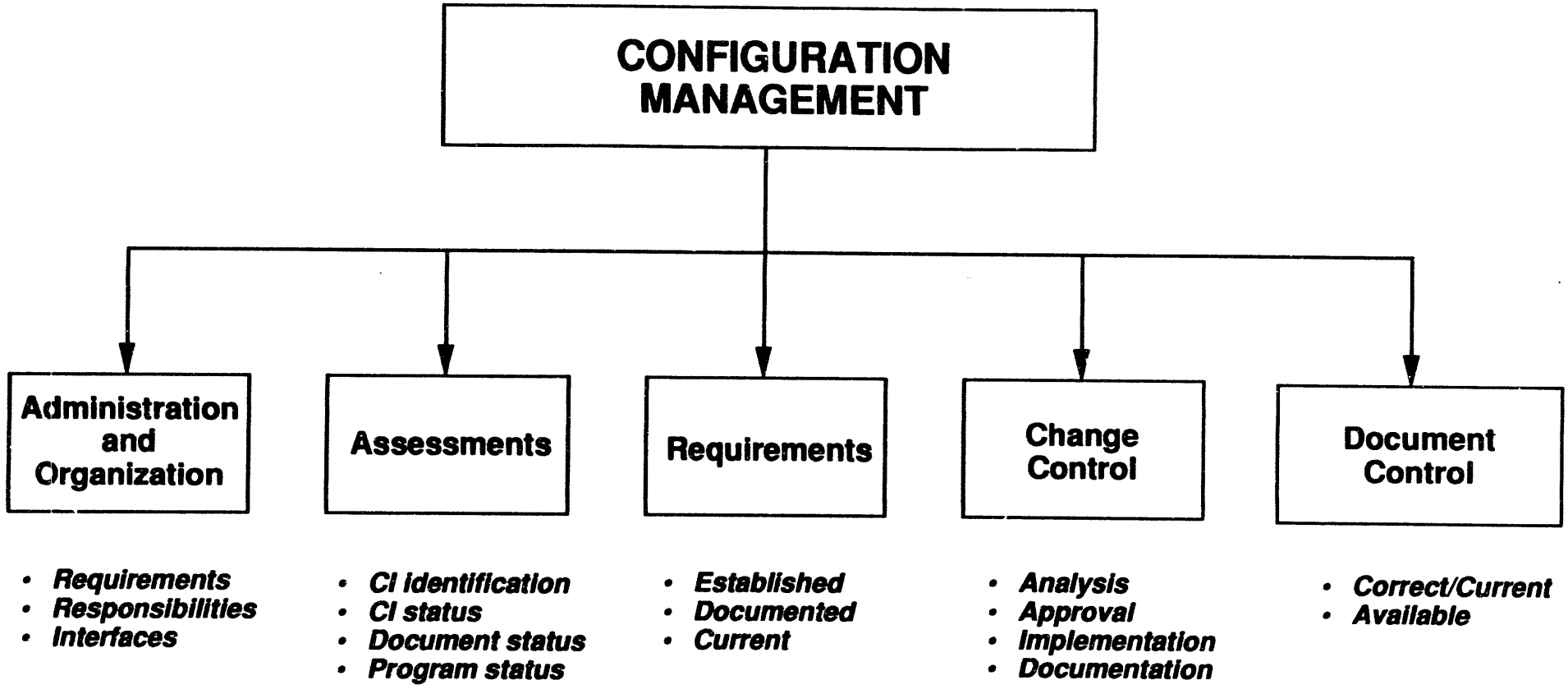

Figure 3

CONFIGURATION MANAGEMENT MODEL

1.3.1 Change Control

The change control element ensures that proposed (physical or administrative) changes to configuration items are properly identified, accepted, developed, reviewed, approved, implemented, validated, documented, and made operational. The objective of change control is to ensure that the changed configuration item satisfies applicable requirements and is accurately reflected in configuration item documentation. To accomplish this, the ways that changes can be made must be identified, controlled, and integrated with the requirements and document control elements. Changes include hardware changes, maintenance changes, process changes, operational changes, temporary modifications, document only changes, and computer software changes. Unauthorized changes must be prevented by administrative or physical (e.g., locked cabinets) means.

Proposed changes to configuration items should be reviewed by technically qualified personnel to determine if they are consistent with approved design and administrative requirements. If not, a review of the design basis by the design authority should be performed to determine if revised design and administrative requirements can be established. The proposed change is permitted only if found to be consistent with approved requirements.

1.3.2 Requirements

The requirements element addresses the functions and constraints that must be satisfied to support the design basis or achieve compliance with permits, laws, orders, or regulations.

The design and administrative requirements are reflected in the documents which define the physical, functional, operational, and performance capabilities and characteristics of configuration items. These documents include the following:

- Safety Analyses, including:
  - Safety Analysis Report (SAR)
  - Facility Safety Evaluation
  - Safety Study
  - System Safety Analysis
  - Safety Assessment
  - previous Unreviewed Safety Question Determinations (USQDs),
  - Hazard Screening reports from the SAR Update Program Phase I
  - Candidate Safety Class Item lists from the SAR Update Program Phase IA
  - Criticality Safety Approval (CSA)
- Technical Safety Requirements (Operational Safety Requirements or Technical Specifications)
- Environmental permits, including:
  - National Pollution Discharge Elimination System (NPDES) permits for water discharges -- individual "out fall" sheets
  - Air Permits for air discharges – individual stack permits
  - Resource Conservation Recovery Act (RCRA) permits for hazardous waste facilities -- Part B permit
- System Descriptions
- Upper-level procedures
- Operating procedures
- Maintenance procedures
- Test procedures
- Training materials
- Vendor manuals and materials
- Industry Codes, Standards, and recommendations
- Equipment Specifications

- Engineering analyses/calculations
- Engineering drawings (layout, flow diagrams, process and instrumentation diagrams, wiring, electrical one line diagrams, logic diagrams)
- Instrument setpoint control sheets
- Audit and other commitments
- Data bases
- Specifications
- Official correspondence
- Records of past or present operational performance

Design and administrative requirements may also be obtained by interviewing experienced personnel, including retirees.

The requirements element identifies and categorizes (e.g., nuclear safety; environmental, safety, and health; mission critical; or designer option) the design requirements and regenerates (as necessary) the design requirements and design bases that are no longer available.

The requirements element interfaces with the change control element by providing a basis for deciding whether changes are acceptable. Likewise, the requirements element interfaces with the document control element because the requirements must be documented and available.

1.3.3 Document Control

The document control element ensures that configuration item documentation, including records, is updated to reflect changes to configuration items in a timely manner, distributed to controlled copy holders, and maintained available to support daily work activities. Configuration item documentation can include paper copies (i.e., drawings, procedures, and manuals), electronic media (i.e., word processor files and computer data bases), and photographic media (i.e., microfilm, microfiche, and photographs). The CI documentation used to perform essential activities (e.g., training) or make important decisions must be kept current with the physical and functional characteristics of the configuration item and with its design and administrative requirements. Configuration item documentation should be controlled for the life of the facility, activity, process, or experiment as changes are made.

This functional element identifies and controls configuration item documentation; updates configuration item documentation to reflect changes to configuration items in a timely manner; tracks configuration item documentation, including change status; and maintains configuration item documentation retrievable.

1.3.4 Assessments

The assessment element systematically evaluates the development and effective implementation of the other configuration management elements. It assesses the adequacy of the relationships between the design and administrative requirements and the configuration items, between the configuration items and the configuration item documentation, and between the design and administrative requirements and the configuration item documentation.

Assessments can be divided into initial assessments and ongoing assessments. The initial assessment examines existing programs and processes (e.g., change control, design, and document control) to identify needed improvements as early as possible. The initial assessment can also aid in identifying configuration items, evaluating the existing condition of these items against the available documentation, and identifying missing requirements information.

A special case of the initial assessment is the preliminary assessment. It is a quick, early, "desk top" assessment by experienced personnel to identify high priority configuration items and major change control and document control process weaknesses. It may also identify nonconforming conditions, such as conflicts between documents and actual conditions, that must be resolved. The preliminary assessment provides a basis for confidence in or correction of these processes so that they will suffice at least until a more thorough assessment can be made and corrective action taken.

The ongoing assessments are conducted on a continuous periodic basis after effective configuration management is established. They examine the effectiveness of upgraded controls and documentation to ensure that proposed changes are acceptable and properly implemented, determine that configuration items continue to satisfy their design and administrative requirements, monitor important characteristics to determine if equipment is performing as designed, and assess the continued effectiveness of all configuration management elements.

1.3.5 Organization and Administration

The organization and administration element ensures that the other configuration management elements are implemented effectively in a consistent, cost effective, and timely manner. To accomplish this, responsibilities, authorities, and interfaces among organizations must be clearly defined and communicated to all personnel.

The organization and administration element ensures that management's requirements and expectations regarding configuration management are developed, documented, and clearly communicated to all levels of the organization. It includes management involvement with configuration management activities and insistence on compliance with configuration management requirements.

Within this element, procedures are developed to ensure that configuration items are consistent with their design and administrative requirements and are accurately reflected in configuration item documentation.

This element also ensures that staffing and resources are sufficient, management and personnel are trained, data bases are provided, and nonconformances are tracked and resolved.

1.4 FUNCTIONAL RESPONSIBILITIES

Effective configuration management is primarily the responsibility of line managers and personnel. They are the people who can directly control the configuration of important facility, activity, process, or experiment features. They include operations, maintenance, test, and other personnel who can physically change an item; and managers who can order or allow a change. Support for configuration management comes from specialists such as the site or major organization CM coordinator, the Configuration Management Working Group (CMWG), engineering, and records management.

This section describes a possible allocation of general responsibilities during the configuration management implementation process, with emphasis on Phase I. Actual responsibilities should be defined for each organization by its procedures and plans.

1.4.1 Site and Major Organization Manager

Each site and other major organization manager has overall responsibility for configuration management implementation at each facility, activity, process, or experiment under his/her control. These responsibilities include development of a site/organization configuration

management plan which incorporates ("rolls-up") the plans of subordinate organizations; identification of facilities or separate activities, processes, and experiments to participate in Phase I; development of effective change and document control guidance; and ensuring that training is provided to appropriate managers, supervisors, and other personnel. The manager will also need to monitor configuration management implementation and initiate corrective action as necessary.

The site or major organization manager may chose to delegate certain responsibilities to other individuals (e.g., CM coordinators).

1.4.2 Division/Department Manager

The division/department manager has responsibility for implementing configuration management at his/her facility, activity, process, or experiment. These responsibilities include ensuring development of a configuration management implementation plan, consistent with the site/major organization plan, which addresses the phases and schedule for configuration management implementation; training is provided to supervisors and personnel; initial and ongoing assessments are performed; configuration items are identified and appropriately graded; effective change control and document control processes are in place and used; design and administrative requirements are identified, documented, and available for use during the change control process; and key documentation is accurate, consistent, and available for use. The manager will also need to monitor configuration management implementation status and initiate corrective action as necessary.

The division/department manager may chose to delegate certain responsibilities to other individuals (e.g., CM coordinators).

1.4.3 Line Personnel

Line personnel are responsible for conforming with all configuration management related procedures including making changes only as approved through appropriate procedures.

1.4.4 Site or Major Organization CM Coordinator

Each Site or Major Organization CM Coordinator (if assigned) has responsibility for coordinating activities for his/her site or organization; providing technical assistance on configuration management-related matters; identifying facilities, activities, processes, or experiments for Phase I; and participating in the Configuration Management Working Group.

1.4.5 Division/Department CM Coordinator

Each Division/Department CM Coordinator (if assigned) has responsibility for coordinating activities; providing technical assistance on configuration management related matters; and acting as a liaison with the site/major organization.

1.4.6 Configuration Management Working Group (CMWG)

The Configuration Management Working Group (see Appendix D) is a committee of configuration management coordinators from the sites and other major organizations. The group is responsible for providing a forum for information exchange, lessons learned, and coordination; providing a forum for establishing consensus (to the extent desirable for minimizing duplicated effort); recommending Level 1 policy, standards, and associated implementation guidance documents; and developing training outlines to promote a common understanding and approach.

1.4.7 Configuration Management Program Manager

The Configuration Management Program Manager has overall responsibility to lead the development and implementation of configuration management for Energy Systems.

2. CONFIGURATION MANAGEMENT IMPLEMENTATION APPROACH

Although conceptually simple, implementation of configuration management on existing facilities, activities, processes, or experiments can be difficult. This chapter outlines a graded three-phase approach that emphasizes early identification and control of the most important configuration items. This emphasis provides relatively high near-term benefit at minimal cost and resource impact.

The three-phase approach to implementing configuration management is shown in Fig. 4. In Phase I, the highest priority configuration items--those whose failure could significantly affect public and worker health and safety or the environment--are identified and placed under interim change and document control. In Phase II, the remaining configuration items are identified, and complete change and document control processes are applied. In Phase III, design requirements and bases are recovered to the extent necessary and documentation updating completed as needed. Phase I applies only to facilities, activities, processes, and experiments identified by the site manager or site CM coordinator as having safety class items 1 or 2 items or environmental permits. Phases II and III expand configuration management to other facilities, activities, processes, and experiments.

The actual implementation plan will be developed by responsible management to cover each facility, activity, process, or experiment. Chapter 3 provides more detailed guidance for Phase I activities. Additional guidance for the subsequent phases will be provided separately.

2.1 PHASE I

Phase I is intended to focus initial configuration management efforts on those items most important to public health and safety and environmental protection. In general, this is limited to high and moderate hazard facilities (as identified by the Facility Safety Department) and to facilities, activities, processes, and experiments subject to environmental permits. Phase I ensures that minimum configuration management steps are taken as early as possible for these operations.

The Phase I activities include a preliminary assessment of the change and document control procedures and practices for possible improvements, identifying high priority configuration items, and implementing interim change and document control measures as necessary. An example flow chart of the Phase I activities is provided in Fig. 5.

The first step of Phase I should be development of an implementation plan. The plan should describe a systematic phased program similar to that outlined in this document, with emphasis on Phase I. The plan should initially scope and schedule the preliminary assessment (Section 3.3). This plan may initially be an informal, one-sheet outline of scope, responsibilities, and anticipated tasks developed in an hour by the CM coordinator and responsible manager. It should be consistent with the site or business unit CM plan. For Phase I, it should reflect the quick identification and control of high priority configuration items, possibly confining all activities to a few hours work by experienced personnel. (Section 3.1 provides additional discussion of the Phase I plan.) After the preliminary assessment, the plan can be revised to organize, schedule, and assign resources to the required activities identified in the assessment.

The second step in Phase I is to provide orientation to managers and training (Section 3.2) to personnel who are performing the preliminary assessment. This step provides the basic understanding needed to efficiently and effectively perform the assessment.

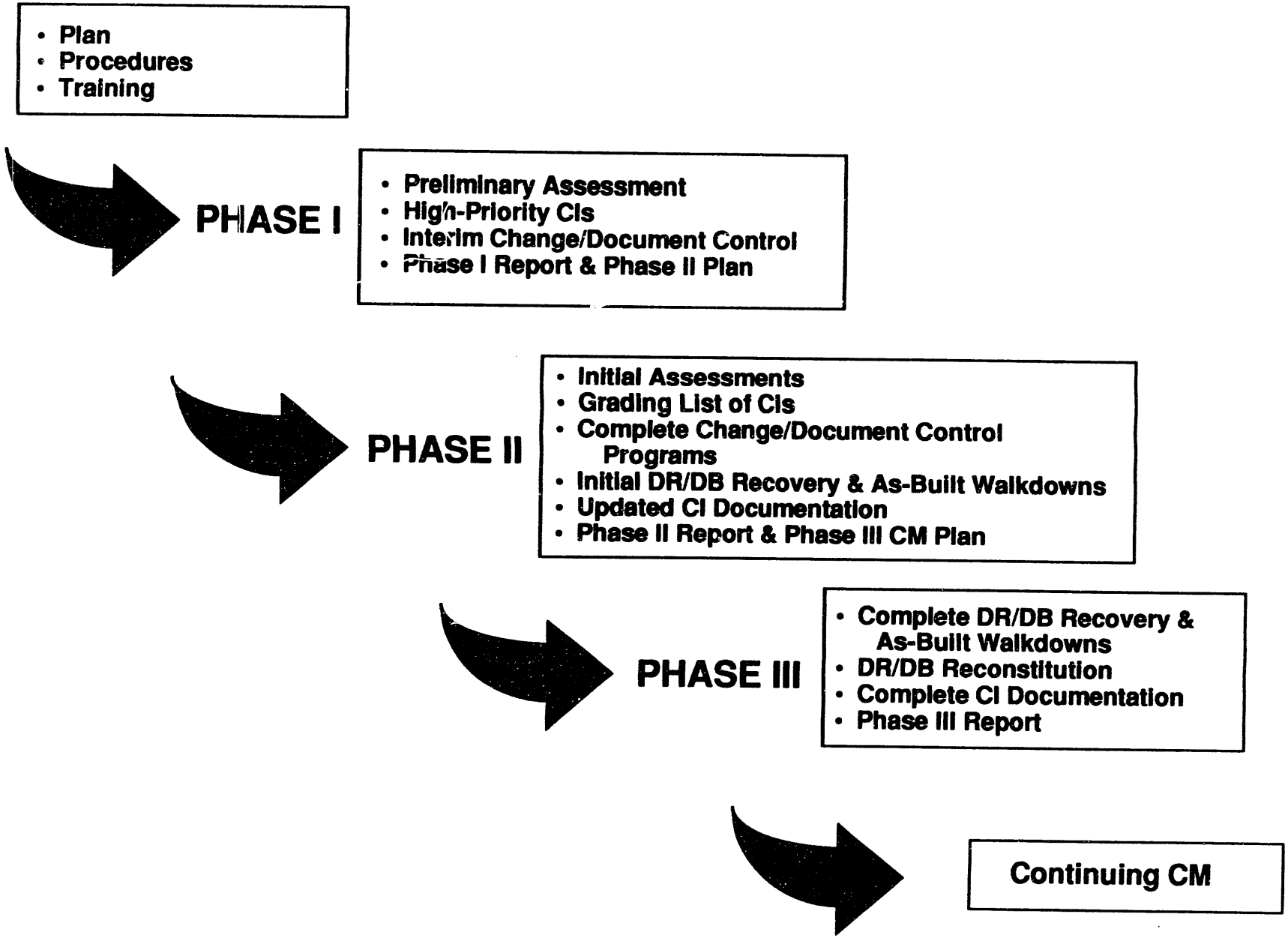

Figure 4

SUGGESTED PHASES OF CM IMPLEMENTATION

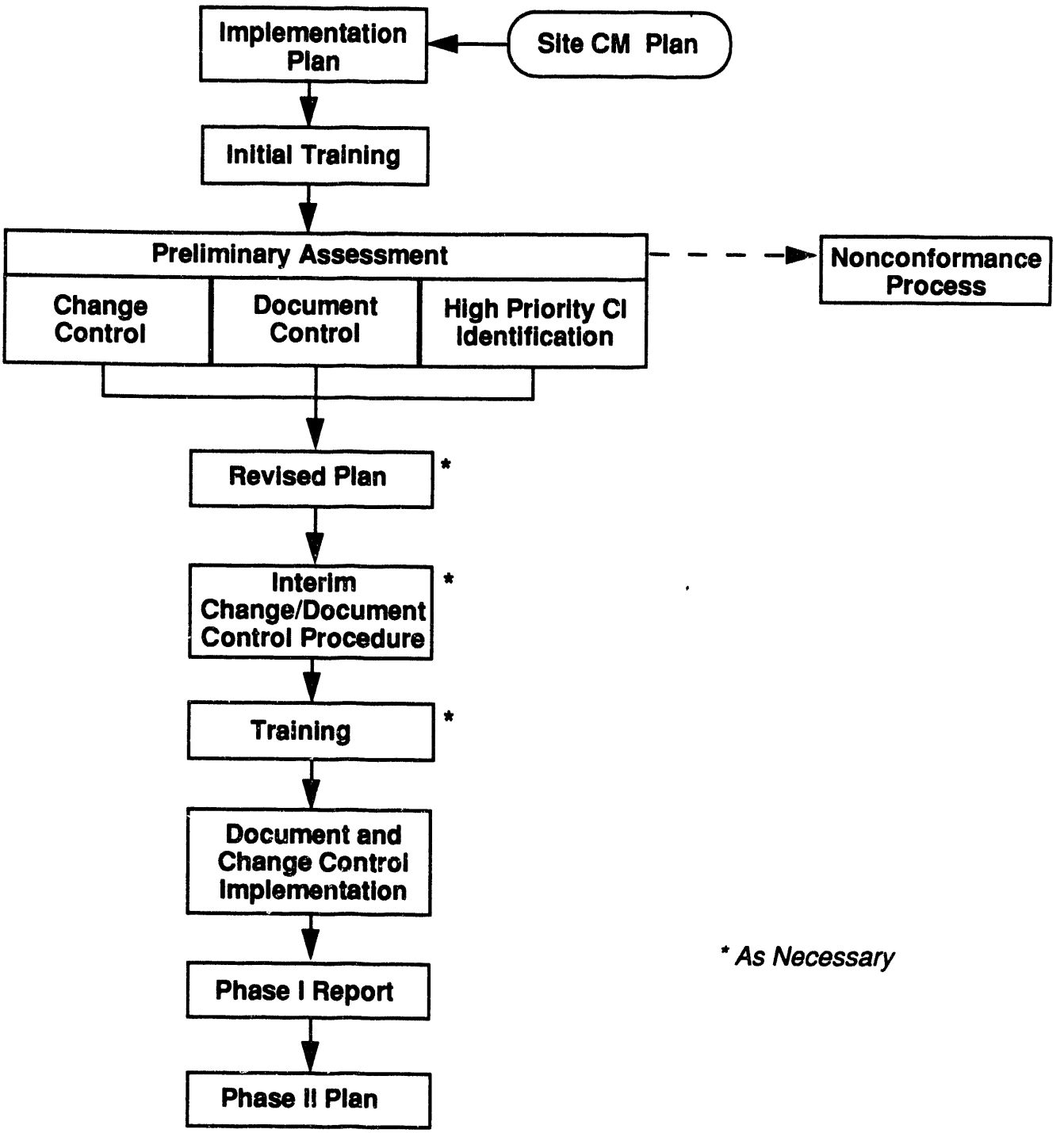

Figure 5

PHASE I

The third step is the preliminary assessment (Section 3.3) which is intended to accomplish two things: it should identify high-priority configuration items and it should identify important weaknesses in the change and document control processes. The identification of high-priority configuration items allows management to focus its efforts. The identification of significant control process weaknesses allows either permanent or interim process corrections to prevent significant new configuration problems from occurring.

Following the preliminary assessment, the Phase I plan can be revised to address the specific actions required to correct weaknesses identified in change and document control. In the event the needed corrections cannot be simply and quickly made, interim (temporary) procedures (Section 3.5 and 3.6) may be implemented. These procedures can be based on available site or division procedures. Their purpose is to ensure that adequate change control and document control processes are in place.

Managers and all personnel who can effect a change at the facility, activity, process, or experiment should be trained in the document and change control procedures. This training should stress responsibilities and procedural requirements, plus the necessity of following the procedures for all changes.

The revised or interim change and document control processes are placed in effect as soon as possible for high-priority configuration items.

The preliminary assessment may identify nonconformances such as conflicts between actual, "as-found" conditions and known requirements. Existing processes should be used to record and resolve these nonconformances (Section 3.7).

The results of Phase I activities are documented in a report (Section 3.8). The report should include a discussion of activities planned and accomplished. Also, the CM plan should be refined for Phase II to include the lessons learned in Phase I.

2.2 PHASE II

Phase II extends configuration management to facilities, activities, processes, and experiments not included in Phase I, and broadens configuration management for the Phase I participants. It is intended to identify and control all configuration items. Its activities include a formal initial assessment, identification of remaining configuration items, and implementation of complete change and document control programs (as necessary). A flow chart of Phase II activities is provided in Fig. 6.

For facilities, activities, processes, and experiments that did not participate in Phase I, the first Phase II steps are planning and initial training. These are similar to the planning and initial training discussed above for Phase I. Phase I participants will have already completed these activities.

The next step is completion of the initial assessment (Section 1.3.4). This assessment is intended to identify and grade all remaining configuration items, fully evaluate the adequacy of change control and document control processes, and identify design and administrative requirements that are known or must be recovered. The initial assessment may be, for many organizations, a step to confirm they have no configuration items to be concerned with. (In this case, the Phase II report can summarize this conclusion and provide a basis for no further action.)

The change and document control processes completed and formalized during Phase II should address all change mechanisms including hardware changes, computer software changes,

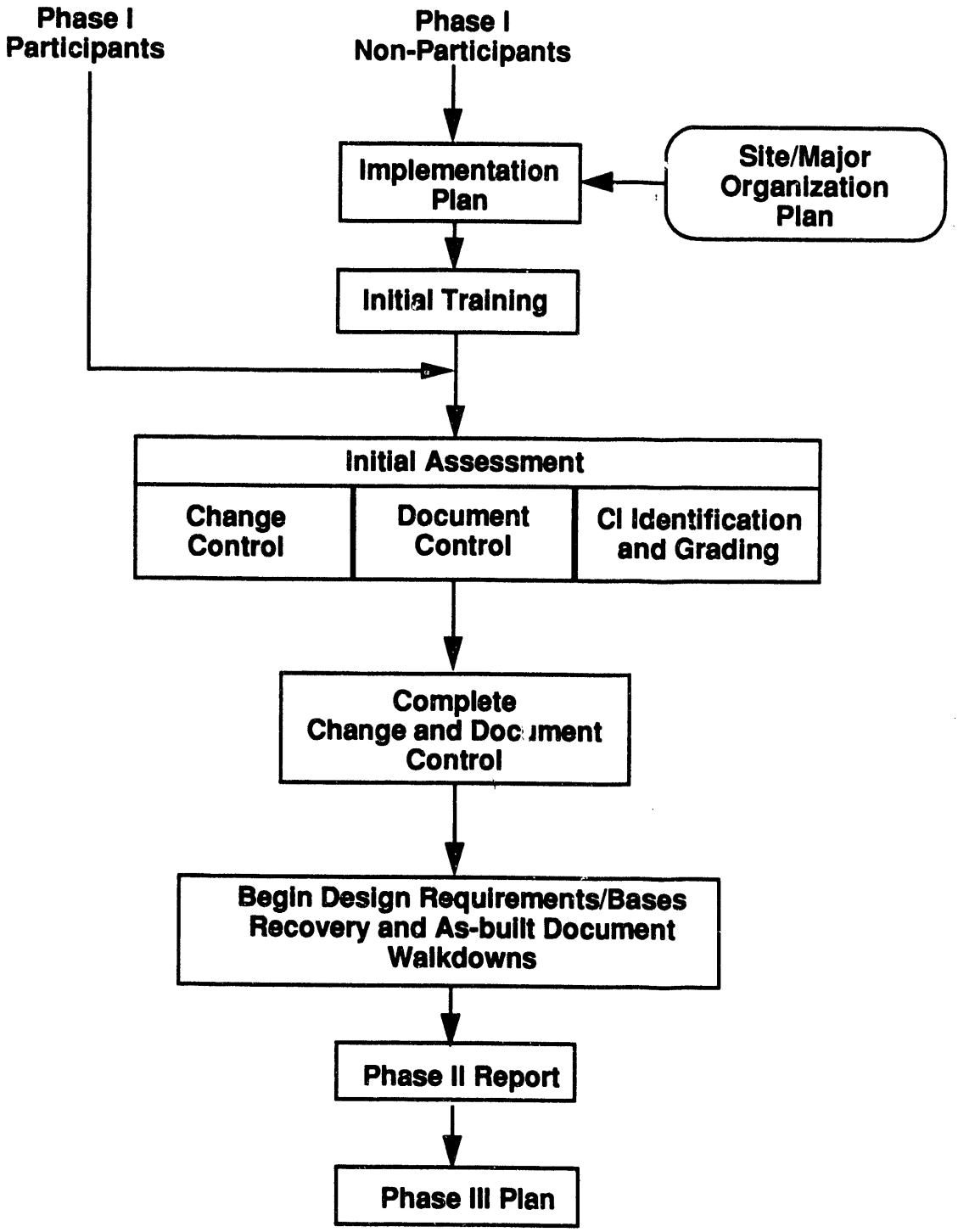

Figure 6

PHASE II

procedure changes, operational changes, and document-only changes. They should ensure that potential changes are identified; reviewed for technical merit (including conformance with known design and administrative requirements); approved by appropriate managers; implemented as approved; and properly documented. They should ensure that no changes are made to configuration items outside of the formal process.

There may be several important differences between the complete change and document control processes and the interim processes that may have been implemented in Phase I. First, the permanent change process may be more structured with increased involvement of managers, the design authority, and other reviewers. Second, comparison of a proposed change with known design and administrative requirements may indicate each requirement be formally identified and addressed.

A major Phase II effort is to identify and grade the configuration items not included in Phase I. Identification will require a thorough review of the facility, activity, process, or experiment against the basic definition of a configuration item: health and safety, environmental protection, compliance, safeguards and security, and preservation of essential capability. Grading will require establishing and applying criteria intended to make the configuration management effort commensurate with the importance of each configuration item.

When the remaining configuration items are identified and graded, they are placed under the completed change and document control processes.

Major efforts that may be initiated during Phase II include recovery of design requirements and bases, and walkdowns. Design requirements/bases recovery is generally necessary for older operations for which available documentation is not complete, accurate, or consistent. It includes identifying missing information; recovering this information through records research, discussions with design or operations personnel, or re-analysis; and documentation.

As its name implies, the walkdown process involves physically going to and studying a configuration item to ensure it is as described in CI documentation such as drawings and procedures. On older facilities, it often results in identification of discrepancies between the actual and documented configuration items. These discrepancies must then be resolved by updating the documentation or modifying the physical configuration.

Both the design requirements/bases recovery and the walkdown efforts may require significant efforts and careful planning. They may be completed in Phase III. The recovery of available design requirements/bases and as-built walkdowns for the high-priority configuration items identified in Phase I should be completed in Phase II.

The Phase II activities should be documented in a report. The report should include a discussion of activities planned and accomplished in Phase II. Also, the CM plan should be refined for Phase III to include the lessons learned in Phase II.

2.3 PHASE III

Phase III is intended to complete the transition to a fully effective, permanent configuration management process. Phase III is a natural follow-on to Phase II, completing long-term activities.

Phase III activities include completing the recovery of available design requirements/basis, completing walkdowns, reconstitution of needed missing or unavailable requirements and bases, final resolution of discrepancies, and implementation of complete and effective change and document control processes. A flow chart of anticipated Phase III activities is provided in Fig. 7.

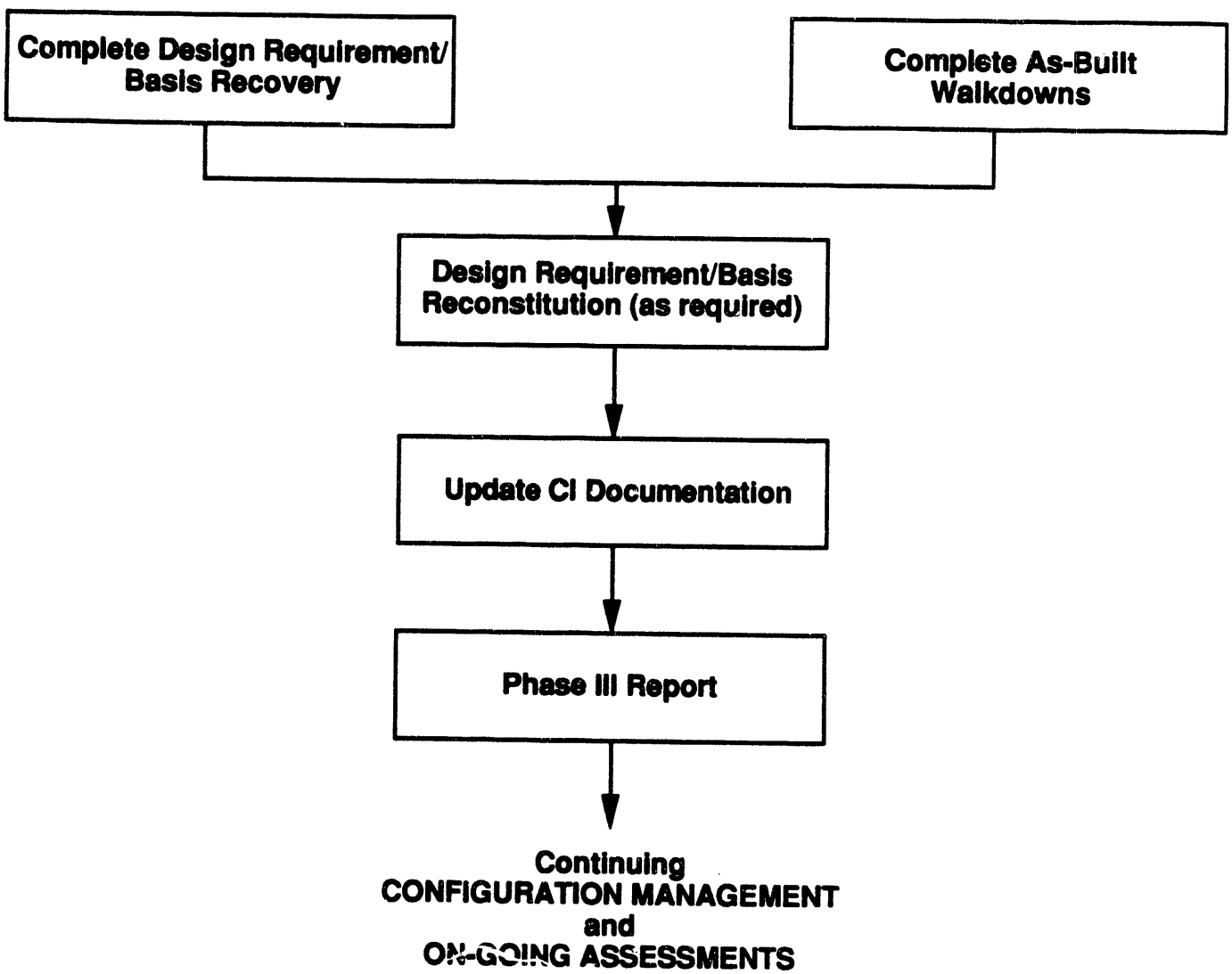

Figure 7

PHASE III

3. PHASE I IMPLEMENTATION GUIDANCE

Phase I is intended to quickly ensure adequate control of the highest priority configuration items, those most important to public health and safety and to environmental compliance. To accomplish this, it must identify these items and provide for them an effective change control process. It must support this with adequate documentation to ensure the effort is not lost.

Phase I is intended to apply only to high and moderate hazard facilities, as designated by the Facility Safety Department, and to facilities, activities, processes, and experiments subject to environmental permits. These facilities, activities, processes, and experiments should be identified by the site manager or site CM coordinator.

The following sections provide additional guidance for identifying high-priority configuration items, providing interim change and document control when needed, and handling nonconformances. The sections also include discussions of the planning, training, and preliminary assessment activities needed to systematically accomplish Phase I objectives.

3.1 PLAN

A brief plan covering the Phase I activities should be developed to cover each facility, activity, process, or experiment. This plan should be consistent with the site plan. The plan will document the overall configuration management implementation approach and provide details for Phase I activities. The Phase I plan may be developed in two stages. In the first, the activities required to perform the preliminary assessment (Section 3.3) can be organized as discussed in Section 2.1. In the second stage, the plan can be revised to reflect the results of the preliminary assessment and describe how to gain control of the high priority configuration items, if needed.

The revised Phase I CM plan, if required, may consist of a one or two page outline of objectives, tasks, methods, schedules, and responsibilities. Its development may be limited to a few hours or days, depending on the complexity of needed changes. It should be highly focused on ensuring high priority configuration items are identified and controlled. The plan should be approved by the responsible facility, activity, process or experiment manager and reviewed by the site/major organization manager or CM coordinator. Figure 8 provides an example plan in the form of a bar chart.

The Phase I plan should define the physical boundaries of the facility, activity, process, or experiment to minimize overlaps or gaps with other efforts. For facilities, these boundaries have been defined as part of the Safety Analysis Report Update Program, and may be obtained from the facility manager or the Facility Safety Department. For activities, processes, and experiments that are not adequately covered by facility Phase I CM plan, the boundary should be defined around specific equipment and procedures. It is anticipated that only a few activities, processes, or experiments will have high priority configuration items not covered by a facility plan. For example, most processes are confined to equipment covered by a facility plan.

Most Phase I CM activities can be performed, in series or parallel, in a few hours or days by a small team of experienced personnel. For example, high priority configuration items can be identified from available documents (see Section 3.4), and the adequacy of change and document control practices can be estimated by comparison with the guidance in Sections 3.5 and 3.6.

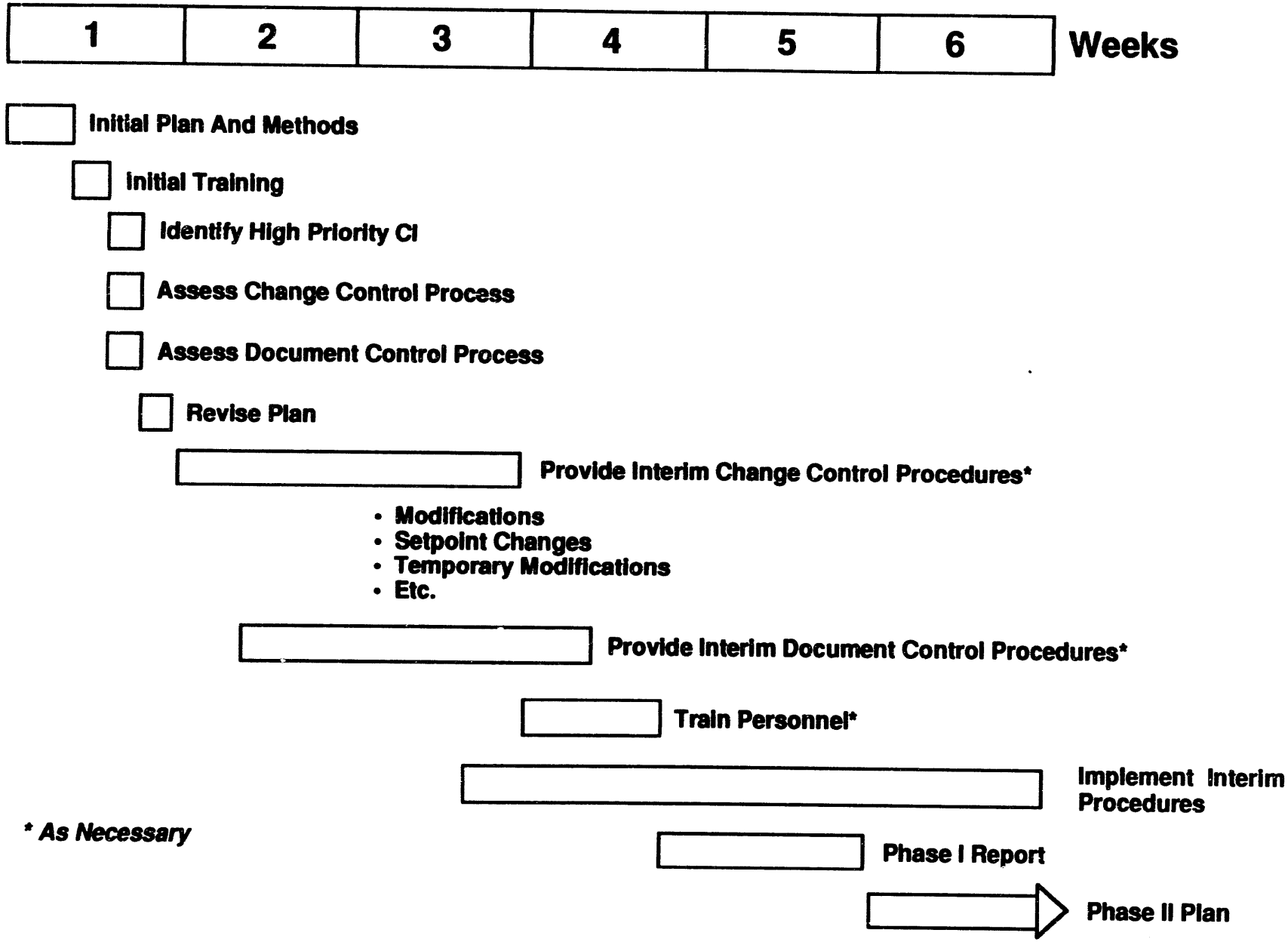

Figure 8

EXAMPLE PHASE I SCHEDULE

3.2 TRAINING

Early in the implementation process, configuration management orientation should be given to all managers and personnel who are in a position to make changes to the facility, activity, process, or experiment. The orientation should cultivate an awareness of configuration management, its importance, and Energy Systems' commitment to it; provide a common understanding of its objectives and elements; and communicate individual and group responsibilities. (The Configuration Management Working Group has developed a general configuration management orientation lesson plan which may be customized for use by the staff of each facility, activity, process, or experiment.)

Personnel performing the preliminary assessment should be trained in the scope, methodology, and objectives of the assessment. In most cases, this training will consist of a simple, informal explanation prior to beginning the task. Its objective is to ensure the assessment is as complete and efficient as practical.

If interim or revised change and document control procedures are developed, managers and personnel should be trained in their use. This training should convey the purpose, methods, and responsibility assignments of the new/revised procedures, and should emphasize the importance of adhering to them for the high priority configuration items. It should also communicate the concept of high priority configuration items and the importance of identifying and controlling them as soon as possible.

3.3 PRELIMINARY ASSESSMENT

The preliminary assessment has two purposes. First, it identifies the high priority configuration items that need to be controlled. Second, it identifies and characterizes any significant weaknesses in the existing change control and document control processes.

The preliminary assessment will generally be a "desk top," or "brainstorm" review of documentation (e.g., drawings, procedures, change packages, or records) and accepted practices by a small team of experienced personnel. It may also include interviews with other experienced people, or a walkdown of equipment to identify components or conditions not accurately identified by the documentation. In general, it can consist of three activities (identify items, assess change control, and assess document control) of a few hours duration that may be performed in series by one team or in parallel by several teams.

Assessment teams should generally consist of a leader and several people from different disciplines who are knowledgeable about the facility, activity, process, or experiment. For example, a facility team looking for high priority configuration items may have representatives from operations and engineering, with assistance from facility safety, environmental management, and site configuration management. A parallel team looking at change control might include operations, maintenance, testing, and engineering; and a team looking at document control might include operations, maintenance, document control and records management, and engineering. In other cases, such as most experiments, two or three senior people may be able to cover all concerns.

High priority configuration items may be identified from the sources described in Section 3.4. They should be documented in a list, and distinctly marked (e.g., labeled "CI") on key drawings, procedures, and other controlled forms such that they can be easily recognized by anyone wishing to make a change to them.

The existing change and document control systems can be assessed by comparing actual current practices, whether formally documented or not, with the general steps and characteristics

outlined in Sections 3.5 and 3.6. Note that these steps and characteristics are intended to be guidelines. They need not be individually addressed or deviations from them justified. The important consideration is that the existing change and document control practices ensure high priority configuration items cannot be altered without adequate review and approval, and that key documents accurately reflect those items physically and functionally.

The preliminary assessment provides a technical basis for taking corrective action and making interim programmatic upgrades. The assessment also provides a foundation for completing the initial assessment in Phase II. The results of the assessment should be documented as part of the Phase I report.

3.4 IDENTIFICATION OF THE HIGH PRIORITY CONFIGURATION ITEMS

During Phase I, emphasis is placed on identifying and controlling high-priority configuration items. High-priority configuration items are those whose failure to satisfy requirements could lead to a loss of life or health to the public or plant personnel, or could lead to significant environmental damage. The configuration items of immediate interest are probably hardware classified as safety class 1 or 2 in safety analyses; software and procedures whose error could lead to an accident (e.g., criticality or explosion); and items whose failure/misuse could directly violate an environmental permit.

Safety class 1 and 2 items will be identified in the Safety Analysis Report (SAR) and in the technical specifications (TS) or operational safety requirements (OSR) of each high or moderate hazard facility. Those high or moderate hazard facilities that do not have a current SAR may use a candidate safety class item list available from the facility manager or the Facility Safety Department. Most of these candidate item lists were developed recently as part of the Safety Analysis Report Update Program (Oak Ridge Facilities) Phase IA and the Safety Analysis Report Upgrade Program (Portsmouth and Paducah) Operational Safety Requirements update phase. The lists identify items that may be safety class 1, 2, or 3 and state the basis for each item's classification. Facilities, activities, processes, and experiments that have not been designated high or moderate hazard by the site Facility Safety Department do not have safety class 1 or 2 items.

Review of environmental permits or permit applications should help in identifying the items whose failure could lead to a permit violation. Environment permits include the National Pollution Discharge Elimination System (NPDES) permits for discharge into water sources (see individual "out fall" pages for each release point); Air Permits for atmospheric discharges (see permits for each stack); and Resource Conservation Recovery Act (RCRA) permits for hazardous waste facilities (see Part B permits). These permits are available from the facility manager or the site Environmental Management Department. Facilities, activities, processes, and experiments that do not have such permits should not have high priority environmental configuration items. Candidate items include equipment that is necessary to monitor releases (e.g., liquid effluent monitors) and components, such as valves and fans, that would be used to terminate an unacceptable release. Backup power and control to these monitors and components would also be candidates.

In the event the above sources are not finalized, need confirmation, or appear to dictate an unmanageable Phase I scope, high priority configuration items can be identified by applying the basic configuration item definition (see Appendix B) to generate a list of potential items. Experienced personnel can then identify the high-priority items from this list. Assistance in identifying high-priority configuration items may be obtained from the Facility Safety Department, the Environmental Management Department, or other knowledgeable technical groups.

Identification and prioritization of configuration items will be a continuous process. Additional high-priority items may be identified in subsequent phases of CM implementation. In order to capture identified information for future retrieval, a database should be developed. This data base should list and cross-reference each configuration item to its design and administrative requirements and configuration item documentation.

3.5 INTERIM CHANGE CONTROL

Changes to high priority configuration items, whether permanent or temporary, physical or non-physical, must be controlled in order to maintain consistency among requirements, physical and functional configuration, and documentation.

Changes can occur in many ways, some of which are not easily identified. They may include hardware and computer software modifications, equipment realignments, replacement parts unlike the original, or alterations in the method or sequence of activities. They may be planned and controlled, such as when a major physical modification is designed and installed, or they may be unintentional, as when maintenance personnel substitute an available part for the unavailable one called for. They may even be made by a new person performing a job differently than his/her predecessor or by accepting an "as-found" physical condition that may not conform to requirements.

The change control process exists in many forms depending on the item controlled, the organization(s) involved, and the nature of the change. However, the fundamental steps of the process, outlined in Fig. 9 and summarized below, are basically the same. These steps may be used as a measure for existing change controls or as the basis for creating an interim change control process.

The formality and detail of the individual steps may be graded according to the complexity of the changes involved, but the overall process (designed specifically for high priority configuration items) is not graded.

The necessary fundamental steps for an interim change control process are:

Proposal The desired change is clearly defined and described.

Acceptance The person responsible for the facility, activity, process, or experiment agrees that the change should be made. (This authority may be delegated.)

Development Details of the change are defined, described, and analyzed.

Inputs to the development step include applicable design and administrative requirements for the affected configuration items, plus the governing design and administrative procedures for the development process. Outputs of the step range from simple annotations on existing documents to detailed design drawings and analyses.

The development step may be graded to reflect the complexity of the proposed change. For example, addition of a line of process machinery may require detailed engineering design, whereas changing the type of lubricant in an existing procedure may involve simply seeking concurrence from the equipment manufacturer.

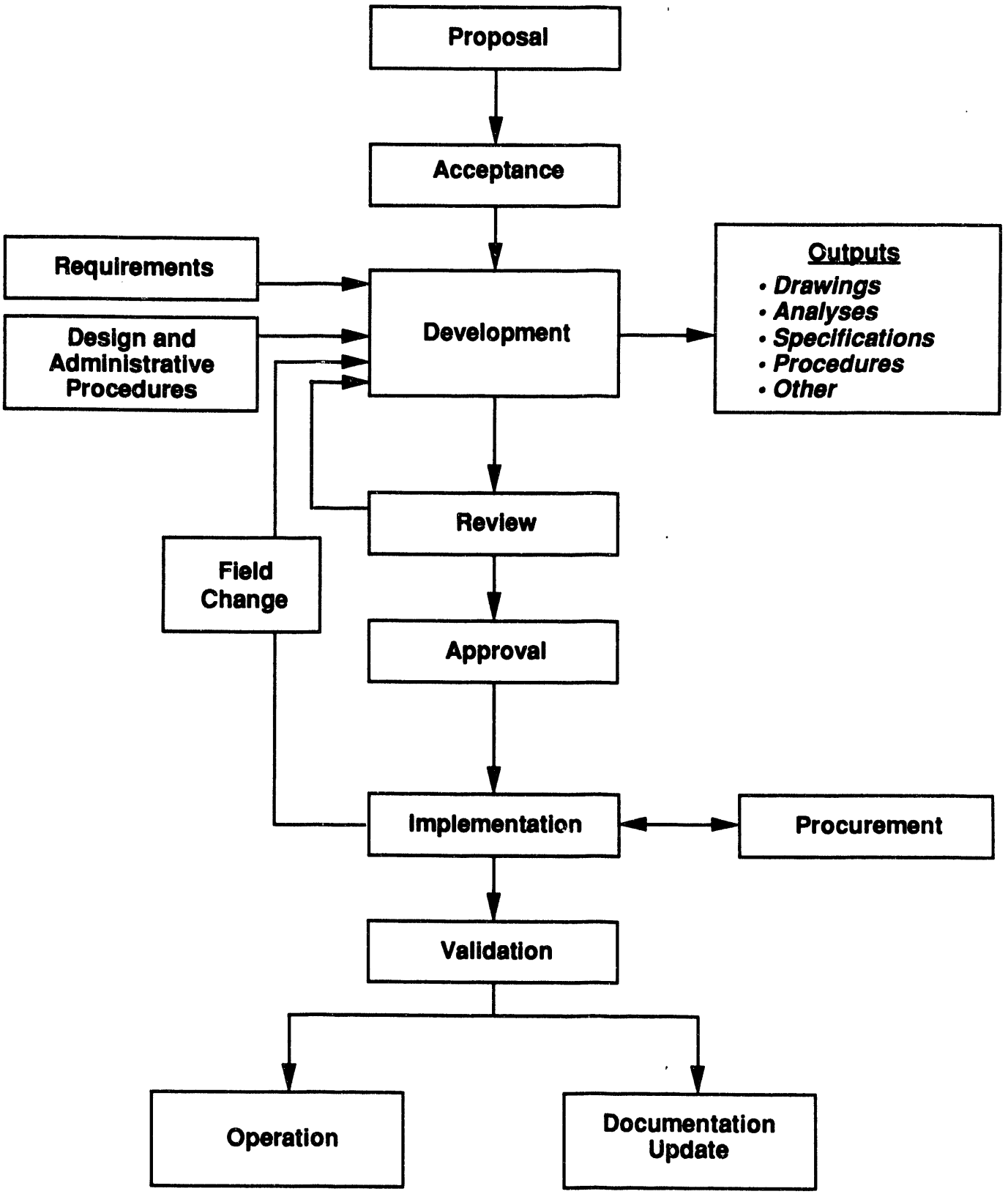

Figure 9

INTERIM CHANGE CONTROL PROCESS

Review The change details are verified to satisfy the original proposal objectives, incorporate applicable requirements, meet procedural and safety requirements, and to be technically correct (e.g., no calculation errors or standards violations).

The review step can be graded according to the complexity of the change. A complex change, such as one not falling within the purview of a single group, may require an internal review by the developing group plus an external review by experts outside that group. In this case, the internal review could verify that the change is technically correct and meets procedural requirements, and the external review could verify that requirements and objectives are satisfied.

Approval The developed change is formally approved for implementation by the person responsible for operation of the facility, activity, process, or experiment. (This authority may be delegated.)

Implementation The change is implemented as approved.

The implementation step includes planning, procurement, and other activities needed to physically or functionally install the change. It may be graded in that some of these activities may be unnecessary or minor for simple changes but discreet and formal for others. For example, relocation of a portable radiation monitor may require no procurement or formal planning. On the other hand, addition of a wing to a building would require formal and extensive planning and procurement.

Validation The implemented change is checked, tested, or monitored to confirm that it satisfies its objectives, meets applicable requirements, and is free of unexpected side effects.

Operation The validated change is made part of ongoing operations. Procedures are updated and personnel are trained for the new configuration.

Documentation The validated change is accurately reflected in configuration item documentation.

In addition to the fundamental steps discussed above, the interim change control process should have the following characteristics to ensure that it is followed and effective:

- It is clearly documented and communicated to all personnel to ensure it is followed consistently and completely.

- It prevents changes that have not been approved using the change control process. This generally requires clearly defining what constitutes a change for each type of configuration item, and stating what types of changes are permitted or forbidden by each person/group/organizational level. For example, it may state that maintenance personnel are permitted to make like-for-like replacements but cannot substitute parts without approval from a responsible engineer; equipment operators are permitted to adjust settings only within an approved envelop of values; procurement administrators are allowed to substitute brands but not change colors without the customer's approval; or security personnel can change the type of lock on a door, but not lock an unlocked door without approval from fire protection engineers and operations manager.

Another acceptable way of preventing unapproved changes is to provide physical barriers, such as locking cabinets.

- It avoids unnecessary changes. Until all requirements are known and a complete change control process in place, every change creates an opportunity for error. Unnecessary changes could make a system that is now operating but not clearly understood into one that fails.

- It ensures that the proposed change is clearly defined so that people reviewing and approving it will understand its purpose, scope and ramifications.

- It clearly defines responsibilities for all steps.

- It ensures available design and administrative requirements are identified and complied with (see Section 1.3.2).

- It ensures that the proposed change is technically reviewed by representatives of all potentially-affected groups, people/groups familiar with the requirements (e.g., the design authority), and by responsible management. Technical reviewers may include operations, maintenance, engineering, radiological protection, toxicology, criticality safety, security, procurement, telecommunications, or any other group with expertise in an affected field.

- It ensures that essential analyses are performed and documented. For safety class 1 and 2 items, these will include a safety analysis and an Unreviewed Safety Question Determination (USQD). [Guidance for performing a USQD is available in CSET-9, "Unreviewed Safety Question Determination Application Guide", (ref. 6)]. These analyses ensure that changes to the physical or functional configuration items important to health and safety are safe and are consistent with DOE's authorization to operate the facility, activity, process, or experiment.

- It ensures that key documentation is updated, or "as-built," to accurately reflect the change. A wide range of documentation may be affected, including many of those listed in Section 1.3.2.

Careful consideration should be given to which documents will be updated. Although affected safety analyses, criticality safety approval, and technical safety requirements generally must be kept current, not all others need to be. For example, it may be necessary to update process and instrumentation drawings, which may be used for operational decisions, but not structural detail drawings.

If existing documentation is not known to be current and accurate, the required updating may be limited to those parts of the document that were addressed by the change. For example, a "cloud" could be drawn around the part of a drawing that was changed and confirmed: this part is now known to be accurate.

Appendix A discusses an example change to a configuration item made through the interim change control process outlined above.

3.6 INTERIM DOCUMENT CONTROL

Documents, whether in paper, electronic, or other form, are our way of recording and communicating information. When this information is important, it must be controlled to ensure that it is correct, consistent, current, and available.

Document controls are intended to ensure that configuration item documents accurately reflect the physical and functional characteristics and the requirements of the configuration item. It should ensure that changes made to high priority configuration items are accurately captured, information developed during assessments and requirements recovery efforts is preserved, and controlled information is readily available to and used by people making approved configuration changes.

An interim document change control process has the same basic steps as the interim change control process: proposal, acceptance, development, review, approval, implementation, and validation. Energy Systems standards--ESS-IO-101, *Records Management* (ref. 7), and ESS-IO-201, *Document Control* (ref. 8)--provide further guidance for effective document change control.

An interim document control process should have the following characteristics:

- It is clearly documented and communicated to personnel to ensure it is followed consistently and completely.

- It prevents use of uncontrolled documents for change control decisions. Operating, design, maintenance, and other activities should require use of only the latest revision of controlled documents for decisions affecting high priority configuration items. Uncontrolled documents often have unapproved changes, such as annotations, that can lead to inappropriate actions. (If the annotations are correct and useful, the controlled document should be revised to incorporate them.).

- It clearly defines responsibility for each document type and for each change step.

- It clearly identifies documents and records to be controlled. These should be the minimum set of documents required to support the approved interim change control process. (Candidate documents include many of those listed in Section 1.3.2.)

- It ensures that approved document changes are clear, legible, and correct. Review of the changes by knowledgeable people, such as the lead person responsible for developing a change to the configuration item, is generally a good way to ensure the document conveys the intended information.

- It ensures that approved document changes are made promptly such that a backlog does not develop. Delayed changes can lead to conflicts between documents or between documents and the actual physical/functional configuration. They can also delay operations and development of approved changes, tempting people to circumvent the change control process.

- It safely stores documents to prevent loss, damage, or unauthorized revision. Alternately, multiple controlled sets may be maintained in separate locations, with strict controls to ensure the sets remain identical.

- It makes controlled documents readily available to all potential users. This may require a 24 hour-a-day service for a few operations to avoid significant work delays or use of uncontrolled information. Locally available document control stations may be required in some areas.

- It tracks distribution to ensure all users have updated information when changes are made. Distribution of controlled documents may be supplemented by "information only" copies or "temporarily controlled" copies with clearly-marked expiration dates.

- It is tightly tied to the interim change control process such that a change is not placed into operation without revision of configuration item documentation.

3.7 NONCONFORMANCES

Nonconformances may be identified as CM assessments are made. For example, drawings may be found to not reflect actual facility hardware, procedures may be found to not incorporate higher level administrative requirements, or design requirements for an important system may be unknown. Nonconformances may arise from documentation discrepancies; undocumented changes; or inconsistent, erroneous, or missing design or administrative requirements. Existing procedures should be followed to document, track, assign, resolve, and close these nonconformances.

3.8 PHASE I REPORT

The results and conclusions of Phase I should be clearly recorded to ensure the information it developed is preserved as a base for Phase II. The report should, as a minimum, record the following information:

- name or description of facility, activity, process, or experiment;
- scope of the preliminary assessment; including the facility, activity, process, or experiment boundaries;
- list of high priority configuration items, and the basis of their selection;
- summary of preliminary assessment methods and participants, and the documents reviewed or people interviewed;
- preliminary assessment findings and conclusions, including nonconformances and their disposition: and
- summary of actions, including interim change and document control procedures and training.

The report should be approved by the responsible manager and transmitted to the site/major organization CM Coordinator for review.

3.9 PHASE II PLAN

At the end of Phase I, a plan can be developed for Phase II activities. As outlined in Fig. 6, Phase II is similar to Phase I, but more formal and complete. Additional guidance being developed by the Configuration Management Working Group should help in planning Phase II.

Appendices

Appendix A

EXAMPLE
INTERIM CHANGE CONTROL CASE

Need: A control valve is no longer functioning correctly due to excessive wear. One-for-one replacement parts are no longer available due to the age of the valve.

Proposal: The maintenance crew requests replacement of the valve with a new model. The proposal states that the valve has an increasing failure rate and that parts are no longer available.

Acceptance: The facility manager agrees to replacement because the valve function is important.

Development: An engineer identifies the applicable design requirements based on available information. Sources reviewed include:

- candidate safety class item list -- identifies the valve as safety class 2;
- National Pollution Discharge Elimination System (NPDES) permit and a system flow diagram -- together indicate the valve does not have an environmental protection role;
- facility Operational Safety Requirements (OSRs) -- specify system operating limits;
- facility operators and maintenance personnel -- explain operational and maintenance needs and preferences;
- test records -- identify actual performance of the existing system;
- engineering process and control diagrams -- indicate the intended valve function; and
- industry codes and standards -- define current design requirements for the new valve.

The engineer then researches vendor manuals and literature to select the replacement valve, and perform necessary calculations to confirm the proposed replacement will perform as required. He then develops a design package, including post-installation test requirements, and initiates revisions to key documents, such as engineering drawings, valve specifications, and operating and maintenance procedures.

Review: Another qualified engineer reviews the calculations and design package to confirm that they are technically correct. A safety analyst performs a safety assessment and an Unreviewed Safety Question Determination (USQD), concluding the modification meets current health and safety requirements and does not require DOE approval. Personnel from operations, maintenance, and testing confirm the replacement valve meets their needs, and that documents to be updated have been identified and revisions drafted.

Approval: The facility manager concurs in the change as designed.

Implementation: The new valve is specified and procured.

An installation plan is developed specifying the steps required for removal of the old valve (e.g., draining and flushing lines, disconnecting the control system, and cutting out the valve) and installation of the new (e.g., grinding and welding, flushing, and reconnection of controls). The plan includes necessary permits (e.g., welding) and arranges for necessary work monitoring (e.g., Quality Assurance check points).

The old valve is removed and the new valve installed as specified in the plan. Quality checks are performed.

Validation: Post-installation testing is performed to confirm the new valve meets requirements as specified in the design package.

Operation: With installation and testing satisfactorily completed, the facility operations staff formally accepts the modified system. Personnel who need to know about the change are trained.

Documentation: Selected engineering drawings; specifications; test, maintenance, and operations procedures; data sheets; and safety analyses are updated to reflect the new valve as installed and tested.

Appendix B

DEFINITIONS

Administrative Requirements - Restrictions on human activities, including limitations, procedures, or methods required to perform activities. (Administrative requirements may be recorded in documents such as the Technical Safety Requirements, Energy Systems Policy, Standards, and Procedure manual; and the site or facility specific Standard Practice Procedures).

As-Built - Documentation and records which have been verified to reflect the actual (as found/existing) configuration/condition of a facility, component, system, structure, or software.

Configuration Item Documentation - Technical documentation that describes the design basis, the design requirements (both physical and functional), and the operational controls of a configuration item. (This documentation includes as-designed or as-built drawings, safety analysis and assessments, design specifications, technical safety requirements, procurement documents, operating procedures, surveillance procedures, maintenance procedures, vendor manuals, training documents, and spare-parts specifications).

Change Control - The process that controls the initiation, assessment, approval, implementation, documentation, verification, and tracking of changes to configuration items. The process includes not only changes to individual configuration items but also the required changes to the configuration item documentation. This process is not limited to design control but includes changes such as maintenance modifications, process improvements, operational modifications, and temporary modifications.

Configuration Item (CI) - Structures, systems, and components; computer hardware and software; communication networks; instructions and procedures; and other physical or administrative items whose failure to satisfy definite design and administrative requirements could lead to a loss of life or health; noncompliance with the law, regulations, orders, or permits; violation of safeguards or security requirements; or significant loss of production or research capability.

Configuration Management (CM) - An integrated management process that ensures that the physical and functional characteristics of CIs conform to approved design and administrative requirements. CM ensures that changes to these characteristics are consistent with design and administrative requirements and are properly identified, controlled, and incorporated into CI documentation.

Design Authority - The person(s) or organization with the knowledge, understanding, and authority to change the design.

Design Basis - The underlying rational for the design requirements. The basis is the design input information that identifies the specific function(s) to be performed and the specific values or range of values that bound the design. (Design basis documents contain the functions, safety limits, assumptions, codes and standards, and safety margins applicable to each CI.)

Design Requirements - The outputs of the design process that specify the detailed parameters that are required to achieve the design basis. (Design requirements are a product of a design process and reflect a specific design that falls within the limits of the design basis for a system, structure, or component. Design requirements are recorded in documents such as design drawings, calculations, and specifications.)

Document - Any written (paper or electronic) or pictorial information describing, defining, specifying, reporting, or certifying activities, requirements, procedures, or results.

Document Control - The process used and actions taken to ensure that documents are reviewed for adequacy, approved for release by authorized personnel, and distributed to and used at the location where the prescribed activity is performed.

Graded Approach - The application of CM performance objectives, criteria, and guidance commensurate with considerations such as programmatic importance, level of hazard and risk involved, and remaining life.

Phased Approach - A strategy used to schedule the implementation of the CM program. This approach initially emphasizes the importance of implementing CM on those items that could have a significant adverse impact on the safety and health of personnel or the public or on environmental compliance.

Records - Information that is preserved or appropriate for preservation as evidence of organization, functions, policies, decisions, procedures, operations, or other activities or because of the informational value of the data.

Records Management - The controlled activities associated with records creation, records maintenance and use, and records disposition. This includes planning, receiving, indexing, storing, preserving, retrieving, and disposing of records.

Appendix C

REFERENCES

1. *Policy for Configuration Management*, ESS-CM-100, Martin Marietta Energy Systems, Inc. (draft).

2. *Standard on Configuration Management*, ESS-CM-101, Martin Marietta Energy Systems, Inc. (draft).

3. *Project Management System*, DOE Order 4700.1, U.S. Department of Energy, Washington, D.C.

4. *Safety of Nuclear Facilities*, DOE Order 5480.5, U.S. Department of Energy, Washington, D.C.

5. *Conduct of Operations Requirements for DOE Facilities*, DOE Order 5480.19, U.S. Department of Energy, Washington, D.C.

6. *Unreviewed Safety Question Determination Application Guide*, ES/CSET-9, Martin Marietta Energy Systems, Inc., September 1991.

7. *Records Management*, ESS-IO-101, Martin Marietta Energy Systems, Inc., September 1991

8. *Standard on Document Control*, ESS-IO-201, Rev. 1, Martin Marietta Energy Systems, Inc., November 15, 1991.

OTHER SOURCES

An Assessment of Design Control Practices and Design Reconstitution Programs in the Nuclear Power Industry, NUREG-1397, U.S. Nuclear Regulatory Commission, February 1991.

Configuration Management Program, DOE Order 5480.CM, U.S. Department of Energy, Washington, D.C. (9/92 draft).

Design Basis Program Guidelines, NUMARC 90-12, Nuclear Management and Resources Council, Inc., October 1990.

General Design Criteria, DOE Order 6430.1A, U.S. Department of Energy, Washington, D.C.

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

Nuclear Safety Analysis Reports, DOE Order 5480.23, U.S. Department of Energy, Washington, D.C.

Personnel Selection, Qualification, Training and Staffing Requirements at DOE Reactor and Non-Reactor Nuclear Facilities, DOE Order 5480.20, U.S. Department of Energy, Washington, D.C.

Policy for Records Management, ESS-IO-100, Rev. 0, Martin Marietta Energy Systems, Inc., September 25, 1991.

Position Paper on Configuration Management Program, NIRMA PP02-1989, Nuclear Information and Records Management Association.

Quality Assurance, DOE Order 5700.6C, U.S. Department of Energy, Washington, D.C.

Records Management, DOE Order 1324.5, U.S. Department of Energy, Washington, D.C.

Report on Configuration Management in the Nuclear Industry, INPO 87-006, Institute of Nuclear Power Operations, July 1987.

Safety Analysis and Review, DOE Order 5481.1B, U.S. Department of Energy, Washington, D.C.

Safety of DOE Owned Reactors, DOE Order 5480.6, U.S. Department of Energy, Washington, D.C.

Supplemental Configuration Management Guidance, CSET-8, Martin Marietta Energy Systems, Inc., June 1991.

Technical Safety Requirements, DOE Order 5480.22, U.S. Department of Energy, Washington, D.C.

Unreviewed Safety Questions, DOE Order 5480.21, U.S. Department of Energy, Washington, D.C.

Appendix D

CONFIGURATION MANAGEMENT WORKING GROUP

K-25 Site
Oak Ridge National Laboratory
Paducah Gaseous Diffusion Plant
Portsmouth Gaseous Diffusion Plant
Research Reactor Division (HFIR)
Y-12 Plant
Business Management and Administration
Engineering
Computing and Telecommunications
Environmental Restoration & Waste Management
Safeguards, Security, & Emergency Management
Energy Systems CM Program Manager
CM Program Coordinator
CMWG Chairperson
DOE-OR (observer)

DISTRIBUTION

D. I. Allen
H. L. Arnold, Jr.
J. L. Arrowood
H. D. Bewley
D. J. Bostock
S. E. Burnette
D. D. Cannon
W. W. Carpenter
P. I. Davis (PORTS)
R. G. Donnelly (PORTS)
R. N. English (PGDP)
G. G. Fee
W. E. Fields
R. W. Glass
L. T. Gordon
L. E. Hall
P. E. Hall
S. C. Harris
C. C. Hopkins
J. J. Hummer
E. Johnson
M. J. Johnson
C. B. Landguth
S. H. Lowe
F. K. Martin
R. O. McCloskey
R. Merriman
M. E. Mitchell
F. R. Mynatt
H. A. Nesteruk
F. S. Patton, Jr.
H. B. Piper
S. A. Polston (PGDP)
J. S. Rayside
G. D. Robbins
L. M. Roseberry
M. W. Rosenthal
R. D. Sabin
K. W. Sommerfeld
M. I. Sparks
D. A. Starling
A. W. Trivelpiece
G. W. Turk

Applied Technology Library
Central Research Library
Laboratory Records Department (2)
Laboratory Records - RC
Patent Section
Y-12 Technical Library

External Distribution

G. W. Benedict, DOE Field Office, Oak Ridge, TN

M. A. Boyd, DOE Field Office, Oak Ridge, TN

V. W. Hankins, DOE Field Office, Oak Ridge, TN

J. D. Jackson, DOE Field Office, Oak Ridge, TN

Office of Scientific and Technical Information
US-DOE, P. O. Box 62, Oak Ridge, TN 37831

END

DATE FILMED

1/11/93