

-DUO-SRE -
Identified in
POSITION marking

Risk-Informed Review of the MOX Facility Licensing Application

V. Mubayi, M.A. Azarm, and R.A. Bari

Brookhaven National Laboratory

February 2007

Table of Contents

	Page
1.0 INTRODUCTION	1
1.1 Scope and Purpose of Licensing Application Review	1
1.2 Applicable Regulatory Requirements	2
1.3 Organization of this Report	4
2. LICENSING REVIEW OF MOX FACILITY SUBMITTAL	5
2.1 Summary of Guidance in Fuel Cycle Facility License Application Review, NUREG-1520	5
2.2 Summary of Guidance in MOX Facility Standard Review Plan, NUREG-1718	6
3. SUMMARY OF MOX FACILITY PROCESSES AND OPERATIONS	8
3.1 MOX Facility and Site Overview	7
3.2 MOX Facility Process Overview	9
3.2.1 AP Process	9
3.2.2 MP Process	10
3.3 Hazards Presented by the Facility	11
3.3.1 Radiological Hazards	11
3.3.2 Chemical Hazards	12
3.3.3 Criticality Hazards	13
3.4 Accidents Contributing to Risk	13
4. RISK-INFORMING THE LICENSING REVIEW	15
4.1 The RIDM Process	17
4.2 Three-Region Diagram	19
4.3 Application to the MOX Facility	20
4.4 Risk Assessment of Red Oil Excursions in the MOX Facility	21
4.4.1 Description of Red Oil Phenomenon	21
4.4.2 Criteria and Condition Tree for Red Oil Excursion	22
4.4.3 Prevention of Red Oil Scenarios	25
4.4.4 Red Oil Events in the AP Process	26
4.4.5 Red Oil Scenarios in the Acid Recovery and Oxalic Mother Liquor Recovery Units	27
4.4.5.1 Acid Recovery System Scenarios	36
4.4.5.2 Oxalic Mother Liquor Recovery System	36
4.5 Possible Risk Importance Measures	40
4.6 Considerations of Defense-in-Depth, Uncertainty, and Safety Margin ...	41

Table of Contents (Continued)

	Page
5. SUPPLEMENTING INTEGRATED SAFETY ANALYSIS REVIEW	43
5.1 Layer of Protection Analysis (LOPA)	45
5.2 Information Needs Pertinent to Risk	45
6. ORGANIZATION OF INFORMATION FOR RISK-INFORMING LICENSING REVIEW	47
6.1 Information Needs of Risk-Informing	47
6.2 Qualitative/Quantitative Risk Assessments: Techniques, Data, Guidance	47
6.3 Examples Illustrating Guidance	49
REFERENCES	51

List of Figures and Tables

Figure		Page
1	AP Process Units	9
2	MP Process	10
3	Risk-Informing Licensing Review	16
4	Three-Region Risk Acceptance Diagram	20
5	Necessary Conditions for a Red Oil Excursion to Occur	22
6	Condition Tree for Red Oil Scenarios	24
7	Red Oil Excursion Risk Evaluation Process	32
8	The Event Tree Representing the EV Scenarios	33
9	The Event Tree for Tank 3000	34
10	An Event Tree for the Specific Scenario in OMLR System	38

Table		Page
1	Summary Results for Red Oil Excursion in Acid Recovery System	35
2	Major Risk Contributors and Areas of Uncertainties for Red Oil Excursion in the Oxalic Mother Liquor Recovery System	40

1. INTRODUCTION

1.1 Scope and Purpose of Licensing Application Review

The purpose of the review of a license application is to allow staff to make a determination of reasonable assurance that the facility will be constructed and operated in such a manner as to adequately protect the health and safety of the public, the workers, and the environment, and the common defense and security. The scope of the review of a license application for a fuel cycle facility extends over all the topics covered in NUREG-1520 [1]. For the mixed oxide (MOX) facility specifically, details about scope and purpose are provided in NUREG-1718 [2]. Fuel cycle facilities are regulated under Part 70 of Title 10 of the Code of Federal Regulations [3].

Apart from financial, organizational and administrative, management and classified matters, the scope and purpose of the licensing review include the following:

- facility and process overview that includes location, site description, boundaries of the controlled area, description of the facility processes involving special nuclear materials (SNM), and the types and amounts of wastes discharged to the environment; the purpose of the review is not a detailed technical analysis but a background check on whether the requirements of 10 CFR 70.22 "Contents of Applications" are met;
- integrated safety analysis (ISA) that includes (i) a safety assessment of the design bases required by Parts 70.22 and 70.23 for the construction permit, and (ii) programmatic commitments needed to obtain a possession license; the latter include an evaluation of all hazards and accident sequences that could result in consequences to the public, workers, or environment specified in Part 70.61 criteria and identification of items relied on for safety (IROFS) that provide reasonable assurance that the safety performance requirements of Part 70.61 are met;
- criticality safety that establishes if the applicant has an adequate organization, program, controls and limits to prevent a nuclear criticality and has assessed appropriate accident sequences documented in the ISA;
- assessment of fire protection in accordance with the requirements of Part 70.64 and the evaluation of radiological consequences of fires to provide assurance that the performance requirements of Part 70.61 are complied with;
- assessment of chemical safety including chemical accident sequences, consequences, and safety controls as described in the ISA, and process safety interfaces that ensure that the chemical safety program will not adversely impact other safety programs such as radiological safety;
- assessment of radiation safety to ensure that facility construction and operation comply with the requirements of Parts 70 and 20, occupational and public doses are as low as reasonably achievable (ALARA), and the IROFS prevent or mitigate radiological consequences of postulated accidents in conformance with the criteria of Part 70.61;
- assessment of environmental protection that includes radiation protection program, effluent and environmental monitoring for normal and off-normal operations and the ISA summary to ensure that the requirements of Parts 20, 70, and 51 are complied with;
- human factors engineering applied to personnel activities that are identified as safety-significant consistent with the findings of the ISA.

Risk informing the licensing review potentially impacts several of these areas, in particular, helping to verify and substantiate the conclusions of the ISA and the designation of the IROFS, criticality

safety, fire protection, chemical safety, and radiation safety. Since human errors, both omission and commission, are important in the risk analysis of accidents, human factors engineering is also an area that is part of risk informing.

1.2 Applicable Regulatory Requirements

The regulatory requirements that govern the licensing of the MOX facility are contained in Title 10 Part 70 of the Code of Federal Regulations (10 CFR 70), in particular Part 70.22 that provides requirements for the content of applications and Part 70.23 that contains the requirements for the approval of applications. Subpart H of Part 70, in particular Part 70.61, defines the requirements for facility performance with respect to limiting worker and public exposure from various accidents categorized by their likelihood of occurrence. Part 70.62 requires licensees to establish a safety program and carry out an ISA of the facility to demonstrate compliance with Part 70.61. Part 70.64 contains requirements, including baseline design criteria, for new facilities such as the MOX facility or new processes at existing facilities, and Part 70.65 requires applicants to submit an ISA summary that includes all of the information used to demonstrate compliance with the performance requirements in Part 70.61.

The performance requirements of 70.61 require each applicant or licensee to evaluate, in the ISA, and demonstrate compliance with the following criteria:

The risk of each credible high-consequence event must be limited. Engineered controls, administrative controls, or both, shall be applied to the extent needed to reduce the likelihood of occurrence of the event so that, upon implementation of such controls, the event is highly unlikely or its consequences are less severe than those of high consequence events, i.e., those internally or externally initiated events that result in:

- (1) An acute worker dose of 1 Sv (100 rem) or greater total effective dose equivalent;
- (2) An acute dose of 0.25 Sv (25 rem) or greater total effective dose equivalent to any individual located outside the controlled area as defined below;
- (3) An intake of 30 mg or greater of uranium in soluble form by any individual located outside the controlled area; or
- (4) An acute chemical exposure to an individual from licensed material or hazardous chemicals produced from licensed material that:
 - (i) Could endanger the life of a worker, or
 - (ii) Could lead to irreversible or other serious, long-lasting health effects to any individual located outside the controlled area. If an applicant possesses or plans to possess quantities of material capable of such chemical exposures, then the applicant shall propose appropriate quantitative standards for these health effects, as part of the information submitted in fulfillment of the requirements of Part 70.65.

The risk of each credible intermediate-consequence event must be limited. Engineered controls, administrative controls, or both shall be applied to the extent needed so that, upon implementation of such controls, the event is unlikely or its consequences are less than those of intermediate

consequence events, i.e., those internally or externally initiated events that are not high consequence events, that result in:

- (1) An acute worker dose of 0.25 Sv (25 rem) or greater total effective dose equivalent;
- (2) An acute dose of 0.05 Sv (5 rem) or greater total effective dose equivalent to any individual located outside the controlled area;
- (3) A 24-hour averaged release of radioactive material outside the restricted area in concentrations exceeding 5000 times the values in Table 2 of Appendix B to Part 20; or
- (4) An acute chemical exposure to an individual from licensed material or hazardous chemicals produced from licensed material that:
 - (i) Could lead to irreversible or other serious, long-lasting health effects to a worker, or
 - (ii) Could cause mild transient health effects to any individual located outside the controlled area. If an applicant possesses or plans to possess quantities of material capable of such chemical exposures, then the applicant shall propose appropriate quantitative standards for these health effects, as part of the information submitted pursuant to Part 70.65.

In addition, the risk of nuclear criticality accidents must be limited by assuring that under normal and credible abnormal conditions, all nuclear processes are subcritical, including use of an approved margin of subcriticality for safety. Preventive controls and measures must be the primary means of protection against nuclear criticality accidents.

Each engineered or administrative control or control system necessary to comply with the requirements defined above shall be designated as an item relied on for safety. The safety program, established and maintained pursuant to Part 70.62 of this subpart, shall ensure that each item relied on for safety will be available and reliable to perform its intended function when needed and in the context of the performance requirements of this section.

Each licensee must establish a controlled area, as defined in Part 20.1003. In addition, the licensee must retain the authority to exclude or remove personnel and property from the area. For the purpose of complying with the performance requirements of this section, individuals who are not workers, as defined in Part 70.4, may be permitted to perform ongoing activities (e.g., at a facility not related to the licensed activities) in the controlled area, if the licensee:

- (1) Demonstrates and documents, in the integrated safety analysis, that the risk for those individuals at the location of their activities does not exceed the performance requirements and criteria of Part 70.61 defined above.
- (2) Provides training that satisfies 10 CFR Part 19.12(a)(1)-(5) to these individuals and ensures that they are aware of the risks associated with accidents involving the licensed activities as determined by the integrated safety analysis, and conspicuously posts and maintains notices stating where the information in 10 CFR 19.11(a) may be examined by these individuals. Under these conditions, the performance requirements for workers specified in the requirements and criteria for Part 70.61 may be applied to these individuals.

1.3 Organization of this Report

Chapter 2 of the report summarizes the existing guidance on license application review contained in NUREG-1520 for a fuel cycle facility and in NUREG-1718 for the MOX facility specifically.

Chapter 3 presents an overview of the MOX facility processes and operations with a focus on the hazards presented by the facility including radiological, chemical, criticality, explosion and fire and summarizes the findings of the NRC final safety evaluation report (FSER), NUREG-1821 [4].

Chapter 4 outlines the issues involved in risk informing the licensing review. Some of the lessons learned from the ongoing work on the risk of red oil excursions are provided and a discussion of information needs pertinent to risk is presented, including design and operational issues, identification of key risk metrics, and approaches based on risk informed decision making.

Chapter 5 discusses the role of risk assessment in supplementing the review of the ISA with a focus on some of the key issues such as establishment of the quantitative bases for event selection, the analysis of system interactions, and a review of the IROFS selection based on risk significance.

Chapter 6 presents the organization of information needed to risk inform the licensing review including the use of both qualitative and quantitative information and provides examples illustrating the guidance.

It should be noted that this report is a limited scope work designed mainly to highlight the issue of risk-informing the licensing review of the proposed MOX facility by integrating insights derived from a quantitative risk assessment of specific plant vulnerabilities. The probabilistic risk assessment of the red oil phenomenon focuses attention on specific elements of the design and procedures that have the most impact on risk and thus help to inform the NRC reviewer of important areas that need to be analyzed in more detail. However, red oil excursions are only one category of accidents that can occur at the MOX facility and a complete risk profile has to take into account the larger number of accidents discussed in the construction authorization request (CAR) submitted by the applicant [5] and analyzed in the NRC Final Safety Analysis Report. This report is also limited in another sense, it does not take into account any information revealed in the ISA recently submitted by the applicant in support of a possession and use license. Such information was not available to BNL in the course of this work.

2. LICENSING REVIEW OF MOX FACILITY SUBMITTAL

Standard Review Plans are at the heart of a licensing review. The two most pertinent documents for the review of the MOX facility are NUREG-1520 and NUREG-1718.

The "Standard Review Plan (SRP) for the Review of a License Application for a Fuel Cycle Facility" (NUREG-1520) provides U.S. Nuclear Regulatory Commission (NRC) guidance for reviewing and evaluating the health, safety, and environmental protection aspects of applications for licenses to possess and use special nuclear material (SNM) to produce nuclear reactor fuel.

The Standard Review Plan (SRP) (NUREG-1718) provides guidance to the NRC staff reviewers in the Office of the Nuclear Material Safety and Safeguards who will perform safety, safeguards, and environmental reviews of the anticipated application for a license to possess and use special nuclear material for a MOX facility under 10 CFR Part 70.

2.1 Summary of Guidance in Fuel Cycle Facility License Application Review, NUREG-1520

NUREG-1520 provides guidance to the staff reviewers in the U.S. Nuclear Regulatory Commission (NRC), Office of Nuclear Material Safety and Safeguards (NMSS) who perform safety and environmental impact reviews of applications to construct or modify and operate nuclear fuel cycle facilities. As such, the SRP ensures the quality, uniformity, and predictability of the staff reviews. The SRP also makes information about licensing acceptance criteria widely available to interested members of the public and the regulated industry. Each SRP section addresses the responsibilities of the staff reviewers, the matters that they review, the Commission's regulations relevant to specific technical matters, the acceptance criteria used by the staff, the process and procedures used to accomplish the review, and the conclusions that are appropriate to summarize the review.

The SRP also addresses the long-standing health, safety, and environmental protection requirements of Title 10, Parts 20 and 70, of the *Code of Federal Regulations* (10 CFR Parts 20 and 70) as well as the amended accident safety requirements reflected in the new Subpart H of 10 CFR Part 70. For example, the chapters concerning radiation safety, environmental protection, emergency management, and decommissioning contain acceptance criteria that are mainly set by regulations that remained unaffected by the recent revision to 10 CFR Part 70. The new Subpart H of 10 CFR Part 70 identifies risk-informed performance requirements and requires applicants and existing licensees to conduct an ISA and submit an ISA Summary, as well as other information. Chapters 3 (ISA) and 11 (Management Measures) of the SRP are the primary chapters that address the staff's review in relation to the performance and other related requirements of Subpart H. The approach and method that is presented in the SRP is an example of one method that is acceptable to the NRC for demonstrating compliance with the regulations. Methods and approaches different from those described in the SRP are acceptable if they provide the needed information and technical basis for the staff to make the determination needed to issue or continue a license.

The SRP focuses on safety and environmental impact reviews. Review criteria applicable to the safeguards sections of license applications were developed earlier and are published in NUREGs 1280 [6] and 1065 [7].

2.2 Summary of Guidance in MOX Facility Standard Review Plan, NUREG-1718

The Standard Review Plan NUREG-1718 provides guidance to the NRC staff reviewers in the Office of the Nuclear Material Safety and Safeguards who are performing safety, safeguards, and environmental reviews of the application for a license to possess and use special nuclear material for a mixed oxide fuel fabrication facility under 10 CFR Part 70. This guidance includes the construction approval review, which has been obtained, specifically related to plutonium processing and fuel fabrication. The Standard Review Plan is aimed at ensuring the quality, uniformity, stability, and predictability of the staff reviews. It presents a prescribed basis from which to evaluate proposed changes in the scope and requirements of the staff reviews. The Standard Review Plan makes information about the NRC acceptance criteria broadly available to interested members of the public and regulated industry. Each Standard Review Plan section addresses the responsibilities of persons performing the review, the review areas, the Commission's regulations relevant to specific technical matters, the acceptance criteria used by the staff, how the review is accomplished, and the conclusions that are appropriate for the Safety Evaluation Report for both the construction approval review and the license review.

Both NUREG-1520 and NUREG-1718 cover the major areas of review of a license application that have been mentioned above in Section 1.1. In particular, as regards safety, Chapter 3 of NUREG-1520 and Chapter 5 of NUREG-1718 contain a description and discussion of the Integrated safety Analysis (ISA) and ISA Summary that is required to be submitted by the applicant. Both reports define the safety program and ISA commitments that the NRC reviewer evaluates for adequacy.

However, while NUREG-1520 is generally applicable to all fuel cycle facilities regulated under 10 CFR 70, NUREG-1718 provides additional detail and specificity for a MOX fuel fabrication facility. Chapter 5 of NUREG-1718 concerns the Integrated Safety Analysis (ISA) and addresses the applicant's safety assessment of the design bases for the MOX facility that demonstrates that the principal systems, structures, and components (PSSCs) of the facility provide protection against natural phenomena and the consequences of other accidents to allow staff to decide if the requirements of 10 CFR 70.23 are met. The review of the ISA includes ISA programmatic commitments and the ISA results and summary. They include the applicant's methods for hazard identification, process hazards analysis, accident sequence and construction, consequence determination and comparison with 70.61, and the likelihood categorization for establishing compliance with 70.61. The review of the ISA results and summary allows staff to determine if the applicant has performed a systematic evaluation of hazards and credible accident sequences and has identified the items relied on for safety (IROFS) and management measures that satisfy 70.61 requirements. The accidents reviewed include radiological releases, nuclear criticality events, or any exposure to radiation from licensed material. They also include releases of hazardous chemicals produced from licensed materials that are toxic, explosive, flammable or corrosive and can pose a threat to human health.

Staff review includes the site and facility descriptions, the detailed description of each process including drawings, ISA team qualifications, ISA methods, definitions of unlikely, highly unlikely, and credible, quantitative standards for chemical consequence levels, information on accident consequences and likelihoods demonstrating compliance with 70.61 performance requirements, the list of IROFS for all accidents in each process identifying, in particular, those IROFS which are the sole item relied on in an accident sequence for meeting 70.61 criteria, and information demonstrating compliance with criticality monitoring requirements of 70.24. Regulatory acceptance

criteria for the safety assessment of the design bases are contained in Section 5.4.3.1 and for the ISA in Section 5.4.3.2 of NUREG-1718. The latter criteria include the following: an ISA of appropriate complexity be conducted for each process based on specific methods, for example, the methods described in NUREG-1513, NUREG/CR-6410, and Appendix A of NUREG-1718; a reasonable assurance that the IROFS will satisfy the performance requirements of 70.61 and appropriate management measures are in place to ensure the availability and reliability of the IROFS to satisfy the likelihood element of the performance requirement.

NUREG-1718 provides detailed guidance on the criteria to be used for ISA methods, including consequences and likelihoods. In particular, guidance is provided on criticality accident sequences for evaluating compliance with 70.61(d) and with ANSI/ANS-8.10 "Nuclear Criticality Safety in Operations With Fissionable Materials Outside Reactors." Appendix A of NUREG-1718 provides details of one acceptable method of likelihood evaluation. Quantitative standards for chemical consequences due to acute chemical exposure to licensed material or chemicals produced from licensed material that are acceptable to NRC staff for meeting 70.61 criteria are the Emergency Response Planning Guidelines (ERPG) and the Acute Exposure Guideline Level sets of standards. Guidance on likelihoods includes acceptance criteria for qualitative definitions of likelihood that incorporate notions of availability and reliability, and methods including risk indexing methods. Acceptance criteria for quantitative definitions of likelihood are also mentioned in NUREG-1718 although quantitative demonstration of compliance is not required by 70.61. Highly unlikely is defined as less than $1E-2/N_h$ per year where N_h is the total number of potential high-consequence accidents in regulated facilities (assumed to be at least 1000). Unlikely is defined as less than $0.04/N_i$ per year where N_i is the total number of intermediate-consequence accidents in regulated facilities. NUREG-1520 states that the guideline for highly unlikely is less than $1E-5$ per-event per-year, and unlikely is less than $1E-4$ per-event per-year. NUREG-1718 provides additional guidance on criticality monitoring for meeting Part 70.24 requirements including appropriate detectors at locations where special nuclear material is handled.

Chapter 6 of NUREG-1718 addresses criticality safety in the MOX facility. Section 6.4 defines acceptance criteria, including regulatory requirements, and provides guidance on technical practices for criticality safety evaluation and criticality safety control including control of mass, geometry, density, isotopics, reflection, moderation, concentration, neutron absorber, volume, heterogeneity, and process variables. Chapter 7 addresses Fire Safety and Chapter 8 provides guidance on review of Chemical Safety.

The ISA is a primary source of information that can be used to develop risk-informed guidance. In particular cases, quantitative risk assessment methods may be usefully employed as described in Chapter 4 to inform the NRC reviewer where attention needs to be focused based on risk.

Guidance on quality assurance (QA) elements relating to organization and the QA function for items designated as IROFS including: their design control, procurement document control, control of purchased items, identification and inspection, control of special processes relating to IROFS, control of tests and measuring and test equipment, handling, storage and shipping, corrective actions, and control of QA records is provided in Appendix G of NUREG-1718. Guidance is also provided on audits and assessments and the applicant's provisions for continuing the QA program.

3. SUMMARY OF MOX FACILITY PROCESSES AND OPERATIONS

The U.S. Nuclear Regulatory Commission (NRC) is in the process of licensing a facility to manufacture mixed oxide (MOX) fuel at the U.S. Department of Energy's (DOE's) Savannah River site in South Carolina. Mixed oxide fuel is a blend of plutonium dioxide and depleted uranium dioxide that will be used as fuel in commercial nuclear power plants. The responsibility for ensuring that the facility is designed, constructed, and operated safely resides with the facility operator, Duke COGEMA Stone & Webster (DCS).

In the MOX fuel fabrication facility that will be constructed and operated by DCS, plutonium dioxide will be mixed with depleted uranium dioxide to form mixed oxide powder. This powder is pressed and bonded into pellets through a heating process called sintering. The pellets are then loaded into corrosion-resistant thin metal tubes called fuel rods. The rods are bundled into fuel assemblies that are shipped to power plants licensed to use MOX fuel.

3.1 MOX Facility and Site Overview

The MOX fuel fabrication facility is proposed to be located in the F-Area of the Savannah River site. The buildings of the facility would consist of the fuel fabrication building, the emergency and standby diesel generator buildings, the secured warehouse, administration, technical support and reagents processing buildings. According to the revised Construction Authorization Report (CAR) submitted by the applicant DCS [5], the MOX Fuel Fabrication Building is comprised of three major functional, interrelated areas: the MOX Processing Area (BMP), the Aqueous Polishing Area (BAP), and the Shipping and Receiving Area (BSR). The MOX Processing Area includes the blending and milling area, pelletizing area, sintering area, grinding area, fuel rod fabrication area, fuel bundle assembly area, a laboratory area, and storage areas for feed material, pellets, and fuel assemblies. The main chemical operations are performed in the Aqueous Polishing area, including purification, solvent recovery, oxalic precipitation and oxidation, acid recovery, and oxalic mother liquor recovery. Space is also provided in the MOX Fuel Fabrication Building for support equipment, such as temporary waste storage; heating, ventilation, and air conditioning (HVAC) equipment; high-efficiency particulate air (HEPA) filters plenums; inverters; switchgear; and pumps. Figure 1.1-2 of the CAR [5] provides a schematic of the MOX fuel fabrication building.

10 CFR 70.61 requires the applicant to establish a controlled area boundary as defined in 10 CFR Part 20.1003. Within the controlled area is a restricted area in which access is limited to protect individuals against undue risks from exposure to radiation as defined in Part 20.1003. For the purpose of evaluating compliance with requirements, NRC's Final Safety Evaluation Report accepts the terminology proposed by DCS for those individuals considered to be "facility workers" (those workers inside a building located in the restricted area), site workers (those located 100 meters from the ventilation stack outside the facility) and individuals outside the controlled area boundary (who, depending on context, can also be considered as members of the general public). The environment is considered to be all areas outside the restricted area.

Staff evaluation of site geography, demography and land use, meteorology, hydrology, and seismic hazards is documented in the FSER and concludes that the design bases of the principal systems, structures and components (PSSCs) provide reasonable assurance of protection against natural phenomena and consequences of potential accidents.

3.2 MOX Facility Process Overview

The MOX facility consists of the following:

- Aqueous Polishing (AP)
- MOX fuel fabrication (MP)

3.2.1 AP Process

The MOX AP process shown in Figure 1, consists of four main areas which are: (1) Plutonium Purification, (2) Recovery Processes, (3) Waste Storage, and (4) the Offgas Unit.

Among the plutonium purification and recovery process units that are illustrated in Figure 1, there are: (1) the plutonium purification process unit, (2) the solvent recovery unit, (3) the oxalic precipitation and oxidation unit, (4) the oxalic mother liquor recovery unit, and (5) the acid recovery unit. Weapons-grade plutonium is received from the proposed pit assembly and conversion facility and alternate feedstock at the Savannah River site. The plutonium is milled into a powder form and then dissolved in a nitric acid medium with silver as a catalyst to promote dissolution. For the alternate feedstock, however, dechlorination is required before dissolution if the chloride content is greater than 500 ppm. , the process takes place at normal (ambient) temperatures ranging from 20 C (68 F) to 40 C (104 F). Plutonium nitrate is then fed to the purification cycle, where plutonium is extracted through a solvent extraction process, using tri-butyl phosphate (TBP) in an organic diluent (hydrogenated propylene tetramer, HPT), that is a modified PUREX process [8].

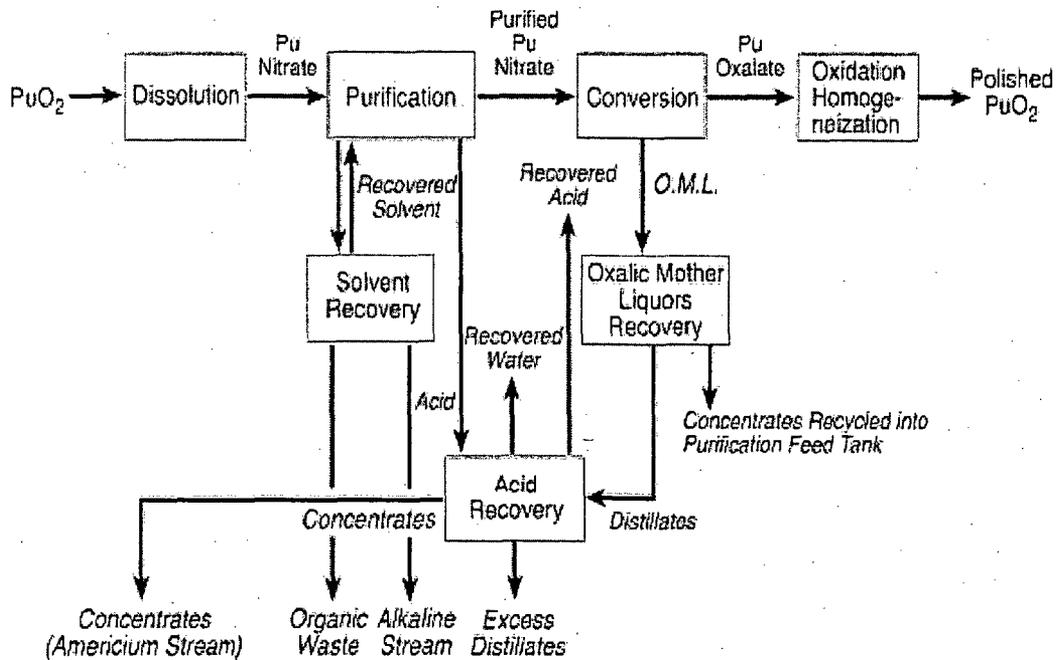


Figure 1 AP Process Units (source: NUREG-1821)

The extraction process removes impurities, such as gallium, and the purified plutonium nitrate is fed to a continuous oxalate calcination process that converts it to a plutonium dioxide powder. The oxalic mother liquors produced in the precipitation to oxalate are recycled to the oxalic mother liquor recovery unit. The solvent is regenerated in the solvent recovery unit and the acid is recycled in the acid recovery unit

The liquid waste storage tanks contain low level and high level alpha liquids, stripped uranium and organic waste streams received from various processes in the AP process for temporary storage and pre-treatment before they are ultimately sent off for final disposal offsite.

3.2.2 MP Process

The MP process receives the polished plutonium dioxide from the AP process and the depleted UO₂ and mixes them to form mixed oxide fuel pellets which are then loaded into fuel rods and assembled into MOX fuel assemblies. Figure 2, taken from the FSER, provides an overview of the MP process which consists of a series of steps. In the first PuO₂ powder is mixed with DUO₂ to form a master blend of approximately 20% PuO₂ content. This blend is then micronized into a fine powder and mixed with more DUO₂ and scrap powder to produce a final blend with the specified Pu content. The blend is homogenized and pelletized and the MOX pellets are sintered, ground and sorted, and loaded into rods which are then inspected. As shown in the Figure 2, the rods are loaded into assemblies which are then inspected and packaged for shipment.

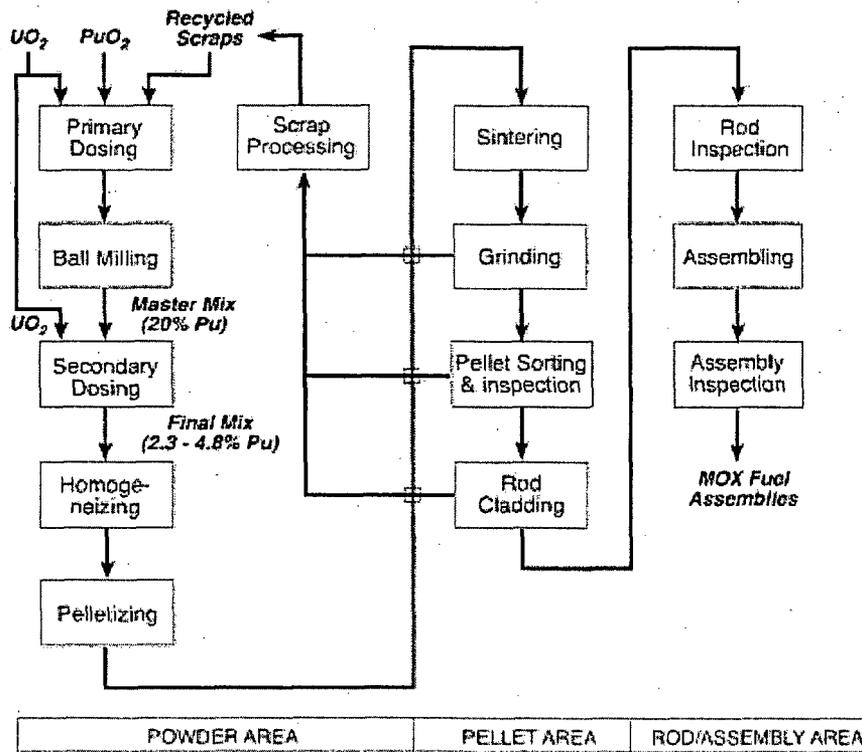


Figure 2: MP Process (Source: NUREG-1821)

3.3 Hazards Presented by the Facility

The hazards presented by the facility can be represented by events that have the potential to release radioactive material or hazardous chemicals that can lead to exposures to the public or workers or releases to the environment in excess of the limits set out in Part 70.61 discussed in Section 1.2 above.

The events that have been considered in the CAR and reviewed in the Safety Evaluation Report (SER) include: natural hazard phenomena such as tornados, extreme winds, and seismic events, manmade external events like fires, explosions or hazardous material releases at nearby facilities, and loss of offsite power, and internal process hazard events. The natural hazard phenomena and most of the external manmade events were screened out based on likelihood of occurrence. The risks of some others, such as potential hazardous chemical or radiological releases from other facilities at the savannah River site, are expected to be reviewed later as part of the license for possession and use.

The internal process hazard events are further subdivided into: (1) events leading to loss of confinement and dispersal of radioactive material, (2) fires, (3) load-handling failures such as drops, (4) explosions, (5) criticality, and (6) chemical releases. These classes of events are discussed further below based on the review information provided in the NRC SER. This discussion is provided to help illustrate the methodology and approach used in the review carried out by the NRC as part of the decision to grant the construction permit.

3.3.1 Radiological Hazards

The radiological hazards presented by the MOX facility arise from the constituents of the weapons-grade plutonium proposed to be used to manufacture mixed oxide fuel. Weapons-grade plutonium contains various isotopes of plutonium (Pu-236, Pu-238, Pu-239, Pu-240, Pu-241, and Pu-242) and small quantities of impurities including radionuclides such as isotopes of uranium and americium, and the decay products of plutonium, uranium, and americium. The uranium isotopes U-235 and U-238 that are present in the feedstock represent ingrowth from the radioactive decay of Pu-239 and Pu-242. The fuel fabrication process also uses depleted uranium that is a major component of the manufactured fuel. However, depleted uranium is not a significant radiological hazard although it is a significant chemical hazard.

The radionuclides are present both in solid powder form and in liquid wastes in different process areas. The aqueous polishing process is designed to remove the impurities from the plutonium oxide feed first and the purified PuO₂ is then transferred to the powder blending and fuel fabrication process. The mainly high-alpha radioactive impurities are stored in waste tanks in solution form before being sent to a waste solidification facility.

Six categories of radioactive sources at the MOX facility that could pose a radiological hazard include: plutonium oxide feed (impure), purified plutonium oxide, high alpha activity waste stream (mainly Am), depleted uranium oxide (DUO₂), and the PuO₂-DUO₂ MOX blends (20% PuO₂ master blend and 6% PuO₂ final blend). Due to the nature of the radionuclides present, the major exposure route for radiological dose to the public and workers is inhalation. Source term estimates from potential accidents at the proposed facility follow the approach recommended in NUREG/CR-6410 [9]. In this handbook, the source term is the product of five factors: the material at risk, the damage ratio, the airborne release fraction (ARF), the respirable fraction (RF, fraction of released material that can be inhaled into the respiratory system), and the leakpath factor (LPF, fraction of

released material passing through a confinement barrier such as a filter). Table 9.1-5 of the FSER lists values of ARFs and RFs from various types of events such as explosive detonation, overpressurization, fire, etc. for different kinds of materials, such as solutions, powders, solid pellets, etc. Staff review of dose assessments to the site workers provided by the applicant in the CAR concluded that the applicant's methodology and results were acceptable for the purposes of radiological safety assessment.

3.3.2 Chemical Hazards

Chemical hazards at the MOX facility arise both from the hazardous nature of some of the chemicals used in the various processes and the byproducts that are generated in the chemical reactions that occur in these processes. In the first category are gases such as hydrogen, liquids such as concentrated nitric acid, and solids like depleted uranium. In the second category are reaction products during both normal and off-normal conditions that include various oxides of nitrogen and, importantly, substances such as red oil that can also present a threat of explosion.

The performance requirements of 10 CFR Part 70.61 include acute chemical exposures to individuals in the definition of high-consequence and intermediate-consequence events. As per the guidance provided in Chapter 5 of NUREG-1718 "Quantitative Standards for Chemical Consequences", chemical consequence limits based on the Environmental Protection Agency (EPA) acute exposure guideline level (AEGL) values or the American Industrial Hygiene Association (AIHA) emergency response planning guideline (ERPG) values are acceptable to NRC staff to meet the criteria of 10 CFR 70.61. DCS provided chemical concentration limits to evaluate the potential consequences to individuals outside the controlled area and workers for an accidental release of chemicals based primarily on the temporary emergency exposure limits (TEELs) adopted by the U.S. Department of Energy (DOE), Subcommittee on Consequence Assessment and Protective Action. Definitions of the TEEL and AEGL values along with a discussion of the chemical consequences and the applicant's consequence analysis is provided in Section 8.1.2.3 of the FSER. A summary of the staff's review of chemical events is provided in Section 5.1.6.3.6 of the FSER. As noted in the staff's evaluation, chemical consequence limits proposed by different bodies are based on scientific information that is subject to issues of data availability, interpretation, and uncertainty, and some values may incorporate larger degrees of conservatism and margin. Also, unlike radiological consequences that are expressed in one common unit (rem or sievert), chemical consequences are expressed in concentrations (ppm or mg/m³) that vary from chemical to chemical. The FSER indicates that chemical exposure limits do not correlate well with risk levels for different categories of exposed populations.

Chemical safety is discussed in Chapter 8 of the FSER. Staff review of the CAR focused on the areas of chemical process safety applicable to the construction authorization stage including: hazardous chemicals and potential interactions affecting licensed materials, chemical accident sequences and consequences, and safety controls. DCS stated in the revised CAR that the facility design incorporates the baseline design criteria required under 10 CFR 70.64(a)(5). This requires that the design must provide for adequate protection against chemical risks produced from licensed material, facility conditions which affect the safety of licensed material, and hazardous chemicals produced from licensed material. Table 8.1-1 of the FSER provides a summary of the chemicals to be used at the MOX facility based on Tables 8-1a to 8-1e and 8-2a to 8-2c of the CAR.

3.3.3 Criticality Hazards

Criticality safety is an important issue in the design and operation of the MOX facility that handles significant quantities of fissile material. Criticality accidents can be caused by violations of safety limits on control of variables such as geometry, mass, density, reflection, moderation, concentration, and isotopics. Criticality events in fuel cycle facilities release a large amount of energy including harmful radiation in a short period of time that can deliver large doses to facility workers.

The CAR provides analyses of potential criticality hazards that are present in the MOX facility and the applicant's approach of carrying out a nuclear criticality safety evaluation and adherence to the double contingency principle in assuring that the risk of criticality remains within acceptable regulatory limits. The review in the FSER focused on the criticality safety design criteria and process description including the nuclear criticality control system in both the AP and MP process units, the design bases of the PSSCs and the commitment to maintaining the double contingency principle and ANSI standards. The review of the applicant's method and approach in NUREG-1821 agrees in principle with the analyses carried out in the CAR although further details are expected to be revealed in the ISA.

3.4 Accidents Contributing to Risk

As mentioned above, there are six types of internal process hazard events or accidents that are reviewed in NUREG-1821. These are (1) loss of confinement accidents (2) fires, (3) load-handling failures such as drops, (4) explosions, (5) criticality, and (6) chemical releases.

The strategy adopted by the applicant is to select a bounding event in each category or sub-category of accidents that, if not prevented or mitigated, could lead to consequences exceeding the performance requirements criteria defined in Part 70.61. A principal structure, system, or component (PSSC) is then defined that would place the event in the appropriate likelihood class defined by 70.61 criteria, i.e., high consequence events would be rendered extremely unlikely and medium consequence events unlikely, etc. In some other cases, such as external natural phenomena hazards, the applicant screened out events based on likelihood alone.

The review by NRC staff provided in Section 5.1.6.3 of the FSER of the evaluation of internal process hazards by the applicant was based primarily on an assessment of the safety strategy and PSSCs at a conceptual level. This was carried out by staff in order to evaluate the potential of the strategy and the PSSCs proposed to guide the development of a design which would meet the 10 CFR 70.61 performance requirements. The criteria that were used in the staff evaluation consisted of a comparison against normally accepted industry practice, consideration of the applicant's design criteria, and the likelihood of performance of the controls based on the consideration of a probability index provided in the standard review plan. Table A-5 in NUREG-1718 contains descriptions of the probability of performance of various types of engineered or administrative controls (primarily for protection of individuals outside the controlled area boundary (IOC)), and/or deterministic arguments primarily for protection of facility workers and/or the environment. Table A-5 also provides a table equating types of controls to approximate probabilities of failure on demand (PFOD).

These values of performance were used at a conceptual level in the staff's safety evaluation and acceptance of the applicant's design and safety strategy for the purpose of granting a construction permit.

The review performed by the NRC in the FSER accepted, in general, the applicant's approach and the designation of PSSCs for preventing or mitigating accident events in various categories. The quantitative risk assessment supplements this determination by showing what performance or reliability has to be displayed by the PSSCs in various accident sequences in order to keep the risk within acceptable limits.

Section 5.1.6.3.1 discusses loss of confinement events, Section 5.1.6.3.2 discusses fire events, Section 5.1.6.3.3 focuses on load handling events and Section 5.1.6.3.4 on explosion events. In each case the total number of postulated events were analyzed by DCS to determine the bounding consequences from each group of events which were then binned into a smaller number of classes to identify a unique prevention or mitigation strategy for each class.

Confirmatory dose calculations were carried out by staff based on the mitigated releases to ensure that the accidents stayed within the criteria of Part 70.61.

Several types of explosion events were analyzed in the CAR ranging from explosions occurring during process operations inside the MOX building to explosions occurring outside in nearby support facilities, in chemical storage areas, and in laboratory facilities. Explosions can result in various kinds of consequences: (1) release of radioactive materials or hazardous chemicals that can lead to exposure of workers, public, and the environment, (2) damage to a confinement boundary, to other PSSCs, or to critical equipment, and (3) potential loss of subcritical conditions. In almost all of the bounding explosion events, the applicant adopted a prevention strategy to lower the likelihood of event occurrence to place it in the highly unlikely category as required by Part 70.61 criteria.

One particular explosive event is a tributyl phosphate-nitrate (red oil) explosion in an AP vessel, tank, or piping. This event is analyzed in some detail in the next chapter in work funded by NRC under a separate project to obtain a quantitative assessment of the risk of a red oil explosion at the MOX facility.

Table 5.1-1 of the FSER provides a summary of the safety assessment of events related to natural phenomena hazards, criticality, external manmade hazards, and chemical hazards, identifying in each case the PSSCs and the safety function they perform. In the case of chemical hazards, the PSSCs include both process safety controls such as the C4 confinement system and administrative controls like process cell entry controls and facility worker actions. Table 5.1-2 provides a safety assessment summary of the process hazards that defines the bounding event selected for each group of hazards, the PSSC that protects the facility worker, site worker, the IOC, or the environment and the safety function it performs. Table 5.1-3 of the FSER summarizes the various PSSCs and their design basis functions and values developed from the safety assessment.

4. RISK-INFORMING THE LICENSING REVIEW

NMSS is moving toward increasing the use of risk insights and information (i.e., risk-informing) in the nuclear materials and waste arenas. Risk insights and information could increase NMSS's efficiency and effectiveness in its regulatory processes: rulemaking, licensing, inspection and enforcement. Guidance for risk-informed decision-making (RIDM) has been developed by NMSS in Risk-Informed Decision-Making for Nuclear Material and Waste Applications [9]. SECY-04-0182 [10] and its Staff Requirements Memorandum provide additional information on the status of risk-informing process within NMSS.

In the license application review process the reviewer must make determinations that the proposed design meets various safety requirements, in particular, those regarding likelihood of consequences in 10 CFR 70.61, and regarding other factors, such as defense-in-depth and double contingency, in 10 CFR 70.64. Guidance for making such determination is found in the MOX Standard Review Plan and supporting Interim Staff Guidance documents. The reviewer has the results of the applicant's ISA to assist in these determinations. However, ISA may be conducted at a level of detail and information quality that is less than a typical quantitative risk assessment. In such cases, a quantitative risk assessment may provide insight into likelihoods, defense-in-depth, and double contingency that would assist in making these licensing determinations. In addition, there is agency guidance on levels of individual risk and other safety factors that could provide an independent perspective on the specific process or control. Failure data from similar processes or controls could be considered in the risk assessment to provide perspective on mechanisms and likelihoods of failure. A well structured risk assessment can also illuminate how well defense-in-depth and double contingency have been achieved. In addition, a quantitative risk assessment can show which accident scenarios have the greatest risk, hence focusing the review on the controls that prevent or mitigate these scenarios. Risk sensitivity studies can evaluate the effectiveness of alternative or improved controls. Thus the role of risk information in these safety determinations is analogous to independent confirmatory deterministic safety analysis by the staff. It is not the direct basis for the reviewers licensing determinations, but provides additional confidence in them.

For the purposes of risk-informing the licensing review of the MOX Facility, the essential elements of a risk-informing process are:

- (1) Performing or adapting a risk assessment that is suitable to the safety or licensing issue in question,
- (2) Obtaining or adapting relative measures related to safety (referred to as risk guidelines in the RIDM) in terms of the metrics calculated in the risk assessment,
- (3) Using a decision algorithm to help guide choices in terms of the outcomes of the risk assessment.

Figure 3 shows a conceptual outline of the process at a high level. The process begins with a delineation of the major issues impacting safety as revealed by the review of the ISA submitted by the applicant. An example of a major safety issue for the proposed MOX facility is red oil excursions in the manufacturing process. These issues are analyzed using a detailed risk assessment methodology appropriate to the problem at hand and the risk is evaluated in terms of a suitable risk metric. In carrying out the risk assessment adequate attention is given to ensure that the assumptions made remain valid through the process of estimating risk, that uncertainties,

both aleatory and epistemic, are considered, and defense-in-depth and safety margins are maintained. If the estimated risk, in terms of the RIDM process defined below, is acceptable then the ISA and design may be considered valid based on the risk calculation which increases confidence in the robustness of the design.

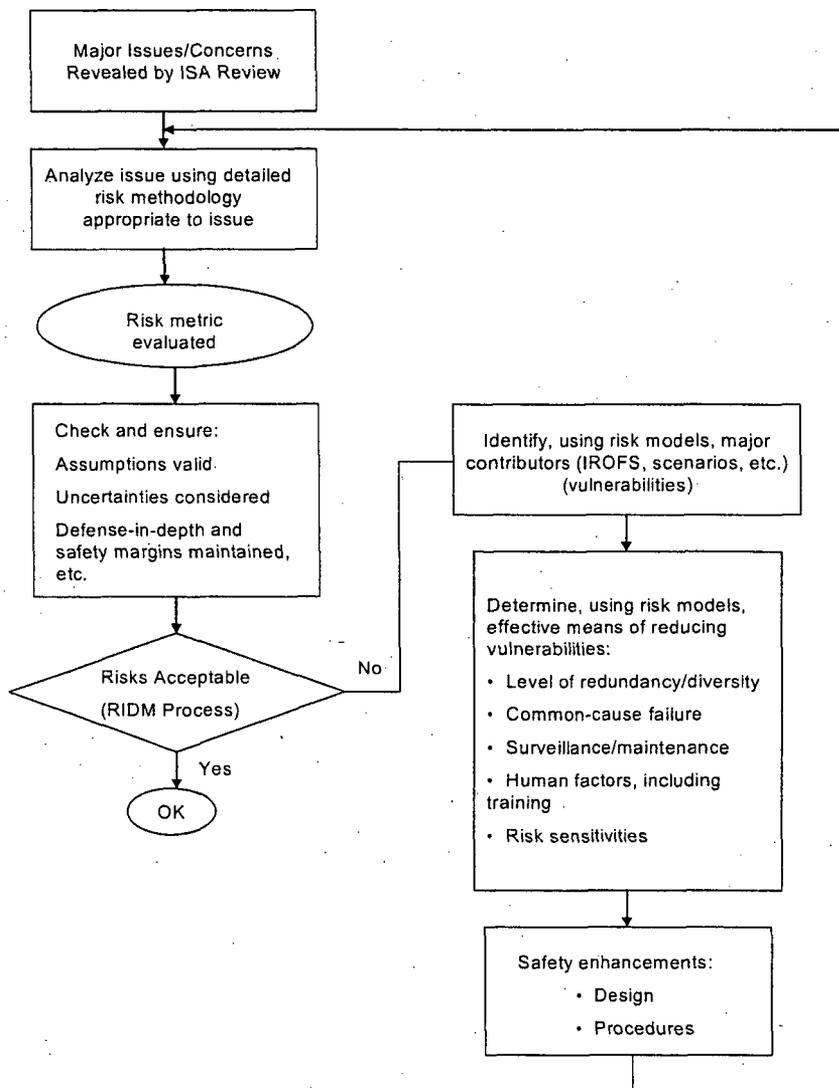


Figure 3 Risk-Informing Licensing Review

However, if the risk estimate is not acceptable, then the main contributors to risk, i.e., the significant vulnerabilities of the design to various kinds of challenges, are identified using the risk models and effective means of reducing the vulnerabilities are determined. This process would examine various factors such as level of redundancy, diversity, independence of events, and common cause failures, in addition to management and administrative measures such as procedures, surveillance, and maintenance and human factors issues such as training. Sensitivity

analyses would also be conducted to indicate where additional attention should be focused. For new, proposed facilities, such as the MOX facility, this process would indicate where possible changes to the design or the procedures might be most effective in reducing vulnerability and enhancing safety

4.1 The RIDM Process

Risk measures or guidelines are one element of the overall risk-informed decision-making process; they serve as a benchmark or yardstick to evaluate the significance of the change in risk due to implementation of the issue or regulatory action alternative and are used to guide a risk-informed decision-making process. Quantitative guidelines do two important things: (1) establish the quantitative metrics for informing safety decisions, and (2) provide the measurable scale for determining the level of risk that exists. Hence, risk guidelines can be used to inform decisions associated with reducing unnecessary conservatism in purely deterministic approaches, or can be used to identify areas with insufficient conservatism in deterministic analyses and provide the supporting information for identifying the potential need for additional requirements or regulatory actions.

In the guidance for Risk-Informed Decision Making for the Nuclear Materials and Waste Arenas [9], six draft quantitative health risk guidelines (QHG) are proposed. The QHGs are couched in terms of the risk of early fatality, risk of latent cancer fatality, and risk of severe injury to both the public and the workers. The formulation in terms of health guidelines was done because it was desirable, in risk terms, to have a framework that is consistent with the reactor counterpart (which was formulated in terms of Reactor Safety Goals in the Policy Statement of 1986 [11]). The six draft QHGs cover the risks of early fatality, latent cancer fatality, and severe injury for both the public and the workers and are stated as follows:

Individual Public Acute (QHG 1): A risk to an individual member of the public of a prompt fatality, due to inadvertent or accidental exposure from nuclear materials and waste activities should not exceed one-tenth of one percent (0.1 percent) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. public are generally exposed. This could be regarded as "negligible additional risk" in risk-informed decisions. The draft QHG1 value is 5E-7 per year.

Individual Public Latent (QHG 2): A risk to an individual member of the public of a latent cancer fatality due to inadvertent or accidental exposure from nuclear materials and waste activities should not exceed one-tenth of one percent (0.1 percent) of the sum of latent cancer fatality risks resulting from other accidents to which members of the U.S. public are generally exposed. This could be regarded as "negligible additional risk" in risk-informed decisions. The draft QHG2 value is 2E-6 per year.

Individual Public Injury (QHG 3): A risk to an individual member of the public of severe injury, due to inadvertent or accidental exposure from nuclear materials and waste activities should not exceed one-tenth of one percent (0.1 percent) of the sum of severe injury risks resulting from other accidents to which members of the U.S. public are generally exposed. This could be regarded as "negligible additional risk" in risk-informed decisions. The draft QHG3 value is 1E-6 per year.

Individual Worker Acute (QHG 4): A risk to a worker of a prompt fatality due to inadvertent or accidental exposure from nuclear materials and waste activities should not exceed one percent of

the prompt fatality risk in all higher risk industries. This could be regarded as "negligible additional risk" in risk-informed decisions. The draft QHG4 value is 1E-6 per year.

Individual Worker Latent (QHG 5): A risk to a worker of a latent cancer fatality due to inadvertent or accidental exposure from nuclear materials and waste activities should not exceed one percent of the latent cancer fatality risk in all higher risk industries. This could be regarded as "negligible additional risk" in risk-informed decisions. The draft QHG5 value is 1E-5 per year.

Individual Worker Injury (QHG 6): A risk to a worker of severe injury due to inadvertent or accidental exposure from nuclear materials and waste activities should not exceed one percent of the severe injury risk in all higher risk industries. This could be regarded as "negligible additional risk" in risk-informed decisions. The draft QHG6 value is 5E-6 per year.

Reference [1] provides a detailed discussion of the rationale for and the bases underlying the chosen values of the various quantitative health guidelines. The reactor safety goals focus only on the individual public risk of acute and latent cancer fatality, i.e., the analogs of QHG 1 and QHG 2 above, and the numerical values recommended by the Commission in its Safety Goal Policy Statement are the same as those shown for QHG 1 and 2.

For fuel cycle facilities, 10 CFR Part 70, in particular, 10 CFR 70.61 requirements outlined in Section 1.2 above, [4] provides regulatory requirements in terms of performance criteria expressed in qualitative terms of likelihood, highly unlikely and unlikely, and quantitative terms of consequences, radiological doses and chemical exposures.

NUREG-1520 [1] and NUREG-1718 [2] provide guidance and examples on the notions of *unlikely* and *highly unlikely* that are introduced in 10 CFR 70.61. In particular, NUREG-1520 provides guidance about the occurrence frequency of unlikely and highly unlikely events, that is less than 1E-4 per-event per-year for unlikely and 1E-5 per-event per-year for highly unlikely. However, the regulation does not require a quantitative determination of likelihoods. The numerical guidance in NUREG-1520 and NUREG-1718 is provided to inform the NRC staff reviewer. 10 CFR 70.61 requires that intermediate consequence events will be rendered unlikely and high consequence events will be rendered highly unlikely. This is consistent with the idea of an iso-risk line, where risk is regarded as probability multiplied by consequence.

There are several potential hazards at the MOX facility that can lead to accidents with varying levels of consequence and likelihood. One of these hazards, mentioned above in Chapter 3, is the red oil excursion, a potentially explosive event. A red oil excursion in a process unit is a high-temperature, high pressure release that can lead to a breach of the vessel or other equipment. In principle, such a release can exceed the criteria for a high consequence event for a facility worker and, in terms of the performance criteria of 70.61, each red oil excursion scenario or sequence would have to be shown to be "highly unlikely" in qualitative terms. (In quantitative terms, based on the guidance contained in NUREG-1520 and NUREG-1718, highly unlikely can be interpreted by an NRC reviewer as having a frequency of < 1E-5 per year). Moreover, a red oil event would also pose a threat to the life of a facility worker in the vicinity of the process unit where the event occurs. Hence the applicable quantitative health guideline for analyzing the risk significance of a red oil excursion event is QHG 4, the worker risk of a prompt fatality.

Thus the evaluation of the frequency of a red oil excursion and the worker prompt fatality risk guideline QHG 4 can be useful in risk-informing an NRC reviewer on the issues related to the acceptability of red oil scenarios and the measures employed to prevent or mitigate them. It should

be pointed out, however, that QHG 4 incorporates all accidents, not only a red oil excursion, that can lead to a worker fatality. Hence the frequency that refers to a comparison with QHG 4 is a sum over the frequency of all accident scenarios that potentially have worker fatality as an outcome. In doing this, one approach is to use a three-level decision diagram as described in Reference 4 and discussed below.

4.2 Three-Region Diagram

SECY-04-0182 [10] provides a discussion of the risk to individuals from a regulatory action that is based on a concept of three regions of risk to individuals.

- (1) If a proposed action results in risk to individuals that is judged to be too high, this may be sufficient grounds to reject it.
- (2) If the resulting level of risk to individuals is judged to lie in the tolerable region (and other factors are adequately addressed), then alternative actions should be preferred based on highest net cost-benefit.
- (3) Proposed new requirements to reduce risk, when it is already in the negligible risk region should normally not be pursued.

Reference [2] indicates that above principles embodied in the three-region decision framework can be applied to managing risk from accidents or unanticipated events (such as, for example, red oil excursions). This risk involves both the frequency or probability of accident occurrence for each scenario, as well as the consequence that would occur. Since there are multiple possible accident scenarios, risk is evaluated as the sum over all scenarios of the product of frequency and consequence (or the probability of fatality given that level of consequence). Thus, in the three-region framework, risk is often expressed as frequency of fatality. However, Reference [10] states that unlike routine doses under 10 CFR Part 20, the Commission has not ascribed generally applicable numerical limits on risk due to accidents. The negligible level of risk that is represented by the value of the relevant QHG is useful as a screening tool. Negligible risk levels are well below the limit levels of risk, and represent an insignificant addition relative to average normal risks.

The three-region risk diagram displayed in Figure 4 is a conceptual representation of these decision considerations. As indicated in Reference [10], the "lines" separating the regions of unacceptable, tolerable, and negligible (or insignificant) risk are not precise but take into account uncertainties that impact the risk. Such uncertainties are often accounted for by incorporating considerations related to defense-in-depth, such as levels of diversity and/or redundancy, and safety margins or by prescribing conservative methods for calculating and analyzing risk.

This diagram divides the risk space for any applicable health risk metrics (public or worker acute fatality, etc.) or equivalent surrogate risk metrics into three regions: an unacceptable risk region, a tolerable risk region, and an insignificant risk region. The lower line shown in Figure 4 that separates the insignificant risk region from the tolerable risk region corresponds to the quantitative health guideline below which there is no measurable benefit of reducing the risk further. As discussed in Reference [2], the upper line corresponds to the risk implication of the regulatory limit that separates the unacceptable risk from the tolerable risk region. The tolerable risk (TR) range is further regarded to be comprised of two regions, an upper TR (UTR) range and a lower TR (LTR) range. This can be helpful in the consideration of the impact of uncertainty on the calculated values of the risk.

The risk-informed decision algorithm process based on the QHGs outlined in Reference [9] focuses on the calculated mean values of the risk metrics. As discussed above, in making decisions with the aid of this diagram, it is very important to also give due consideration to factors such as defense-in-depth and safety margins and assure that they are maintained throughout the risk acceptance process.

4.3 Application to the MOX Facility

To apply the risk-informed decision making scheme in Figure 4 to particular accidents in the MOX facility a risk metric appropriate to the class of accidents that have the same outcome should be selected, and its value, summed over all accidents in the class, should be compared to the relevant quantitative health guideline. For example, for the analysis of red oil excursions, the applicable QHG to consider is QHG 4, and the relevant risk metric is the risk of worker prompt fatality. The proposed value of QHG 4 in Reference [9] is $1E-6$ per year which sets the boundary between the negligible and the tolerable risk regions. In some of the pilot applications of the risk-informed decision making process [1], the boundary between the tolerable and unacceptable regions was set two orders of magnitude higher than the QHG level. This approach has also been taken by the UK Health and Safety Executive [12] in its risk-informed decision making approach to public and worker safety issues. This approach would imply that for QHG 4 the boundary separating the tolerable from the unacceptable would be set at $1E-4$ per year. If the frequencies are plotted on a logarithmic scale, the "highly unlikely" likelihood guideline of $1E-5$ per year or less for potentially high consequence events such as red oil excursions extends downwards from the lower tolerable to the negligible region of Figure 4.

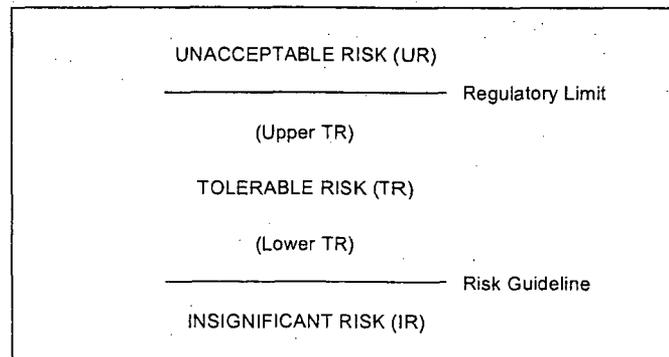


Figure 4 Three-Region Risk Acceptance Diagram

However, the highly unlikely guideline category applies to individual scenarios or sequences while the QHGs are an aggregate over all sequences that have the same outcome. Hence, in terms of Figure 4, the sum of the frequencies of all outcomes, that pertain to the risk metric in question, must be summed to compare with the QHG.

If we conservatively identify the occurrence of a red oil excursion with a conditional probability of 1.0 for a worker prompt fatality, then the total frequency of red oil excursion seems to be a useful subsidiary parameter that can be equated, in principle, with QHG 4. In this way, the frequency of red oil scenarios estimated using probabilistic risk assessment methods can serve two purposes.

First, individual sequences can be evaluated against the highly unlikely likelihood guideline established by the performance categories of 70.61. Second, the total frequency can be used as a surrogate for the worker prompt fatality risk metric in assessing risk in terms of the risk-informed decision making scheme proposed in Reference [2] and illustrated in Figure 4.

The risk guideline decision algorithm process focuses on the calculated mean values of the risk metrics before and after the action or issue under consideration is implemented. In making decisions with the aid of this diagram, it is very important to also give due consideration to other factors, such as to defense-in-depth and safety margins and to assure that they are maintained throughout the risk acceptance process.

4.4 Risk Assessment of Red Oil Excursions in the MOX Facility

Recently, a draft quantitative risk assessment [13] of red oil excursions in the MOX facility has been completed based on the design details revealed in the CAR [5] and reviewed in the FSER [4]. Even though the numerical results are preliminary and approximate, some of the methods and results and insights gained from this work are summarized here to indicate how probabilistic risk assessment can usefully supplement the qualitative risk work and thus assist the regulatory process by focusing attention on the areas impacted by risk.

4.4.1 Description of Red Oil Phenomenon

The purification and/or separation of metals in the MOX facility is accomplished by a process known as liquid-liquid extraction or solvent extraction that is also commonly used in the chemical and petrochemical industries. In this process, one or more components, e.g., metal and impurities, are transferred between two immiscible liquid phases, typically an organic phase and an acid aqueous phase. The solvent proposed to be used in the MOX facility is tributyl phosphate (TBP) diluted in an organic matrix to improve the physical characteristics of the organic phase. The diluent is hydrogenated propylene tetramer (HPT) (a relatively inert and radiation resistant organic chemical), it reduces the viscosity and density of the organic phase to improve phase separation and also act to lower actinide concentration in the liquid and hence reduce criticality concerns.

Red oil is defined as a substance of varying composition formed when organic constituents react with nitric acid. In the AP process, these substances may form by reactions of tributyl phosphate (TBP), its decomposition products, and impurities in the diluent with nitric acid. Previous studies have shown that red oil decomposition is exothermic and involves an explosive process leading to a sudden release of a large amount of energy, therefore, there is a risk of a runaway reaction(s) and overpressurization.

The risk of red oil formation and decomposition exists in any area that leads to a contact of TBP and other organics with an oxidizing agent, nitric acid, or receives organic material that may have previously contacted nitric acid or aqueous material that may have come in contact with organic compounds. The undesirable reactions are promoted by the presence of unstable organic constituents, such as TBP decomposition products, high nitric acid concentration, high temperature and long residence time. Severity of events, such as rupture of primary containment, is increased by inadequate heat removal and inadequate vent area.

The rate of formation and possible decomposition of red oil and/or organic components, such as TBP, is enhanced by:

1. Nitric acid concentration (in the proposed facility, this varies from low acidity to about 13.4 molar)
2. Temperature (normal operating temperatures, except in the calciner, are maintained below 130 C)
3. Residence time (depending on the equipment involved, this may vary from a few minutes to many days for storage)
4. Efficiency of contact (mass transfer)

as shown in Figure 5.

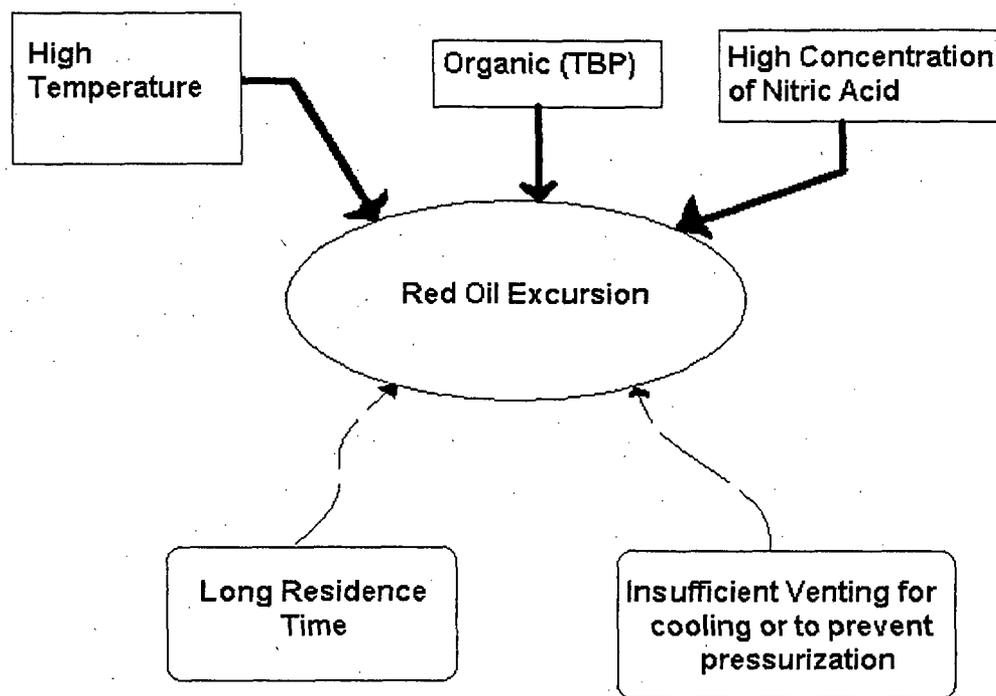


Figure 5 Necessary Conditions for a Red Oil Excursion to Occur

Some previous studies have indicated that the rate of red oil exothermic decomposition is negligible below 130°C. While this may be a reasonable criterion for process equipment where residence times tend to be minutes or less, and the material is renewed frequently, it may not be so in tanks and dead legs in the piping system. Conditions for red oil reactions are likely to be present for days, even months, in such locations.

4.4.2 Criteria and Condition Tree for Red Oil Excursion

It is useful to identify certain criteria that serve to categorize the conditions under which red oil excursions can be initiated. At the outset, it is assumed that organic material (TBP) and nitric acid

is present in the same location as this is a necessary condition for the red oil reaction to be initiated. This can happen due to a number of reasons that have been discussed in more detail in Reference . Once the materials are present, the remaining issues affecting the reaction relate to the temperature, the temperature ramp rate, the presence of impurities, and adequate venting. Venting is a means of removing heat and, for a closed vessel, aqueous makeup must be available to provide a means for removing the heat of the exothermic reaction. Essentially, these conditions determine whether the red oil excursion occurs at all or takes place at a high or low pressure which has further implications for the consequences of the excursion.

A review of experimental data showed that if there is no vent or the vent size is small, and the temperature reaches 130 C or higher the red oil excursion will occur at a high pressure. On the other hand, the Tomsk event in 1993 showed that in the absence of a vent and the presence of impurities, the red oil excursion could be initiated at a much lower temperature estimated to be approximately in the range of 90°C. Impurities such as extractable salts, or degradation products of hydrolysis or radiolysis reactions that are not removed, can influence the red oil excursion phenomenon. Conversely, if there is a sufficient vent the red oil excursion may not occur at all or, if it does get initiated for some reason, may occur only at a low pressure. Between 90°C and 130°C, an intermediate temperature is the boiling point of butanol, approximately 117°C, that can serve as a precursor to a red oil excursion. These considerations permit the development of the following screening criteria for the initiation temperature of the red oil excursion phenomenon that can be applied to the development of accident event sequences:

If the vent is large and there are no impurities the initiation temperature $T = 130^{\circ}\text{C}$

If the vent is small and impurities are present, the initiation temperature $T = 90^{\circ}\text{C}$

If the vent is small and there are no impurities, the initiation temperature $T = 117^{\circ}\text{C}$

If the vent is large and impurities are present, the initiation temperature $T = 117^{\circ}\text{C}$

These temperatures are identified for the sake of scenario identification and development in conjunction with events which can lead to partial vent failure or where there is a potential for impurities in the process vessel. These possibilities are graphically displayed in the event tree shown in Figure 6. Following convention, the upper line at each branch point indicates success and the lower line failure. The entry point in the tree is the presence of the materials, organics (TBP) and nitric acid, that are necessary for a red oil excursion. If venting succeeds and there are no impurities such as extractable salts, etc., then the following questions relate to the temperature, in terms of the four criteria stated above, that determines the outcome of that particular sequence of events.

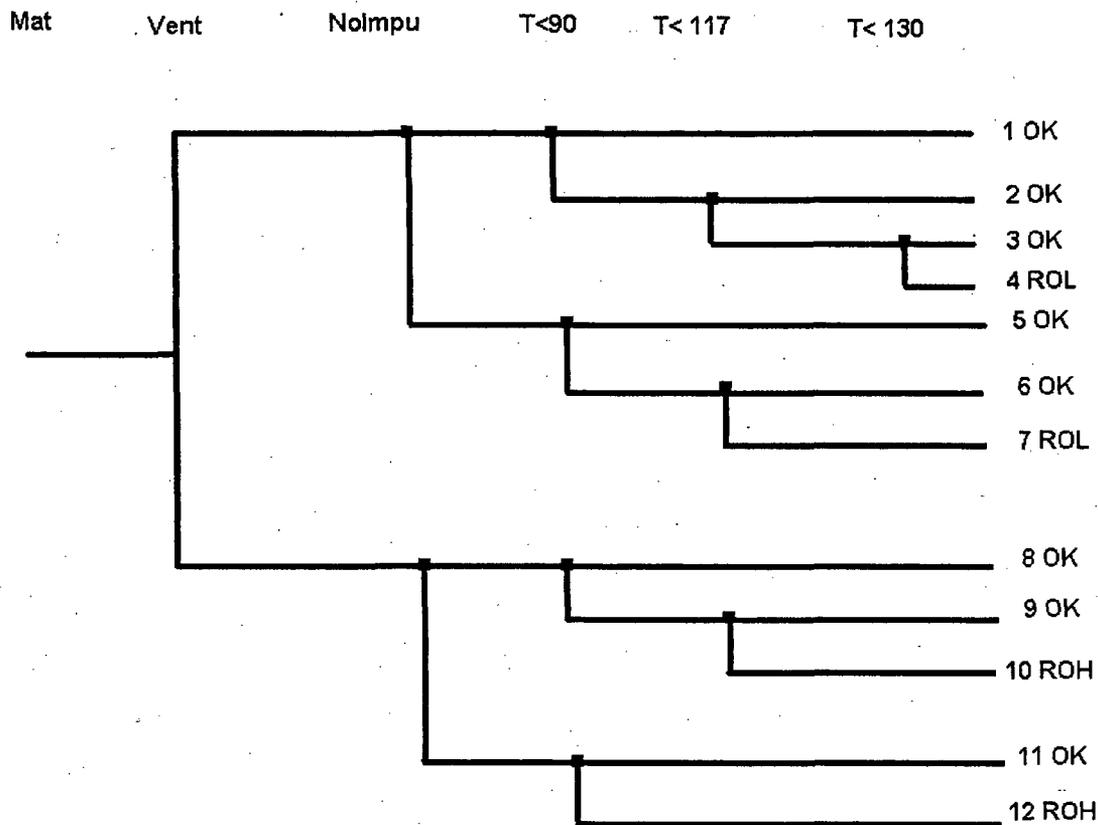


Figure 6: Condition Tree for Red Oil Scenarios

In Figure 6, the end state ROH (red oil excursion at high pressure) describes all the scenarios which occur when the vent size of the vessel or equipment containing TBP, nitric acid, and other degradation products or impurities, is below the criterion provided in the CAR of mass of organics per unit vent area (i.e., 32 kg/cm²). The end state ROL (red oil excursion at low pressure) describes scenarios where a red oil reaction is initiated but there is sufficient vent area available in the vessels or equipment containing TBP, nitric acid, and other byproducts so as to prevent over-pressurization and a runaway reaction from excessive oxidation due to initiation of the red oil reaction. Sufficient venting for the ROL scenarios is defined to be a vent size that is consistent with Figure 8.1-2 in the NRC Final Safety Evaluation Report [4]. This figure provides a relationship between vent area, the mass of organic material present and the internal pressure generated by the red oil reaction. A limit of about 32 kg/cm² of organic material per unit vent area demarcates the safe from the unsafe range as displayed in Figure 8.1-2 of the FSER. The CAR [2] mentions a design basis of 12.5 kg of organic material per cm² of vent area for the offgas treatment system which provides a safety margin of approximately a factor of 2.5 with respect to the above criterion. For closed systems, the CAR provides for temperature controls and aqueous inventory makeup to remove 1.2 times the energy generated in the system by the external heat source and the chemical energy of the reaction, as stated in the CAR and the FSER.

4.4.3 Prevention of Red Oil Scenarios

As a safety precaution against the red oil excursion, the facility design proposes a defense in-depth strategy to prevent and control potential red oil events. They include chemical safety controls, the Process Safety Control System (PSCS), and the offgas treatment system. The safety functions achieved by each of these systems are noted below. The statements in italics are taken or interpreted from the CAR document. They are consistent with the analyses provided in the FSER.

Chemical Safety Control: Ensure that the diluents used are not degraded and have no cyclic chain hydrocarbons.

The control measure used to ensure this is not known at this time. However, it is expected to be addressed through procedures, administrative controls, sampling procedures, etc. This could include a series of actions needed prior to startup and routine sampling/analyses of tanks and vessel contents. It is also important to note that issues regarding Butanol could also be addressed as a part of the chemical safety control process.

Process Safety Control System ensures that the following items are controlled:

Temperature of the solution containing organics is restricted to temperatures within safety limits such that the rate of energy generation is maintained within the safety limits.

The temperature of steam (hot water) used to heat the process vessel is limited to 133°C.

Adequate aqueous phase inventory is available to provide evaporative cooling in a closed system.

Bulk fluid maximum temperature of 125°C with a maximum heat up rate of 2°C per minute is used to control the aqueous phase continuous feed and injection (the steam heating may also be shut off).

Note that such cooling is effective only when the pressure is atmospheric since the nitric acid /water azeotrope boiling point is 120.4°C. So a vessel has to either be open or vented for cooling to be successful.

The residence time of organics containing oxidizing agents and potentially exposed to high temperature and/or radiation field are limited.

It will be addressed in the ISA.

Offgas Treatment System provides that the following systems are designed and maintained:

An adequate exhaust path for aqueous phase evaporative cooling in the process vessel is available, thereby providing a mechanism for heat removal.

Venting of equipment/vessel that contains TBP and its associated by-products is available to prevent over-pressurization in the event of the excessive oxidation of TBP or its degraded products.

NUREG-1821 notes that the "applicant indicated that solvent carryover can be considered as an anticipated event in the facility" and that DCS "has committed to further evaluate the red oil phenomena." Since carryover (and perhaps accumulation) of organics is an anticipated event, the

performance and reliability of the systems, equipment, and administrative controls that are in place to prevent or mitigate a red oil excursion become an important issue to be analyzed from a risk standpoint. The staff concluded that "operational concerns related to...possible abnormal conditions are best addressed in the ISA when more specific design information is expected to be available." The assessment of red oil excursions in the MOX facility is intended to focus attention on the more risk significant aspects of the facility in order to help NRC staff with their review of the forthcoming ISA.

4.4.4 Red Oil Events in the AP Process

There are five process units where organics and nitric acid actually or potentially come into contact during the AP process. These are: (1) Purification Cycle Unit, (2) Solvent Recovery Cycle Unit, (3) Oxalic Precipitation and Oxidation Unit, (4) Oxalic Mother Liquor Recovery Unit, and (5) the Acid Recovery Unit.

These five units are potential candidates where red oil excursions can occur since they are the only units in the MOX facility where the acid and organic phases come in contact. Recalling the necessary conditions for the initiation of the autocatalytic oxidation (red oil excursion) reaction, each of the five process units is reviewed below in terms of the equipment it employs, the sequence of operations, and the conditions under which the operations occur.

In Reference [13], the accident risk space for red oil excursions was divided into two parts: the first can be termed a generic risk of red oil excursion due to the occurrence of events, such as fire, that can potentially happen in any of the five process units and serve as an external energy source to raise the temperature of acid-organic phases to a level where the autocatalytic reaction can be initiated. For example, TBP degrades by hydrolysis to form, successively, dibutyl phosphoric acid, monobutyl phosphoric acid, or phosphoric acid, and butanol. Butanol has a low flash point of around 40°C and a relatively low boiling point (117°C) and is, therefore, a potential combustible hazard in case of a fire. The degradation rates for TBP increase with temperature and nitric acid concentration and, above a certain temperature, the degradation which is exothermic proceeds at a fast enough rate to generate large amounts of heat and detonable vapor. The heat generated increases the bulk liquid temperature and, therefore, the rate of reaction and can ultimately lead to an autocatalytic reaction characteristic of the red oil excursion.

The second part of the accident space is from events that are specific to the operations that are carried out in each unit. A scoping qualitative assessment of the operations in each unit was carried out to ascertain which of the units presented a higher risk of a red oil excursion and should be studied further quantitatively. In two units, the acid recovery and oxalic mother liquor recovery units, the risks were judged to be higher due to the conditions under which the operations are conducted and these were taken up for a quantitative analysis. In the purification and solvent recovery units, the risks were judged to be lower because the operations are conducted at either relatively low (ambient) temperature or they involve very low nitric acid concentration. There is a possibility of a red oil excursion in the oxalic precipitation and oxidation unit exists if organic material manages to reach this unit, however, by design, this unit is designed to handle large volumes of gas flow so even if some red oil is formed the chances of a high-pressure event are low.

4.4.5 Red Oil Scenarios in the Acid Recovery and Oxalic Mother Liquor Recovery Units

Major components within the acid recovery and oxalic mother liquor recovery systems were examined for potential for red oil scenarios. Approximate inventories of various materials were determined. The operating temperatures for the major components were identified and they were compared to the required temperatures for the red oil scenarios considered in the condition tree showed in Figure 6. If the necessary condition for a red oil scenario was not satisfied, a failure in administrative control, system hardware, or operator action was simulated to induce a red oil scenario consistent with those shown in Figure 6. As an example, if the necessary material was not present, a potential for improper transfer of the needed materials for red oil scenario from adjacent components was examined. The examination was in most cases limited to identifying a single path where the materials could have been inadvertently transferred either through faults in operation or failures of the safety barriers that are either administrative or hardware oriented. Various mechanisms for component heat up were examined. The objective was to identify a fault mechanism within or adjacent to the component where a temperature of at least 90°C could be achieved by the materials such that the red oil scenarios in the presence of degraded chemicals could not have been ruled out. Depending on the heatup mechanism and the expected material temperature, the potential for presence of degraded chemicals were also examined. Two types of heat up mechanisms were typically considered. Generic sources of heat such as ex-vessel fire or in-vessel combustion, and system specific heat sources such as chemical, radioactive heating, hot steam, hot water, and electrical components were considered as a part of the analysis. Each red oil scenario which was identified in this manner was examined for the various built-in prevention strategies against the initiation of red oil scenarios including the administrative controls. Finally, the built-in mitigation capabilities for controlling the consequence of red oil scenarios including venting were identified for further analysis. A major component in the system was screened out if no mechanism could be found for exposing the required materials to the necessary temperature for red oil scenario. Some components could have been screened out since the likelihood of the red oil scenario was judged to be significantly smaller than other scenarios already included.

Using the above approach, all applicable scenarios were defined and mapped into the conditions provided by the condition tree of Figure 6.

4.4.5.1 Acid Recovery System Scenarios

Two types of red oil scenarios are defined for the acid recovery system and equipment: generic scenarios, and specific scenarios. Generic scenarios are applicable to an entire class of components (in contrast to a specific component). The components considered for the generic scenarios in the Acid Recovery System are mainly tanks or vessels including the evaporators that meet the required material conditions for red oil scenario but lack the heat source or required high temperature. The specific scenarios, on the contrary, are component specific and they are revealed through systematic application of the scenario identification procedure that was discussed earlier.

Three generic heat sources were considered for potentially causing a red oil scenario. These are ex-vessel fires, in-vessel combustion, and slow internal heat up of the materials due to slow chemical reactions or radiation.

Fires in a process cell could provide the heat source to the materials contained in the affected vessel or tank for initiating a sustained red oil scenario. The likelihood of fire in these process cells

are controlled by preventing the introduction of ignition sources from outside by operators or facility workers through strict administrative control requirements. During normal operation, the process cell design precludes the entry of personnel who could introduce ignition sources. The design of the fire cell walls and fire barriers ensures that a fire from the outside of the cell cannot be propagated inside to the process unit. The potential for in-situ ignition sources is also eliminated through the following design features:

1. No use of electrical equipment within the process cells,
2. Grounding of equipment within process cells, and
3. The use of controls that ensure that potential chemical reactions that may result in a fire are made highly unlikely.

The third item above is discussed further in connection with the next two scenarios: combustion, and slow heat up.

The likelihood of a fire in the vicinity of components in the acid recovery system which could initiate a red oil scenario is expected to be low, in the range of $1.0E-3$ to $1.0E-4$ per year. This range of likelihood is determined based on the equivalent fire frequency in Nuclear Power Plants caused by transient fires in clean areas with low combustible loading. If one includes a severity factor of about 0.1, that is 10% of such fires would be large enough to cause the heat up of the liquid contained in the tank and initiate a red oil scenario, an accident likelihood range of $1.0E-4$ to $1.0E-5$ per year would be estimated.

Combustion caused by other flammable materials both in-vessel and ex-vessel could induce a red oil exothermic reaction. A general concern is the presence of degraded chemicals such as butanol. This facility is designed such that the various materials, including even distilled water, are recycled to the maximum extent possible. The degraded organic byproducts could recycle through the system for a relatively long time, before they are detected and removed. Butanol is one of the last byproducts of the chemical decomposition of the organics. Butanol's solubility in water and its boiling point of about 117°C , makes it a companion candidate to the process water as it is transported either as liquid or vapor through various stages of the process. The low flash point of butanol ($\sim 38^{\circ}\text{C}$) makes it a highly flammable material in various pipes, tanks, and vessels. The failure to control butanol and its removal from the system could create a potential for a heat source that could initiate the red oil scenario in those areas where the material is available but the process temperature is relatively low.

The likelihood of this scenario cannot be estimated at this time pending availability of more information on how butanol concentration is maintained in a safe range through various administrative controls during operation. The frequency range for butanol combustion is accordingly assumed to be comparable to that of the fire initiators.

Slow heatup due to various chemical reactions and radiation heating is possible if the heat transfer area for cooling is limited. This may occur when there is a low level in the tank (which limits heat transfer), long residence time (such as a long shutdown) causing chemical degradation, and failure of administrative controls. The likelihood of such events is expected to be low and the frequency is assumed to be in the range of $1.0E-4$ to $1.0E-5$ per year comprised of the following elements: 0.1 factor assumed for long shutdowns, 0.01 ($5E-3$ to $5E-2$ per SRS data) for failure of

administrative controls, and 0.1 probability for occurrence and/or persistence of the vulnerable conditions in which the physical phenomenon can occur.

Red oil formation and decomposition is most likely in the evaporator EV 6000 because of its higher operating temperature and higher nitric acid concentration, and in tank TK 3000 which could heat up due to its radioactive contents. Detailed descriptions of the lay out and configuration of these components are available in the CAR [5] and in Reference [13]. The following scenarios are considered for a red oil excursion in EV 6000:

800
SRI

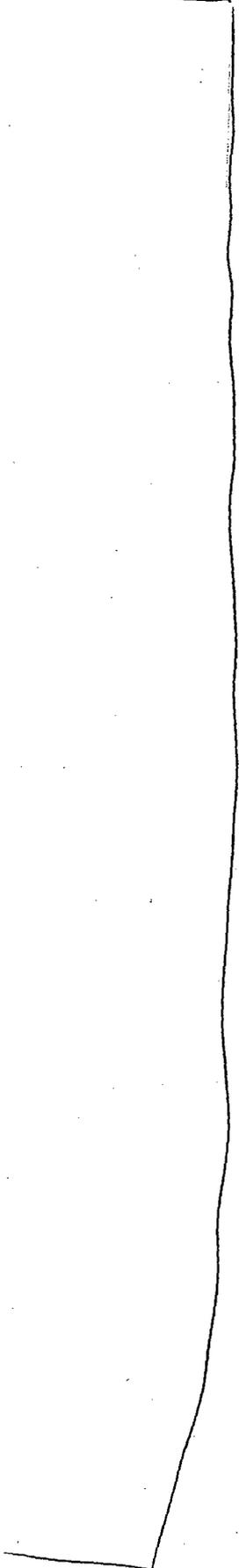
BUO
SRE



040
SRE

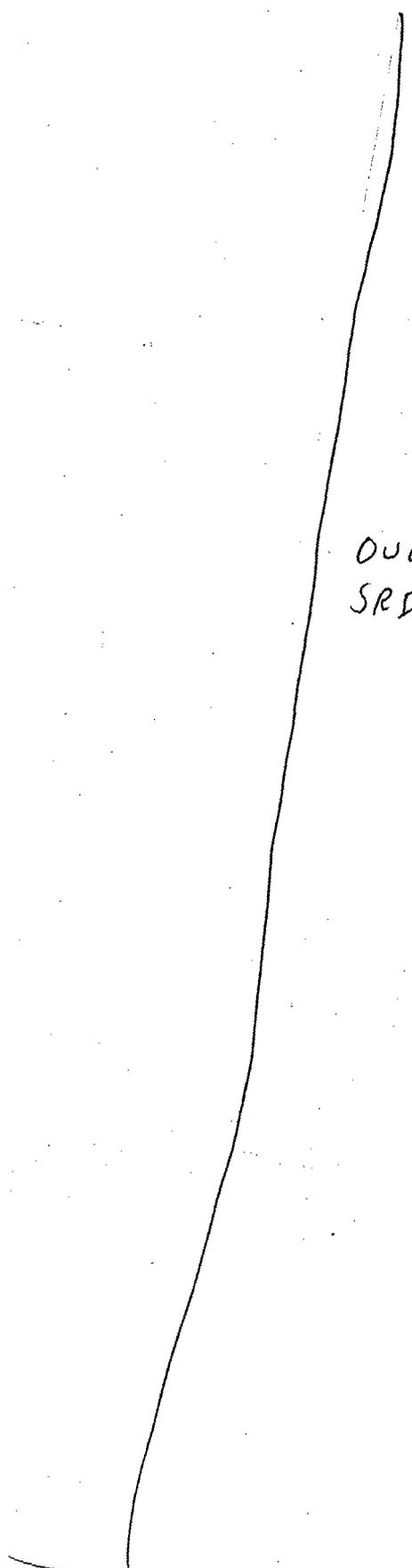
000
SRP

000
SRP

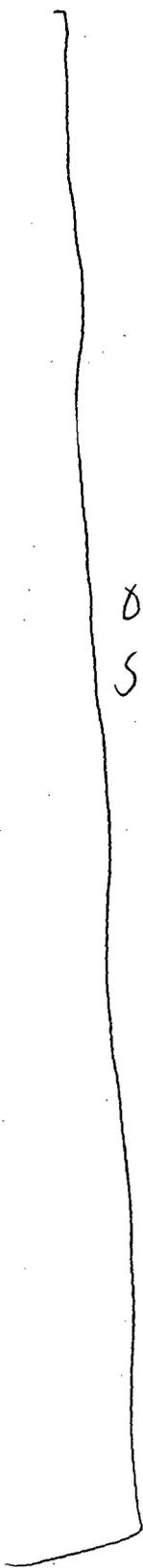


000
SRE

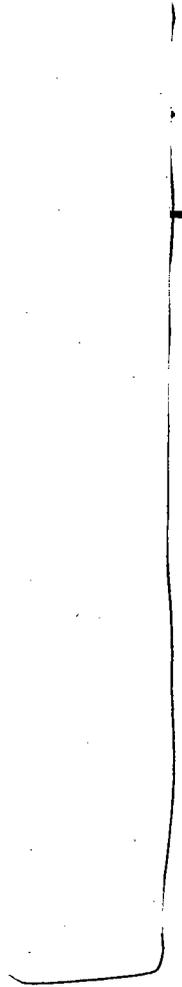
000
SRT



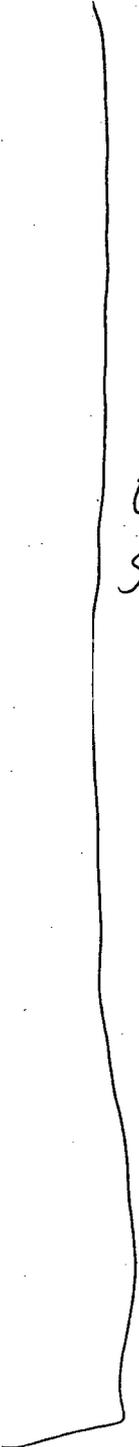
OUU
SRF



000
SRE



000
SRE



000
SRE

DWO
SRI

4.5 Possible Risk Importance Measures

Risk importance measures are an important part of the risk assessment since they help to establish which plant features, systems, structures, and components, (SSCs), along with procedures are important to controlling risk. They can be used to identify the relative safety significance of various SSCs and thus help to establish administrative programs such as special treatment which help to ensure that a particular system or component for which credit is taken will actually perform under accident conditions.

At this stage of the design of the MOX facility and the state of knowledge about risk technology that is applicable to such facilities, it is premature to attempt to describe risk importance measures. They will be taken up at a later stage of development of the risk assessment.

4.6 Considerations of Defense-in-Depth, Uncertainty, and Safety Margin

NRC's safety philosophy has emphasized the concept of defense-in-depth to compensate for uncertainty and ensure that there is adequate safety margin between the severity of the phenomena that may occur in the course of an accident and the ability of a system to accommodate them. A Commission White paper [17] on risk-informed and performance-based regulation states "Defense-in-depth is an element of the NRC's Safety Philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident or naturally caused event occurs at a nuclear facility." In its discussion on risk-informed approach and defense-in-depth the White Paper further states, "Although uncertainties associated with the importance of some elements of defense may be substantial, the fact that these elements and uncertainties have been quantified can aid in determining how much defense makes regulatory sense." In a broad sense, the objective of defense-in-depth is to ensure that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility.

The principles of defense in depth include the following: measures for both accident prevention and mitigation should be provided, the accomplishment of key safety functions should not be dependent upon a single element of design, construction, maintenance or operation, and uncertainties in equipment and human performance should be accounted for in meeting reliability and risk goals. Defense-in-depth measures associated with these principles include redundancy, diversity, and safety margins. Redundancy enhances the reliability of independent means; diversity (and separation) generally provide protection against dependent (common cause) failures of multiple means. Allowances in excess of minimum requirements for physical parameters such as the capacities of hydraulic, electrical and structural components contribute to safety margins that ensure unanticipated increases in demand can be met. Allowances in excess of minimum requirements for temporal parameters, such as time needed for operator actions and preventive systems to correct for deviations, contribute to safety margins that ensure deviations can be remedied even after some initial lapses.

Uncertainties are generally been categorized into random, or stochastic uncertainty (also referred to as aleatory) and state-of-knowledge uncertainty (also referred to as epistemic) [18]. Random uncertainty arises from the fact that events or phenomena occur in a random or stochastic manner, such as a pump failing to start due to a random failure. Random uncertainty is well suited to analysis via probability theory and this type of uncertainty is addressed in PRAs because it is embedded within the structure of the probabilistic models used to describe the occurrences of these events.

State-of-knowledge uncertainty arises from a lack of knowledge or lack of scientific understanding that may be due to a variety of factors, such as inadequate experimental data, measurement uncertainty, etc. Random and state-of-knowledge uncertainties are often intertwined and may be difficult to distinguish: measurement uncertainty usually has a random component; some apparent randomness may prove to be state-of-knowledge after closer examination. The state-of-knowledge

uncertainties that need to be accounted for in a PRA fall into three basic categories:

Parameter uncertainty is the uncertainty associated with basic data used in safety analysis such as failure rates, ultimate strength, etc. Part of parameter uncertainty is already included within random uncertainty, such as the beta or error factor; however, another part such as the limitations in data affecting the choice of failure distribution may be characterized as state-of-knowledge uncertainty. Parameter uncertainties are those associated with the values of parameters of the PRA models. Parameter uncertainties are typically characterized by establishing probability distributions on the parameter values. These distributions can be interpreted as expressing a degree of belief in the values these parameters could take, based on current knowledge and conditional on the underlying model being correct.

Model uncertainty is the uncertainty associated with the data limitations, analytical physical models and acceptance criteria used in the safety analysis. PRA models, as well as those used in traditional deterministic engineering analyses, are composed of models for specific events or phenomena. Often the state of knowledge regarding these events and phenomena is incomplete and there are varying expert opinions on how particular models should be formulated. Such uncertainties arise, for example, in modeling human performance; common cause failures; and mechanistic failures of structures, systems and components. While some model uncertainties will apply over a large number of technologies, each particular technology will have its own special model uncertainties.

Completeness uncertainty is the uncertainty associated with factors not accounted for in the safety analysis such as safety culture, unknown or unanticipated failure mechanisms, etc. Completeness uncertainty can be regarded as one aspect of modeling uncertainty, but because of its importance is usually discussed separately. In one sense, it can be considered a scope limitation. Because completeness uncertainty reflects the unanalyzed contribution to risk it is difficult to estimate its magnitude, and this can translate to difficulties estimating the true magnitude of the overall risk.

The preliminary risk assessment of red oil events in the MOX facility provides some insight on the kinds of uncertainty that are important to the estimation of the risk of a red oil excursion. Uncertainty in the modeling of the accident progression are very important ranging from a very basic estimate of the quantity of material in various vessels and tanks as a function of time to the conditions that pertain at various stages of the reaction and how complete the reaction is. This is the analog of thermal-hydraulic modeling in light-water reactors that is used to determine the success criteria. Another uncertainty that was faced can be described as state-of-knowledge but only in the sense that the work was being performed on a preliminary design with some important design details, like P&IDs, missing. A third type of uncertainty encountered is the parameter uncertainty caused mainly by a lack of relevant data appropriate to the type of equipment being used and operations being performed. There was also, in some cases, a lack of well-defined procedures that made it difficult to estimate human errors.

Safety margin has been described as an integral part of defense-in-depth, since the basic purpose of safety margins is to cope with uncertainty. In addition, the compensatory measures that are also part of defense-in-depth must have some margins embedded in them to deal with the accident, malfunction, etc. Compensatory measures that lack margin are not usable.

5. SUPPLEMENTING INTEGRATED SAFETY ANALYSIS REVIEW

Part 70 requires that an ISA of the fuel cycle facility is performed before a possession and use license, i.e., a license to operate, is granted. NUREG-1513 [19] provides guidance on carrying out an ISA for fuel cycle facilities licensed by the NRC, and Chapter 5 and Appendix A of NUREG-1718 contain guidance on conducting an ISA specifically for the MOX facility.

The ISA of the MOX facility is expected to be completed by the applicant in the fall of 2006. Below are some general remarks on how the probabilistic risk assessment (PRA) of the facility, in particular the risk assessment of red oil excursions at the MOX facility, can usefully supplement the ISA in providing insights regarding accident sequences, likelihoods, and the performance of key safety systems which can help in the review of the ISA.

The ISA and PRA are both structured to identify the accident scenarios, their likelihoods, and the associated consequences. They are, therefore, structured similarly and contain fundamentally similar steps in the analyses. However, the two methods differ in their level of detail, scope of analyses, the input required, whether the analysis is qualitative or quantitative, the tools utilized, the degree of integration, and the results presented. Most of these differences stem from the degree of sophistication and complexity of one method over the other. Generally speaking, the ISA approach is somewhat less rigorous in analysis and as indicated in NUREG-1718 and NUREG-1513 quantification of the likelihood of accidents is not required for compliance with the performance criteria of 10 CFR 70.61. However, an ISA is likely to be more cost effective, more explicit and, perhaps, more traceable in the results generated than a PRA. Generally, an ISA should be considered as the foundation for a PRA and the steps and information generated in the course of an ISA should be included as a part of any PRA submittal without sacrificing the rigor and additional insights that could be generated by PRA methods.

It is sometimes claimed that the degree of sophistication offered by the PRAs may not justify the additional cost and effort involved when dealing with a relatively simple system and the types of regulatory needs that the NMSS office may require. There is merit in the statement which states that the rigor of the analysis should be commensurate with the needs (graded approach), as long as the short cuts taken do not miss a vital step in analysis and the simplifying assumptions do not provide a false or a highly biased result. This issue, however, can only be addressed by specific case studies and a detailed comparison of actual systems in the context of regulatory needs.

The Advisory Committee on Reactor Safeguards (ACRS) have recommended [20] that the ISA analyses should be gradually enhanced in the direction of the more rigorous PRA technology and also that PRA technology may need modification to address some of the unique issues that are addressed by the ISA.

Focusing on fuel cycle facilities, there are indeed some unique issues not addressed by PRA technology that was originally developed for reactors. These are:

1. The concept of initiators: As opposed to a reactor PRA, an initiator cannot be defined as an event that can lead to a scram or a change in the operational mode. Initiators in fuel cycle facilities are the occurrence of one of many conditions that are required for an accident to occur. These conditions could be caused by hardware failure, out-of control physical processes, or human errors that if not corrected and combined with some other events could

cause an accident. Initiators therefore should be modeled and evaluated with care. The model should take into account, using appropriate probability laws, combining condition probabilities and event frequencies. Note that the ISA provides some approximate treatment for combining frequency and probabilities (FP or PF event type evaluation).

2. The concept of fault exposure time: The concept of fault exposure time is typically driven by periodic surveillance test intervals in PRAs. However, in fuel cycle facilities for most failure modes of interest, the components are not directly monitored and the detection of an anomaly is usually done based on indirect measurements or routine analyses of certain samples. Therefore, it is important to formulate and evaluate how long a fault would stay in the system before it is detected and properly recovered.
3. The embedded modeling of instrumentation and control in human error evaluation: In fuel cycle facilities many human errors could cause a process to become out of control rather than totally fail (loss of level control, temperature control, density control, etc). For an event or condition to occur, the dynamics of the system, the effectiveness of the instrumentation and control, and the detection probability of the anomalies play an important role. Probabilistic models that include the dynamic control and the adaptive feedback loops supported by the empirical data may be needed.
4. Experience data: Reliability databases have been developed for both hardware and routine operator actions for use in the PRAs for nuclear power plants. The database could be updated with experience data from fuel cycle facilities. In addition, reliability data for pre- and post-accident conditions in fuel cycle facilities, including the potential for harsh environment that could increase component failure probabilities, should be evaluated. This also plays an important role in Common Cause Failure (CCF) models.
5. Consequence Analysis: The models for evaluating the worker, public, and environmental consequences of accidents in a fuel cycle facility could be streamlined.

Similarly, there are some areas in the ISA approach that can benefit significantly from more enhancement and streamlining; however, this can be more specifically identified in the process of the review and examination of the ISA application to the MOX facility. Generally, ISAs could benefit from more rigorous analysis of system interactions, common cause failures, human error analysis, and reliability data evaluation. ISA could also benefit from more aggregation and assembly of the accident sequences, likelihood, and consequences to an overall facility risk measure and perhaps the associated uncertainties.

One possibility for developing an understanding of how the PRA can usefully supplement an ISA analysis, considering the potential enhancements needed in both technologies, is to develop a well thought out review guide that could reveal the risk significant issues where the ISA technology may lack rigor. These issues or systems then could be addressed, to the extent possible, through a systematic PRA approach that builds on the original ISA to verify if the concern is of merit. Lessons learned from such case studies could eventually lead to both improving the ISA and the PRA methods and data.

5.1 Layer of Protection Analysis (LOPA)

The various measures for prevention and mitigation of major accidents may be thought of as 'lines of defence' (LODs) or 'layers of protection' (LOPs). These lines or layers serve to either prevent an initiating event (such as loss of cooling or overcharging of a material to a reactor, for example) from developing into an incident (typically a release of a dangerous substance), or to mitigate the consequences of an incident once it occurs. The concept of layers of protection and an approach to analyze the number of layers needed was first published by the Center for Chemical Process Safety (CCPS) in the 1993 book *Guidelines for Safe Automation of Chemical Processes* [14].

LOPA is a semi-quantitative risk analysis technique that is applied following a qualitative hazard identification tool such as HAZOP or a process hazard analysis. LOPA is semi-quantitative because the technique does use numbers and generates a numerical risk estimate. However, the numbers are selected to conservatively estimate failure probability, usually to an order of magnitude level of accuracy, rather than to closely represent the actual performance of specific equipment and devices. The result is intended to be conservative (overestimating the risk), and is usually adequate to understand the required safety level for the safety instrumented functions. If a more complete understanding of the risk is required, more rigorous quantitative techniques such as fault tree analysis or quantitative risk analysis may be required.

LOPA has been used extensively in the chemical industry to analyze health, environmental, and economic risks. Further details of the technique and its application are provided in References [15], [16], and [17].

5.2 Information Needs Pertinent to Risk

Risk information is generated based on mathematical representation of the failure combinations that can result in occurrence of an undesired event, failure probabilities and failure rates associated with each failure, and the appropriate probabilistic routines for evaluating the occurrence probability of the combined failures. Reliability data provides the failure probabilities and failure rates with their associated uncertainties. Failure rates and failure probabilities are, to the extent possible, estimated for the specific failures of interest. However, for a facility under construction such failure rate estimates will not be available and generic reliability data should be tailored for the risk applications. Generic databases should therefore have the appropriate scope and level of detail. The scope of a generic database should include the following example items:

1. Initiating Events

- Failures of process controls during facility operation caused by human errors
- Failures of process controls during facility operation caused by hardware failures
- Other types of initiating events caused by failures of the systems or actions needed for facility support

2. Unavailability contribution and hardware failures

- Component Failure rates per unit time and the associated repair time
- Common Cause Failure Parameters
- Maintenance durations and frequency

- Failure per demand and the associated restoration time
- Failure detection duration and surveillance strategy

3. Human Error Probabilities

- Routine operational human actions
- Emergency procedural operator actions
- Recovery actions

4. Time related failure probabilities

- Frequency of anomalies (e.g., inappropriately high or low concentration of certain materials in a container)
- Detection probabilities for anomalies as a function of time (or other parameters such as concentration)

Two major sources of generic reliability data were identified as potentially useful for the risk evaluation of a MOX facility. These are: Idaho Chemical Processing Plant Failure Rate Database [18], and Savannah River Generic Database Development [19]. There is also a compendium of Savannah River Site human error databases [20] which specifies the parameters for some non-model based generic human error estimations. There is quite a bit of cross-pollination between these sources of data and the databases for nuclear power plants. These databases, however, generally lack information needed for evaluating the initiating events and time related failure probabilities. The human error probabilities are defined in groups that are not easily carried over into a new design of a fuel cycle facility. Generic estimates for parameters associated with a human error model could have been utilized across different fuel cycle facilities. The generic component failure rate data appears to be quite useful for future risk evaluation of the fuel cycle facilities. However, such databases have to be maintained and new components and updated failure rates have to be incorporated. There are also some commercially available chemical industry databases that could potentially provide some useful information on event occurrence that would be relevant to the MOX facility. Access to these databases and maintaining them for future application would require adequate resources on the part of sponsors of risk assessments.

Risk assessment has to be based on the design of the facility and its operating characteristics and procedures, including procedures for both normal and off-normal operation, maintenance, and surveillance.

The MOX facility design is at a preliminary stage and several types of safety systems and controls and their associated procedures and criteria need to be defined. Many of these details are expected to be revealed in the forthcoming ISA and the risk study can benefit from the additional information regarding design and operation that will become available.

6. ORGANIZATION OF INFORMATION FOR RISK-INFORMING LICENSING REVIEW

6.1 Information Needs of Risk-Informing

There are four major sources of data needed for risk evaluation as discussed before. These are :

1. Initiating event frequencies
2. Unavailability contribution and hardware failure probabilities
3. Human error probabilities
4. Surveillance, control, and maintenance strategies

There are generally five different types of tools and models needed for risk informing:

1. System analysis tools to simulate the hardware impact of a failure or condition
2. Accident analysis tools that define the physical conditions that could cause an accident
3. Fault tree tools to propagate system impact of a combination of failures and estimate system failure probabilities
4. Event tree tools to propagate accident impact of combination of system failures/degradation and estimate the accident frequency
5. Consequence analysis models and tools to address the source term (amount of toxic/radiological materials potentially available for release), release fractions, dispersion and health effect.

6.2 Qualitative/Quantitative Risk Assessments: Techniques, Data, Guidance

There is no single, unique methodology for performing a risk analysis. Each particular methodology offers specialized schemes and tools for analyzing facilities or processes. However, all methodologies are systematic and tend to provide a disciplined approach to the evaluation of safety or risk. The materials and waste arenas present a wide range of technologies for risk assessment. Some technologies are comparatively complex, whereas others are rather straightforward. The assessment of risk involves an estimate of both frequency and consequences. Compared with power reactors, there is a much wider variety of combinations of frequencies and consequences found in materials and waste facilities and activities. Some activities involve continuous exposures with low consequences; others involve low-frequency events with fatal consequences, but to only a very few persons. Only a few facilities are similar to reactors, involving low-frequency events with large numbers of persons potentially exposed to high consequences. Identifying the population at significant risk is a critical part of assessing the risk from NMSS-regulated applications. NMSS activities also involve a variety of safety design approaches, many relying on human control. This

variability in risk and in safety design results in a variety of risk-analysis approaches. However, the fundamental considerations of frequency and consequence are always involved, if only implicitly.

Central to performing a risk assessment is determining the scope and depth of the analysis that would support decision-making related to the regulatory issue or licensing action. In some cases, a simplified risk assessment would be warranted. In other situations, sufficient information on risk might already be available in reports and papers. The reviewer should gather all pertinent information with regard to the licensing issue before starting a risk assessment. Historical data with regard to the occurrence of similar events in related facilities can be relevant. Data on failure rates of systems, components, and structures are also relevant. Physical and chemical consequence analyses that have been performed should also be collected. Entire studies that have been informed on related facilities can also be helpful. This information should be collected and organized for use, and for future reference.

Risk analyses may be performed in response to technical and/or regulatory requirements. Regardless of the reason, risk assessments are performed to provide an estimate of the type and amount of damage or personal injury that may be anticipated from exposure to a specific risk [21]. An example of a risk analysis performed in response to a regulatory requirement would be an Integrated Safety Analysis (ISA). As discussed in NUREG-1513, NRC promulgated a revised 10 CFR Part 70, on September 18, 2000, that addressed requirements for facilities using special nuclear material. This rulemaking included a requirement that these licensees conduct a specific type of risk assessment, an ISA. The ISA would form the basis for the facility's safety program, to ensure adequate controls and systems are in place for continued safe operation. These regulations are applicable to all licensees authorized to possess greater than a critical mass of special nuclear material and engaged in the following: enriched uranium processing, fabrication of uranium fuel or fuel assemblies, uranium enrichment, fabrication of mixed-oxide fuel or fuel assemblies, scrap recovery of special nuclear material, or any other activity that could significantly affect public health and safety. The 10 CFR Part 70 regulations do not apply to gaseous diffusion plants or decommissioned facilities.

In addition to regulatory requirements, a facility operator or regulator may decide to conduct a risk assessment purely for technical or economic reasons, such as improved design or optimized operation. Such analysis would assist the regulators in assessing the significance and the effects anticipated from these changes. From this information, various responses to reduce the overall significance of these risks can be evaluated; these could include new or revised regulations, changed inspection and enforcement oversight, process or equipment modifications, or a change in emphasis on operator performance. Risk assessments can be limited in scope and address a unique or specific process or be all-encompassing and address all the special hazards present at a facility, including nuclear and chemical risks.

In addition to the specific reason for performing a risk analysis (e.g. regulatory compliance, technical) and the specific tool chosen (e.g., PRA, ISA, Hazard and Operability Analysis (HAZOP)), there are many other potential benefits. Regulatory Guide 1.174 [22] encourages the increased use of PRAs to improve safety decision-making and regulatory efficiency for reactors. Similar results could be realized for specific NMSS applications. NRC inspectors may also benefit from such studies by focusing their oversight on the most important aspects of a facility's operation.

Licensees can use risk analyses to support decisions to modify a facility's licensing basis, as made

in license amendments and technical specification changes. Specific information can be obtained on whether a facility meets current regulations, maintains a defense-in-depth philosophy, provides sufficient safety margins; and develops performance measurement strategies to monitor change over time. When performing the detailed review necessary to support a risk analysis, the licensee may identify regulatory requirements or commitments that may be deemed overly restrictive or unnecessary, or may discover a lack of compliance in some area. Similarly, such an analysis may identify aspects of a design or operational process that require enhanced safety measures. Defense-in-depth is an important component of power reactor design that, until recently, was not commonly thought of in the NMSS arena. In a letter to the Commission [23], the Chairmen of the Advisory Committee for Nuclear Waste (ACNW) and the Advisory Committee for Reactor Safeguards (ACRS) observed:

- The treatment of defense-in-depth for transportation, storage, processing, and fabrication should be similar to its treatment for reactors. Defense-in-depth for industrial and medical applications can be minimal and addressed on the basis of actuarial information.
- Since the balancing of compensatory measures to achieve defense-in-depth depends on the acceptability of the risk posed by the activity or facility, risk-acceptance criteria should be developed for all NMSS activities.

6.3 Examples Illustrating Guidance

The American National Standards Institute submitted a petition for a rulemaking to remove a current regulatory requirement. The petition was for a rule change to remove the requirement for panoramic industrial sterilization irradiators to have a qualified operator physically present onsite, or at the facility, at all times during operations. These irradiators use gamma sources that often total between (2 million) and (5 million) curies for pool-type irradiators. Entry of a worker into the shielded irradiation room during operation would result in a fatal exposure. Such entry is prevented by a number of safety features and practices, one of which is the presence of the trained operator onsite. The request was to have the qualified operator on call but not present onsite at all times. In the case of system malfunctions, the operator would be called to take appropriate action. This is estimated to increase the risk to a non-operator worker who loads products on the continuously operating conveyor leading into the irradiator, since he might attempt to remedy a malfunction in a way that would expose him to a lethal dose. Personnel entry without the qualified operator's knowledge is difficult, and there are automatic protective features. However, unauthorized access is possible for certain designs. Such accidents have, in fact, occurred on several occasions overseas, although not at NRC-regulated facilities.

The use of a risk-informed process to evaluate this proposed rule change would have positive implications for both internal and external stakeholders. For internal stakeholders, use of a RIDM process would provide NRC staff with a consistent, systematic, and defensible way to make risk-management decisions. For external stakeholders, the use of a risk-informed process would provide an objective way to assess a change that would reduce the licensees' burden, as a tradeoff against a small increase in the risk of an accidental acute fatality to workers. The question is whether the increase in risk to workers would be acceptable.

To quantify the change in risk that would occur from a possible rule change, the staff conducted a risk assessment. The risk under the current regulatory framework, as well as the change in risk

from the proposed rule change were assessed. The risk assessment estimated the risk of worker acute fatality per facility to be 5×10^{-8} per year, under the current regulatory framework. If the operator were not always required to be present, but only on call, as the petition requested, the risk was estimated as 4×10^{-6} per year.

Using the draft risk guidelines (QHG4 is the base approach) indicated 4×10^{-6} per year is no longer less than the 1×10^{-6} per year limit of the negligible category. Therefore, the estimated individual risk with the removal of the current requirement is not considered negligible. However, with a factor of 4 greater than QHG 4, the risk is unlikely to be in the unacceptable region. The decision-maker would need to determine whether it is cost-beneficial to grant the exemption. Such a discussion also needs to be balanced by the consideration of security needs, assurance of defense-in-depth, and maintenance of adequate safety margin.

REFERENCES

1. U.S. Nuclear Regulatory Commission, "Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility", NUREG-1520, January 2002.
2. U.S. Nuclear Regulatory Commission, "Standard Review Plan for the Review of an Application for a Mixed Oxide (MOX) Fuel Fabrication Facility," NUREG-1718, August 2000.
3. Code of Federal Regulations, Title 10 Part 70, "Domestic Licensing of Special Nuclear Material", U. S. Government Printing Office, Washington, DC
4. U.S. Nuclear Regulatory Commission, "Final Safety Evaluation Report on the Construction Authorization Request for the Mixed Oxide Fuel Fabrication Facility at the Savannah River Site, South Carolina", NUREG-1821, March 2005.
5. "Mixed Oxide Fuel Fabrication Facility Construction Authorization Request, Duke Cogema Stone & Webster, in transmittal letters to the U.S. Nuclear Regulatory Commission, October 31, 2002 through February 9, 2005.
6. U.S. Nuclear Regulatory Commission, "Standard Format and Content Acceptance Criteria for the Material Control and Accounting (MC&A) Reform Amendment, NUREG-1280, April 1995.
7. U.S. Nuclear Regulatory Commission, "Acceptable Standard Format and Content for Fundamental Nuclear Material Control (FNMC) Plan Required for Low-Enriched Uranium Facilities", NUREG-1065, Rev. 2, December 1995.
8. M. Benedict, T.H. Pigford, and H.W. Levi, "Nuclear Chemical Engineering", Second Edition, McGraw-Hill Book Company, New York, 1981.
9. U.S. Nuclear Regulatory Commission, "Risk-Informed Decision-Making for Nuclear Material and Waste Applications," Draft for Trail Use, ADAMS Accession # ML042730524, May 11, 2005.
10. U.S. Nuclear Regulatory Commission, "Status of Risk-Informed Regulation in the Office of Material Safety and Safeguards," SECY-04-0182, October 7, 2004.
11. U.S. Nuclear Regulatory Commission, Safety Goals for the Operation of Nuclear Power Plants Policy Statement", Federal register, Vol. 51, p. 30028 (51 FR 30028), August 4, 1986.
12. United Kingdom Health and Safety Executive, "Safety Assessment Principles for Nuclear Plants," ISBN 0 11 882043 5, 1992.
13. Risk Assessment of Red Oil Excursions in the MOX Facility, BNL Draft Report, November 2006.
14. Center for Chemical Process Safety (CCPS), "Guidelines for Safe Automation of Chemical Processes," American Institute of Chemical Engineers, New York, NY, 1993.

15. Center for Chemical Process Safety (CCPS), "Layer of Protection Analysis, Simplified Process Risk Assessment," American Institute of Chemical Engineers, New York, NY, 2001.
16. A.M. Dowell, III, "Layer of Protection Analysis: A New PHA Tool, After HAZOP, Before Fault Tree Analysis," Presented at Center for Chemical Process Safety International Conference and Workshop on Risk Analysis in Process Safety, Atlanta, GA, October 21, 1997, American Institute of Chemical Engineers, New York, NY, 1997.
17. A.M. Dowell, III, "Layer of Protection Analysis and Inherently Safer Processes," Process Safety Progress, **18**, 4, 214-220, 1999.
18. T.G. Alber, Idaho Chemical Processing Plant Failure Rate Database, INEL-95/0422, August 1995.
19. A. Blanchard, "Savannah River Site Generic Data Base Development", WSRC-TR-93-262, Rev. 1, January 2000.
20. H.C. Benhardt, J.E. Held, L.M. Olsen, et al., "Savannah River site Human Error Data Base Development for Nonreactor Nuclear Facilities," WSRC-TR-93-581, February 1994.
21. U.S. General Accounting Office, "Chemical Risk Assessment: Selected Federal Agencies' Procedures, Assumptions, and Policies," GAO-01-810, August 2001.
22. U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment In Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," July 1998.
23. U. S. Nuclear Regulatory Commission, Letter B. J. Garrick and D. A Powers to R. A Meserve, "Use of Defense-in-depth In Risk-Informing NMSS Activities," May 25, 2000.