Shaw | AREVA
MOX SERVICES, LLC

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, DC 20555

DCS-NRC-000255
13 October 2009

SUBJECT: Docket No. 070-03098
Shaw AREVA MOX Services Response to the Request for Additional Information Regarding Human Factors Engineering

REFERENCE: 1. Letter from Kevin Morrissey to Dealis Gwyn dated March 27, 2009 entitled "Request for Additional Information Regarding the Review of the Human Factors Engineering Information in the License Application and Integrated Safety Analysis Summary for the Mixed Oxide Fuel Fabrication Facility"

Shaw AREVA MOX Services hereby submits its responses (Enclosure 1) to the Request for Additional Information (RAI) contained in Reference 1.

Associated changes to the License Application are provided by separate submittal.

If you have any questions, please contact Dealis Gwyn, Licensing and Regulatory Compliance Manager, at (803) 819-2780.

Sincerely,

David Stinson
President and COO

NMSS01
NMSS

Enclosures:

(1) Response to Request for Additional Information Regarding the Review of the Human Factors Engineering

cc: (w/enclosures)

David Tiktinsky, USNRC/HQ
EDMS: Corresp\Outgoing\NRC\2009 NRC\DCS-NRC-000255

cc: (w/o enclosures)

Mike Brickey, MOX Services
Mostafa Dayani, NNSA/SRS
Carol R. Elliott, NNSA/SRS
Walter Elliott, MOX Services
Sam Glenn, NNSA/SRS
William Gloersen, USNRC/RII
Dealis Gwyn, MOX Services
William Hennessy, MOX Services
Jean-Michel Marin, MOX Services
Kevin Morrissey, USNRC/HQ
Deborah Seymour, USNRC/RII
Donald Silverman, Esq., ML&B LL

Enclosure 1

Response to Request for Additional Information Regarding the Review of Human Factors Engineering

NRC HFE RAI RESPONSES

Human Factors Engineering (HFE) Planning

Section 12.4.3.B.i of NUREG-1718 states that the applicant's approach for planning HFE design review should include identification of appropriate goals and scope to ensure that HFE practices and guidelines are implemented during design, construction, and operation of the facility. The applicant's HFE planning activities are described in Section 12.2.1 of the license application (LA), the Human Factors Engineering Program Plan (HEPP), and the Human Factors Engineering Implementation Plan (HEIP).

HFE – 1 Scope of HFE Activities

HEPP Section 1.1 provides for application of HFE in design, construction, test and evaluation, startup, and operation of the Mixed Oxide Fuel Fabrication Facility (MFFF). Section 1.3 states that the HFE program is focused on human-system integration (HSI) vis-à-vis engineering and administrative items relied on for safety (IROFS) and that it is only applicable to integrated safety analysis (ISA)-identified IROFS functions. Section 1.4 and Section 1.5 also state that the HEPP is only applicable to ISA-identified IROFS functions. However, another constraint in Section 1.5 states that HFE is also applied to eliminate or reduce the possibilities of challenges to the performance capability of operators or maintainers. Title 10 of the *Code of Federal Regulations* (10 CFR) 70.64, Section (b)(2) states that facility and system design and facility layout must be based on defense-in-depth practices. The design must incorporate, to the extent practicable features that enhance safety by reducing challenges to IROFS. Defense-in-depth practices and their relation to safety are further described in footnote 1 of the regulation. Chapter 12 of NUREG-1718 notes that HFE is to be applied to personnel activities identified as safety significant consistent with the ISA. This is noted to include activities identified as IROFS and personnel activities that support safety. Defense-in-depth items are identified in the ISA as supporting safety and are required by 10 CFR 70.64, which notes that they enhance safety. Please clarify that the scope for the HEPP and HEIP includes the controls, displays, and alarms associated with both administrative and the engineering IROFS, the defense-in-depth items, and their related control rooms.

HFE – 1 Response

MOX Services has revised the LA to reflect that the HFE scope includes a graded approach to Defense-in-Depth items as defined in the HEPP and HFIP. The HEPP and HFIP have also been appropriately revised.

HFE – 2 Analysis Personnel Actions

Section 4 of the HEIP indicates that a subset of events is analyzed within the ISA that may involve personnel actions that have the potential to result in negative actions. Please clarify what is meant by negative actions. It also states that HFE evaluations performed for the ISA include evaluating errors of commission in addition to omission. How is the evaluation of errors of commission accomplished?

Please clarify what is meant by negative actions.

HFE – 2 Response

The HFIP has been clarified to replace "negative actions" with "adverse consequences".

The evaluation of "errors of commission" is not yet widely developed in the HFE research literature regarding the case before the design validation phase. There are no satisfactory models developed at this time. Our HFE evaluation is trying to determine what the operator may do before it is actually done, by asking questions during table top task analysis. The operator either can accomplish the action correctly without error or incorrectly by committing error(s). There are two places in design where the evaluations of "errors of commission" can be accomplished. One is during the task analysis, when questions are asked about operator actions (IROFS Administrative Controls). For example, an operator must verify "A," an error of commission occurs if the operator misreads "A." Then the question is asked on how to prevent misreading "A," in the first instance? For another example, there is an IROFS Administrative Control requiring the operator to analyze solution samples before transferring a solution to a tank, how is the operator stopped from transferring the solution before results are back, considering this is an administrative control? The other place in design that allows the opportunity to evaluate errors of commission is during the validation phase, where the operator is observed performing the credited administrative control.

The focus is to ensure the operator correctly follows an IROFS procedure. Understanding the procedure will be necessary and the controls and displays (HMI) must be provided, where necessary. The HFDG Attachment E a substantial amount of information regarding information processing and human error. The material captures the work of recognized researchers in the field of human error and may certainly be used as a guide during the task analysis and validation.

HFE – 3 HEIP Level of Specificity

Much of the HEIP is written with the following characteristics:

- The guidance is very general. For example, it states that when necessary, the human factors engineering (HFE) team should perform studies to examine special features of the system design to support engineering. How does the team know when it is necessary and what studies will be performed?

- The guidance does not commit to a specific methodology.
- The guidance is derived from NUREG-0711 with little modification. For example, almost the entire validation and verification (V&V) section is close to a restatement of the NUREG-0711 review criteria. NUREG-0711 provides criteria for reviewing an applicant's HFE methodology and HFE products. While there are some exceptions, it does not serve as stand-alone executable guidance by design personnel.

Is more detailed, specific guidance available to the HFE design team for performing HFE activities?

HFE – 3 Response

Yes, the HFE Team has completed the HFE Design Guidelines (HFDG) document which is intended to provide engineers guidance regarding standard HFE principles, practices, and guidance and applying HFE to their system design, in particular, with respect to IROFS tasking and interaction with IROFS equipment. For example, the Operations Group uses a RAMI (Reliability, Availability, Maintenance, and Inspection) checklist incorporating HFE principles and practices as checkpoints. The HFE team has reviewed the project generic RAMI checklist and provided HFE feedback to Operations, which was incorporated in the revised RAMI checklist.

The HFE program has purposefully left open the methodology, as was declared in the HFIP introduction. The HFE methodology (e.g., table top analysis, interviews, checklists, independent studies, reference plant comparisons, observations and/or participation in demonstrations, use of mockups and use of part-task simulations) are supplemented by the HFE Design Guidance. Applying the HFE Design Guidelines in support of the HFE methodology will help assure the successful integration of Operators and Maintainers in the MFFF design. The guide covers a broad range of human factors topics that pertain to automation, maintenance, human interface, workplace design, documentation, system security, safety, the environment, and anthropometry. The intended use of the MFFF HFDG is to assist meeting a need to ensure inclusion of Human System Interface in future MFFF designs, modifications, procurements, and retrofitting. The HFDG will be made available for staff review. Additionally, HFE is conducting training on using the HFDG for HFE points-of-contact among the functional engineering groups and the HFE team to ensure there is an awareness of this document and to provide a guidance application multiplier for the HFE effort..

It should also be noted that the MFFF design is based on reference plant designs and the detailed reference plant designs are modified as necessary to meet US safety requirements and cultural calibration.

Methodology will be discussed in the Summary Reports concluding each phase of our HFE program. MOX Services feels this is a good approach, with the HFE team in a position to study the next phase of design and agree on a specific method for accomplishing HFE during that phase. This also gives us more time to discuss the possible methods to be employed and select one that is appropriate to the task at hand. Most of the methodology concerned with HFE is done via table top analyses, reviewing drawings, and talking to system Responsible Engineers to understand better their systems, and conducting group meetings with representatives from the various design groups and other interested persons.

The HFE team will know studies may be needed when questions are being asked and there appear no data available to make a decision. An example of an HFE study that is recognized as needing accomplishment is to identify the areas in the control rooms and determine console (workstation) space availability. This study initially could be accomplished using pencil and paper and progressing to computer aided design. Alternatively, the HFE Team has examined (studied) an existing model of workstations used by another group at the Savannah River Site (SRS), for possible use at the MFFF. Another study is the estimated time requirement for accomplishing an Administrative Control to demonstrate that the operator will not be able to do the required task in the time required. The result of this study was entered into the HED system. Other studies may be available at the request of the Responsible Engineer's, Operations group, Manufacturing Group, or Software Design Group.

Issue Tracking

Section 12.4.3.B.iii of NUREG-1718 states that an applicant's approach for planning HFE design review should include an HFE team that attains the HFE goals and scope through established processes and procedures and that tracks HFE issues. The applicant's HFE issue tracking is described in the LA, Section 12.2.4 and in the HEPP and HEIP.

HFE – 4 Tracking System Methodology

The HEIP discusses tracking of HFE issues. Please clarify the use of the MOX Project Action Tracking System and the Action Tracking System for HFE issue tracking. Please provide additional information on the methodology, documentation, and responsibilities of system users.

HFE – 4 Response

Management Directive 006 stipulates the use of MOX Action Suite for Action Tracking purposes. This is a computer based action tracking program. Project personnel currently are being trained on the use of Action Suite. HFE Team has put into the MOX Action Tracker a category for HFE and a subcategory for HEDs. Project Procedure PP9-28, Human Engineering Discrepancy (HED) will clearly identify the HED process and who uses it, including a flow chart for ease of use. HEDs are tracked to resolution.

Operating Experience

Section 12.4.3.C of NUREG-1718 states that an applicant should identify safety-related HFE events or potential events that have occurred in existing facilities that are similar to the proposed facility. The applicant should:

- Review the HFE-related events or potential events for relevance,
- Analyze the HSI technology employed for the relevant HFE events or potential events, and
- Conduct (or reviewed existing) operator interviews and surveys on the HSI technology for relevant HFE events or potential events.

Use of operating experience is described in the LA, Section 12.5 and in the HEPP and HEIP.

HFE – 5 Tracking of MELOX Lessons Learned

The report "MOX Processing Area Lessons Learned from Experience at MELOX, Overall Summary," dated September 29, 2006, provides a list of recommended modifications to the MFFF based on discussions with the MELOX operator. Please provide a discussion of how the implementation status of these recommendations is being tracked and a reference to where that status can be reviewed by the NRC.

HFE – 5 Response

The MFFF Project also has a dedicated Lessons Learned Program (Project Procedure 1-7). These "lessons learned" are reviewed by a Lessons Learned Review Committee (LLRC). The method used in processing "lessons learned" includes: received lessons learned are categorized first by whether each lesson learned applies to the MFFF; second which group should receive the lessons learned (e.g., engineering group, operations group, or quality group), and then decide should the lesson learned be sent out as "Response Required" or "For Information Only." Lessons learned from the reference plants are also reviewed by the LLRC for determination of who should receive the lessons learned for review. Not only are the lessons learned sent out via the MOX Manager "representative" for distribution, but lessons learned are made available for review by all project personnel. Lessons learned, including past and present reference plant lessons learned transferable to MFFF, are tracked in a project data base managed by the Lessons Learned Review Committee (LLRC).

The Lessons Learned procedure and the Lessons Learned database containing all of the Reference Plants are available onsite. Note, also, this information is provided in the newly written Operating Experience Review (OER) that is also available onsite. The OER also cites the source locations for all the reference plant lessons learned. Process specific lessons learned documentation from the French reference plants is on file within the MOX Project and where appropriate the lessons learned have been reviewed by the RE's and Leads and incorporated into the design of the MFFF. Most of the lessons learned are mechanical engineering lessons, but there are operator lessons learned cited, as well, derived from reference plant(s) operator interviews.

The implementation status of the items identified in "MOX Processing Area Lessons Learned from Experience at MELOX" is found in the Lessons Learned database.

HFE – 6 Operating Experience Review (OER) for HSI Technology

The OER process addresses predecessor plant experience; however, it appears to be missing reviews of the reactor operating experience for planned HSIs in MFFF. Will the MFFF use the same HSIs and the reference plants? If yes, discuss the applicability and advisability of using old technology. If not, what aspects will be different and what are the plans for conducting OER of HSI technologies planned for use at the MFFF?

HFE – 6 Response

The MFFF will generally use the same HSI as the reference facility. The MOX digital computers and workstation display monitors that present the HSI to the operators has been updated, using a different product and a different operating system. However, the reference plant HSI is replicated as much as practicable. For example, older CRT displays are replaced with flat panel LCD displays and the Sun Micro workstations are replaced with PC workstations. The information that will be provided to the operators at the PC workstations is derived directly from the workstation displays in use in the reference facilities. Regarding local HSI, e.g., maintenance at the glovebox, the MFFF will use similar but updated technology. The U.S. MFFF design is based on maximizing the use of proven practices. HSIs, are modified when necessary due to specific U.S. MFFF requirements and lessons learned from operation of the reference plants and to render the displays in English.

Refer to response to RAI #5 for a discussion of OER. The LLRC reviews lessons learned experiences and should pass along HSI related materials to the HFE team for review.

Function Allocation

Section 12.4.3.D.i of NUREG-1718 states that the functional allocation analysis should be based on the OER. Personnel activities are functionally allocated to take advantage of human strengths and to avoid demands that are not compatible with human capabilities. The applicant's function allocation analysis is described in the LA, Section 12.3 and in the HEPP and HEIP.

HFE – 7 Function Allocation Methodology

The HEIP indicates that function allocation will be based on HFE principles using a structured well-documented methodology that seeks to provide personnel with logical, coherent, meaningful tasks. What methodology will be used to accomplish this? Given that the MFFF operations are highly automated, how will the plant design and allocation of functions support operators to maintain operator vigilance and provide acceptable workload levels, i.e., to minimize periods of operator underload [sic] and overload?

HFE – 7 Response

The function allocation methodology is found in the Integrated Safety Analysis (ISA). The ISA demonstrates that the IROFS are adequate to perform their intended safety functions when necessary, including the allocated Administrative Controls.

During the PrHAs, the emphasis of the ISA team was to identify passive and active engineered controls (PEC & AEC) to credit as IROFS to prevent event sequences from exceeding the performance requirements of 10CFR70.61 (as described in Section 5.1.2.7 of the ISA Summary). However, when the ISA team could not credit a PEC or AEC and instead credited administrative controls, the team would consider the following:

- Did the representatives of operations (former or current La Hague/MELOX personnel having direct MOX operational experience) consider performing the administrative control viable?
- Were the tasks associated with performing the administrative control known or understood, in other words was the administrative control logical and coherent?
- How complex were the tasks?
- Was there more than one means to respond and meet/satisfy the safety function?
- Were all the tools necessary for operations to perform the task(s) available and did they need to be IROFS (i.e., would this be an enhanced administrative control, EAC, or a simplified administrative control, AC)?
- Was there sufficient time for operations to perform the task(s)?
- Were there sufficient personnel available to perform the task(s)?
- How frequent might the operation be required?

The Operations group is involved in the evaluation of IROFS administrative controls. This evaluation included the examination of human actions and the availability of engineered features and the verification that the allocation of functions did closely follow or match the "Reference Facilities." In the PrHA environment there was a reliance on the response from the process group and Operations to "what did they do at La Hague/MELOX?" to resolve the issue.

The MFFF plant operators are not isolated from the process operation. Operators are provided with written engineered documentation that follows the process operation. The automation periodically requires input from the operators for verification of process conditions, feed stock information, manually enter or record data and other activities that require that the operator be involved and attentive.

Functions that are identified as IROFS and allocated to operators will be subject to task analysis to identify the required operator actions and the HSI associated with the actions. The facility is designed to accommodate the operator in accordance with the HFE design guidelines and the design will be reviewed by the HFE team to verify that it is appropriate for the operator.

HFE will be focused on the Operator tasks and ensuring the tasks are within the capabilities of the Operator (cognitive and physical). In this way, the operator can be brought right into the center of the process, and actually be the most central function. For example, on the operators workstations there will be "Operator Call," signals requiring operator input. The right information must be obtained and inserted into the computer. The operator is given a decisive role in determining the production function and the production results in terms of both quality and speed.

It is anticipated that when developing the MFFF operating and maintenance procedures, the reference plants will provide much insight into tasking levels for the operators.

HFE – 8 Basis of Automation

The functional allocation element in the HFE plans and the document "Basis of Design for I&C" state that the base design goal is to automate MFFF operations as much as possible. They also state that this reduces the chances and consequences of error or incident. Please provide the basis for this reduction in the: chances of error, chances of incident, consequences of error and consequences of incidents.

HFE – 8 Response

An automated control system strategy requires that every manufacturing or process operation is understood and analyzed into its fundamental steps. The relation between each elementary step is evaluated to understand the process dynamics. This takes place in the Functional Analysis. Once this understanding is achieved an appropriate control algorithm for each step is developed. These control algorithms are then implemented in the control machinery. The control machinery for the MFFF shall generally be built around Programmable Logic Controllers (PLC) that are in turn, built around software controlled microprocessors. The control algorithms are coded into the appropriate software, which is loaded into the controllers. In the automated system manufacturing and processing operations are carried out in strict accordance with a set of planned steps and procedures that have been programmed into the automatic controllers. In other words, the automation will operate the process or perform manufacturing actions exactly as instructed in the engineered specifications, i.e., the control program. The results of each step or the conditions following the completion of each procedure are monitored and measured. The results are compared with established criteria and when the automation detects a deviation from a process setpoint or other required condition the automation will rapidly and automatically initiate the mitigating action required by process engineering. The human operators are notified and the automatic controls take steps to put the process in a planned safe state that is appropriate for the identified condition.

This control technique provides a very consistent product with minimum variability. It provides the earliest identification and notification of products that are not within specification and prevents any substandard product from being used in the next process. At the same time both the chances and the consequences of an error or incident are greatly reduced, because the operators follow an exact engineered sequence of operations and pre-planed responses result in early mitigation action which minimizes consequences. This is the direct experience of automation at the reference plants and modern industrial processes worldwide.

The ISA does consider and examine failures of automation but does not credit any human action. The reason is because the safety systems are designed using IEEE 603 (Section 5 and Section 5.8.2) requirements. In addition, IEEE 338 (periodic surveillance testing) is applied to the MFFF systems to confirm that the safety system is performing as required..

Task Analysis

Section 12.4.3.D.ii of NUREG-1718 states that task analysis includes:

- the task analysis scope
- identification and analysis of critical tasks
- detailed description of personnel demands (e.g., input, processing, and output)
- iterative nature of the analysis
- incorporation of job design issues

The task analysis should address each operating mode for each personnel activity (e.g., startup, normal operations, emergency operations, and shutdown) and its results should support the functional allocation. The applicant's task analysis is described in the LA, Section 12.4 and in the HEPP and HEIP.

HFE – 9 Task Analysis Scope

The task analysis scope includes administrative IROFS and personnel activities that support safety. Does this include the range of human actions discussed in the request for additional information (RAI) number HFE - 1? The plans also indicate that task analysis addresses each operating mode, e.g., startup, normal operations, emergency operations, and shutdown. Is the scope of human actions subject to tasks analysis in these analyses limited to administrative IROFS and personnel activities that support safety?

HFE – 9 Response

As noted in the response to RAI-1, MOX Services will evaluate HFE, including Task Analysis, on Defense-in-Depth items in a graded manner as defined in the HEPP and HFIP.

HSI Design

Section 12.4.3.E of NUREG-1718 states the following:

- The HSI design should incorporate the functional allocation analysis and task analysis into the detailed design of safety-significant HSI components (e.g., alarms, displays, controls, and operator aids) through the systematic application of HFE (HSI design inputs).
- The HSI design should include the overall work environment, the work space layout (e.g., control room and remote shutdown facility layouts), the control panel and console design, the control and display device layout, and information and control interface design details (HSI design scope).
- The HSI design process should ensure the application of HFE to the HSI required to perform personnel activities (HSI design process).
- The HSI design process should exclude the development of extraneous controls and displays (extraneous HSIs).
- The HSI design documentation should include a complete HSI inventory and the basis for the HSI characterization (HSI design documentation).

The applicant's HSI design is described in the LA, Section 12.6 and in the HEPP and HEIP.

HFE – 10 HSI Design Scope

If the HSI design process is only applied to HSIs not carried over from the reference facility and those that have been substantially changed, please indicate how consistency between the new and old HSIs is assured?

HFE – 10 Response

Software driven HSI, i.e., the operator's computer workstations, are all developed using common design rules which are derived from the reference facilities. Any HSI display not derived directly from the reference facility interface will therefore have the same attributes as the rest of the HSIs. Hardware HSIs are developed using the HF design standards developed for the project and reviewed by using the MOX human factors engineering design guide and NUREG 0700. In addition, "cultural calibration" is applied to the reference facility interfaces during transfer to the MFFF.

HFE – 11 HSI Design Style Guide

HSI design is addressed in LA Section 12.6 and in HEIP Section 8.5. These sections indicate that prior to detailed design work, the MFFF HFE team will compose and provide an appropriate "guidelines document" or "style guide" limited to suitability for the evaluation of IROFS equipment that have human interfacing. Does this mean the style guide will only be used for evaluation? Why is the scope limited to IROFS equipment? If limited as such, might that create inconsistencies in design between IROFS and non-IROFS HSIs? What is the general content of the style guide and how will it be maintained? Will it contain procedures for its use?

HFE – 11 Response

Does this mean the style guide will only be used for evaluation?

No. It also will be used to guide the Human Machine Interface (HMI) design development. HFIP section 8.5 was clarified to remove "style guide limited to suitability," and insert "for design guidance and evaluation of IROFS equipment having human interfacing." Note: the HFE Team decided to provide a Human Factors Design Guide (HFDG), not a "style guide."

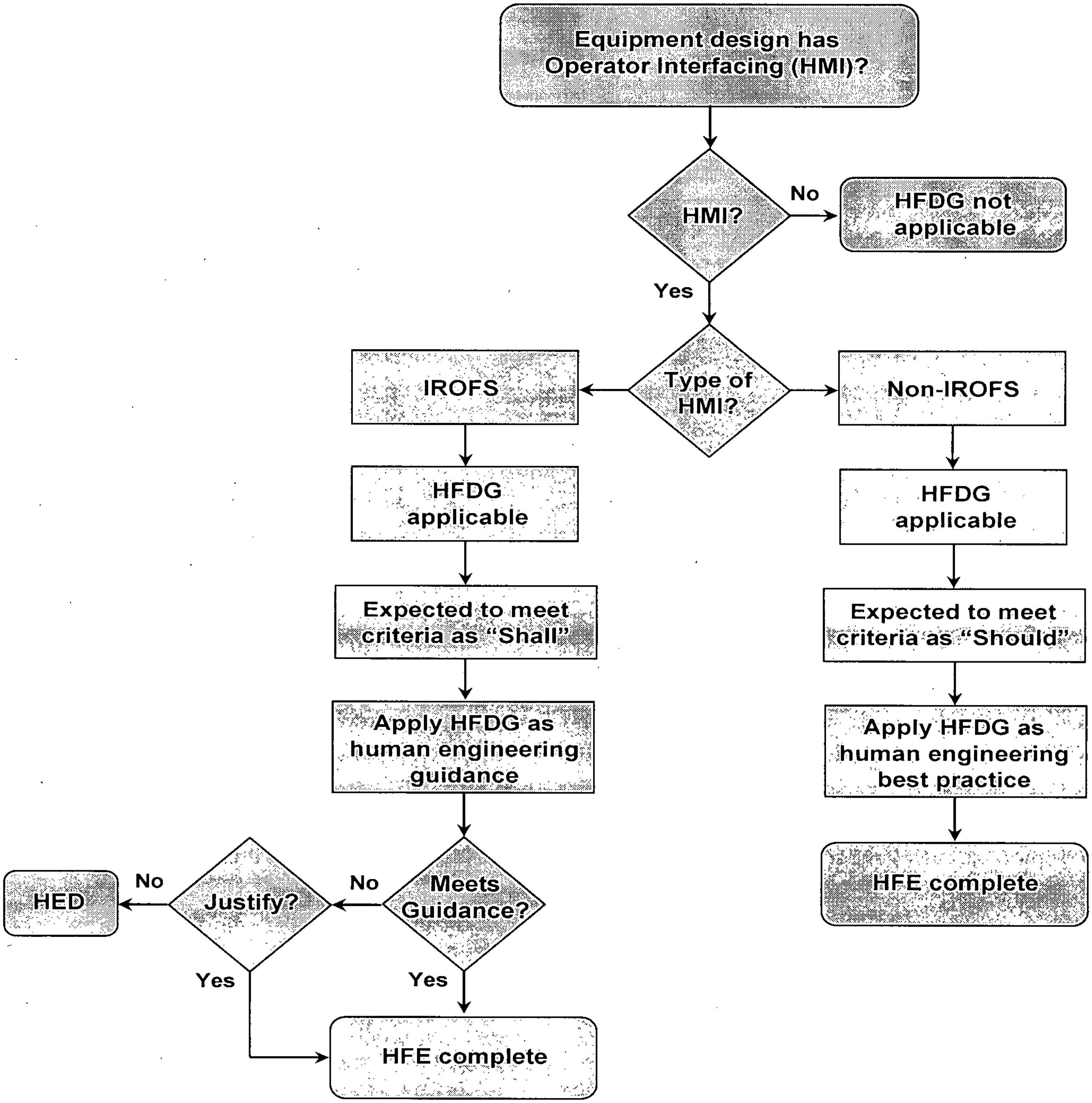
Why is the scope limited to IROFS equipment?

The MFFF project has committed to applying HFE principles to HSI associated with operator actions interfacing with IROFS. HFE principles will be applied to Defense-in-Depth items as defined in the HEPP and HFIP. There is no commitment to apply the HFE program to other non-IROFS HSIs. The current design of non-IROFS equipment and systems has been on-going utilizing the reference plant design concepts and the HFDG will not be utilized as retroactive design review. The HFDG is now issued and training on the use will be performed in the near future. The HFDG will be utilized as "good engineering practices" where appropriate for non-IROFS equipment and systems.

The following flow chart figure is explained in the HFDG and training teaches the attendees how the flow chart works. Our utility document, HFDG, provides a MFFF oriented easy-to-use source of human factors guidance. The MFFF HFDG presents human factors design guidance that **shall** apply to IROFS and **should** apply to non-IROFS MFFF facilities, systems, processes, and equipment managed, operated, and maintained by the MFFF operators. If IROFS having HMI are present, the HFDG is applied as a "shall" document; this agrees with the figure. If non-IROFS having HMI are present the HFDG is applied as a "should" document. The reason for this is to keep consistency in the HFE design across the plant and to further reduce human error. The non-IROFS "should," applies to engineering changes or modification affecting HMI, and for new equipment. The control rooms are included in the non-IROFS side of the chart, except for the few equipment items that are IROFS in the control room, for example the annunciator panels, or the safety panels that "shall" meet the HFDGs. The figure is viewed as accommodating the D-in-D, the control rooms and the other non-IROFS modified or new equipment and thus does not need changing.

Since the same design practices shall generally be applied to those instrument and control systems that are not classified as IROFS, inconsistencies in design between IROFS and non-IROFS HSIs should not be created.

MOX HFE Team is providing a human factors engineering design guideline (HFDG), not a style guide, and it is consistent with NUREG 0700 Rev 2. This utility document will provide a MFFF oriented easy-to-use resource for human factors guidance. The guide covers a broad range of human factors topics that pertain to automation, maintenance, human-machine interface, workplace design, documentation, system security, safety, the environment, and anthropometry. The HFDG will be subject to updates and revision as the need arises. Because the human factors design guide is an approved project document it is revised, reviewed, approved and maintained in accordance with approved project records management procedures. The flowchart below shows the procedure for using the HFDG, and is included in the HFDG:


Equipment design has Operator Interfacing (HMI)?
HMI?
No
HFDG not applicable
Yes
Type of HMI?
IROFS
Non-IROFS
HFDG applicable
HFDG applicable
Expected to meet criteria as "Shall"
Expected to meet criteria as "Should"
Apply HFDG as human engineering guidance
Apply HFDG as human engineering best practice
HFE complete
Meets Guidance?
No
Justify?
No
HED
Yes
Yes
HFE complete

HFE – 12 Review of the Style Guide

Will the style guide(s) be consistent with NUREG 0700? If not, please justify an acceptable alternative.

HFE – 12 Response

Yes. MOX HFE Team is providing a human factors engineering design guideline (HFDG), not a style guide, and it is consistent with NUREG 0700 Rev 2.

HFE – 13 Designs for Error Tolerance

What approaches will be used in the design of operator interfaces to minimize operator error and provide for error detection and recovery?

HFE – 13 Response

The operating experience of the reference plants in France provided the basis for the designs of the operator interface. The results of the OER were included in the design of the operator interfaces. The MOX Lessons Learned program continues to supply information that may go into making HMI decisions. Engineering application of the MOX HFE design guidelines helps focus attention on the HMI. The design of operator interfaces using shapes, color-coding, and labeling all contribute to minimizing human error. HFE reviews IROFS drawings with HMI for discrepancies with NUREG 0700, the HFDG, or other appropriate HFE references (for example, MIL-STD-1472F if the HMI of interest is not covered under NUREG 0700). There are lockout and reset mechanisms that prohibit continuation of a “faulted” process until all underlying causes have been discovered and corrected, particularly for IROFS safety panels. Other positive interlocks include redundant operator interfaces in the Emergency Control Room (ECR) such as provisioning two reset control buttons that the operator must push simultaneously, to reset a safety function. This is designed to mitigate the chance that operators return a system to its normal state from the emergency state before all faults are corrected. These all represent design approaches to operate the MFFF safely and provide for operator safety.

HFE – 14 Alarms for Automation Failure

If an automatic safety action fails and there is no automatic backup, is an alarm generated to signal operator action? For example, what happens if the automatic response that triggers a safety actuation warning fails? Is operator backup required and how is the operator notified of the need for action? Are these actions proceduralized?

HFE – 14 Response

The design of the MFFF must meet the criteria of IEEE 603, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations” and also must meet the Single Failure Criteria of IEEE 379, “Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems”. IEEE 603 requires that “...the power, instrumentation, and control portions of each safety system shall be comprised of more than one safety group of which any one safety group can accomplish the safety function..." For the MFFF, the safety function(s) are required to be carried out in spite of the failure of any single component within the structure, system, or in an associated system that supports its operation. This design requirement assures that for automatically executed safety functions there is always a "backup." Coincident failure of both channels is beyond the design basis. When an automated safety function is executed operator notification is provided at the operators' workstation.

Safety functions may be fully automated or may be manually executed. Where manual execution is required two channels of safety alarms are normally provided to notify the operator that a manual safety action is required. Manual responses to safety alarms are proceduralized and the procedures are classified as Administrative Controls (IROFS). In the case where a single alarm channel is provided the safety analysis has shown that the alarm function is redundant to a physical barrier or constraint that would prevent or mitigate the safety event.

Control actions related to prevention of adverse incidents (e.g., criticality or loss of confinement) are implemented through dual, redundant Safety Programmable Logic Controllers (SPLCs). These SPLCs are independent of the NCS (Normal Control System). As much as practical, the process information necessary for the control functions is acquired by two separate and independent sensors. Except in specific cases (for example, scales), criticality safety control sensors are not to be the same as normal control sensors. The SPLCs override the instructions of the NPLC and inform the NPLC of SPLC actions that place the normal control system into frozen mode if an incident is detected. In case of loss of power, the system fails in a safe mode. Sensors and actuation circuits feed information to the SPLCs.

HFE – 15 Alarm/warning Selection Criteria

HEIP Section 7.4.2 (p.95) states that one of the alarm/warning selection criteria is "[t]he operator's normal surveillance activities cannot be relied on to alert them to the condition." Relying on surveillance may delay the detection of important conditions and may result in those conditions being overlooked altogether. Please clarify why important conditions should not have an alarm or warning to ensure that the operators are aware of them.

HFE – 15 Response

Important conditions are identified for alarms from the ISA process. The entire section 7.4.2 Action Criteria (now appearing on HFIP page 86, revision 0) has been clarified as follows:

"The ISA process identifies event sequences and conditions that have safety consequences and requires the design to incorporate IROFS to prevent or mitigate the identified event sequences and conditions having safety consequences. Process alarms are selected when an event sequence requires an immediate operator action to initiate a safety function."

HFE – 16 Operator Action Criteria for Alarms

HEIP Section 7 states that alarm or warning conditions not within the operating responsibilities may be candidates for elimination or combination. What types of conditions degrade plant or HSI performance even if remedial actions are outside the operators responsibly? Are such conditions sent elsewhere, e.g., are lower level alarms sent to maintenance personnel?

HFE – 16 Response

This question refers to the HFIP, Section 7.4.4 Definition of Control Room Operator Responsibilities, "...It is also important to identify system or functions for which responsibility does not reside with the control room operators, since any existing alarms or warnings for these systems/functions may be candidates for elimination or combination." An example of a condition the control room operator will not have control over is a process room glovebox differential pressure alarm. The local operators respond to this alarm by evacuating the local area, but there is no immediate control room operator response, thus this alarm was removed from the control room, and kept at the local level. The control room operators will receive a warning display to alert them to the glovebox differential pressure alarm activation. Added this example to HFIP text.

HFE – 17 Alarm Reduction, Conditioning, and Processing

HEIP Section 7 discusses alarm conditioning to help prevent nuisance alarms. Mention is made of time delay and input logic. Can additional detail be provided as to how alarms will be conditioned and how the conditioning will prevent the elimination of true alarms? How is prioritization of alarms based on urgency of action determined?

HFE – 17 Response

Alarms may be conditioned by introducing a time delay between exceeding the setpoint and the actuation of the alarm. Such is the case with fan starts. The low pressure trip signal is delayed long enough to allow the fan to accelerate to its operating speed without generating spurious alarms. The appropriate time delay will be determined by calculation or system testing.

Process alarms require an operator response and therefore, alarms are treated "equally" regarding response by the operator. Warnings (provided on the operator's workstation) are prioritized. Process alarms are derived and determined from the ISA.

MFFF has a nominal amount of alarms compared to the NPP alarm system. MFFF alarms are individually hard-wired to an annunciator panel in the control room. Set points are calculated using ANSI/ISA 67.04.01 (Setpoints for Nuclear Safety-Related

Instrumentation), surveillances, periodic channel tests, and evaluating the performance of replacement materials, parts, and components will minimize the occurrence of nuisance alarms. The following steps can be employed to address nuisance alarms: 1) at the onset of a "nuisance" alarm, the control room should be calling for technical assistance to correct the problem, 2) training should support the handling of the nuisance alarm situation by instructing the operators that during a nuisance alarm occurrence the operators must pay additional attention to the alarm annunciator panel in case a new alarm is activated – the operators can not fall into the trap for ignoring the annunciator panels. Note that MFFF Operators can not re-set alarm setpoints.

MFFF operators generally will be afforded 2 hours for process alarm response; however, there will be some alarms requiring more urgent action. For example, the local glovebox differential alarms require an immediate operator response to evacuate the glovebox room. An "immediate" action alarm in the control room will be differentiated from the "2-hour response" by using a technique such as color coding and placement of the "immediate response alarm" on the annunciator. Each process also has its own Emergency Stop switch (both a physical workstation switch and a soft control switch in the process SCADA (screen). In addition, there will be a dedicated global Emergency Stop in each control room to simultaneously stop all processes that are associated with that control room. Each process alarm requires an operator response.

Current estimates of Control Room alarm numbers are:

- B-142 Control Room (Powders and Pellets) – 4 – 8 alarms
- B-319 Control Room (Alternate Utilities) – 74 alarms
- D-301 Control Room (Normal Utilities and Auxiliary Utilities, and Aqueous Polishing) – 100 alarms
- D-318 Control Room (Emergency, Train A) – 64 alarms
- D-319 Control Room (Emergency, Train B) – 64 alarms

Warnings are not IROFS and are presented on the SCADA screens, not on annunciator panels. Warnings may be accessed from any SCADA from any room. There are approximately non-IROFS 44,000. Estimates of warnings include

- Safety Alarm Warning: 11
- Safety Actuation Warnings: 800
- High Priority Warnings: 8,230
- Low Priority Warnings: 35,150

Warnings are predominantly notifications of equipment or component malfunctions that impact the ability of manufacture fuel and are expected to be infrequent.

HFE – 18 Higher-Level Alarms

Are there higher-level alarms/warnings, e.g., event alarms or system level that indicate the meaning of patterns of lower-level alarms/warnings? Such alarms help operators to quickly understand the "big picture" in situations were there are many lower-level alarms/warnings.

HFE – 18 Response

Process alarms are not prioritized. Process alarms are specifically called out by the ISA. They all require an operator action to complete a proceduralized safety function. The IROFS alarm must be "set" in order for Operators to be able to respond within 2-hours. The determination of the alarm setpoint also takes into account various factors such as: (1) transient volumes between a shutoff valve or pump and the tank in question and (2) instrument measurement uncertainties. There are three hierarchical categories of warning and these are found on HFIP revision 0, page 102:

- Safety Actuation Warning – Warnings associated with an automated engineered response to an abnormal or hazardous condition. The Safety PLC (safety controller) will automatically take direct corrective action (IROFS) and at the same time relay the actuation information to the normal controller (non-IROFS). The normal controller then generates and transmits the warning annunciation signal to the SCADA screen for operator notification. The process is frozen in a safe condition.

- High Priority Warning – High Priority Warnings are events corresponding to situations of less severity than an "Alarm". The warning signal indicates a compromised operation of the process machine GEPFs, i.e., Group of Elementary Process Functions, and timely operator action is required. The "High Priority Warning" is not an ISA IROFS function. However, it is important enough to warrant the operator's timely attention. The operator will need to investigate the fault cause and take the corrective action to clear the fault.

- Low Priority Warning – Low Priority Warnings are events compromising proper operation of the facility in terms of the process, for which delayed action by the operator is tolerable and which do not require stoppage of the machine. The "Low Priority Warning" is not an ISA IROFS function. The operator will need to investigate the cause first and take the corrective action.

At this time, there are no pattern alarms. The MFFF volume of alarms is considerably less than that found in the NPP by several orders of magnitude.

HFE – 19 User-Defined Alarms

The HEIP Section 7 indicates this capability will be available. How is this functionality implemented? Does this mean user-defined alarms? Can users reset setpoints or logic on nonuser- defined alarms?

HFE – 19 Response

There will be no user defined alarms originating from the ISA process. The Operator will not be able to change a calculated safety designed setpoint. The operator will be able to adjust setpoints associated with particular requirements of a given production run as provided by engineered instructions for the purposes of normal process control. This category of setpoints is variable and is different from the alarm setpoints, which are not variable and not adjustable.

HFE – 20 Alarm Management

HEIP Section 7, (p.106) suggests that all alarms don't need acknowledgement. Why is that?

HFE –20 Response

The requirement is to acknowledge an alarm, but in accordance with good human factors engineering, the operator should not be required to use two different controls to acknowledge a single alarm condition. All alarms and warnings require acknowledgement. NUREG 0700, section 4.3.7-4, additional information specifically says, "If alarm information is presented redundantly on tile and VDU displays, then alarm acknowledgement via one device (i.e., either the VDU or tile panel control station) should cause the redundant alarm to be automatically acknowledged on the other device."

HFE – 21 Use of Safety Injection [SI] Units in Displays

Section 8 indicates that HMI devices are calibrated in SI units in the English language. Is this appropriate for U.S. operators and maintainers?

HFE – 21 Response

The MFFF has committed to the use of the SI (System International) system of measurements. Early in the MFFF project discussions with operations managers of domestic commercial fuel fabrication facilities (Uranium operations) indicated that the use of SI was common. Many of the process control parameters, such as nuclear criticality control, Materials Control and Accountability (MC&A) are provided only in SI units. All process engineering calculations are performed in SI units. Converting between SI and US conventional units would create a significant source of operational errors, production errors and communication errors between operations and process engineering, all of which is best avoided by using a consistent system of measurement units.

MFFF Engineering Guideline 56-4, "Units of Measure and Conversion" defines the engineering units of measure to be utilized on design documents and equipment operating and performance requirements and establishes a standardized approach for operational display requirements (i.e., instrumentation and control displays and readouts). The Systême International d'Unités (SI) is used for all system and equipment parameters necessary to operate and maintain the MFFF.

HFE – 22 Color Coding on Maintenance and Mechanical Dismantling Displays

The "General Specification for Equipment Labeling..." in Section 43.0 specifies color codes (e.g., orange, purple, etc.) for electric cables, circuits, raceways, and electrical equipment. Will these colors also be used on screen displays for the same electric equipment or for other equipment powered from these electric supplies? If so, where will the guidelines for such usage be documented?

HFE – 22 Response

The answer is no. The operator's workstation does not present this level of detail for electrical equipment. Color may be used to represent status changes, for example, fluid color as tanks filling occurs.

Colors on the operator's workstation screens are defined in a project SCADA general rules and principles document.

<u>Staffing</u>

Section 12.4.3.F of NUREG-1718 states that staffing should be based on a review of the number and qualifications of personnel for each personnel activity during all plant operating conditions. The applicant should conduct this review in a systematic manner that incorporates the functional allocation and task analysis results. Categories of personnel should be based on the types of personnel activities. Staffing considerations should include issues identified in the OER, functional allocation, HSI design, procedure development, and V&V. The applicant's description of staffing is contained in the LA, Section 12.7 and in the HEPP and HEIP.

HFE – 23 MFFF Staffing

Section 6 of the HEIP discusses staffing and Figure 6.1 shows the expected MFFF organization for full production operation. The figure includes staff numbers which total 787. Missing from this section is the number and type of personnel on a full normal shift and the number of shifts planned. Please provide this information. Additionally, the HEIP does not provide discussions of shift staff teamwork and communication. Pease provide this information.

HFE – 23 Response

The MFFF organization will be comprised of five major subgroups – Business, Engineering, Licensing, Quality, and Plant Operations. Of interest here is the Operations, Maintenance and Technical Support groups within Plant Operations.

The following information is added to HFIP Section 6.4.2 Plant Operations:

"The initial staffing levels are estimated at this time based on reference plants experience and discussions with NRC licensed U.S. fuel assembly manufacturers. The initial staffing requirements will be determined by the Operations Manager. Shift staffing (including number and type of personnel on a full normal shift and the number of shifts planned) will be determined with HFE input/reviews.

Regarding, shift staff teamwork and communications. This again is based on the reference plants and NRC licensed fuel assembly manufacturers, and probably will be modified when the time comes for the Operations group to provide more details about staffing. At this time, staffing communications information is being developed. Generally, the Operations Manager should meet with the staff to provide top level instructions for the work. The AP Manager and MP Manager should develop their workbooks containing work instructions for their shifts. This information should be provided to the Shift Leaders who in turn should be composing a unit by unit workbook to accomplish the instructions given by the Managers. The Operators should have their own workbook containing very specific instructions for the work and also to record results, generally maintaining a record of the process. It is expected that during shift change over there will be approximately 30 minutes of overlap to allow the operating shift to brief and update the on-coming shift. During the shift, staff members will have direct communication with each other.

MOX Services has available onsite detailed study report of room or area occupancies based on recent staffing projections and knowledge/experience from the reference plants in France and the UO_2 fuel fabrication facilities in the U.S. This is a best estimate at MFFF staffing levels that will become clearer as detailed design is finalized and planning for plant operation as a fuel production facility is well underway.

__Procedures__

Section 12.4.3.G of NUREG-1718 states that an applicant's procedure development for personnel activities should incorporate HFE principles and criteria, along with all other design requirements to develop procedures that are technically accurate, comprehensive, explicit, easy to use, and validated consistent with the acceptance criteria in Section 15.5.4. Because procedures are considered an essential component of the HSI design, they should be derived from the same design process and analyses as the other components of the HSI (i.e., displays, controls and operator aids) and subject to the same evaluation processes. Procedures should include, as needed to support the personnel activity: generic technical guidance, plant and system operations, abnormal and emergency operations, tests (i.e., preoperational, startup, and surveillance) and alarm response. The applicant's procedures are described in the LA, Section 12.8 and in the HEPP and HEIP.

HFE – 24 Alarm Procedures

HEIP Section 7 suggests that both hardcopy and computer-based procedures may be used. If so, how is it determined which will be implemented in computer form?

HFE – 24 Response

Operations, Software Design Group, and the MFFF HFE Team have reached a consensus that the MFFF procedures are going to be hard-copy. There will not be any computer-based procedures at this time. HFIP section 7.24 computer based procedure retrieval is deleted.

HFE – 25 Procedure V&V

Section 8 of the HEPP states that all applicable procedures will be verified and validated to ensure they can be carried out as required. Section 9.8 of HEIP states that the MFFF HFE team will review the writers' style guides and the IROFS procedures. They will also verify and validate the IROFS procedures. The scope of V&V for procedures in Section 9.8 of HEIP is not clear and appears to be too limited. Please clarify.

HFE – 25 Response

HFIP Section 9.8 indicates: "The MOX HFE Team will review the writers' style guides and IROFS procedures [i.e., Administrative Control procedures], and later on verify and validate the IROFS procedures with the inclusion of Operations, Maintenance, and Training."

The following clarification has been added to the HFIP at Section 9.8:

"The HFE Team will verify the hard copy Administrative Control procedures (IROFS) of the ISA required Administrative Controls and conduct a validation of the administrative procedures by observing operator "walk through" or "talk through" of the administrative procedure the operator is required to perform." The validation sampling will include all task analysis identified "generic" ISA Administrative Controls (the ISA results and the task analysis of the ISA results indicate there are approximately forty (40) ACs that may be considered "generic."

A review all of Administration Control (IROFS) procedures will be performed by using first a review of the procedure itself, followed by observing operator "walk through" or "talk through" of the administrative procedure the operator is required to perform. The LA was revised to indicate all of the IROFS (Administrative Control) procedures identified in the ISA will be reviewed during the HFE review.

Also, the NCSE/NSE identified D-in-D items will be reviewed for ensure operator success in completing the D-in-D specified procedure. Refer to response to HFE-1.

Training

Section 12.4.3.H of NUREG-1718 states that an applicant's training program development should address all personnel activities. The training program development should indicate how the knowledge and skill requirements of personnel will be evaluated, how the training program development is coordinated with the other activities of the HFE design process, and how the training program will be implemented in an effective manner consistent with human factors principles and practices. The training program development should address the areas of review and acceptance criteria described in Section 15.4.4 and should result in a training program that provides personnel with the qualifications commensurate with the personnel activities. The applicant's training is described in the LA, Sections 12.9 and 15 and in the HEPP and HEIP.

HFE – 26 Scope of Personnel Training

The HEPP doesn't specifically address who gets trained. The HEIP, Section 10.4 [section 10.3 in revision 0], "General Approach Outline," states that the overall scope of training includes "The categories of personnel (e.g. managers, supervisors, operators, etc.)." Please clarify what is meant by "etc." and identify all staff that will be trained by category.

HFE – 26 Response

Etc. would refer to additional categories, for example Technicians, Maintenance personnel, laboratory personnel. "Etc." will be removed from the text and it place of "Etc. will be listed "technicians, maintenance and laboratory personnel."

Added a new bullet item for Section 10.3 as follows: "All personnel (except visitors who will have a visitor's indoctrination and familiarization program appropriate to their need of the visit) that have a need for MFFF plant access will be provided a General Employee Training (GET), along with more specified training according to position requirements. All the various functional groups of employees will be required to be trained in the aspects of their job responsibilities. Required training is all the training exercises that have been assigned to an individual. An individual will be assigned role-required training and other training that may develop skills and knowledge but is not necessary for role qualification. Training requirements are tied to individuals whereas qualification requirements are tied to roles."

MOX Services has developed a project document that provides an overview of the hiring and training strategy that has been developed for the Operations organization. The perspective is an integrated view of the different elements of the hiring and training program versus a discussion of the details of each of the elements. Some detailed examples are included in the report to ensure understanding of the depth of the program.

Integrated System Validation

Section 12.4.3.I.iii of NUREG-1718 states that an applicant should commit to a performance based evaluation of the integrated design to ensure that the HFE/HSI supports safe operation of the plant. Integrated system validation should be performed after HFE problems identified in HFE design activities are resolved or corrected because these may negatively affect performance and, therefore, validation results. Validation should be performed by evaluating personnel activities using appropriate measurement tools. All personnel activities should be tested and found to be adequately supported in the design, including personnel activities outside the control room. The applicant's integrated system validation is described in the LA, Section 12.10 and in the HEPP and HEIP

HFE – 27 Verification vs. Validation

HEPP indicates that "integrated system validation is intended to evaluate the acceptability of those aspects of the design that cannot be determined through such analytical means as the two verifications." However, integrated system validation has a different objective (to evaluate performance using the integrated system) than the two verifications, thus performing verification does not eliminate the need for validation. Please clarify.

HFE – 27 Response

It is noted in NUREG 0711, Section 11.4.3.1 Integrated System Validation Review Objective that the ISV "... [ISV] is intended to evaluate the acceptability of those aspects of the design that cannot be determined through such analytical means as HSI task-support verification and HFE design verification." The ISV is still needed, it is not eliminated.

Therefore, the first paragraph of the MFFF HEPP Section 10.2 Integrated System Validation Review Objective has been revised as follows:

"Integrated system validation is the process by which an integrated system design (i.e., hardware, software, and personnel elements) is evaluated using performance-based tests to determine whether the design acceptably supports safe MFFF operation. The design verification includes both HSI task support verification and HFE design verification. HSI task support verification evaluates that the HSI supports operator task requirements as defined by task analysis. HEDs are identified when the HSI does not fully support the identified operator task requirements (i.e., controls or information is not available or not displayed in the proper format for the specific task) or the presence of HSI components which may not be needed to support operator tasks or that impede operator tasks. HFE design verification is a static evaluation that verifies that the individual HSI components and details accommodate the human capabilities and limitations reflected in HFE guidelines. HEDs are identified if the design is inconsistent with the project specific HFE guidelines (i.e., the MFFF Human Factors Design Guide, and NUREG 0700 as a backup to the HFDG). Accomplishing these verifications does not eliminate the need for integrated system validation."

HFE – 28 Validation Scope Modifications

As new HSIs are integrated into the plant, they may interact with existing HSIs whose design is essentially the same as the reference plants. Selection of what to validate should be based on operational sampling methods and not specifically whether an individual HSI has been modified or not. Also, system or plant changes might change the acceptability of the HSIs that are not being modified, i.e., HSIs that were appropriate for use in the reference plants are no longer appropriate in the MFFF. Please clarify the scope of the validation activities.

HFE – 28 Response

Operational sampling is discussed in the HFIP section 11.7.1 and it was revised to state the following:

"The sampling methodology employed by the MFFF HFE Team will identify a range of operational conditions to guide the Verification and Validation activities. Of particular importance to the team are the Administrative Controls (IROFS) and the plant or process conditions in which these controls are accomplished. For example, during plant startup if something goes awry, what will be the conditions at that time that the IROFS administrative control is accomplished, what will the operator actions and what controls and displays will be required to perform the operator action. Also of interest will be a sampling of conditions where IROFS equipment is has to be maintained (for example, IROFS filter change outs in the HVAC system. The team will want to examine scenarios involving complex MFFF conditions such as a glovebox breech or the response to HVAC alarms. A methodology for the HFE Team to follow will be to review many of the scenarios reviewed during the ISA process. Additionally, the operating experience of the reference plants and the lessons learned file will be consulted to provide ideas and scenarios for consideration."

The remainder of Section 11.7 provides the HFE Team information for consideration in developing its operational conditions sampling.

HFE – 29 Validation Test bed

The HFIP states that no simulator will be available for impulse safety valves [Integrated System Validation]. It states that "Validation will begin as final design winds down. If procedures and training are in place for augmented administrative controls (or enhanced administrative controls) and station air compressor, and the HMIs are in place there is no reason not to begin validating those parts of the HSI design that are complete. During cold startup, a dynamic control room environment will be available and can be used to validate the few remaining HSIs." This raises a few questions:

- How can integrated performance be validated prior to the availability of a dynamic control room environment?
- How will performance during scenarios of primary interest, such as event and failure scenarios, be assessed?
- Many of the performance measures described would seem to require a simulator; how will they be measured using the actual plant?

HFE – 29 Response

This RAI appears to apply to the following section of the HFIP: "Section 11.9.2 Validation Test-bed". A test-bed is the HSI representation used to perform validation evaluations. The MFFF is the validation test-bed.

It is expected that during non-fissile or "cold start-up" operators will be in place to go through their start-up procedures. The MFFF facility will have completed construction and all equipment, controls, and displays are in their proper place. The control rooms will be outfitted with the designed furnishings and equipment required to be in the control room and this equipment will be operational. This is when scripted scenarios will be observed and evaluated to see that the operators understand and know what to do when following specific IROFS procedures, or responding to practice or drill alarms.

The HFE Team in coordination with other groups such as software design, manufacturing design, ISA, Operations, Training, and the Test and Startup Group, will script and provide scenarios that are representative of failure modes of interest, to see how operators would respond by following a procedure. It will be important to know that the operator recognizes and understands what is taking place (event) and how to correctly respond to it.

Scenarios of interest will be evaluated in the cold start-up environment by one of many methods (e.g., checklist, observation, operator interviews). The first step is to ensure the fidelity of the HMI or HSI; the HFE Team has to make sure required interfaces are installed and working for operator use. Next, the HFE Team must have the appropriate operations or maintenance procedures and ensure the procedure is complete. Next, the HFE Team must ensure the operators or maintenance staff has been trained in the procedure. Then the scenario is explained to the operating staff and the evaluation criteria, for example, IROFS must be able to be completed without error. The HFE Team will develop a guidance document for using the cold startup MFFF as a validation test bed. The test bed will be verified for conformance characteristics called for in the HFE Team procedure before any validation is accomplished. The HFE Team procedures will be included in the HFE Summary report.

HFE – 30 Operational Condition Sampling

HFIP Section 11.7.1 indicates that operational condition sampling for validation may be used. What criteria will be used to determine whether it will be used or not?

HFE – 30 Response

HFIP Section 11.7.1 has been revised to remove the phrase, "if applied." The HFE Team will apply Operational Conditional Sampling, as now indicated in the revised Section 11.7.1. (Refer to HFE-28)

HFE – 31 Design Implementation Methodology

Section 11 of the HEPP and Section 12 of the HEIP provide a high level commitment to the two criteria from NUREG-1718 and the three criteria from NUREG-0711 on Design Implementation. Section 12.4 of the HEIP provides some more detailed discussion of how these criteria are to be implemented. However, it does not provide any detail for one criterion, namely the comparison of the final as-built HSIs to the final detailed design description. For example, are 100% of screens, icons, controls, labels, location aids, and labels to be verified or is a sampling program to be used? Please provide added description to address this criterion.

HFE – 31 Response

LA Section 12.10.5, HEPP Section 11, and HFIP Section 12.4 were revised to state the following: "

"The start-up and test program is the process by which the constructed facility is reconciled against the final design. The HFE Team will ensure IROFS having HMI are reconciled between the "as built" and the final detailed design description. All of the Control Room IROFS will be reviewed. Emergency Procedures are reviewed to ensure the procedure, the required displays (including labeling) and controls, and the human action are compatible and in accordance with the final design description. Alarms and the required operator alarm responses will be reviewed for comparison between the "as built" and the detailed final design."