

## MFFFPEm Resource

---

**From:** Tiktinsky, David  
**Sent:** Thursday, February 04, 2010 8:38 AM  
**To:** Cleavenger, Sabrina; Morrissey, Kevin; Roman, Cinthya  
**Cc:** Oesterle, Eric; MFFFHearingFile Resource  
**Subject:** FW: Management Measures Inclusion in MPQAP  
**Attachments:** tech.gif; LA Ch 5, 15, ISAS 1.0, 5.1 Mgmt Meas Chg Pages.pdf

**Follow Up Flag:** Follow up  
**Flag Status:** Flagged

---

**From:** Gwyn, Dealis W. [mailto:DWGwyn@moxproject.com]  
**Sent:** Wednesday, February 03, 2010 5:00 PM  
**To:** Tiktinsky, David  
**Subject:** Management Measures Inclusion in MPQAP

Dave,

Attached are proposed change pages that reflect the inclusion of management measures (previously discussed in LA Chapter 15) in the MPQAP.

If you have any questions, please let me know.

Dealis

---

**\*\*\*\*Internet Email Confidentiality Footer\*\*\*\* Privileged/Company Confidential Information may be contained in this message. If you are not the addressee indicated in this message (or responsible for delivery of the message to such person), you may not copy or deliver this message to anyone. In such case, you should destroy this message and notify the sender by reply email. Please advise immediately if you or your employer do not consent to Internet email for messages of this kind. Opinions, conclusions, and other information in this message that do not relate to the official business of Shaw Areva MOX Services LLC or its subsidiaries shall be understood as neither given nor endorsed by it.**

**Hearing Identifier:** MixedOxideFuelFabricationFacility\_Public  
**Email Number:** 107

**Mail Envelope Properties** (0A64B42AAA8FD4418CE1EB5240A6FED10E0E74342C)

**Subject:** FW: Management Measures Inclusion in MPQAP  
**Sent Date:** 2/4/2010 8:38:07 AM  
**Received Date:** 2/4/2010 8:38:12 AM  
**From:** Tiktinsky, David

**Created By:** David.Tiktinsky@nrc.gov

**Recipients:**

"Oesterle, Eric" <Eric.Oesterle@nrc.gov>  
Tracking Status: None  
"MFFFHearingFile Resource" <MFFFHearingFile.Resource@nrc.gov>  
Tracking Status: None  
"Cleavenger, Sabrina" <Sabrina.Cleavenger@nrc.gov>  
Tracking Status: None  
"Morrissey, Kevin" <Kevin.Morrissey@nrc.gov>  
Tracking Status: None  
"Roman, Cinthya" <Cinthya.Roman@nrc.gov>  
Tracking Status: None

**Post Office:** HQCLSTR02.nrc.gov

<b>Files</b>	<b>Size</b>	<b>Date &amp; Time</b>
MESSAGE	1133	2/4/2010 8:38:12 AM
tech.gif	927	
LA Ch 5, 15, ISAS 1.0, 5.1 Mgmt Meas Chg Pages.pdf		464274

**Options**

**Priority:** Standard  
**Return Notification:** No  
**Reply Requested:** No  
**Sensitivity:** Normal  
**Expiration Date:**  
**Recipients Received:** Follow up



## **15.0 MANAGEMENT MEASURES**

MOX Services has submitted Management Measures under separate cover within the MOX Project Quality Assurance Plan (MPQAP).

## **5.0 SAFETY PROGRAM AND INTEGRATED SAFETY ANALYSIS**

Shaw AREVA MOX Services, LLC (MOX Services) has established and maintains a safety program, including an integrated safety analysis (ISA), that demonstrates compliance with the performance requirements of Title 10 of the Code of Federal Regulations (CFR) §70.61.

### **5.1 SAFETY PROGRAM**

The Mixed Oxide (MOX) Fuel Fabrication Facility (MFFF) safety program consists of process safety information; an ISA that analyzes MFFF hazards and potential accident sequences, and identifies Items Relied Upon for Safety (IROFS); and management measures to ensure that IROFS are available and reliable to perform their function when needed. These three elements of the safety program as described in 10 CFR §70.62 and §70.65 are discussed below.

#### **5.1.1 Process Safety Information**

MOX Services compiles and maintains current written process safety information for the MFFF to identify and understand the hazards associated with the processes, and to update the ISA as required. This information is contained in analyses, specifications, drawings, and other documentation that are prepared, reviewed, and approved in accordance with the MFFF configuration management process (see MPQAP). Process safety information includes the following:

- A description of the hazards, including information on the pertinent chemical or physical properties of hazardous materials (e.g., toxicity, acute exposure limits, reactivity, thermal and chemical stability, or other applicable information that would typically be included on Material Safety Data Sheets)
- A description of the equipment used in the process (e.g., information of a general nature on such topics as the materials of construction, piping and instrumentation diagrams, ventilation, design codes and standards employed, material and energy balances, safety systems, interlocks, fire detection or suppression systems, electrical classification, relief system design, and the design bases)
- A description of the technology of the process (e.g., block flow or simplified process flow diagrams, a brief outline of the process chemistry, upper and lower limits for controlled parameters, and an evaluation of health and safety consequences of process deviations).

#### **5.1.2 Integrated Safety Analysis**

An ISA is conducted with an appropriate level of detail for the complexity of the processes involved (10 CFR §70.62(c)). MOX Services has conducted this ISA to demonstrate compliance with 10 CFR §70.61. The ISA supports preparation of an ISA Summary (as a separate submittal that is not a part of this License Application—as specified by 10 CFR §70.65(b)), a document that summarizes the conclusions of the analyses done as a part of the ISA process. The ISA is a systematic analysis to identify: plant internal and external hazards and their potential for initiating event sequences; the potential event sequences; their likelihood and consequences; and

the structures, systems, and components (SSCs) and activities of personnel that are relied on for safety (i.e., IROFS).

The consequence severity levels that are used in the hazard evaluation are based on 10 CFR §70.61 and are provided in Table 5.1-1. Risk is the product of the event likelihood and consequences. The risk of each credible event is determined by cross-referencing the severity of the consequence of the unmitigated accident sequence with the likelihood of occurrence in a risk matrix. A risk matrix, shown in Table 5.1-2, is used to determine the requirement for IROFS.

The ISA demonstrates that the IROFS are adequate to perform their intended safety functions when necessary. The ISA is an ongoing process and is maintained during all phases of the facility life cycle. MOX Services has completed an ISA in accordance with the methods and criteria contained in the ISA Summary and the programmatic commitments discussed below. MOX Services commits to maintaining the ISA.

### **5.1.3 Management Measures**

Management measures are applied to IROFS by providing the administrative and programmatic framework for configuration management, maintenance, training and qualification, procedures, audits and assessments, incident investigation, and records management. IROFS and appropriate management measures are implemented based on the results of the ISA to ensure compliance with the performance requirements of 10 CFR §70.61. MOX Services implements and maintains these management measures, as described in the MPQAP, to ensure the required reliability and availability of IROFS. The application of management measures to IROFS is described in Section 5.2.5.2.4

### **5.1.4 Control Of Facility And Process Changes**

MOX Services maintains the ISA, ISA Summary, and License Application (LA) so that they are accurate and up-to-date by means of the MFFF configuration management processes, which include written procedures. MOX Services evaluates changes to the facility and its processes for impact on the ISA and LA, and updates the LA and ISA Summary, as needed, in order to ensure their continued accuracy. The evaluation of the facility and process changes includes identification and impact of changes to parameters used in the postulated accident sequences of the ISA (including event likelihood and consequences). Responsibility for maintaining and updating the ISA, ISA Summary, and the LA belongs to the manager of the support services function, as described in Chapter 4.

MOX Services will address safety-significant vulnerabilities or unacceptable performance deficiencies, if any are identified, in the evaluation of the proposed facility and process changes. MOX Services will take prompt and appropriate actions to address vulnerabilities that are identified.

MOX Services controls facility and process changes in accordance with the following requirements:

the foundation for ensuring that IROFS are robust and incorporate lessons learned from the nuclear, mechanical, electrical, and instrumentation and control disciplines. Thus, they provide an effective set of engineering and procedural guidelines used to design, construct, and operate the IROFS. Application of codes and standards provides assurance that controls utilized to implement the single failure criterion or double contingency principle are sufficiently reliable.

#### 5.2.5.2.4 Application of Management Measures

The fourth design criterion, application of management measures, is particularly important in the context of IROFS failure detection. IROFS failure detection is meant to include detection of IROFS failures and repair of the IROFS or the process is shutdown. As described in NUREG 1718, *Standard Review Plan for the Review of an Application for a Mixed Oxide (MOX) Fuel Fabrication Facility*, U.S. Nuclear Regulatory Commission, August 2000, IROFS failure detection can significantly reduce the likelihood of an accident scenario. For an accident scenario to proceed to completion, failure of one IROFS must occur, its failure must go undetected, and a second IROFS must fail.

Management measures are applied to the identified IROFS to ensure that they are reliable and available on demand. The MPQAP specifically describes the QA requirements, implementing procedural controls, and documentation requirements to address management measures as described in NUREG-1718. The set of applied management measures consists of applicable elements of the following management measures programs: quality assurance, configuration management, maintenance, training and qualification of plant personnel, plant procedures, audits and assessments, incident investigations, and records management.

Management measures are assigned based on the following types of IROFS classifications and the risk reduction level attributed to that particular IROFS:

- Passive Engineered Controls (PEC) – A device that uses only fixed physical design features to maintain safe process conditions without any required human action
- Active Engineered Controls (AEC) – A physical device that uses active sensors, electrical components, or moving parts to maintain safe process conditions without any required human action
- Enhanced Administrative Controls (EAC) – A procedurally required or prohibited human action, combined with a physical device that alerts the operator that the action is needed to maintain safe process conditions, or otherwise adds substantial assurance of the required human performance (i.e., augmented administrative control)
- Administrative Controls (AC) – A procedural human action that is prohibited or required to maintain safe process conditions (i.e., a simple administrative control).

The specific elements of the various management measures programs assigned to each IROFS classification are provided in the MPQAP. The MPQAP illustrates how management measures are applied to the above IROFS classifications. For the enhanced administrative controls (EAC), the specific management measures for the physical device are covered under the active engineered controls (AEC) classification.

accordance with the design change control and configuration management programs (see MPQAP).

### 5.2.6.2 Nuclear Criticality Safety Evaluations

Operations with fissionable materials at the MFFF introduce risks of a criticality accident. Criticality safety must be ensured through design and administrative practices. Criticality safety is included in the ISA through the PrHAs described in Section 5.2.2.. NCSEs are performed to develop and document the safety basis for facility operations relating to the criticality events identified in the PrHAs. NCSEs are the main source of information demonstrating the adequacy of criticality controls and the effectiveness of administrative practices.

Criticality analysis design methods require a high level of validation. Criticality analysis methods used in MFFF design activities and facility safety programs comply with the technical guidance of ANSI/ANS-8.1-1983 (R1988), *Nuclear Criticality Safety in Operations with Fissionable Materials Outside Reactors*, American Nuclear Society, Hinsdale, Illinois, September 9, 1998. Limits are developed specific to MFFF design applications (that is, limiting fissile material isotopic composition) using validated and approved computational methods. Validated and approved computational methods are also used to demonstrate criticality safety through analysis of specific design applications. Computational methods applied in MFFF design analysis include the KENO VI Monte Carlo criticality code and related computer code modules included in the SCALE system of codes for reactivity determination.

The validation process establishes method bias by comparing measured results from laboratory critical experiments to method-calculated results for the same systems. The verification and validation processes are controlled and documented as required by program QA procedures. Hardware system access controls are put in place to ensure that the same codes and data used in the validation are used in NCSE applications. Changes or maintenance to approved software is formally controlled and documented to the same level of control as the original verification and validation procedure.

The validation establishes a method bias by correlating the results of critical experiments with results calculated for the same systems by the method being validated. Critical experiments are selected to be representative of the systems to be evaluated in specific design applications. The range of experimental conditions (for example, material compositions and geometric arrangements) encompassed by a selected set of benchmark experiments establishes the "area(s) of applicability" over which the calculated method bias is applicable.

The validation process was documented and provided to NRC for review as part of the Construction Authorization process. MOX Services submitted its validation report in three separate parts by letter dated January 8, 2003. The latest revision to Parts I and III was submitted by letter dated July 2, 2003. The MFFF validation is described in three validation reports covering the five Areas of Applicability (AOAs) as follows:

#### Part I:

- Pu-nitrate aqueous solutions

**Table 1-1. 10 CFR §70.65 Regulatory Requirements Roadmap to ISA Summary  
(continued)**

Regulatory Requirement	Applicable NUREG-1718 Guidance	ISA Summary Sections
<p>§70.65 (b)(4) Information that demonstrates the licensee's compliance with the performance requirements of §70.61, including a description of the management measures; the requirements for criticality monitoring and alarms in §70.24; and, if applicable, the requirements of §70.64;</p>	<p>NUREG-1718, Section 5.4.3.2.B.viii, 6.4.3.3.6.B, 6.4.3.3.6.C, 10.4.3.C.ii.b, and 8.4.3.4</p>	<p>Information demonstrating compliance with 10 CFR 70.61 is presented in Sections 5.3.x by event types and event groups</p>
	<p>NUREG-1718, Sections 6.4.3.2, 10.4.3.C.ii.e and 15</p>	<p>A description of management measures are contained within the MPQAP</p>
	<p>NUREG-1718, Section 5.4.3.2.B.xiii and 6.4.3.3.3</p>	<p>A description of the criticality monitoring systems and alarms is contained in Section 4.13</p>
	<p>NUREG-1718, Sections 5.4.3.2.B.xiv and 6.4.3.3.5</p>	<p>Sections 4.3 through 4.9, and 4.11 through 4.13 identify codes and standards applicable to IROFS</p>
		<p>Section 3.1 provides the design details of the facility structures.</p>
		<p>Sections 3.2 and 3.3 describe the seismic qualification of equipment and components</p>
<p>§70.65 (b)(5) A description of the team, qualifications, and the methods used to perform the integrated safety analysis;</p>	<p>NUREG-1718, Section 5.4.3.2.B.iv</p>	<p>The ISA team is described in Section 5.2</p>
	<p>NUREG-1718, Section 5.4.3.2.B.v, and 10.4.3.C.ii.c</p>	<p>The ISA methodology is described in Section 5.1.</p>

the IROFS. Application of codes and standards provides assurance that controls utilized to implement the single failure criterion or double contingency principle are sufficiently reliable.

#### Application of Management Measures

The fourth design criterion, application of management measures, is particularly important in the context of IROFS failure detection. (see the MFFF License Application Chapter 6 and the MPQAP) IROFS failure detection is meant to include detection of IROFS failures and repair of the IROFS or the process is shutdown. As described in NUREG 1718, *Standard Review Plan for the Review of An Application for a Mixed Oxide (MOX) Fuel Fabrication Facility*, U.S. Nuclear Regulatory Commission, August 2000, IROFS failure detection can significantly reduce the likelihood of an accident scenario. For an accident scenario to proceed to completion, failure of one IROFS must occur, its failure must go undetected, and a second IROFS must fail.

Management measures are applied to the identified IROFS to ensure that they are reliable and available on demand. The MPQAP specifically describes the QA requirements, implementing procedural controls, and documentation requirements to address management measures as described in NUREG-1718. The set of applied management measures consists of applicable elements of the following management measures programs: quality assurance, configuration management, maintenance, training and qualification of plant personnel, plant procedures, audits and assessments, incident investigations, and records management.

Management measures are assigned based on the following types of IROFS classifications and the risk reduction level attributed to that particular IROFS:

- Passive Engineered Controls (PEC) – A device that uses only fixed physical design features to maintain safe process conditions without any required human action
- Active Engineered Controls (AEC) – A physical device that uses active sensors, electrical components, or moving parts to maintain safe process conditions without any required human action
- Enhanced Administrative Controls (EAC) – A procedurally required or prohibited human action, combined with a physical device that alerts the operator that the action is needed to maintain safe process conditions, or otherwise adds substantial assurance of the required human performance (i.e., augmented administrative control)
- Administrative Controls (AC) – A procedural human action that is prohibited or required to maintain safe process conditions (i.e., a simple administrative control).

The specific elements of the various management measures programs assigned to each IROFS classification are provided in Table 5.1-5. This table illustrates how the various management measures elements apply to the different IROFS classifications. For the enhanced administrative controls (EAC), the specific management measures for the physical device are covered under the active engineered controls (AEC) classification.

The following information provides a brief overview of the MOX management measures programs.

that of the corrective action process. Upon completion, a report on the incident and its investigation is made to the production manager, who initiates appropriate action(s), if determined necessary.

**Records Management** – MOX records are managed in accordance with the records management program under the requirements of the MPQAP. Records management program procedures have been established to address the receipt, processing, indexing, filing, storage, access control, preservation, retrieval, correction, and retention of QA records developed or received by the MOX project.

Management measures are further described in the MPQAP.

Effective application of these well defined qualitative criteria will ensure that event sequences are highly unlikely. The application of the single failure criterion or double contingency principle and IROFS failure detection ensure that multiple undetected failures are required for an accident sequence to proceed to conclusion. Application of appropriate codes and standards and an NQA-1 QA program ensure that IROFS will be designed, operated, and maintained in a reliable manner. The application of these qualitative design criteria ensure that adequate risk reduction is achieved to satisfy the requirements of 10 CFR §70.6

#### IROFS Reliability and Availability

Implementation of 10 CFR 50 Appendix B, NQA-1 and commitments to industry codes and standards provide confidence that safety system and component failure rates are unlikely to fail. To ensure that the IROFS meet this criterion, the following qualities of IROFS are shown in process safety documents (as appropriate):

- Safety function: the credited safety function of each IROFS is stated in the safety evaluation with a description of the controlled safety parameter.
- Quality classification: IROFS are classified to the highest level of quality, i.e., a quality classification of QL-1.
- Operating range and limits: the functional range of the IROFS is ensured to encompass both the normal operating range and the safety limit with an acceptable sensitivity over this full range.
- Emergency capabilities: operational requirements for an IROFS under emergency conditions (e.g., loss of power, etc.) is identified and demonstrated to be implemented in the design.
- Testing and maintenance requirements: testing and maintenance requirements are specified for each IROFS including a description of the means to detect failures, if available, and the applied management measures.
- Environmental design factors: environmental design characteristics necessary to ensure the IROFS remains available and reliable to perform its safety function are identified for each IROFS. These characteristics account for both short-term and long-term exposures to environmental conditions potentially detrimental to the operation of an IROFS (such as long-term chemical degradation impacts or short-term temperature transient impacts).

scenario and the IROFS required to implement the safety strategy. A description of each IROFS is included to show that the IROFS is capable of reliably performing its safety function. The safety function of the IROFS is identified together with the associated parameters, set points, justification for satisfying the single failure criteria, environmental qualification, failure modes, failure detection, and operating and surveillance requirements. Codes and standards, QA requirements and management measures applicable to the IROFS are described. A summary of the analyses demonstrating that the IROFS can perform the assigned safety function is provided.

The NSE contains a hazard assessment summary that identifies the applicable PHA and PrHA events for each event group being evaluated. Based on a review of the applicable PHA and PrHA events, the hazard assessment summary defines the NSE event groups to be evaluated.

The NSE events defined by the hazards assessment summary have been evaluated, with a list of credited IROFS and defense-in-depth features. A general description of each NSE event provides the causes of the event and the event location. The description includes a summary of process operations, sequence of events or event phenomena, as necessary to fully understand the event. The unmitigated consequences are provided for each receptor. The safety strategy is identified for each event, providing the basis for the selection of IROFS. Failure detection methods are identified for each of the cited IROFS. Defense-in-depth features that limit the challenges to these IROFS are also described. A summary is provided that includes how the performance requirements of 10 CFR §70.61 are met with the application of the identified IROFS.

The NSE identifies any specific operator actions required to implement the administrative control, the conditions related to the action, and any additional instrumentation and controls required to effectively perform the action.

Nuclear safety during design and operation is ensured for the MFFF through design and administrative practices. MFFF design and safety features are documented and controlled through the implementation of a rigorous configuration management program. Nuclear safety calculations and NSEs are maintained up-to-date and consistent with existing facility process and design features and administrative practices. Changes to these documents are controlled in accordance with the design change control and configuration management programs (see the MFFF License Application Chapter 6 and MPQAP)

#### **5.1.2.7.2 Nuclear Criticality Safety Evaluations**

Operations with fissionable materials at the MFFF introduce risks of a criticality accident. Criticality safety must be ensured through design and administrative practices. Criticality safety is included in the ISA through the PrHAs described in Section 5.1.2.1. NCSEs were performed to develop and document the safety basis for facility operations relating to the criticality events identified in the PrHAs. NCSEs are the main source of information demonstrating the adequacy of criticality controls and the effectiveness of administrative practices.

Criticality analysis design methods require a high level of validation. Criticality analysis methods used in MFFF design activities and facility safety programs comply with the technical guidance of ANSI/ANS-8.1-1983 (R1988), *Nuclear Criticality Safety in Operations with*

- The passively controlled equipment has management measures to ensure that the configuration is controlled and unchanging under the facility's configuration management program (see MPQAP).

For other units for which potential events are credible, the criteria for judging events highly unlikely are as follows:

- At least two independent robust (that is, unlikely to fail) controls are provided.
- Active or passive engineered controls are unlikely to fail. This determination was based on consideration of all applicable "available and reliable" qualities per NUREG-1718; also the controls are identified as IROFS.
- Administrative controls are robust and unlikely to fail. This determination was based on consideration of all applicable "available and reliable" qualities per NUREG-1718; also administrative controls are simple and unambiguous.

For each independent and unlikely to fail control relied on for compliance with the double contingency principle, one of the following additional measures are utilized to ensure that the associated event sequences are highly unlikely to occur:

- A means to detect a failure of the control on a period (for example, of one month or less) is provided, as justified in the NCSEs, or
- A safety margin is shown that demonstrates that multiple (three or more) failures of each independent control (i.e., IROFS) does not result in a loss of subcriticality, or
- Other measure(s), with justification.

The rationale for demonstrating an event is highly unlikely was provided in the NCSEs.

An approved design configuration requires criticality safety design input. See Figure 5.1-3 for a diagram that illustrates an overview of the steps that are involved in developing an MFFF NCSE. During preliminary design, criticality safety calculations were performed to justify the preliminary design concept. These calculations assessed both the normal operating and assumed accident conditions. Where practical, criticality was precluded by demonstrating that the design was subcritical without the need to implement controls or by making appropriate design changes to render criticality not credible. In the cases where it was not practical to make criticality not credible, criticality control parameters were selected and limits on these parameters were established.

Criticality safety during design and operation is ensured for the MFFF through design and administrative practices. MFFF design and safety features are documented and controlled through the implementation of a rigorous configuration management program. Criticality safety calculations and NCSEs are maintained up-to-date and consistent with existing facility process and design features and administrative practices. Changes to these documents are controlled in accordance with the design change control and configuration management programs (see the MFFF License Application Chapter 6 and MPQAP).