Cornerstone Development

The U.S. Nuclear Regulatory Commission (NRC) staff developed two approaches for cornerstones: hazards analysis-based cornerstones and operations-based cornerstones. This enclosure describes how the hazard analysis-based cornerstones and operations-based cornerstones were derived from the NRC Strategic Plan. In addition, this enclosure includes the pros and cons of each cornerstone approach.

Hazards Analysis-Based Cornerstones

As a starting point for the development of the hazards analysis-based cornerstones, the NRC staff considered the process used to develop cornerstones for the Reactor Oversight Process (ROP), adapting the process to fuel cycle facilities. The staff used a top-down, hierarchical approach to develop the fuel cycle regulatory framework. The fuel cycle regulatory framework starts at the highest level with the NRC mission. The NRC mission is to license and regulate the Nation's civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety, promote the common defense and security, and protect the environment.

The staff used the agency's strategic goals of safety and security as the second level of the fuel cycle regulatory framework. The associated strategic outcomes formed the third level of the fuel cycle regulatory framework as the strategic performance areas of "Fuel Facility Safety," "Radiation Safety," and "Safeguards." The Commission established strategic outcomes to meet this mission in the NRC Strategic Plan (NUREG-1614, Volume 4, "Strategic Plan: Fiscal Years 2008–2013," issued February 2008).

Specifically, the "Fuel Facility Safety" strategic performance area was derived from the strategic outcomes of preventing the occurrence of any (1) inadvertent criticality events, (2) acute radiation exposures resulting in fatalities, and (3) releases of radioactive materials that result in significant radiation exposures. In addition to radioactive materials, the "Fuel Facility Safety" strategic performance area extends to hazardous chemicals used with, or produced from, licensed radioactive material consistent with Title 10 of the *Code of Federal Regulations* (10 CFR) Part 70, "Domestic Licensing of Special Nuclear Material," and proposed amendments to 10 CFR Part 40, "Domestic Licensing of Source Material." Similarly, the "Radiation Safety" strategic performance area was derived from the strategic outcomes of preventing the occurrence of any (1) acute radiation exposures resulting in fatalities, (2) releases of radioactive materials that result in significant radiation exposures, and (3) releases of radioactive materials that cause significant adverse environmental impacts. Finally, the "Safeguards" strategic performance area was derived from the strategic outcome of preventing any instances in which licensed radioactive materials are used domestically in a manner hostile to the United States.

With a risk-informed perspective, the NRC staff then identified the most important elements in each of these strategic performance areas that form the foundation for meeting the agency mission. These elements were identified as the cornerstones of safety and security in the fourth level of the fuel cycle regulatory framework. These cornerstones are the fundamental building blocks for the fuel cycle oversight process (FCOP).

The hazards analysis-based approach developed cornerstones that aligned with the way that licensees typically developed their integrated safety analysis (ISA). This organization of cornerstones also leads to an oversight program that is similar to the framework used in the ROP. The cornerstones under the hazards analysis-based approach are "Accident Sequence Initiators," "Safety Controls," "Emergency Preparedness," "Public Radiation Safety," "Occupational Radiation Safety," and "Security/Material Control and Accounting (MC&A)."

In developing each cornerstone, the NRC staff identified the objective, the desired results, the key attributes of licensee performance necessary to achieve the results, the scope of what the NRC needs to assess to ensure that the objectives are met, and the metrics used to evaluate performance in the cornerstone.

Safety cornerstones were developed recognizing the requirements under 10 CFR Part 20, "Standards for Protection Against Radiation," 10 CFR Part 40, 10 CFR Part 70, and 10 CFR Part 76, "Certification of Gaseous Diffusion Plants." Licensees are required by 10 CFR Parts 40, 70, and 76 to develop safety analyses to support their operations. For 10 CFR Part 70 licensees this includes an ISA. The one operating uranium conversion plant developed an ISA to support licensing under 10 CFR Part 40

The security-related cornerstone proposed for fuel cycle facilities would be conceptually similar to that used in the ROP. Similar to the ROP, certain findings pertaining to the security-related cornerstone would not be publicly available to ensure that potentially useful information is not provided to a possible adversary.

Figure 1 shows the fuel cycle regulatory framework using the hazards analysis-based cornerstones. The proposed hazards analysis-based cornerstones and their objectives are summarized below. Appendix A of this enclosure presents the results of the ongoing development of the "Accident Sequence Initiators" cornerstone as an example of the development of the hazards analysis-based cornerstones.

Accident Sequence Initiators—The objectives of this cornerstone are to verify that a licensee does the following:

- Limits the frequency of accident sequence initiators that lead to the need for items relied on for safety (IROFS), nuclear criticality safety (NCS) controls, or other safety controls (non-IROFS that are designed to prevent or limit the consequences of accident sequences). The ISA assumed a frequency for accident sequence initiators in establishing IROFS and NCS controls. These IROFS or NCS controls would be required by 10 CFR Part 70 as a result of the ISA or NCS analysis showing that they are needed to limit the likelihood of intermediate- or high-consequence accidents or prevent a nuclear criticality accident.

- Evaluates and limits, as appropriate, accident sequence initiators that are not required to be limited or controlled by IROFS, NCS controls, or other safety controls (non-IROFS). These are accident sequence initiators that the licensee has determined do not need to be prevented or have their likelihood limited based on the ISA. This could be because the ISA shows that they may be allowed to occur without causing the likelihoods or consequences defined in 10 CFR Part 70.

- Identifies in the ISA all accident sequence initiators associated with uses of materials licensed under 10 CFR Part 70 and appropriately assessed the accident sequences to

identify those that require IROFS or NCS controls to prevent or mitigate intermediate- or high-consequence events and to prevent nuclear criticalities.

Safety Controls—The objective of this cornerstone is to verify the availability, reliability, and capability of IROFS, NCS controls, or other safety controls. These IROFS, NCS controls, and other safety controls prevent, limit the frequency of, or mitigate accident sequences that could lead to intermediate- or high-consequence accidents or a nuclear criticality.

Emergency Preparedness (identical to the objective in the operations-based approach)—The objective of this cornerstone is to verify that the licensee is capable of implementing adequate measures to protect public health and safety in the event of a radiological or chemical emergency (for those chemicals under NRC jurisdiction[1]).

Public Radiation Safety—The objective of this cornerstone is to ensure adequate protection of public health and safety from exposure to radiation and radioactive effluents during normal (nonaccident) operations and from transportation of licensed materials.

Occupational Radiation Safety—The objective of this cornerstone is to ensure adequate protection of worker health and safety from exposure to radiation and radioactive materials during normal (nonaccident) operations.

Security/MC&A (identical to the objective in the operations-based approach)—The objectives of this cornerstone are to verify the following:

- The licensees' security and MC&A systems use defense-in-depth approaches, prevent or minimize the malevolent use or diversion of nuclear material, adequately detect and protect against loss or diversion of nuclear material, and facilitate the location and recovery of missing special nuclear material (SNM), and that the licensees' information protection program for classified, safeguards, and controlled unclassified information is adequate to prevent unauthorized disclosure of classified and sensitive unclassified information and protect the Nation's common defense and security

- The licensee adequately detects unauthorized production and/or unauthorized levels of enrichment of SNM at enrichment facilities.

Pros and Cons of the Hazards Analysis-Based Cornerstones

Pros: This approach would result in similar regulatory frameworks across NRC program areas.

The cornerstones are organized in the same way that licensees organize the hazard analysis and controls development in the ISAs.

Key attributes for ISA-related activities are integrated into cornerstones that reflect the way licensees' ISAs were developed and are maintained.

Cornerstones would be consistent across 10 CFR Part 40, 70, and 76 licensees (e.g.,

[1] Those chemicals under NRC jurisdiction are specified in 10 CFR 70.4 under the definition of "hazardous chemicals produced from licensed materials." A memorandum of understanding between the NRC and the Occupational Safety and Health Administration (Volume 53 of the *Federal Register*, page 43,950; October 31, 1988) delineates the general areas of responsibility of each agency in relation to occupational safety and health at NRC-licensed facilities.

the staff would not have to delete the "Criticality Safety" cornerstone for 10 CFR Part 40 licensees).

Cons: The use of the "Accident Sequence Initiators" cornerstone might have a negative impact on stakeholder communications. Some internal and external stakeholders might confuse the "Accident Sequence Initiators" cornerstone with the "Initiating Events" cornerstone in the ROP. However, these two cornerstones are not the same.

Operations-Based Cornerstones

The operations-based cornerstones were developed using same the top-down approach used for the development of the hazards analysis-based cornerstones. These cornerstones are more aligned with how licensees implement their safety programs during operations. In contrast with the hazards analysis-based cornerstones, the operations-based cornerstones do not have a "strategic performance areas" level, but rather the cornerstones are associated directly with the Strategic Outcomes from the Strategic Plan. "Criticality Safety" and "Chemical Safety" cornerstones are used rather than "Accident Sequence Initiators" and "Safety Controls." Also, the operations-based cornerstones combine the "Public Radiation Safety" and "Occupational Radiation Safety" cornerstones into one cornerstone, "Radiation Safety." The operations-based cornerstones distribute the ISA-related issues across the "Criticality Safety," "Chemical Safety," and "Radiation Safety" cornerstones.

Figure 2 shows the fuel cycle regulatory framework using the operations-based cornerstones. The "Emergency Preparedness" and "Security/MC&A" cornerstones under the operations-based cornerstones are identical to those under the hazards analysis-based cornerstones. The other proposed operations-based cornerstones and their objectives are summarized below. Appendix B of this enclosure presents the results of the ongoing development of the "Criticality Safety" cornerstone as an example of the development of the operations-based cornerstones.

Criticality Safety—The objective of this cornerstone is to verify that NCS controls and IROFS protect worker and public health and safety by preventing criticalities. This includes verifying adequate NCS analyses and verifying the availability, reliability, and capability of NCS controls and IROFS.

Chemical Safety—The objective of this cornerstone is to verify that chemical safety IROFS or controls protect worker and public health and safety by preventing and controlling chemical releases (for those chemicals under NRC jurisdiction) that could cause intermediate or high consequences (as defined in 10 CFR Part 70). This includes verifying adequate chemical process safety analyses and verifying the availability, reliability, and capability of chemical safety IROFS or controls.

Radiation Safety—The objective of this cornerstone is to ensure adequate protection of public and worker health and safety from exposure to radiation and radioactive materials during normal operations, as a result of accidents and emergencies, and from transportation of licensed material.

Pros and Cons of the Operations-Based Cornerstones

Pros: The cornerstones are organized along safety program lines similar to the safety areas in 10 CFR Part 70 and how licensees implement safety at their facilities.

The cornerstones are easy to communicate with external stakeholders because they use the structure of day-to-day operations.

Cons: Key attributes for ISA-related inspections are similar across cornerstones, thus separating what might be a common inspection into separate areas. A single failure would impact several cornerstones and thus could inappropriately move the licensee across an action matrix for a problem in one area of performance.

This cornerstone construct would result in two different oversight frameworks for oversight within the agency (FCOP and ROP).

Cornerstones would not be the same across 10 CFR Part 40, 70, and 76 licensees (e.g., the “Criticality Safety” cornerstone is not applicable to 10 CFR Part 40 licensees).

Figure 1 Fuel Cycle Regulatory Framework with Hazards Analysis-Based Cornerstones

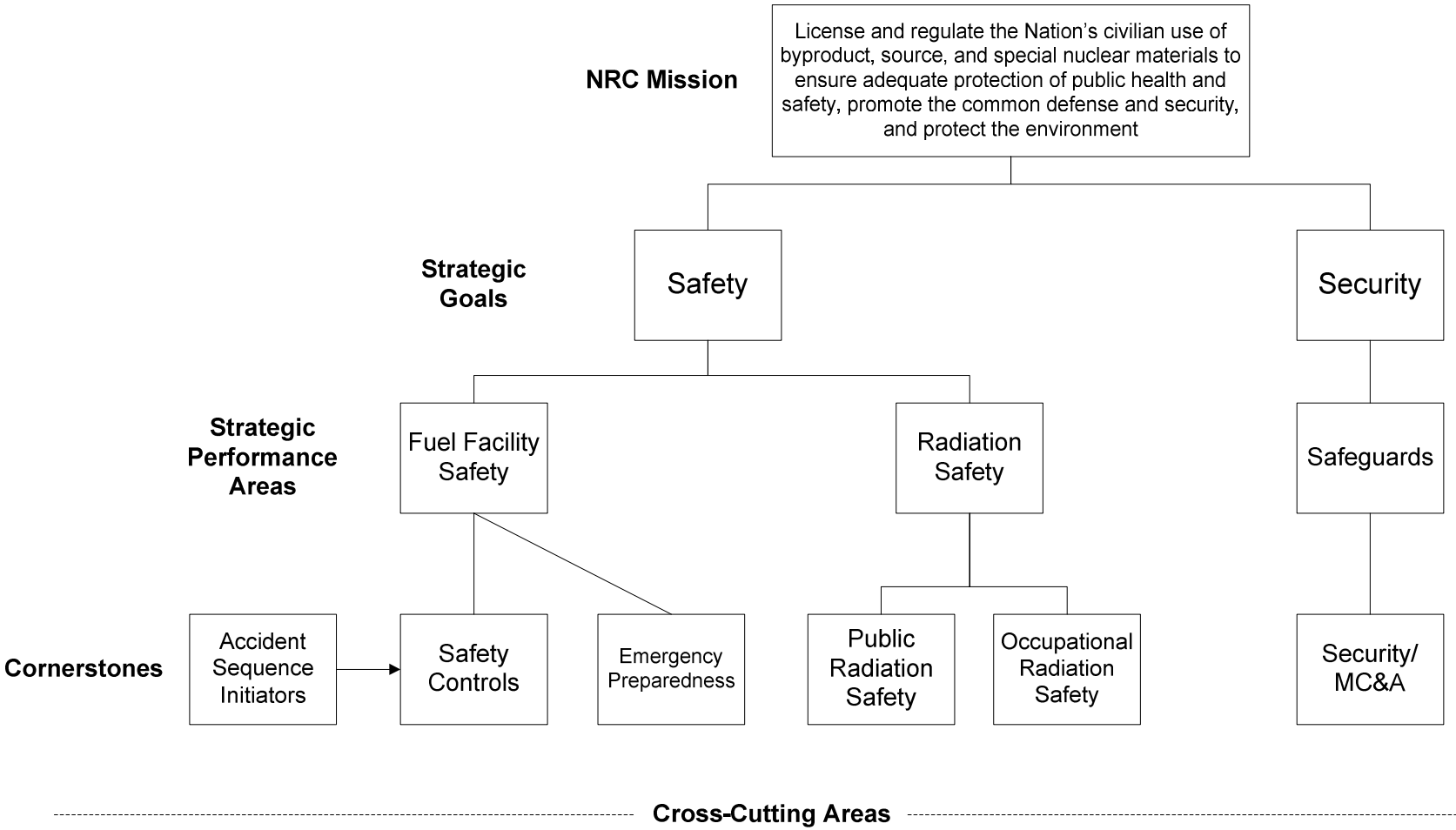
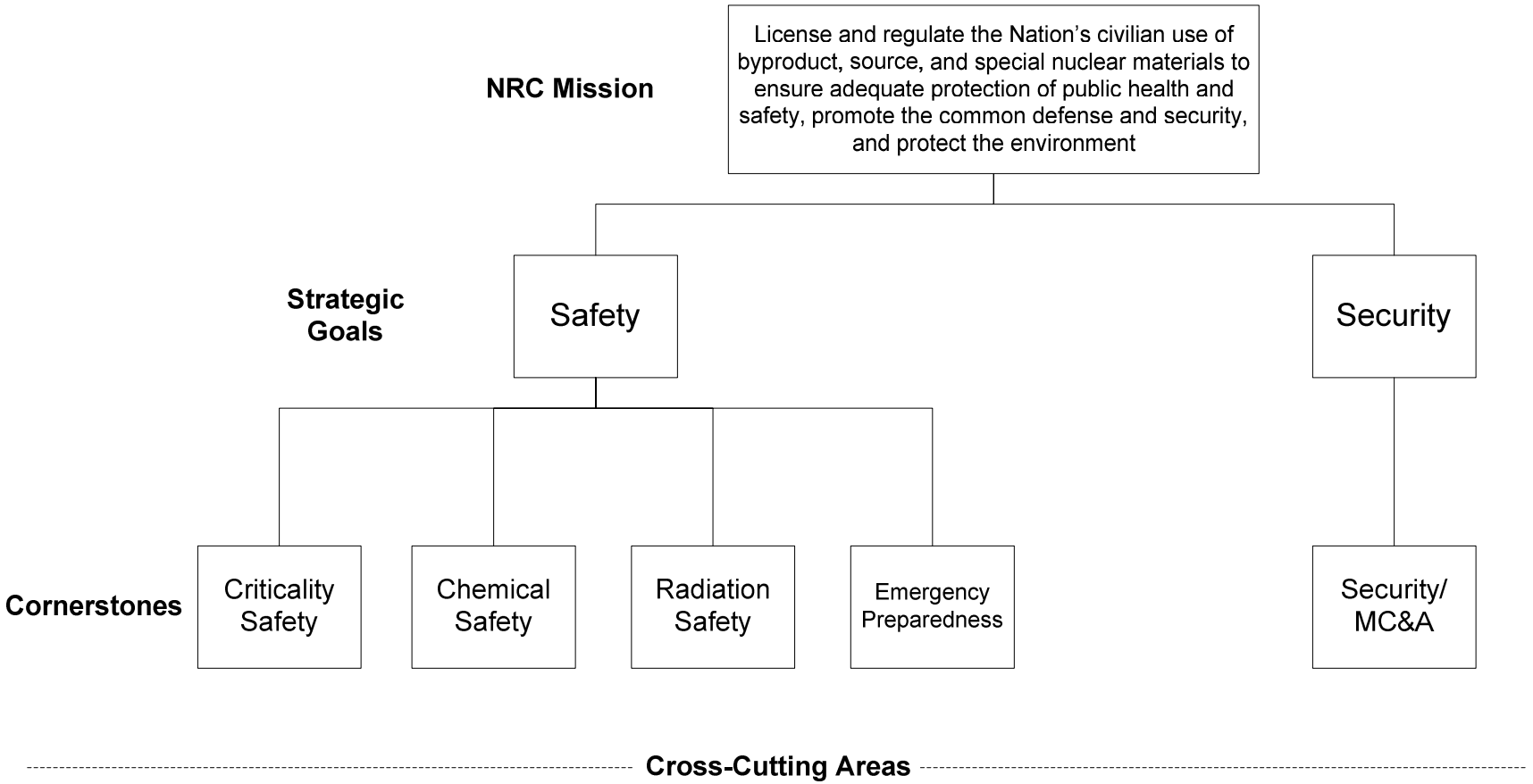


Figure 2 Fuel Cycle Regulatory Framework with Operations-Based Cornerstones



Appendix A
Accident Sequence Initiators Cornerstone

Background

Title 10 of the *Code of Federal Regulations* (10 CFR) 70.62, "Safety Program and Integrated Safety Analysis," requires licensees to implement a safety program that includes process safety information, an integrated safety analysis (ISA), and management measures to ensure that engineered controls and control systems that are identified as items relied on for safety (IROFS) are designed, implemented, and maintained to ensure that they are available and reliable. In developing the ISA, licensees are required to identify potential hazards and potential accident sequences caused by process deviations, other internal events, and credible external events. In 10 CFR 70.72, "Facility Change and Change Process," the U.S. Nuclear Regulatory Commission (NRC) requires licensees to implement a configuration management program to manage changes. Licensees are also required by 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material," to track failures of IROFS or management measures.

In developing the revised 10 CFR Part 70, the NRC developed two key companion documents, NUREG-1520, "Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility" (now Revision 1, issued May 2010), and NUREG-1513, "Integrated Safety Analysis Guidance Document," issued May 2001. These NUREGs provide background information for this cornerstone. In explaining an accident sequence as used in developing an ISA, NUREG-1513 (Section 2.6.5.1) notes the following:

> An accident sequence involves an initiating event, any factors that allow the accident to propagate (enablers), and any factors that reduce the risk (likelihood or consequence) of the accident (controls). The accident sequence is a sequence of specific real events. The initiating event is often the failure of some device or feature of the process that is an item relied on for safety. Such events are sometimes process upsets, but the frequency of such upsets is almost always controlled by features of the design or by operating procedures. Hence, these process features are being relied on for safety. Alternatively the initiating event could be a challenge from outside the system, that is, an external event. For an initiating event to lead to the consequences of concern it must usually be above a certain level of severity. For example, excursions of process parameters beyond normal conditions may be an upset, but if within safety limits, there is no chance of further progression. The subsequent events in the accident sequence are usually failures of hardware controls or manual procedures to limit or prevent damage.

Appendix C to NUREG-1520 (page 3-C-1) notes that initiating events can be (1) an external event such as a hurricane or earthquake, (2) a facility event external to the process being analyzed (e.g., fires, explosions, failures of other equipment, flooding from facility water sources), (3) deviations from normal operations of the process (credible abnormal events), or (4) failures of an IROFS in the process.

Appendix B to NUREG-1520 (page 3-B-4) notes that, in developing the ISA, initial conditions and bounding assumptions must be identified and, if susceptible to change over the lifetime of the facility (such as through process deviations or facility changes), must be appropriately maintained. Appendix C to NUREG-1520 (page 3-C-4) notes that the safety program required

by 10 CFR 70.62(a) should have provisions for implementing the appropriate management controls to maintain the validity of the initiating event frequencies.

The "Accident Sequence Initiators" cornerstone includes evaluation of the following elements to determine whether they were adequately analyzed by the licensee in the ISA or other safety analysis and whether they continue the ISA's assumptions (such as frequency or credibility):

- Initiating events—external events (external to the facility), facility events external to the process being analyzed, and deviations from normal operations of the process (credible abnormal events). Failures of IROFS that are initiating events are considered in the "Safety Controls" cornerstone.

- Enabling conditions—conditions or assumptions whose increase or change is credible and, if changed adversely, could cause an increase in accident frequency.

- Unforeseen events or errors of commission.

Objectives

The objectives of this cornerstone are to verify that a licensee does the following:

- Limits the frequency of accident sequence initiators that lead to the need for IROFS, nuclear criticality safety (NCS) controls, or other safety controls.[2] The ISA or safety analysis assumed a frequency for accident sequence initiators in establishing IROFS, NCS controls, and other safety controls. These IROFS, NCS controls, and other safety controls would be required by the license or 10 CFR Part 70 as a result of the safety analysis, ISA, or NCS analysis showing that they are needed to limit the likelihood of intermediate- or high-consequence accidents or prevent a nuclear criticality accident.

- Evaluates and limits, as appropriate, accident sequence initiators that are not required to be limited or controlled by IROFS, NCS controls, or other safety controls (non-IROFS). These are accident sequence initiators that the licensee has determined do not need to be prevented or have their likelihood limited based on the ISA. This could be because the ISA shows that they may be allowed to occur without causing the likelihoods or consequences defined in 10 CFR Part 70.

- Has identified in the ISA or safety analysis all accident sequence initiators associated with uses of licensed materials and appropriately assessed the accident sequences to identify those that require IROFS, NCS controls, or other safety controls to prevent or mitigate intermediate- or high-consequence events and to prevent nuclear criticalities.

Desired Results

Demonstration that there is reasonable assurance that accident sequence initiator frequencies are consistent with the safety analysis or ISA (for accident sequences that both require and do

[2] Other safety controls—NCS controls, chemical safety controls, or radiation safety controls at facilities not licensed under 10 CFR Part 70 that are identified in the license, technical safety requirements, license or certificate application, or safety analysis. For facilities licensed under 10 CFR Part 70, NCS controls, chemical safety controls, or radiation safety controls required by the license or described in the ISA, or safety analysis that are not IROFS or NCS controls required by 10 CFR Part 70.

not require IROFS, NCS controls, or other safety controls) and that all accident sequence initiators have been identified by the licensee.

Key Attributes and Scope

Figure A-1 shows the attributes of licensee performance that affect accident sequence initiators. Table A-1 shows those metrics used to measure accident sequence initiators key attributes.

1. Protection against External Events

   External events such as flooding, cold or hot weather, and loss of offsite power can lead to risk of loss of NCS controls, IROFS, or other controls. Protective systems, such as freeze protection, and backup power can reduce the impact of external events on the plant.

   a. Fire Protection Scope—This inspection is conducted to evaluate fire protection against fires external to the facility. The inspection is conducted in two phases. Phase 1 consists of annual assessment of conditions related to ignition sources, control of combustible materials, and fire protection systems and equipment. (For licensees with resident inspectors, Phase 1 is conducted at the frequency specified in resident inspection procedures.) Phase 2 is a periodic inspection that is a more in-depth review of fire protection for IROFS and other fire protection aspects required by the license.

   b. Flood Protection Scope—Inspection activities in this area focus on a licensee's readiness to protect IROFS, NCS controls, and other safety controls from potential internal and external flooding. These inspection activities would include walkdowns of key plant areas to determine whether flood protection features are adequately implemented, review of procedures including verification of key operator actions credited for coping with flood, and evaluation of compensatory measures during impending conditions of flooding or heavy rains. The inspectors would also focus on determining whether the licensee's flooding mitigation plans and equipment are consistent with the licensee's ISA or safety analysis.

   c. Cold or Hot Weather Protection Scope—Inspection activities in this area focus on a licensee's readiness to protect IROFS, NCS controls, and other safety controls from potential impacts from cold or hot weather. These inspection activities would include walkdowns of key plant areas to determine whether cold or hot weather protection features are adequately implemented, review of procedures including verification of key plant staff actions credited for coping with cold or hot weather, and evaluation of compensatory measures during impending conditions of cold or hot weather. The inspectors would also focus on determining whether the licensee's cold or hot weather protection plans and equipment are consistent with the licensee's ISA or safety analysis.

   d. Offsite Power Reliability Scope—Inspection activities in this area focus on a licensee's actions to ensure the reliability of offsite power during adverse weather conditions such as freezing rain or high winds.

   e. Surveillance Testing Scope—Inspection activities focus on determining whether surveillance testing is adequate to determine the readiness for protecting IROFS,

NCS controls, and other safety controls from external factors such as earthquakes, tornados, hurricanes, high winds, high temperatures, cold weather, fires external to the facility, and other adverse weather-related conditions. Inspectors determine whether IROFS, NCS controls, and other safety controls would perform within the design assumptions for adverse weather or other external events. Inspectors review surveillance test results for adequacy in meeting the requirements, observe ongoing testing to evaluate staff performance, and verify that test acceptance criteria are in agreement with IROFS, NCS control, and other safety control specifications.

2. Design (To Identify Accident Sequence Initiators)

Proper initial and subsequent design is essential to ensuring the identification of when IROFS, NCS controls, or other controls are necessary to met the requirements of 10 CFR Parts 40, 70, or 76 or the license. Proper design includes evaluation of accident sequences to identify any initiating events or enablers and assessment to determine if IROFS, NCS controls, or other safety controls are needed to meet requirements. Licensees implement design controls to ensure implementation of IROFS, NCS controls, and other safety controls. Failure to identify accident sequence initiators (initiating events and enablers) has led to situations where licensees have not adequately implemented IROFS, NCS controls, or other safety controls and thus operated without properly controlled accident sequences.

a. Licensee Analysis Scope—Inspection activities in this area focus on selected systems processing licensed material to determine whether the accident sequence initiators and accident sequences evaluated as part of the safety analysis, ISA, or ISA development effectively identified accident sequence initiators. Inspectors should review the licensee's analyses of selected systems and activities (included in the safety analysis or ISA or excluded from the ISA or safety analysis because the licensee determined that the accident sequence was noncredible). As part of this evaluation, inspectors should observe the installed equipment and licensee staff activities to operate the equipment. If inspectors are unable to observe equipment operation during the inspection, inspectors should conduct walkthroughs with plant staff to evaluate equipment operation. In evaluating whether the ISA or safety analysis has identified accident sequence initiators appropriately, inspectors should consider the following:

   i. Staff Performance—Inspections should focus on whether the licensee's ISA or safety analysis considered appropriately the complexity of actions required by licensee staff and considered potential staff performance deficiencies appropriately in accident sequence initiator determination.

   ii. Procedure Quality—Inspections should focus on whether the licensee's ISA or safety analysis appropriately considered the complexity of actions required by licensee staff, provided adequate guidance in procedures, and appropriately considered in accident sequence initiator determination the potential staff performance deficiencies resulting from deficient procedures.

   iii. Facility and Equipment Performance—Inspections should focus on whether the licensee's ISA or safety analysis appropriately considered

potential facility or equipment failure modes and frequencies. Inspectors should observe equipment operation to identify potential failure modes and resultant accident sequence initiators and compare them to those analyzed in the ISA or safety analysis.

b. Configuration Control Scope—Inspectors should review select systems to determine whether the licensee's ISA or safety analysis design has been adequately maintained in the equipment, as installed and used, such that the licensee did not introduce new accident sequence initiators with plant modifications. If the licensee has not maintained the ISA or safety analysis design, inspectors should identify any potential accident sequence initiators introduced by configuration control issues.

c. Management Measures Scope – If inspectors identify a problem with design or converting the design into the actual facility, inspectors should identify the cause(s) of the problem, including consideration of whether there was a failure of design management measures (design configuration management, design maintenance, design training and qualification, design audits and assessments, design procedures, design incident investigation, and design records management).

3. Accident Sequence Initiator Frequency

Licensees, in developing accident sequences, identify accident sequence initiators to include initiating events, enablers, and controls. This analysis includes establishing frequencies of initiating events and enablers to determine whether controls are needed to meet the design objectives and 10 CFR Parts 40, 70, or 76. Licensees monitor the frequency of these accident sequence initiators' occurrence to ensure that the design assumptions remain valid. If in actual operation the accident sequence initiators occur at a frequency greater than that in the initial design assumptions, the licensee analysis that led to the decisions related to IROFS, NCS controls, or other controls could be invalid, resulting in failure to meet regulatory requirements.

a. Accident Sequence Initiators that Result in IROFS, NCS Controls, or Other Safety Controls Scope—Inspectors should first identify the accident sequence initiators (from the ISA or other safety analysis) for selected accident sequences that resulted in the licensee establishing IROFS, NCS controls, or other safety controls. Inspectors then should determine the actual frequency of the occurrence of the initiators to the selected accident sequences. Inspectors should evaluate these actual frequencies to determine whether the actual frequencies of the initiators are consistent with the frequency assumptions in the ISA or other safety analysis. Inspectors then should review the licensee's evaluation of the causes of the failures that resulted in the accident sequence initiator. If the licensee has not evaluated the cause of the initiator, inspections should determine the causes (such as staff performance, procedure quality, design, facility and equipment performance, or configuration control) and then determine the effectiveness of the licensee's actions to prevent or control the occurrence of the initiator.

b. Accident Sequence Initiators that Do Not Result in IROFS, NCS Controls, or Other Safety Controls Scope—Inspectors first identify the accident sequence

initiators (from the ISA or other safety analysis) to selected accident sequences that, because of low likelihood, do not require that licensees establish IROFS, NCS controls, or other safety controls. Inspections then determine the actual frequency of the occurrence of the initiators to the selected accident sequences. Inspectors evaluate these actual frequencies to determine whether the actual frequencies of the initiators are consistent with the frequency assumptions in the ISA or other safety analysis. If the actual frequencies are higher than the frequency assumptions in the ISA or other safety analysis, the NRC reviews the licensee's actions that result from the increased frequencies, such as establishing IROFS because of the increased likelihood of the accident sequence.

4. Corrective Action Program

Maintaining configuration control of NCS controls, IROFS, and other safety controls is essential to ensure these controls and IROFS are capable, available, and reliable when needed. Thus there is no compromise of the ability to prevent or mitigate the consequences of a significant event.

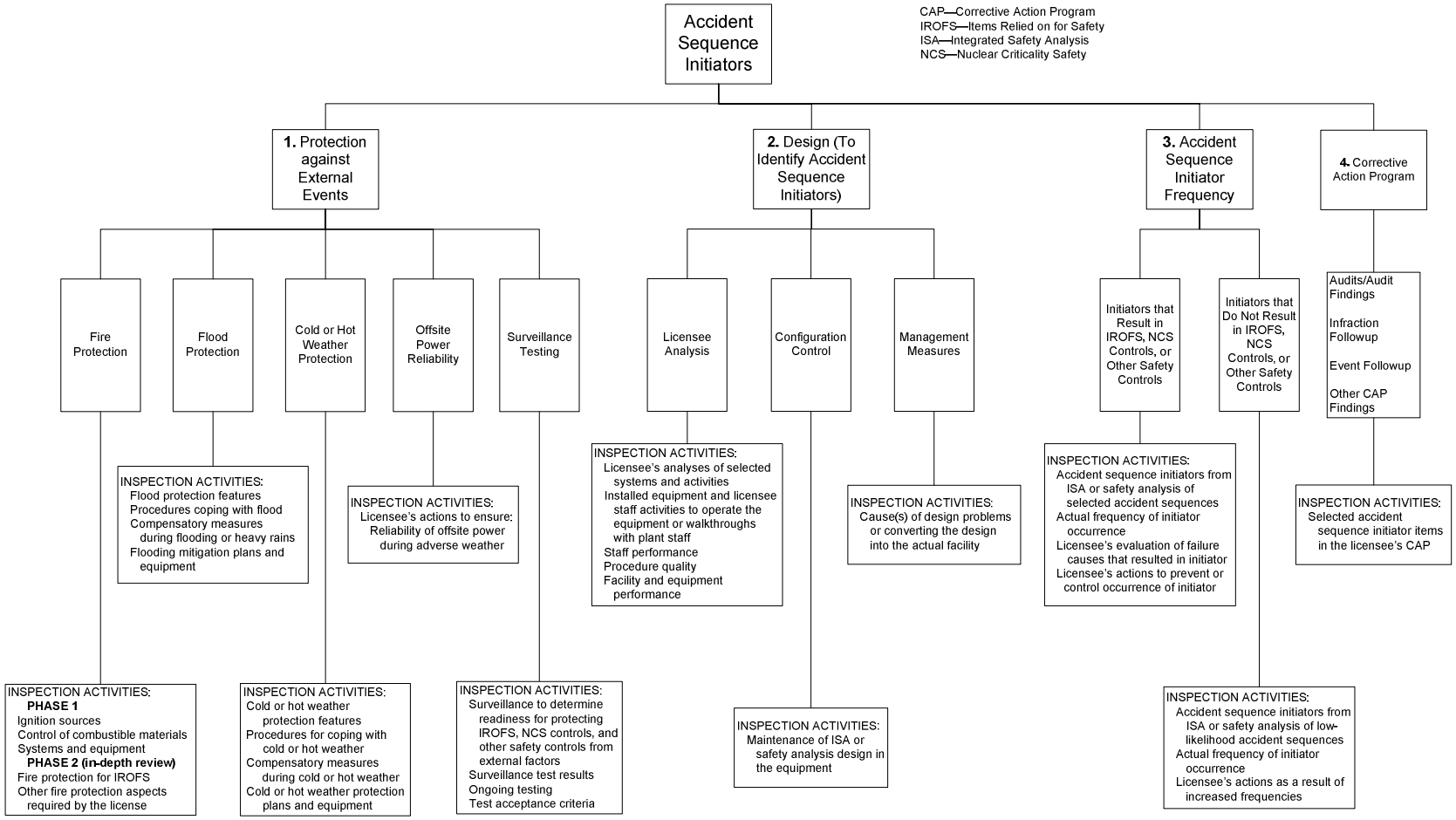
Corrective Action Program (CAP) Scope (Audits/Audit Findings, Infraction Followup, Event Followup, and Other CAP Findings)—Inspection activities include reviews of selected accident sequence initiator items in the licensee's CAP to determine whether the items were adequately identified and corrected. This inspection is to complement the periodic inspection of the CAP program that evaluates implementation of the overall CAP program. This process is a management measure for licensees under 10 CFR Part 70.

Table A-1 Metrics Used To Measure Accident Sequence Initiators Key Attributes

Key Attribute	Area to Measure	Metric
Protection against External Events	Fire protection	Licensee actions ensure the availability and reliability of controls and IROFS per 10 CFR Part 70 and ISA and safety analysis and license
	Flood protection	Licensee actions ensure the availability and reliability of controls and IROFS per 10 CFR Part 70 and ISA and safety analysis and license
	Cold or hot weather protection	Licensee actions ensure the availability and reliability of controls and IROFS per 10 CFR Part 70 and ISA and safety analysis and license
	Offsite power reliability	Licensee actions ensure the availability and reliability of controls and IROFS per 10 CFR Part 70 and ISA and safety analysis and license
	Surveillance testing	Results in capable, available, and reliable protection per 10 CFR Part 70 and ISA and safety analysis and license
Design (To Identify Accident Sequence Initiators)	Licensee analysis in ISA or safety analysis	Results in credible accident sequence initiators and accident sequences identified as required by 10 CFR Part 70 and license
	Configuration control to assure that accident sequence initiators and accident sequences in ISA or safety analysis are adequate	Meet 10 CFR 70.61 and 10 CFR 70.72 and license requirements
Accident Sequence Initiator Frequency	Those that result in IROFS, NCS controls, or other safety controls	Meet or below ISA-assumed frequency
	Those that do not	Meet or below ISA-assumed

Key Attribute	Area to Measure	Metric
	result in IROFS, NCS controls, or other safety controls	frequency
Corrective Action Program	Audits/Audit findings	Audits conducted as required by license and findings resolved adequately and in a timely manner
	Infraction followup	Followup resolves issue, prevents reoccurrence, and adequately considers the extent of the condition
	Event followup	Followup resolves issue, prevents reoccurrence, and adequately considers the extent of the condition
	Other CAP findings	Other IROFS or criticality safety issues in CAP are adequately resolved

Figure A-1 Accident Sequence Initiators Cornerstone Key Attributes



Appendix B
Criticality Safety Cornerstone

Objective

The objective of this cornerstone is to verify that nuclear criticality safety (NCS) controls and items relied on for safety (IROFS) protect worker and public health and safety by preventing criticalities. This includes verifying adequate NCS analyses and verifying the availability, reliability, and capability of NCS controls and IROFS.

Desired Results

Demonstration that there is reasonable assurance that inadvertent nuclear criticality events would be prevented.

Key Attributes and Scope

Figure B-1 shows those attributes of licensee performance that affect criticality safety. Table B-1 shows those metrics used to measure criticality safety key attributes.

1. Staff Performance

   Staff performance in day-to-day activities, prior to any initiating event, influences the performance of NCS controls and IROFS through the conduct of operational, maintenance, and test activities. Staff actions are also important to equipment response to initiating events. Staff performance is critical to reducing the frequency of certain accident sequences and mitigating the resultant consequences. Staff actions can be NCS controls or IROFS. Examples of staff actions that are important to the performance of NCS controls or IROFS would include staff action in response to alarms for high uranium concentration in solutions, for temperature in vessels containing uranium, or for pH. Staff performance during initial and re-qualification provide an indication of expected staff performance.

   a. Staff Training and Qualification Scope—Inspection activities in this area focus on the effectiveness of the licensee's program for conducting initial NCS training, qualification, and requalification training for plant staff through observation of plant staff performance during operations and during walkthroughs conducted by inspectors. Inspectors evaluate any deficient performance to determine if it results from deficient training and qualification.

   b. Temporary Instruction Scope—Inspection activities in this area focus on plant staff actions taken because of equipment deficiencies, degradation, or unavailability. In these cases, operators would likely be using temporary procedure changes or instructions. Inspectors evaluate the impact on plant staff performance because of temporary instructions. Inspection activities focus on temporary instructions that have the potential to degrade NCS controls and IROFS.

2. Procedure Quality

To ensure proper functioning of NCS controls and IROFS, the procedures regarding NCS controls and IROFS use, maintenance and testing must be correct. Maintenance and testing procedures influence the capability of NCS controls and IROFS to respond when needed. Standard operating procedures and abnormal operating procedures are essential to ensuring NCS controls and IROFS, which are frequently contained in these procedures, are implemented as required by regulations and the license. Unclear procedures or procedures that are out of sequence could result in staff errors that lead to the failure of NCS controls or IROFS.

NCS Control and IROFS Clarity Scope—Inspection activities in this area focus on the clarity of plant procedures with regard to NCS controls and IROFS. Inspection activities include observation of plant staff performance during operations and during walkthroughs by inspectors. Inspectors evaluate any deficient performance to determine if it results from inadequate, deficient, or unclear procedures. While reviewing the use of procedures, inspectors also evaluate whether the procedure and activities observed result in compliance with regulations and license requirements. In addition, inspectors review selected changes to procedures to determine whether the procedures provide adequate guidance to plant staff to meet U.S. Nuclear Regulatory Commission (NRC) requirements.

3. Facility and Equipment Performance

Adequate capability, availability, and reliability of facilities and equipment that function as NCS controls and IROFS are crucial to preventing and mitigating the consequences of events that could lead to a criticality. In addition, proper functioning of criticality warning systems is critical to mitigating the consequences of a criticality accident if one happens. Maintenance, testing, and fire protection ensure equipment functions when needed. In addition, external events such as flooding, cold or hot weather and loss of offsite power can lead to risk of loss of NCS controls or IROFS. Protective systems, such as freeze protection, and backup power can reduce the impact of external events on the plant.

a. Maintenance Effectiveness Scope—Inspection activities in this area review selected items to determine whether the licensee is assuring adequate NCS controls and IROFS performance (including criticality alarms) by applying this management measure appropriately, including reviewing the failure evaluations of selected IROFS to determine the cause as required by Title 10 of the *Code of Federal Regulations* (10 CFR) 70.62(a). In addition, inspectors observe maintenance activities for NCS controls and IROFS to evaluate work practices.

b. Surveillance Testing Scope—Inspection activities focus on determining whether licensee surveillance testing of NCS controls and IROFS (including criticality alarms) assures that they are capable of performing their intended safety functions. This includes evaluating the surveillance to determine the licensee's readiness to protect NCS controls and IROFS from external factors such as earthquakes, tornados, hurricanes, high winds, high temperatures, cold weather, and other adverse weather-related conditions. Inspectors determine whether NCS controls and IROFS would perform within the design assumptions for adverse weather. Inspectors review surveillance test results for adequacy in meeting the requirements, observe ongoing testing to evaluate staff

performance, and verify that test acceptance criteria are in agreement with NCS control and IROFS specifications.

c. Postmaintenance Testing Scope—Inspection activities focus on determining whether the postmaintenance test procedures and test activities are adequate to verify NCS controls and IROFS (including criticality alarms) would perform their intended function after the maintenance.

d. Fire Protection Scope—These inspections are conducted to evaluate protection against fires within and external to the facility. These inspections would be conducted in two phases. Phase 1 consists of annual assessment of conditions related to ignition sources, control of combustible materials, and fire protection systems and equipment. (For licensees with resident inspectors, Phase 1 is conducted at the frequency specified in resident inspection procedures.) Phase 2 is a periodic inspection that is a more indepth review of fire protection of NSC controls and IROFS and other fire protection required by the license.

e. Flood Protection Scope—Inspection activities in this area focus on a licensee's readiness to protect NCS controls and IROFS from potential internal and external flooding. These inspection activities would include walkdown of key plant areas to determine whether flood protection features are adequately implemented, review of procedures including verification of key plant staff actions credited for coping with flood, and evaluation of compensatory measures during impending conditions of flooding or heavy rains. The inspectors would also focus on determining whether the licensee's flooding mitigation plans and equipment are consistent with the licensee's integrated safety analysis (ISA) or safety analysis.

f. Cold or Hot Weather Protection Scope—Inspection activities in this area focus on a licensee's readiness to protect NCS controls and IROFS from potential impacts from cold or hot weather. These inspection activities would include walkdown of key plant areas to determine whether cold or hot weather protection features are adequately implemented, review of procedures including verification of key plant staff actions credited for coping with cold or hot weather, and evaluation of compensatory measures during impending conditions of cold or hot weather. The inspectors would also focus on determining whether the licensee's cold or hot weather protection plans and equipment are consistent with the licensee's ISA or safety analysis.

g. Offsite and Onsite Power Reliability Scope—Inspection activities in this area focus on a licensee's actions to ensure the reliability of offsite power during adverse weather conditions, such as freezing rain or high winds. In addition, inspection activities include a licensee's actions to ensure the availability, reliability, and capability of onsite backup power such as batteries and emergency diesel generators.

4. Design

Proper initial design and subsequent design are essential to ensuring the capability, availability, and reliability of NCS controls and IROFS. This includes assurance of

assumptions regarding accident sequence initiators. The ISA should reflect the hazard identification and controls that meet regulatory requirements.

a. NCS Controls and IROFS Design and Performance Capability Scope—Inspection activities in this area include review of the ISA summary and ISA or safety analysis, as-built conditions, modifications, testing, and normal and emergency operation of risk-significant systems. This would be an indepth review of a selected risk-significant system and support systems.

b. Analysis Scope—Inspection activities in this area focus on selected systems processing licensed material to determine whether the accident sequence initiators and accident sequences evaluated as part of the ISA, ISA development, or safety analysis effectively identified accident sequence initiators. Inspectors review the licensee's analyses of selected systems and activities (included in the ISA or safety analysis, or excluded from the ISA or safety analysis because the licensee determined that the accident sequence was noncredible). As part of this evaluation, inspectors should observe the installed equipment and licensee staff activities to operate the equipment. If inspectors are unable to observe equipment operation during the inspection, inspectors should conduct walkthroughs with plant staff to evaluate equipment operation. In evaluating whether the ISA or safety analysis has identified accident sequence initiators appropriately, inspectors should consider the following:

   i. Staff Performance—Inspections focus on whether the licensee's ISA or analysis considered appropriately the complexity of actions required by licensee staff and considered potential staff performance deficiencies appropriately in accident sequence initiator determination.

   ii. Procedure Quality—Inspections focus on whether the licensee's ISA or safety analysis appropriately considered the complexity of actions required by licensee staff, provided adequate guidance in procedures, and appropriately considered in accident sequence initiator determination the potential staff performance deficiencies resulting from deficient procedures.

   iii. Facility and Equipment Performance—Inspections focus on whether the licensee's ISA or safety analysis appropriately considered potential facility or equipment failure modes and frequencies. Inspectors observe equipment operation to identify potential failure modes and resultant accident sequence initiators and compare them to those analyzed in the ISA or safety analysis.

c. Frequency of Accident Sequence Initiators that Result in IROFS, NCS Controls, or Other Safety Controls Scope—Inspectors first identify the accident sequence initiators (from the ISA or other safety analysis) to selected accident sequences that resulted in the licensee establishing IROFS, NCS controls, and other safety controls. Inspectors then determine the actual frequency of the occurrence of the initiators to the selected accident sequences. Inspectors should evaluate these actual frequencies to determine whether the actual frequencies of the initiators are consistent with the frequency assumptions in the ISA or other safety analysis. Inspectors then review the licensee's evaluation of the causes of the failures that

resulted in the accident sequence initiator. If the licensee has not evaluated the cause of the initiator, inspections determine the causes (such as staff performance, procedure quality, design, facility and equipment performance, or configuration control) and then determine the effectiveness of the licensee's actions to prevent or control the occurrence of the initiator.

d. Accident Sequence Initiators that Do Not Result in IROFS, NCS Controls, or Other Safety Controls Scope—Inspectors first identify the accident sequence initiators (from the ISA or other safety analysis) to selected accident sequences that, because of low likelihood, do not require that licensees establish IROFS, NCS controls, and other safety controls. Inspections then determine the actual frequency of the occurrence of the initiators to the selected accident sequences. Inspectors evaluate these actual frequencies to determine whether the actual frequencies of the initiators are consistent with the frequency assumptions in the ISA or other safety analysis. If the actual frequencies are higher than the frequency assumptions in the ISA or other safety analysis, the NRC reviews the licensee's actions that respond to the increased frequencies, such as establishing IROFS because of the increased likelihood of the accident sequence.

5. Configuration Control

Maintaining configuration control of NCS controls or IROFS is essential to ensure these NCS controls and IROFS are capable, available, and reliable when needed. Thus there is no compromise of the ability to prevent or mitigate the consequences of a criticality.

a. Permanent Plant Modifications Scope—Inspection activities in this area include the review of design, installation, configuration control, and postmodification testing for risk-significant permanent modifications potentially affecting NCS controls and IROFS. Inspection activities include an indepth review of changes to the initial licensed design, ISA and ISA summary or safety analysis, management measures, and normal and emergency operating procedures. Inspectors determine whether the licensee's evaluations of the modifications meet the requirements of 10 CFR 70.72, "Facility Changes and Change Process."

b. Temporary Plant Modifications Scope—Inspection activities in this area include a review of design, installation, configuration control, and postmodification testing for selected potentially risk-significant temporary modifications that impact NCS controls and IROFS. Inspectors determine whether the licensee's evaluations of the modifications meet the requirements of 10 CFR 70.72.

c. Equipment Alignment Scope—Inspection activities determine whether equipment is aligned in accordance with procedures and the ISA or safety analysis and whether there are discrepancies that impact the NCS controls or IROFS. This includes conducting periodic partial walkdown inspections to determine whether NCS controls and IROFS are properly aligned. In addition, inspectors would periodically perform a complete walkdown.

6. Criticality Analysis

The initial criticality analysis and subsequent analyses can affect NCS controls and IROFS. If the criticality analyses are done improperly, licensees could lose safety margin and potentially implement inadequate NCS controls and IROFS. The analysis is required to be done in a way that meets regulatory requirements.

Criticality Analysis Scope (Analytical Assumptions and Adequate Subcritical Margin)—Inspection activities include regular reviews of new and changed criticality analyses to determine the adequacy of analytical assumptions and the resulting subcritical margin. The inspectors evaluate the overall adequacy of the criticality safety basis, resulting IROFS and controls, and the effect of changes on assumptions, conclusions, and the subcritical margin.

7. Corrective Action Program

The licensee's CAP is expected to identify and correct problems or indications of problems in the above key attributes that could lead to degraded NCS controls or IROFS. The CAP should identify early indications of problems before they have actual safety impacts.

Corrective Action Program (CAP) Program Scope (Audits/Audit Findings, Infraction Followup, Event Followup, and Other CAP Findings)—Inspection activities include reviews of selected NCS items in the licensee's CAP to determine whether the items were adequately identified and corrected. This inspection is to complement the periodic inspection of the CAP program that evaluates implementation of the overall CAP program. This process is a management measure for licensees under 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material."

Table B-1 Criticality Safety Metrics Used To Measure Key Attributes

Key Attribute	Area to Measure	Metric
Staff Performance	Staff training and qualification	Training adequate to assure effective procedure use
	Temporary instructions	Temporary changes evaluated per license and adequately implemented
Procedure Quality	NCS control and IROFS clarity	Controls and IROFS adequately implemented and properly used
Facility and Equipment Performance	Maintenance effectiveness	Capable, available, and reliable per regulation and license or certificate
	Surveillance testing	Capable, available, and reliable per regulation and license or certificate
	Postmaintenance testing	Capable, available, and reliable per regulation and license or certificate
	Fire protection	Licensee actions ensure availability and reliability of controls and IROFS per regulation and license or certificate
	Flood protection	Licensee actions ensure availability and reliability of controls and IROFS per regulation and license or certificate
	Cold or hot weather protection	Licensee actions ensure the availability and reliability of controls and IROFS per regulation and license or certificate
	Offsite and onsite backup power	Meets 10 CFR 70.61 and 10 CFR 70.62 and license
Design	NCS control and IROFS design	Meets 10 CFR 70.61 and 10 CFR 70.62 and license
	Analysis	Done in accordance with license ISA or safety analysis
	Frequency of accident sequence initiators that result	Meets or below ISA or safety analysis frequency

Key Attribute	Area to Measure	Metric
	in IROFS or NCS controls	
	Frequency of accident sequence initiators that do not result in IROFS or NCS controls	Meets or below ISA or safety analysis frequency
Configuration Control	Permanent plant modifications	Meets 10 CFR 70.72, 10 CFR 70.61, and 10 CFR 70.62 and license
	Temporary plant modifications	Meets 10 CFR 70.72, 10 CFR 70.61, and 10 CFR 70.62 and license
	Equipment alignment	Properly aligned in accordance with analysis and procedures
Criticality Analysis	Criticality safety basis, IROFS and controls, and the effect of changes on assumptions, conclusions, and subcritical margin	Meet 10 CFR 70.61 and 10 CFR 70.72 and license requirements
Corrective Action Program	Audits/Audit findings	Audits conducted as required by license and findings resolved in a timely manner
	Infraction followup	Followup resolves issue, prevents reoccurrence, and adequately considers extent of condition
	Event followup	Followup resolves issue, prevents reoccurrence, and adequately considers extent of condition
	Other CAP findings	Other criticality safety issues in CAP adequately resolved

Figure B-1 Criticality Safety Cornerstone Key Attributes

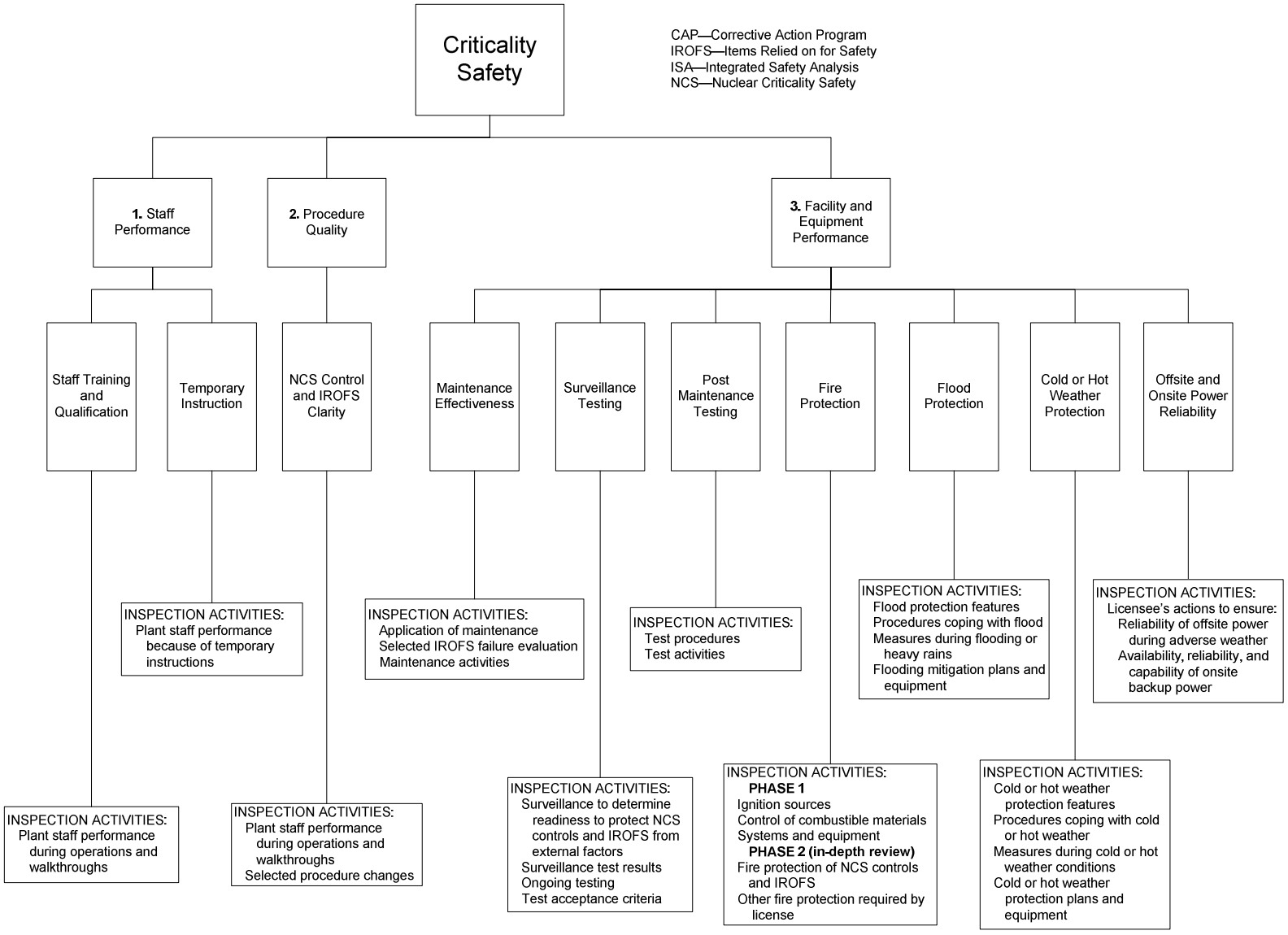


Figure B-1 Criticality Safety Cornerstone Key Attributes (continued)