NUMARC 91-06

Guidelines for Industry Actions to Assess Shutdown Management

December 1991

**Nuclear Management and
Resources Council, Inc.
1776 Eye Street, N.W.
Washington, DC 20006-2496**

ACKNOWLEDGEMENTS

The Guidelines for Industry Actions to Assess Shutdown Management were developed by the NUMARC Shutdown Plant Issues Working Group, chaired by Harold W. Keiser, Senior Vice President - Nuclear, Pennsylvania Power & Light Company. This working group consisted of representatives from sixteen utilities, the Babcock & Wilcox Owners Group, the Boiling Water Reactor Owners Group, the Combustion Engineering Owners Group, the Westinghouse Owners Group, the Institute of Nuclear Power Operations, and the Electric Power Research Institute.

FOREWORD

This document is intended for the use of NUMARC members in association with the formal industry position approved by the NUMARC Board of Directors on November 20, 1991. The approved formal industry position is:

> ASSESS CURRENT PRACTICES, USING NUMARC 91-06, "GUIDELINES FOR INDUSTRY ACTIONS TO ASSESS SHUTDOWN MANAGEMENT," TO PLAN AND CONDUCT OUTAGES.
>
> IMPROVEMENTS ADOPTED AS A RESULT OF THE ASSESSMENT WILL BE IMPLEMENTED FOR OUTAGES STARTED AFTER DECEMBER 31, 1992.

TABLE OF CONTENTS

LIST OF FIGURES

1.Ø INTRODUCTION

Industry experience has shown that plants can be susceptible to a variety of events that can challenge safety during shutdown. While these events have neither posed nor indicated an undue risk to public health and safety, they do serve to underscore the importance of effective outage planning and control. Proper management of outage activities can reduce both the likelihood and consequences of events, which ultimately enhances safety during shutdown.

Analysis of shutdown events has provided a better understanding of vulnerabilities that certain systems and components have during shutdown plant conditions. In addition, many activities including generic communications, site visits, workshops, studies and surveys sponsored by the Nuclear Regulatory Commission (NRC), the Institute of Nuclear Power Operations (INPO), the Electric Power Research Institute (EPRI), and the Nuclear Steam Supply System (NSSS) Owners' Groups, have heightened the awareness of shutdown concerns. This awareness is a prerequisite to enhancing shutdown safety. This document reflects many of the recommendations and lessons learned from these industry and regulatory activities.

The scope of activities that each utility undertakes during a normal refueling outage is large and diverse. Besides refueling, activities associated with preventive and corrective maintenance, modifications, surveillance testing, in-service inspection, and the administrative activities that support these tasks make outage planning and control a significant challenge. The coordination of these activities with the objective to manage risk and maintain key safety functions is essential and goes beyond compliance with technical specifications requirements during shutdown. In addition, while the scope of activities for an unplanned or forced outage is far less than that of a refueling outage, the same awareness of vulnerabilities during shutdown conditions is required to safely conduct these outages.

NUMARC formed the Shutdown Plant Issues Working Group to coordinate industry activities relating to shutdown safety and to provide the focal point for industry interaction with the NRC on shutdown plant issues. The goal of the working group was to identify these issues and develop guidance that addresses both industry and regulatory concerns. This document is the main product of the working group's effort. The intent of this document is to provide guidance to utilities on assessing and enhancing their current practices for planning and conducting outages., The underlying premise of this guidance is that proper outage planning and control, with a full understanding of the major vulnerabilities that are present during shutdown conditions, is the most effective means of enhancing safety during shutdown. Over the long term, the guidance contained in this document along with the lessons learned from utility assessments of shutdown safety will be included in revisions of INPO's outage management guidelines as appropriate.

Section 2.Ø of these guidelines contains a list of definitions of commonly used terms related to shutdown activities. These definitions are intended to apply only within the framework of this document to facilitate a better understanding of its content. In addition, these definitions were chosen to provide a distinction between shutdown terms and those generally found in technical specifications. Many of the terms defined in this section are capitalized throughout the document to reinforce the intended meaning.

Section 3.Ø discusses outage planning and control and its importance as the principal means of enhancing safety during shutdown. Key elements that contribute to effective outage planning and control are described and guidelines are provided to support an assessment of current practices. These elements and guidance are directly associated with the process of managing outage activities.

Section 4.Ø discusses the principal shutdown safety issues. These issues are categorized under the following key safety functions: decay heat removal capability, inventory control, power availability, reactivity control and containment. The issues described in each subsection are considered the major sources of risk during shutdown based on operating experience, results of related studies to date, and a survey of current utility practices. The importance to shutdown safety of each issue is discussed. Specific guidelines are provided that represent appropriate measures to address these issues.

The process discussed in Section 5.Ø provides a general approach for assessment of current practices for planning and conducting outages from a safety perspective using the information contained in this document. This section also discusses monitoring the effectiveness and evaluating the performance of outages.

Section 6.Ø lists references that provide additional information on the issues discussed in the document and outage experience related to shutdown safety.

2.Ø DEFINITIONS

AVAILABLE (AVAILABILITY): The status of a system, structure or component that is in service or can be placed in service in a FUNCTIONAL or OPERABLE state by immediate manual or automatic actuation.

CONTAINMENT CLOSURE: The action to secure primary (PWR) or secondary (BWR) containment and its associated structures, systems, and components as a FUNCTIONAL barrier to fission product release under existing plant conditions.

CONTINGENCY PLAN: An approved plan of compensatory actions:

- o To maintain DEFENSE IN DEPTH by alternate means when pre-outage planning reveals that specified systems, structures or components will be unavailable;

- o To restore DEFENSE IN DEPTH when system AVAILABILITY drops below the planned DEFENSE IN DEPTH during the outage;

- o To minimize the likelihood of a loss of KEY SAFETY FUNCTIONS during HIGHER RISK EVOLUTIONS.

DECAY HEAT REMOVAL CAPABILITY: The ability to maintain reactor coolant system (RCS) temperature and pressure, and spent fuel pool (SFP) temperature below specified limits following a shutdown.

DEFENSE IN DEPTH: For the purpose of managing risk during shutdown, defense in depth is the concept of:

- o Providing systems, structures and components to ensure backup of KEY SAFETY FUNCTIONS using redundant, alternate or diverse methods:

- o Planning and scheduling outage activities in a manner that optimizes safety system AVAILABILITY;.

- o Providing'administrative controls that support and/or supplement the above elements.

DEFUELED: All fuel assemblies have been removed from the reactor vessel and placed in the spent fuel pool or other storage facility.

FUNCTIONAL (FUNCTIONALITY): The ability of a system or component to perform its intended service with considerations that applicable technical specification requirements or licensing/design basis assumptions may not be maintained.

HIGHER RISK EVOLUTIONS: Outage activities, plant configurations or conditions during shutdown where the plant is more susceptible to an event causing the loss of a key safety function.

INVENTORY CONTROL: Measures established to ensure that irradiated fuel remains covered with coolant to maintain heat transfer and shielding requirements.

KEY SAFETY FUNCTIONS: During shutdown, they are decay heat removal, inventory control, power availability, reactivity control, and containment.

MID-LOOP: PWR condition with fuel in the reactor vessel and level is below the top of the hot legs at their junction to the reactor vessel.

OPERABLE: The ability of a system to perform its specified function with all applicable technical specifications requirements satisfied.

REACTIVITY CONTROL: Measures established to preclude inadvertent dilutions, criticalities, power excursions or losses of shutdown margin, and to predict and monitor core behavior.

REDUCED INVENTORY: PWR condition with fuel in the reactor vessel and level is lower than three feet below the reactor vessel flange.

RISK MANAGEMENT: Integrated process of assessing and reducing the likelihood and/or consequences of an adverse event.

SHUTDOWN: Plant status when the reactor core is subcritical and a startup is not in progress.

STARTUP: Plant status commencing with activities to heatup the RCS above 200 degrees F and to bring the reactor core to a critical condition and up to 5% of rated thermal power.

3.Ø OUTAGE PLANNING AND CONTROL

Effective outage planning and control is the primary means of enhancing safety during shutdown. Managing risk and maintaining safety functions during a multitude of outage activities requires a clear understanding of the utility safety philosophy, appropriate involvement of organizational levels, planning, coordination, communication, and the awareness of plant status by the personnel involved in those activities. The focus of outage safety in the past has often been on systems or components that were out of service for maintenance or repair during the outage. Outage safety can be improved by focusing on the AVAILABILITY of systems that provide and support KEY SAFETY FUNCTIONS as well ***as*** on measures that can reduce both the likelihood and consequences of adverse events.

The following sections present key elements of outage planning and control that are important to shutdown safety. Guidelines are also provided for assessment of current practices.

3.1 Integrated Management

The complexity, diversity, and number of activities that take place during an outage require a high degree of coordination in order to maintain DEFENSE IN DEPTH. integrated planning and decision making can preclude situations in which KEY SAFETY FUNCTIONS may be compromised due to a lack of thorough knowledge and understanding of plant conditions and work evolutions. Frequent interaction with the involved disciplines can ensure a comprehensive planning effort and can also reduce late changes to the outage schedule that may impact plant safety. Timely and effective communication can also ensure that outage personnel are aware and informed of plant conditions, HIGHER RISK EVOLUTIONS, safety system AVAILABILITY, and other factors that contribute to a safe and effective outage.

Guidelines

1) A senior management policy stating the utility outage nuclear safety philosophy should be established and communicated to personnel involved in the planning and execution of the outage. This policy should incorporate the DEFENSE IN DEPTH concept discussed in this document.

2) Outage schedules should be developed through interaction with involved organizations and disciplines to assure that the planning provides DEFENSE IN DEPTH throughout the outage. Outage activities should be controlled and implemented in accordance with the approved schedule.

3) The philosophy and basis used to develop the initial schedule should also be applied to any safety significant schedule changes that might occur before or during the outage. For any schedule changes, criteria should be established that define the level of review and approval authority necessary to implement the change.

4) The current plant status, including the AVAILABILITY of key safety systems or equipment, should be communicated on a regular basis to personnel who may affect plant safety. HIGHER RISK EVOLUTIONS should also be conveyed including any appropriate precautions or compensatory actions necessary during these periods.

5) A post-outage critique should be conducted that assesses outage performance from a safety perspective. The results of the critique should be used as a basis for improvements to planning and control of future outages.

3.2 Level of Activities

A well-designed outage schedule carefully balances the activities assigned to each group or organization throughout the outage. Overextending the resources or capabilities of a given group, particularly during HIGHER RISK EVOLUTIONS, can lead to stressful situations that may result in challenges to plant safety. Additionally, shutdown risks may not be apparent if the nature, grouping, or level of activities in the outage schedule are not accurately or clearly reflected. For example, several activities in the same general area that require temporary power supplies or welding machines may inadventently create a potential fire hazard.

Guidelines

1) The outage work scope and schedule should realistically match resources to activities. Additional resources should be available to meet anticipated changes, such as increases to the outage scope.

2) Activities in the outage schedule should be sufficiently detailed and organized to accurately convey the impact on complex evolutions, plant conditions, and equipment AVAILABILITY.

3) Activities that may impact KEY SAFETY FUNCTIONS should be limited and strictly controlled during HIGHER RISK EVOLUTIONS or infrequently performed evolutions.

4) Outage planning and execution should consider the potential introduction of hazards (e.g., fire, flooding, etc.) posed by the level and/or scope of activities in a given area of the plant and establish compensatory measures as appropriate.

5) An outage overtime policy should be established. Overtime hours for outage personnel should be pre-approved by the appropriate level of supervision or management.

3.3 Providing Defense in Depth

A fundamental element of outage planning and control is to ensure that the systems and components that perform KEY SAFETY FUNCTIONS during shutdown are AVAILABLE when needed. The objectives are to provide backup for KEY SAFETY FUNCTIONS, particularly during HIGHER RISK EVOLUTIONS, to optimize safety system AVAILABILITY, to provide administrative controls that support the FUNCTIONALITY of key equipment, and to provide procedures designed to mitigate the loss of KEY SAFETY FUNCTIONS.

Guidelines

1) The outage schedule should establish the systems, structures and components that will provide backup for KEY SAFETY FUNCTIONS that is commensurate with plant conditions.

2) Outage planning should optimize safety system AVAILABILITY. Systems should be returned to service as soon as practicable following completion of scheduled work.

3) The FUNCTIONALITY of systems and components should be assured by post maintenance testing, monitoring of key parameters with the system in service, or through verification of system alignment and administrative control by operations personnel.

4) Systems, structures and components identified to provide DEFENSE IN DEPTH during periods of the outage should be controlled such that they remain AVAILABLE during these periods.

5) Procedures should be developed that are designed to mitigate the loss of KEY SAFETY FUNCTIONS.

3.4 Contingency Planning

The AVAILABILITY of equipment and personnel to respond to degraded conditions during an outage is an important element of shutdown safety. CONTINGENCY PLANS can be used to reestablish DEFENSE IN DEPTH if planned systems or equipment become unavailable or to protect AVAILABLE equipment. In general, as the level of planned DEFENSE IN DEPTH decreases, the use of CONTINGENCY PLANS should increase. CONTINGENCY PLANS may take the form of mandatory prerequisite activities, procedures, pre-outage schedules or changes to the schedule during the outage, or other approved direction.

Guidelines

1) CONTINGENCY PLANS should be available when entering a HIGHER RISK EVOLUTION;

2) CONTINGENCY PLANS should be developed when system AVAILABILITY drops below the planned DEFENSE IN DEPTH.

3) CONTINGENCY PLANS should consider the use of alternate equipment to respond to the loss of dedicated safety and monitoring equipment, and should also consider additional monitoring or controls to minimize the potential for unplanned equipment unavailability.

4) Personnel who may be required to implement a CONTINGENCY PLAN should be identified and familiar with the plan.

3.5 Training

Outage activities during shutdown conditions present a number of unique situations and evolutions for both the permanent plant staff and for temporary personnel, such as additional craft and technicians. For example, operators will be relied upon to conduct many infrequently performed activities and will also be responsible for maintaining the plant in a safe condition under various plant configurations. A systematic approach to training on the risks during shutdown conditions can enhance operator awareness and provide knowledge of the appropriate response to potential challenges. For temporary personnel, indoctrination to work control requirements, procedures, and the outage nuclear safety policy can greatly enhance the proper conduct of the outage and can help to minimize unnecessary challenges to plant safety.

Guidelines

1) Operator training should provide knowledge of the applicable shutdown safety issues described in Section 4.Ø. To the extent practicable, simulator training for shutdown conditions should also be included.

2) Plant personnel, including contractors and others temporarily assigned to support the outage, should be trained in areas that are applicable to their particular role in outage activities and that contribute to the safe conduct of the outage.

3.6 Outage Safety Review

Following development of the outage schedule and before final approval, a review of the schedule from a nuclear safety perspective provides added assurance that the outage can be conducted in a safe manner. This review would focus on maintaining adequate DEFENSE IN DEPTH, commensurate with plant conditions during the outage. It would also include a review of CONTINGENCY PLANS developed to support the outage.

Guidelines

1) Prior to the outage, the schedule should be critically reviewed by personnel knowledgeable in management expectations for outage nuclear safety and plant operations. The review should not be conducted solely by those directly involved in the development and preparation of the outage schedule.

2) The outage safety review should assure the adequacy of the DEFENSE IN DEPTH provided for the duration of the outage and consistency with management's shutdown safety policy. This review should also include a detailed examination of the outage schedule, including system interactions, support system AVAILABILITY, and the impact of temporarily installed equipment.

3) The outage safety review should ensure that HIGHER RISK EVOLUTIONS are clearly identified in the schedule, and that CONTINGENCY PLANS and mitigating procedures have been developed and are adequate.

4) Consistent with the criteria established per Section 3.1, Guideline 3, that defines the level of review and approval authority fur emergent schedules changes, safety significant changes should be reviewed by the same process used to review the original schedule.

4.Ø SHUTDOWN SAFETY ISSUES

The issues that are described in this section have been identified through review of industry experience, analytical insights of conditions during plant shutdown, and through discussions with experienced individuals from utilities, nuclear industry organizations, and the NRC staff. The issues are categorized into five main sections that represent the KEY SAFETY FUNCTIONS (decay heat removal capability, inventory control, power availability, reactivity control, and containment - primary/secondary) during shutdown. A description of each issue is provided that discusses its relationship to safety. The associated guidelines provide measures that adequately address each issue.

Some of the issues that are described may parenthetically denote either PWR or BWR as the reactor type associated with that issue. It is suggested, however, that all issues be reviewed initially to gain any potential insights to related plant systems and equipment. The assessment process described in Section 5.Ø includes a screening of issues for applicability to a given plant.

4.1 Decay Heat Removal Capability

Maintaining decay heat removal (DHR) capability is a KEY SAFETY FUNCTION during shutdown conditions, whether fuel remains in the reactor vessel or is off-loaded to the spent fuel pool. During normal refueling outage conditions, the DHR system and its supporting systems are the primary means of removing decay heat when fuel is in the reactor vessel. Upon loss of the normal DHR function, other systems and components can be used to remove decay heat depending on a variety of factors, including the plant configuration, AVAILABILITY of other key systems and components, and the ability of operators to diagnose and respond properly to the event. Providing a DEFENSE IN DEPTH for decay heat removal capability, commensurate with the plant conditions identified in the outage schedule, can effectively enhance shutdown safety.

4.1.1 Loss of Decay Heat Removal

An extended loss of the DHR function can lead to coolant boiling and potentially result in a depletion of reactor coolant and eventual uncovering of the core. While irradiated fuel remains in the reactor vessel during an outage, maintaining the DHR function remains a key to shutdown safety. The risk associated with a loss of DHR event is dependent on a number of factors, including the decay heat Toad present and the existing plant configuration. Section 4.2.1 discusses the reduced inventory condition, which encompasses a significant portion of overall shutdown risk for PWRs. A comprehensive understanding of the factors that contribute to the risk associated with a loss of DHR 'is an essential element in effectively planning and controlling an outage and in effectively mitigating a loss of DHR event.

Guidelines

1) A procedure should be established to address loss of the normal DHR capability during shutdown conditions. The procedure should prioritize the alternate cooling methods available (e.g., gravity feed and bleed, low pressure pump feed and bleed, high pressure pump feed and bleed, reflux cooling, etc.) and that would be employed for a given set of conditions that are planned for the outage. The procedure should have a sound technical basis that includes the following:

   0 initial magnitude of decay heat

   0 time to boiling

   0 time to core uncovery

   0 initial RCS water inventory condition (e.g., filled, reduced, mid-loop, refueling canal filled, reactor cavity flooded, etc.)

- RCS configurations (e.g., open/closed, nozzle dams installed or loop isolation valves closed, steam generator manways on/off, vent paths available, temporary covers or thimble tube plugs installed, main steam line plugs installed, etc.)

- natural circulation capability with heat transfer to steam generator shell side

2) The technical basis used to develop the above procedure should also be used ***as*** an input to determining and planning an adequate DEFENSE IN DEPTH of the DHR function for the outage that is commensurate with plant conditions.

3) Containment hatches (equipment and personnel) and other penetrations that communicate with the containment atmosphere (primary or secondary, as appropriate) should either be closed or capable of being closed prior to core boiling following a loss of DHR and should be addressed in procedures.

4.1.2 Planning and Control of Outage Activities Impacting the DHR System

Many of the events involving loss of DHR were initiated by outage activities, such as preventive maintenance and surveillance testing, on components within ***or*** that directly interface with the DHR system. The planning and conduct of these activities is an important factor in reducing the likelihood of a loss of DHR event and the consequences of such an event. For example, performance of a surveillance test on a pressure or flow switch during REDUCED INVENTORY conditions inadvertently closed a DHR isolation valve that resulted in loss of core cooling. Effective planning and control can eliminate or reduce both the likelihood and consequences of such an event.

Guidelines

1) DHR system logic/interlocks should be evaluated for applicability to shutdown conditions. Consideration should be given to disabling logic or interlocks that are evaluated as detrimental for a given condition.

2) Outage activities on components within or that directly interface with the DHR system should be evaluated for risk/impact before being performed during REDUCED INVENTORY conditions or other HIGHER RISK EVOLUTIONS.

3) Activities which may impact the core cooling system/components should be scheduled during periods of low decay heat or maximum coolant inventory or during defueled conditions. if such activities must be scheduled during periods of high decay heat or REDUCED INVENTORY, then CONTINGENCY PLANS should be established.

4.1.3 Loss of Spent Fuel Pool Cooling

Many utilities have chosen to off-load the core to the spent fuel pool (SFP) during their refueling outages. This practice shifts decay heat removal requirements from the RCS to the SFP. An event that results in the loss of SFP cooling may have the same undersirable effects as a loss of DHR event if appropriate compensatory actions are not taken.

Guidelines

1) The outage schedule should provide a DEFENSE IN DEPTH commensurate with the risk associated with loss of SFP cooling.

2) A procedure should be established for response to a loss of SFP cooling event.

4.2 Inventory Control

Control of reactor coolant system inventory is essential to maintaining the overall decay heat removal function. During REDUCED INVENTORY operations, boiling and potential core uncovery can occur in a relatively short time period. The reactor coolant system boundary expands during shutdown periods to include the decay heat removal piping, spent fuel pool, refueling canal and other connected support systems. This presents a significant number of potential inventory loss flow paths that are normally isolated during power operation.

4.2.1 Reduced Inventory Operations (PWR)

REDUCED INVENTORY operation occurs when the water level in the reactor vessel is lower than 3 feet below the reactor vessel flange. A special case of REDUCED INVENTORY operation is MID-LOOP operation, which occurs when the RCS water level is below the top of the hot legs at their junction with the reactor vessel. Similar conditions can exist when the reactor vessel is isolated from steam generators by closed loop isolation valves or nozzle dams with the reactor vessel head installed or prior to filling the reactor cavity. REDUCED INVENTORY, MID-LOOP, and operation with closed loop isolation valves or nozzle dams installed as described above are vulnerable conditions because the heat removal capacity of the RCS volume is reduced. Upon loss of DHR under these conditions, coolant boiling and core uncovery can occur if decay heat removal is not restored or provided by some alternate means. In addition, during MID-LOOP operation, DHR can be lost by poor RCS level control or by an increase in DHR flow (either of which can ingest air into the DHR pump). Therefore, RCS level control and DHR flow control are critical during MID-LOOP operations.

Guidelines

1) Prior to entering a REDUCED INVENTORY condition, equipment requirements that provide or support KEY SAFETY FUNCTIONS should be verified.

74.07 The outage schedule should delay, to the extent practical, going to REDUCED INVENTORY conditions when decay heat load is high.

3) The outage schedule should minimize the overall time that the plant is in a REDUCED INVENTORY condition.

4) Outage activities potentially impacting RCS level control or DHR flow control should be suspended during MID-LOOP operation.

5) Training, including shift briefings, should be conducted prior to entering a REDUCED INVENTORY condition.

6) Particular attention should be paid to the guidelines in Section 4.1.1 during REDUCED INVENTORY conditions.

4.2.2 Inadvertent Transfer of Coolant from RCS

During shutdown periods, the RCS boundary is expanded because low-pressure systems, such as the decay heat removal system, are connected to the RCS. The plant configurations and activities during outages increase the possibility of a valve misalignment that can result in a loss of RCS inventory. Events have included inadvertent transfers to the refueling water storage tank, the containment sump and the containment spray system.

Guidelines

1) A procedure should be established to address loss of RCS inventory during shutdown conditions. The procedure should consider the following:

- identifying the potential source and magnitude of the loss
- providing sufficient makeup capability
- coping with high radiation levels in containment

2) Plant configurations where a single active failure or personnel error can result in a rapid loss of RCS inventory should be identified and minimized.

3) For activities that may impact RCS coolant inventory, procedures or work instructions should clearly stipulate the initial plant conditions and should also include appropriate warnings and precautions.

4) Restoration guidance for returning systems to service should emphasize the proper sequencing of steps and proper positioning of critical valves.

5) Evolutions that deliberately alter the RCS coolant inventory flow paths should be strictly controlled and monitored.

6) Freeze seals employed in locations that can impact RCS inventory should be carefully and continuously monitored. Appropriate CONTINGENCY PLANS should be established and ready for implementation in the event of freeze seal failure.

7) Removal of control rods and control rod drives should not be performed simultaneously without first establishing controls to preclude inadvertent loss of vessel inventory (BWR).

4.2.3 Inventory Loss to Suppression Pool (BWR)

There are potential inventory loss paths through the DHR system to the suppression pool when DHR is aligned for shutdown cooling. Some can be initiated by a single mispositioned valve. Many BWRs have automatic protective features that can mitigate the inventory loss and provide defense against this type of event.

Guidelines

1) The automatic isolation function of the DHR system (on low RPV level) should be maintained functional during shutdown cooling periods.

2) Special administrative controls should be used for valves which can cause rapid inventory loss.

4.2.4 Inventory Loss Through Main Steam Lines (BWR)

Outage activities associated with the main steam lines (e.g., safety/relief valve removal, automatic depressurization system testing, main steam isolation valve maintenance, etc.) can create a drain down path for the reactor cavity and fuel pool.

Guidelines

1) Maintenance and testing of relief valve actuation logic or support systems should not be scheduled during fuel movement unless main steam line plugs are installed. If these activities must be performed, procedures should require that valve actuation be disabled. Operators should monitor vessel water level during the activity and be prepared to take mitigative actions.

2) Use of main steam line plugs should be considered during the outage in order to prevent reactor cavity or fuel pool drain down through safety relief valves or main steam isolation valves.

3) When the main steam line plugs are the sole barrier preventing draindown, a makeup source of sufficient injection capacity should be AVAILABLE to compensate for a main steam line plug failure.

4.2.5 Reactor Cavity Seal Failure

Some loss of fuel pool water events can result in draining the entire contents of the reactor cavity.- In most plants, if the spent fuel pool were to be drained to the bottom of the fuel transfer canal or tube, the'water level in the spent fuel pool would typically be below the suction piping for spent fuel cooling. Fuel being moved would be uncovered if the cavity drained. Fuel with less than adequate water cover for shielding, including fuel being moved or suspended from manipulators, would result in high radiation levels in containment.

Guidelines

1) Preventive maintenance/inspection or post-installation testing should be performed on reactor cavity seals prior to filling the reactor cavity to preclude potential seal failure. Leakage monitoring should be performed thereafter to ensure seal integrity. The FUNCTIONALITY of associated reactor cavity and cavity seal failure instrumentation and alarms should also be verified.

2) A procedure should be developed that addresses recovery from reactor cavity seal failure and loss of cavity inventory. The procedure should include consideration of the following:

   - o coping with high radiation levels
   - o equipment loss by flooding
   - o alternate spent fuel pool cooling methods
   - o temporary cooling for fuel in transit

4.3 Power Availability

Power availability is a fundamental element of shutdown safety. Numerous events have occurred during shutdown as a result of the loss of AC power. This type of event not only presents a challenge to maintaining key safety functions, it also complicates recovery under abnormal conditions. Providing

DEFENSE IN DEPTH through effective outage planning is the best means of reducing the likelihood of this event. In addition, awareness and control of outage activities on electrical equipment can minimize challenges to plant safety.

4.3.1 Sources of AC Power

AC power is required during shutdown conditions to maintain cooling to the reactor core and spent fuel pool, to transfer decay heat to the heat sink, to achieve containment closure when needed, and to support other important functions. Planning and control of outage activities on AC power sources can significantly reduce risk by providing a DEFENSE IN DEPTH that is commensurate with the plant condition. In the event that off-site and emergency AC power is unavailable, temporary hookups and the AVAILABILITY of alternate AC power can reduce risk to loss of power events.

Guidelines

1) The outage plan should provide DEFENSE IN DEPTH for AC power sources that is commensurate with plant conditions. Maintenance and testing activities on these sources should be scheduled accordingly and the equipment should be returned to service in a timely manner.

2) Modifications and other work activities should be reviewed to ensure that they do not affect existing operable power supplies (e.g., inadvertent relay actuation causing a loss of power).

3) Plant personnel should be aware of the status of electrical systems and unusual interdependencies created due to outage configurations.

4) When AC power source AVAILABILITY drops below the planned DEFENSE IN DEPTH, CONTINGENCY PLANS for the use of temporary or alternate AC power should be implemented.

5) Applicable breaker locations should be clearly identified to allow switching operations of key components.

6) Equipment and tools for temporary AC power should be staged to allow for quick hookup. Walk-through exercises should be performed to identify key breaker locations and to verify that CONTINGENCY PLANS can be executed efficiently.

7) A procedure should be established to address loss of the power availability KEY SAFETY FUNCTION during shutdown conditions.

4.3.2 Switchyard/Transformer Yard and Electrical Equipment Activities

It is necessary to maintain control over switchyard and transformer yard activities as this directly affects offsite power AVAILABILITY. Proper planning and awareness of these activities is a fundamental element of reducing the likelihood and consequences of adverse events during shutdown.

Guidelines

1) A policy for administrative control of switchyard/transformer yard activities should be established.

2) Special precautions should be taken while performing activities near incoming and outgoing transmission lines and in the switchyard/transformer yard to protect power AVAILABILITY. Such precautions may include erecting caution signs or physical barriers near the activities and pre-job briefings.

3) The switchyard/transformer yard and high voltage feeds into the station should be evaluated for single failure susceptibility. Periodic inspections of work areas and activities should be made by utility safety and management personnel in order to detect developing hazards or improper work practices.

4) Maintenance activities on power lines and transformers which -provide sole off-site power to the plant should be avoided during HIGHER RISK EVOLUTIONS and when redundant power trains are out of service.

5) The switchyard/transformer yard should not be used as a storage or laydown yard. If there are no other viable alternatives, staging areas should be located away from energized equipment.

4.3.3 AC/DC Instrumentation and Control Power

AC and DC power is required to support systems that provide KEY SAFETY FUNCTIONS during shutdown. As such, the AVAILABILITY of AC and DC power for monitoring and controlling the equipment that provide these functions is an important element of the planned DEFENSE IN DEPTH for the outage.

Guidelines

1) In assessing the functionality of systems that provide DEFENSE IN DEPTH during an outage, appropriate consideration should be given to associated AC/DC power sources.

2) Removal of AC/DC power sources from service, or testing of these sources, should not be performed when these sources are supporting systems that are actively providing KEY SAFETY FUNCTIONS.

4.4 Reactivity Control

An important element of shutdown safety is maintaining reactivity control. The main aspects of this KEY SAFETY FUNCTION include maintaining adequate shutdown margin in the RCS and spent fuel pool and proper planning and control of all fuel handling activities.

4.4.1 Boron Dilution (PWRs)

Boron dilution events during shutdown conditions have resulted in reductions to reactivity shutdown margin. These events are of concern because of their potential for unexpected reactor criticalities. In such cases, criticality can occur even with the rods fully inserted into the core. Gradual decreases in boron concentration are difficult to detect because detection relies on RCS sampling, on-line analyzers, and the source range detector counts.

While highly unlikely, there is a potential for a rapid reduction in boron concentration if a reactor coolant pump (RCP) were started and a pocket of unborated or diluted water is present, particularly in the RCP suction. The unborated water would be pumped into the core, causing a rapid positive reactivity increase that may result in an inadvertent criticality.

Cuidelines

1) Boron dilution paths should be identified for each planned shutdown configuration. Flow paths that may cause a boron dilution should receive appropriate administrative controls.

74 Simultaneous filling of the RCS and the refueling water storage tank should be carefully controlled to reduce the potential for underborated water injection into the core.

3) Shutdown margin calculations should be verified and any differences should be immediately resolved. As a minimum, an evaluation of the shutdown margin should be performed whenever changes are planned that could affect shutdown margin.

4) Plant operators should be aware and have procedural controls that identify circumstances where starting the RCPs might inject unborated water into the core. Under these circumstances, measures should be taken to ensure uniform RCS boron concentration.

5) The addition of unborated water to the refueling cavity or the primary side of the steam generators should be strictly administratively controlled.

6) Source range detectors should be frequently monitored during shutdown conditions, particularly during activities that could result in boron dilution.

7) Redundant boration paths should be available to respond to a boron dilution event'.

4.4.2 Unplanned Criticality/Low Temperature

During periods of cold weather, the RCS water temperature can decrease below the minimum value used to analyze reactor shutdown margin and fuel pool shutdown margin. Cold water adds positive reactivity, decreasing the shutdown margin. This effect applies to both the core and the spent fuel pool.

Guidelines

1) Analyses for adequate shutdown margin in the RCS and the spent fuel pool should include consideration of the minimum temperature expected at the plant. Procedural controls should maintain reactor coolant and spent fuel pool temperatures above the minimum analyzed temperatures.

2) Fuel movement should be prohibited during times when temperatures are below the analyzed temperatures. Safety analyses used for fuel movement should specifically address low coolant temperatures.

4.4.3 Fuel Load/Unload Problems; Inadvertent Control Rod Withdrawal/Misplaced Fuel

During refueling, improper sequencing of control rods or fuel assemblies is possible because of numerous movements. For BWRs, soluble boron is not used to control reactivity during refueling, and therefore, reactivity margins are smaller than PWRs. Shutdown margins can be significantly reduced during refueling when control blades or fuel assemblies are not loaded in the proper sequence. Due to the limited number of source range monitors, the core reloading pattern is important. An improper loading sequence can allow regions of the core to approach criticality without early detection by the source range monitor.

Guidelines

1) Fuel movement in the reactor vessel should not occur simultaneously with control rod drive mechanism maintenance unless an engineering analysis has been performed to demonstrate adequate shutdown margin exists and that controls exist to prevent entering an unanalyzed condition. (BWR)

2) Fuel cells should be loaded only after positive verification of control rod insertions.

3) Procedures that implement refueling sequences should have a sound technical basis that addresses shutdown margin and source range monitor detector response. Computer codes used to generate and/or perform the shutdown margin calculation should be verified and validated.

4) Shutdown margin analyses should include intermediate fuel assembly positions during the refueling sequence. Any refueling errors should be evaluated for shutdown margin'before corrective actions are taken.

5) Changes to the refueling sequence should be controlled using the same technical bases used to develop the original refueling sequence.

6) Fuel moves should be verified by knowledgeable personnel.

4.5 Containment - Primary/Secondary

During shutdown plant conditions, it is necessary to ensure that CONTAINMENT CLOSURE can be achieved in sufficient time to prevent potential fission product release; This time is dependent on a number of factors, including the decay heat level and the amount of RCS inventory available.

Guidelines

1) A procedure for CONTAINMENT CLOSURE should be established to assure that closure can be accomplished in a time commensurate with plant conditions. This procedure should be consistent with the procedure to respond to loss of DHR and should also consider the unavailability of AC power and expected environmental conditions in containment.

2) Personnel responsible for CONTAINMENT CLOSURE should be trained and knowledgeable in using the procedure for executing closure.

3) Methods should be established to alert personnel to evacuate containment in the event of adverse environmental conditions.

5.Ø ASSESSMENT PROCESS

This section provides a general approach for a utility's self-assessment of current practices for planning and conducting outage activities. The approach is built around a review of the issues, elements and guidelines described in Sections 3.Ø and 4.Ø. The assessment should determine those issues applicable to a given plant and should evaluate current practices using the guidelines that address those issues. The results of the assessment should be used as a basis for developing improvements to the outage planning and control program. The underlying premise is that a utility that plans and conducts its outages consistent with the intent of the guidelines should enhance safety during shutdown.

Figure 5-1 is a flow chart of the assessment process. The following discussion elaborates on the individual elements of the process.

The process begins with the set of shutdown safety issues discussed in Section 4.Ø. Some of the issues may not be applicable to all reactor types. Each issue should be thoroughly screened to determine those issues applicable to a given design. For those that are found not applicable, the basis for that determination should be documented. This documentation should serve to minimize future resource expenditures in reviewing similar events or issues. Those issues that are determined applicable will continue through the assessment process.

The outage planning and control elements and guidelines discussed in Section 3.Ø should apply to all plants and therefore are not screened in this process.

The next step is to evaluate current practices related to the outage planning and control elements and applicable shutdown safety issues against the associated guidelines. Current practices may include a variety of measures, such as reliance on administrative controls, existing technical specification requirements, design features, procedures, or personnel knowledge and skills, and may or may not be addressed in the existing outage planning program. The objective is to determine whether present measures are consistent with the intent of the guidelines and whether these measures are effective. If so, the basis for this determination should be documented. The bases developed can aid in the review of future outage plans. If current practices are not consistent with the intent of the guidelines, additional actions or measures should be developed and implemented.

The measures developed and implemented to address the remaining issues should be consistent with the intent of the associated guidelines. Additional measures should not be limited to any particular type of action. A utility might establish a new administrative control, submit a change to technical specifications, implement a design modification, develop a procedure, or provide additional training to personnel. In addition, important items that were not covered by the existing outage planning program should be incorporated and institutionalized such that the process for planning and conducting future outages will address these items.

The final element, effectiveness monitoring, applies both to issues where current practices are consistent with the intent of the guidelines and to issues where additional measures are warranted. As outage performance is reviewed, the results of the monitoring element should be fed back into the process and evaluated.

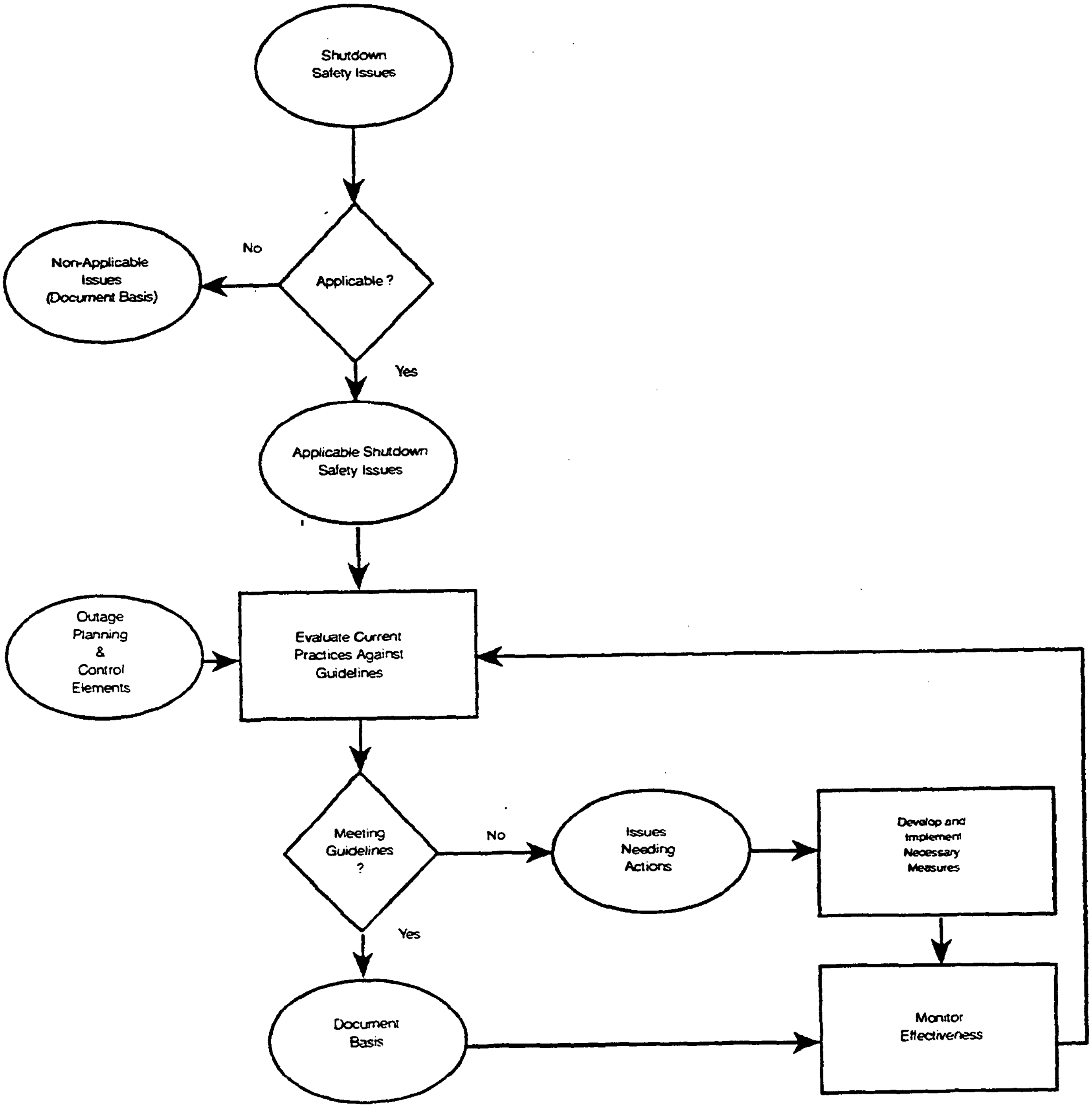
The ability to monitor and assess outage performance from a safety perspective is an important element of effective outage management. Methods and mechanisms should be employed that offer reasonably objective indications of how well outage planning and control practices are managing risk and maintaining safety during shutdown. Feedback from these monitoring activities should provide management with a valuable tool for evaluating outage safety and for the development of further improvements.

One method for evaluating outage safety should be a review of shutdown events, both at one's own plant and from other related industry experience. The outage program should be reviewed to determine'how outage planning and control could prevent a particular event or mitigate its consequences. If deficiencies in current practices are discovered through this review, corrective actions or improvements should be implemented.

Mechanisms should be employed to evaluate risk management and safety performance during shutdown. One approach would be to determine how well the outage planning and schedule were adhered to during the actual implementation of the outage. For example, was the planned DEFENSE IN DEPTH actually AVAILABLE during the required periods? Was the time spent in higher risk configurations mimimized in accordance with the outage schedule? Were CONTINGENCY PLANS effective in reestablishing DEFENSE IN DEPTH or in protecting AVAILABLE equipment? Another means of assessing performance from a safety perspective is to establish goals for key outage items or parameters. For example, goals can be established in areas such as collective radiation exposure, number of ESF actuations, personnel errors, etc. The intent is to obtain objective feedback that provides an indication of safety performance. While no single indicator could likely provide a comprehensive indication of outage safety, there are many mechanisms that collectively can provide such feedback.

Effectiveness monitoring should be a continuing element of the assessment process. Along with the insights gained from previous outages, new industry experience should be factored in and evaluated for applicability to the plant's program for planning and conducting outages.

Figure 5-1
Assessment Process



6.Ø REFERENCES

NRC

1) USNRC IE INFORMATION NOTICE NO. 8Ø-34, Boron Dilution of Reactor Coolant During Steam Generator Decontamination, September 26, 198Ø.

2) USNRC IE INFORMATION NOTICE NO. 81-1Ø, Inadvertent Containment Sprav Due To Personnel Error, March 25, 1981.

3) USNRC IE INFORMATION NOTICE NO. 83-35, Fuel Movement With Control Rods Withdrawn At BWRs, May 31, 1983.

4) USNRC IE BULLETIN NO. 84-Ø3, Refuelina Cavity Water Seal, August 24, 1984.

5) USNRC IE INFORMATION NOTICE NO. 84-42, Equipment Availabilitv For Conditions During Outages Not Covered By Technical Specifications, June 5, 1984.

6) USNRC IE INFORMATION NOTICE NO. 84-7Ø, Reliance on Water Level Instrumentation With a Common Leg, September 4, 1984.

7) USNRC IE INFORMATION NOTICE 84-81, Inadvertent Reduction in Primary Coolant Inventory in Boiling Water Reactors During Shutdown and Startup, November 16, 1984.

8) USNRC IE INFORMATION NOTICE NO. 84-93, Potential For Loss of Water From The Refueling Cavity, December 17, 1984.

9) USNRC IE INFORMATION NOTICE NO. 85-75, Improperly Installed Instrumentation Inadequate Qualitv Control and Inadequate Postmodification Testing, August 3Ø, 1985.

10) USNRC INFORMATION NOTICE NO. 86-74, Reduction of Reactor Coolant Inventory Because of Misalignment of RHR Valves, August 20, 1986.

11) USNRC INFORMATION NOTICE NO. 87-46, Undetected Loss of Reactor Coolant, September 30, 1987.

12) USNRC INFORMATION NOTICE NO. 87-57, Loss of Emergency Boration Capability Due to Nitrogen Gas Intrusion, November 6, 1987.

13) USNRC GENERIC LETTER NO. 88-17, Loss of Decay Heat Removal, October 17, 1988.

14) USNRC INFORMATION NOTICE NO. 88-36, Possible Sudden Loss of RCS Inventory During Low Coolant Level Operation, June 8, 1988.

15) USNRC INFORMATION NOTICE NO. 88-65, Inadvertent Drainages of Spent Fuel Pools, August 18, 1988.

16) USNRC BULLETIN NO. 89-03, Potential Loss of Required Shutdown Margin During Refueling Operations, November 21, 1989.

17) USNRC INFORMATION NOTICE NO. 90-06, Potential For Loss of Shutdown Cooling While at Low Reactor Coolant Levels, January 29, 1990.

18) USNRC INFORMATION NOTICE NO. 90-55, Recent Operating Experience On Loss of Reactor Coolant Inventory While In A Shutdown Condition, August 31, 1990.

19) USNRC INFORMATION NOTICE NO. 91-17, Fire Safety of Temporary Installations or Services, March 11, 1991.

20) USNRC INFORMATION NOTICE NO. 91-22, Four Plant Outage Events Involving Loss of AC Power or Coolant Spills, March 19, 1991.

21) USNRC INFORMATION NOTICE NO. 91-41, Potential Problems With the Use of Freeze Seals, June 27, 1991.

22) USNRC INFORMATION NOTICE NO. 91-42, Plant outage Events Involvina Poor Coordination Between Ooerations and Maintenance Personnel During Valve Testing and Manipulations, June 27, 1991.

23) USNRC NUREG-1269, loss of Residual Heat Removal Svstem, April 10, 1987.

24) USNRC NUREG-1410, Loss of Vital AC Power and the Residual Heat Removal Svstem During Mid-Loop Operations at Vogtle Unit 1 on March 20. 1990, May 1990.'

EPRI

1) NSAC-52, Residual Heat Removal Experience and Safetv Analvsis - PWRs, January, 1983.

2) NSAC-83, Brunswick Decay Heat Removal Probabilistic Safetv Study, October, 1985.

3) NSAC-84, Zion Residual Heat Removal Probabilistic Risk Assessment, July, 1985.

4) NSAC-88, Residual Heat Removal Experience Review and Safety Analysis, March, 1986.

5) NSAC-156, Residual Heat Removal Experience Review and Safetv Analysis - PWRs - 1982-1989, August 1991.

6) NSAC-157, Residual Heat Removal Experience Review and Safetv Analysis - BWRs - 1984-1989, June, 1991.

7) NSAC-166, Losses of Off-Site Power at U.S. Nuclear Power Plants Through 1990, April, 1991.

8) NSAC-I73 (Draft), Survev of BWR Plant Personnel on Shutdown Safety Practices and Risk Management Needs, October, 1991.

9) NSAC-1.74 (Draft), PWR Outage Risk Assessment and Management Survey Results, October, 1991.

INPO

Additional information on outage experience related to shutdown safety is available upon request to INPO.