Revision 2, July 2004

NATIONAL
ENRICHMENT
FACILITY

SAFETY ANALYSIS REPORT

TABLE OF CONTENTS

3.0 INTEGRATED SAFETY ANALYSIS SUMMARY

The requirement to prepare and submit an Integrated Safety Analysis (ISA) Summary for Nuclear Regulatory Commission (NRC) approval is stated in 10 CFR 70.65(b) (CFR, 2003a). 10 CFR 70.65(b) (CFR, 2003a) also describes the contents of an ISA Summary. The ISA Summary has been developed following the guidance of NUREG-1520 (NRC, 2002) which meets the format, structure, and content of an ISA Summary that is consistent with the requirements of 10 CFR 70 (CFR, 2003b).

The information provided in the ISA Summary, the corresponding regulatory requirement, and the section of NUREG-1520 (NRC, 2002), Chapter 3 in which the NRC expectations for such information are presented are summarized below.

Information Category and Requirement	10 CFR 70 Citation	NUREG-1520 Chapter 3 Reference
Section 3.1 General Information		
• ISA methodology description	70.65(b)(5)	3.4.3.2(5)
• ISA Team description	70.65(b)(5)	3.4.3.2(5)
• Quantitative standards for acute chemical exposures	70.65(b)(7)	3.4.3.2(7)
• Definition of terms	70.65(b)(9)	3.4.3.2(9)
• Compliance with baseline design criteria and criticality monitoring and alarms	70.64 & 70.65(b)(4)	3.4.3.2(4D) 3.4.3.2(4C)
• Safety Program commitments	70.62(a)	3.4.3.1
Section 3.2 Site Description		
• Site description	70.65(b)(1)	3.4.3.2(1)
Section 3.3 Facility Description		
• Facility and Major Civil Structural Descriptions	70.65(b)(2)	3.4.3.2(2)
Section 3.4 Enrichment and Other Process Descriptions		
• Description of processes analyzed	70.65(b)(3)	3.4.3.2(3)
Section 3.5 Utility and Support Systems		
• Description of support systems analyzed	70.65(b)(3)	3.4.3.2(3)
Section 3.6 Process Hazards		
• Identification of hazards	70.65(b)(3)	3.4.3.2(3)
Section 3.7 Accident Sequences		
• General types of accident sequences	70.65(b)(3)	3.4.3.2(3)
• Risk ranking	70.65(b)(3)	3.4.3.2(3)
• Characterization of intermediate and high-risk accident sequences	70.65(b)(3)	3.4.3.2(3)
Section 3.8 Items Relied on For Safety (IROFS)		
• List and descriptions of IROFS at the system level	70.65(b)(6)	3.4.3.2(6)
• IROFS management measures	70.65(b)(4)	3.4.3.2(4B) 3.4.3.2(6)
• Sole IROFS	70.65(b)(8)	3.4.3.2(8)

3.0.1 References

CFR, 2003a. Title 10, Code of Federal Regulations, Section 70.65, Additional content of applications, 2003.

CFR, 2003b. Title 10, Code of Federal Regulations, Part 70, Domestic Licensing of Special Nuclear Material, 2003.

NRC, 2002. Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility, NUREG-1520, U.S. Nuclear Regulatory Commission, March 2002.

TABLE OF CONTENTS

Page

LIST OF TABLES

3.1 GENERAL INTEGRATED SAFETY ANALYSIS (ISA) INFORMATION

3.1.1 ISA Methods

This section outlines the approach utilized for performing the integrated safety analysis (ISA) of the process accident sequences. The approach used for performing the ISA is consistent with Example Procedure for Accident Sequence Evaluation, Appendix A to Chapter 3 of NUREG-1520 (NRC, 2002). This approach employs a semi-quantitative risk index method for categorizing accident sequences in terms of their likelihood of occurrence and their consequences of concern. The risk index method framework identifies which accident sequences have consequences that could exceed the performance requirements of 10 CFR 70.61 (CFR, 2003c) and, therefore, require designation of items relied on for safety (IROFS) and supporting management measures. Descriptions of these general types of higher consequence accident sequences are reported in the ISA Summary.

The ISA is a systematic analysis to identify plant and external hazards and the potential for initiating accident sequences, the potential accident sequences, the likelihood and consequences, and the IROFS.

The ISA uses a hazard analysis method to identify the hazards which are relevant for each system or facility. The ISA Team reviewed the hazard identified for the “credible worst-case” consequences. All credible high or intermediate severity consequence accident scenarios were assigned accident sequence identifiers, accident sequence descriptions, and a risk index determination was made.

The risk index method is regarded as a screening method, not as a definitive method of proving the adequacy or inadequacy of the IROFS for any particular accident.

The tabular accident summary resulting from the ISA identifies, for each sequence, which engineered or administrative IROFS must fail to allow the occurrence of consequences that exceed the levels identified in 10 CFR 70.61 (CFR, 2003c).

For this license application, two ISA Teams were formed. This was necessary because the sensitive nature of some of the facility design information related to the enrichment process required the use of personnel with the appropriate national security clearances. This team performed the ISA on the Cascade System, Contingency Dump System, Centrifuge Test System and the Centrifuge Post Mortem System. This ISA Team is referred to as the Classified ISA Team. The Non-Classified Team, referred to in the remainder of this text as the ISA Team, performed the ISA on the remainder of the facility systems and structures. In addition, the (non-classified) ISA Team performed the External Events and Fire Hazard Assessment for the entire facility.

In preparing for the ISA, the Accident Analysis in the Safety Analysis Report (LES, 1993) for the Claiborne Enrichment Center was reviewed. In addition, experienced personnel with familiarity with the gas centrifuge enrichment technology safety analysis where used on the ISA Team. This provides a good peer check of the final ISA results.

A procedure was developed to guide the conduct of the ISA. This procedure was used by both teams. In addition, there were common participants on both teams to further integrate the approaches employed by both teams. These steps were taken to ensure the consistency of the results of the two teams. A non-classified summary of the results of the Classified ISA has been prepared and incorporated into the ISA Summary.

3.1.1.1 Hazard Identification

The hazard and operability (HAZOP) analysis method was used for identifying the hazards for the Uranium Hexafluoride (UF_6) process systems and Technical Services Building systems. This method is consistent with the guidance provided in NUREG-1513 (NRC, 2001) and NUREG-1520 (NRC, 2002). The hazards identification process results in identification of physical, radiological or chemical characteristics that have the potential for causing harm to site workers, the public, or to the environment. Hazards are identified through a systematic review process that entails the use of system descriptions, piping and instrumentation diagrams, process flow diagrams, plot plans, topographic maps, utility system drawings, and specifications of major process equipment. In addition, criticality hazards identification were performed for the areas of the facility where fissile material is expected to be present. The criticality safety analyses contain information about the location and geometry of the fissile material and other materials in the process, for both normal and credible abnormal conditions. The ISA input information is included in the ISA documentation and is available to be verified as part of an on-site review.

The hazard identification process documents materials that are:

- Radioactive
- Fissile
- Flammable
- Explosive
- Toxic
- Reactive.

The list of hazardous materials at the facility, including maximum intended inventory amounts and location is provided in Chapter 6, Chemical Process Safety.

The hazard identification also identifies potentially hazardous process conditions. Most hazards were assessed individually for the potential impact on the discrete components of the process systems. However, for hazards from fires (external to the process system) and external events (seismic, severe weather, etc.), the hazards were assessed on a facility wide basis.

For the purpose of evaluating the impacts of fire hazards, the ISA team considered the following:

- Postulated the development of a fire occurring in in-situ combustibles from an unidentified ignition source (e.g., electrical shorting, or other source)
- Postulated the development of a fire occurring in transient combustibles from an unidentified ignition source (e.g., electrical shorting, or other source)
- Evaluated the uranic content in the space and its configuration (e.g., UF_6 solid/gas in cylinders, UF_6 gas in piping, UF_6 and/or byproducts bound on chemical traps, Uranyl Fluoride (UO_2F_2) particulate on solid waste or in solution). The appropriate configuration

was considered relative to the likelihood of the target releasing its uranic content as a result of a fire in the area.

In order to assess the potential severity of a given fire and the resulting failures to critical systems, the facility Fire Hazard Analysis was consulted. However, since the design supporting the license submittal for this facility is not yet at the detailed design stage, detailed in-situ combustible loading and in-situ combustible configuration information is not yet available. Therefore, in order to place reasonable and conservative bounds on the fire scenarios analyzed, the ISA Team estimated in-situ combustible loadings based on information of the in-situ combustible loading from Urenco's Almelo SP-5 plant (on which the National Enrichment Facility (NEF) design is based). This information from SP-5 indicates that in-situ combustible loads are expected to be very low.

The Fire Safety Management Program will limit the allowable quantity of transient combustibles in critical plant areas (i.e., uranium areas). Nevertheless, the ISA Team still assumed the presence of moderate quantities of ordinary (Class A) combustibles (e.g., trash, packing materials, maintenance items or packaging, etc.) in excess of anticipated procedural limits. This was not considered a failure of the associated administrative IROFS feature for controlling/ minimizing transient combustible loading in all radiation/uranium areas. Failure of the IROFS is connoted as the presence of extreme or severe quantities of transients (e.g., large piles of combustible solids, bulk quantities of flammable/combustible liquids or gases, etc.). The Urenco ISA Team representatives all indicated that these types of transient combustible conditions do not occur in the European plants. Accordingly, and given the orientation and training that facility employees will receive indicating that these types of fire hazards are unacceptable, the administrative IROFS preventing severe accumulations has been assigned a high degree of reliability. Refer to Section 3.8.3 for additional discussion.

Fires that involve additional in-situ or transient combustibles from outside each respective fire area could result in exposure of additional uranic content being released in a fire beyond the quantities assumed above. For this reason, fire barriers are needed to ensure that fires cannot propagate from non-uranium containing areas into uranium (U) areas or from one U area to another U area (unless the uranium content in the space is insignificant, i.e., would be a low consequence event). Fire barriers shall be designed with adequate safety margin such that the total combustible loading (in-situ and transient) allowed to expose the barrier will not exceed 80% of the hourly fire resistance rating of the barrier.

For external events, the impacts were evaluated for the following hazards:

External events were considered at the site and facility level versus at individual system nodes. Specific external event HAZOP guidewords were developed for use during the external event portion of the ISA. The external event ISA considered both natural phenomena and man-made hazards. During the external event ISA team meeting, each area of the plant was discussed as to whether or not it could be adversely affected by the specific external event under consideration. If so, specific consequences were then discussed. If the consequences were known or assumed to be high, then a specific design basis with a likelihood of highly unlikely would be selected.

Given that external events were considered at the facility level, the ISA for external events was performed after the ISA team meetings for all plant systems were completed. This provided the best opportunity to perform the ISA at the site or facility level. Each external event was assessed for both the uncontrolled case and then for the controlled case. The controlled cases could be a specific design basis for that external event, IROFS or a combination of both. An Accident Sequence and Risk matrix was prepared for each external event.

External events evaluated included:

- Seismic
- Tornado, Tornado Missile and High Wind
- Snow and Ice
- Flooding
- Local Precipitation
- Other (Transportation and Nearby Facility Accidents)
- Aircraft
- Pipelines
- Highway
- Other Nearby Facilities
- Railroad
- On-site Use of Natural Gas
- Internal Flooding from On-Site Above Ground Liquid Storage Tanks.

The ISA is intended to give assurance that the potential failures, hazards, accident sequences, scenarios, and IROFS have been investigated in an integrated fashion, so as to adequately consider common mode and common cause situations. Included in this integrated review is the identification of IROFS function that may be simultaneously beneficial and harmful with respect to different hazards, and interactions that might not have been considered in the previously completed sub-analyses. This review is intended to ensure that the designation of one IROFS does not negate the preventive or mitigation function of another IROFS. An integration checklist is used by the ISA Team as a guide to facilitate the integrated review process.

Some items that warrant special consideration during the integration process are:

- Common mode failures and common cause situations.
- Support system failures such as loss of electrical power or city water. Such failures can have a simultaneous effect on multiple systems.
- Divergent impacts of IROFS. Assurance must be provided that the negative impacts of an IROFS, if any, do not outweigh the positive impacts; i.e., to ensure that the application of an IROFS for one safety function does not degrade the defense-in-depth of an unrelated safety function.
- Other safety and mitigating factors that do not achieve the status of IROFS that could impact system performance.
- Identification of scenarios, events, or event sequences with multiple impacts, i.e. impacts on chemical safety, fire safety, criticality safety, and/or radiation safety. For example, a flood might cause both a loss of containment and moderation impacts.

- Potential interactions between processes, systems, areas, and buildings; any interdependence of systems, or potential transfer of energy or materials.
- Major hazards or events, which tend to be common cause situations leading to interactions between processes, systems, buildings, etc.

3.1.1.2 Process Hazard Analysis Method

As noted above, the HAZOP method was used to identify the process hazards. The HAZOP process hazard analysis (PHA) method is consistent with the guidance provided in NUREG-1513 (NRC, 2001). Implementation of the HAZOP method was accomplished by either validating the Urenco HAZOPs for the NEF design or performing a new HAZOP for systems where there were no existing HAZOPs. In general, new HAZOPs were performed for the Technical Services Building (TSB) systems. In cases for which there was an existing HAZOP, the ISA Team, through the validation process, developed a new HAZOP.

For the UF_6 process systems, this portion of the ISA was a validation of the HAZOPs provided by Urenco. The validation process involved workshop meetings with the ISA Team. In the workshop meeting, the ISA Team challenged the results of the Urenco HAZOPs. As necessary the HAZOPs were revised/updated to be consistent with the requirements identified in 10 CFR 70 (CFR, 2003b) and as further described in NUREG-1513 (NRC, 2001) and NUREG-1520 (NRC, 2002).

To validate the Urenco HAZOPs, the ISA Team performed the following tasks:

- The Urenco process engineer described the salient points of the process system covered by the HAZOP being validated.
- The ISA Team divided the process "Nodes" into reasonable functional blocks.
- The process engineer described the salient points of the items covered by the "Node" being reviewed.
- The ISA Team reviewed the "Guideword" used in the Urenco HAZOP to determine if the HAZOP is likely to identify all credible hazards. A representative list of the guidewords used by the ISA Team is provided in Table 3.1-1, HAZOP Guidewords, to ensure that a complete assessment was performed.
- The ISA Team Leader introduced each Guideword being considered in the ISA HAZOP and the team reviewed and considered the potential hazards.
- For each potential hazard, the ISA Team considered the causes, including potential interactions among materials. Then, for each cause, the ISA Team considered the consequences and consequence severity category for the consequences of interest (Criticality Events, Chemical Releases, Radiation Exposure, Environment impacts). A statement of "No Safety Issue" was noted in the system HAZOP table for consequences of no interest such as maintenance problems or industrial personnel accidents.
- For each hazard, the ISA Team considered existing safeguards designed to prevent the hazard from occurring.
- For each hazard, the ISA Team also considered any existing design features that could mitigate/reduce the consequences.

- The Urenco HAZOP was modified to reflect the ISA Team's input in the areas of hazards, causes, consequences, safeguards and mitigating features.
- For each external event hazard, the ISA Team determined if the external hazard is credible (i.e., external event initiating frequency >10^{-6} per year).
- When all of the Guidewords had been considered for a particular node, the ISA Team applied the same process and guidewords to the next node until the entire process system was completed.

The same process as above was followed for the TSB systems, except that instead of using the validation process, the ISA Team developed a completely new HAZOP. This HAZOP was then used as the hazard identification input into the remainder of the process.

The results of the ISA Team workshops are summarized in the ISA HAZOP Table, which forms the basis of the hazards portion of the Hazard and Risk Determination Analysis. The HAZOP tables are contained in the ISA documentation. The format for this table, which has spaces for describing the node under consideration and the date of the workshop, is provided in Table 3.1-2, ISA HAZOP Table Sample Format. This table is divided into 7 columns:

GUIDEWORD	Identifies the Guideword under consideration.
HAZARD	Identifies any issues that are raised.
CAUSES	Lists any and all causes of the hazard noted.
CONSEQUENCES	Identifies the potential and worst case consequence and consequences severity category if the hazard goes uncontrolled.
SAFEGUARDS	Identifies the engineered and/or administrative protection designed to prevent the hazard from occurring.
MITIGATION	Identifies any protection, engineered or otherwise, that can mitigate/reduce the consequences.
COMMENTS	Notes any comments and any actions requiring resolution.

This approach was used for all of the process system hazard identifications. The "Fire" and "External Events" guidewords were handled as a facility-wide assessment and were not explicitly covered in each system hazard evaluation.

The results of the HAZOP are used directly as input to the risk matrix development.

3.1.1.3 Risk Matrix Development

3.1.1.3.1 Consequence Analysis Method

10 CFR 70.61 (CFR, 2003c) specifies two categories for accident sequence consequences: "high consequences" and "intermediate consequences." Implicitly there is a third category for accidents that produce consequences less than "intermediate." These are referred to as "low consequence" accident sequences. The primary purpose of PHA is to identify all uncontrolled and unmitigated accident sequences. These accident sequences are then categorized into one

of the three consequence categories (high, intermediate, low) based on their forecast radiological, chemical, and/or environmental impacts.

For evaluating the magnitude of the accident consequences, calculations were performed using the methodology described in Section 6.3.2, Consequence Analysis Methodology. Because the consequences of concern are the chemotoxic exposure to hydrogen fluoride (HF) and UO_2F_2, the dispersion methodology discussed in Section 6.3.2 was used. The dose consequences for all of the accident sequences were evaluated and compared to the criteria for “high” and “intermediate” consequences. The inventory of uranic material for each accident considered was dependent on the specific accident sequence. For criticality accidents, the consequences were conservatively assumed to be high for both the public and workers.

Table 3.1-3, Consequence Severity Categories Based on 10 CFR 70.61, presents the radiological and chemical consequence severity limits of 10 CFR 70.61 (CFR, 2003c) for each of the three accident consequence categories. Table 3.1-4, Chemical Dose Information, provides information on the chemical dose limits specific to the NEF.

3.1.1.3.2 Likelihood Evaluation Method

10 CFR 70.61 (CFR, 2003c) also specifies the permissible likelihood of occurrence of accident sequences of different consequences. “High consequence” accident sequences must be “highly unlikely” and “intermediate consequence” accident sequences must be “unlikely.” Implicitly, accidents in the “low consequence” category can have a likelihood of occurrence less than “unlikely” or simply “not unlikely.” Table 3.1-5, Likelihood Categories Based on 10 CFR 70.61, shows the likelihood of occurrence limits of 10 CFR 70.61 (CFR, 2003c) for each of the three likelihood categories.

The definitions of “not unlikely”, “unlikely” and “highly unlikely” are taken from NUREG-1520 (NRC, 2002). The definition of “not credible” is also taken from NUREG-1520 (NRC, 2002). If an event is not credible, IROFS are not required to prevent or mitigate the event. The fact that an event is not “credible” must not depend on any facility feature that could credibly fail to function. One cannot claim that a process does not need IROFS because it is “not credible” due to characteristics provided by IROFS. The implication of “credible” in 10CFR70.61 is that events that are not “credible” may be neglected.

Any one of the following independent acceptable sets of qualities could define an event as not credible:

a. An external event for which the frequency of occurrence can conservatively be estimated as less than once in a million years

b. A process deviation that consists of a sequence of many unlikely human actions or errors for which there is no reason or motive (In determining that there is no reason for such actions, a wide range of possible motives, short of intent to cause harm, must be considered. Necessarily, no such sequence of events can ever have actually happened in any fuel cycle facility.)

c. Process deviations for which there is a convincing argument, given physical laws that they are not possible, or are unquestionably extremely unlikely.

3.1.1.3.3 Risk Matrix

The three categories of consequence and likelihood can be displayed as a 3 x 3 risk index matrix. By assigning a number to each category of consequence and likelihood, a qualitative risk index can be calculated for each combination of consequence and likelihood. The risk index equals the product of the integers assigned to the respective consequence and likelihood categories. The risk index matrix, along with computed risk index values, is illustrated in Table 3.1-6, Risk Matrix with Risk Index Values. The shaded blocks identify accidents of which the consequences and likelihoods yield an unacceptable risk index and for which IROFS must be applied.

The risk indices can initially be used to examine whether the consequences of an uncontrolled and unmitigated accident sequence (i.e., without any IROFS) could exceed the performance requirements of 10 CFR 70.61 (CFR, 2003c). If the performance requirements could be exceeded, IROFS are designated to prevent the accident or to mitigate its consequences to an acceptable level. A risk index value less than or equal to four means the accident sequence is acceptably protected and/or mitigated. If the risk index of an uncontrolled and unmitigated accident sequence exceeds four, the likelihood of the accident must be reduced through designation of IROFS. In this risk index method, the likelihood index for the uncontrolled and unmitigated accident sequence is adjusted by adding a score corresponding to the type and number of IROFS that have been designated.

3.1.1.4 Risk Index Evaluation Summary

The results of the ISA are summarized in tabular form (see Section 3.7, General Types of Accident Sequences). This table includes the accident sequences identified for this facility. The accident sequences were not grouped as a single accident type but instead were listed individually in the table. The Table has columns for the initiating event and for IROFS. IROFS may be mitigative or preventive. Mitigative IROFS are measures that reduce the consequences of an accident. The phrase “uncontrolled and/or unmitigated consequences” describes the results when the system of existing preventive IROFS fails and existing mitigation also fails. Mitigated consequences result when the preventive IROFS fail, but mitigative measures succeed. Index numbers are assigned to initiating events, IROFS failure events, and mitigation failure events, based on the reliability characteristics of these items.

With redundant IROFS and in certain other cases, there are sequences in which an initiating event places the system in a vulnerable state. While the system is in this vulnerable state, an IROFS must fail for the accident to result. Thus, the frequency of the accident depends on the frequency of the first event, the duration of vulnerability, and the frequency of the second IROFS failure. For this reason, the duration of the vulnerable state is considered, and a duration index is assigned. The values of all index numbers for a sequence, depending on the number of events involved, are added to obtain a total likelihood index, T. Accident sequences are then assigned to one of the three likelihood categories of the risk matrix, depending on the value of this index in accordance with Table 3.1-8, Determination of Likelihood Category.

The values of index numbers in accident sequences are assigned considering the criteria in Tables 3.1-9 through 3.1-11. Each table applies to a different type of event. Table 3.1-9, Failure Frequency Index Numbers, applies to events that have *frequencies* of occurrence, such as initiating events and certain IROFS failures. When failure *probabilities* are required for an event, Table 3.1-10, Failure Probability Index Numbers, provides the index values. Table 3.1-11, Failure Duration Index Numbers, provides index numbers *for durations* of failure. These are used in certain accident sequences where two IROFS must simultaneously be in a failed state. In this case, one of the two controlled parameters will fail first. It is then necessary to consider the duration that the system remains vulnerable to failure of the second. This period of vulnerability can be terminated in several ways. The first failure may be "fail-safe" or be continuously monitored, thus alerting the operator when it fails so that the system may be quickly placed in a safe state. Or the IROFS may be subject to periodic surveillance tests for hidden failures. When hidden failures are possible, these surveillance intervals limit the duration that the system is in a vulnerable state. The reverse sequences, where the second IROFS fails first, should be considered as a separate accident sequence. This is necessary because the failure frequency and the duration of outage of the first and the second IROFS may differ. The values of these duration indices are not merely judgmental. They are directly related to the time intervals used for surveillance and the time needed to render the system safe.

The duration of failure is accounted for in establishing the overall likelihood that an accident sequence will continue to the defined consequence. Thus, the time to discover and repair the failure is accounted for in establishing the risk of the postulated accident.

The total likelihood index is the sum of the indices for all the events in the sequence, including those for duration. Consequences are assigned to one of the three consequence categories of the risk matrix, based on calculations or estimates of the actual consequences of the accident sequence. The consequence categories are based on the levels identified in 10 CFR 70.61 (CFR, 2003c). Multiple types of consequences can result from the same event. The consequence category is chosen for the most severe consequence.

In summarizing the ISA results, Table 3.7-1, Accident Sequence and Risk Index, provides two risk indices for each accident sequence to permit evaluation of the risk significance of the IROFS involved. To measure whether an IROFS has high risk significance, the table provides an "uncontrolled risk index," determined by modeling the sequence with all IROFS as failed (i.e., not contributing to a lower likelihood). In addition, a "controlled risk index" is also calculated, taking credit for the low likelihood and duration of IROFS failures. When an accident sequence has an uncontrolled risk index exceeding four but a controlled risk index of less than four, the IROFS involved have a high risk significance because they are relied on to achieve acceptable safety performance. Thus, use of these indices permits evaluation of the possible benefit of improving IROFS and also whether a relaxation may be acceptable.

3.1.2 ISA Team

There were two ISA Teams that were employed in the ISA. The first team worked on the non-classified portions of the facility and is referred to in the text as the ISA Team. The second team, referred to as the Classified ISA Team, performed the ISA on the classified elements of the facility. Both teams were selected with credentials consistent with the requirements in 10 CFR 70.65 (CFR, 2003a) and the guidance provided in NUREG-1520 (NRC, 2002). To facilitate consistency of results, common membership was dictated as demonstrated below (i.e., some members of the Non-Classified Team participated on the Classified Team. One of the members of the Classified Team participated in the ISA Team Leader Training, which was conducted prior to initiating the ISA. In addition, the Classified ISA Team Leader observed some of the non-classified ISA Team meetings.

The ISA was performed by a team with expertise in engineering, safety analysis and enrichment process operations. The team included personnel with experience and knowledge specific to each process or system being evaluated. The team was comprised of individuals who have experience, individually or collectively, in:

- Nuclear criticality safety
- Radiological safety
- Fire safety
- Chemical process safety
- Operations and maintenance
- ISA methods.

The ISA team leader was trained and knowledgeable in the ISA method(s) chosen for the hazard and accidents evaluations. Collectively, the team had an understanding of all process operations and hazards under evaluation.

The ISA Manager was responsible for the overall direction of the ISA. The process expertise was provided by the Urenco personnel on the team. In addition, the Team Leader has an adequate understanding of the process operations and hazards evaluated in the ISA, but is not the responsible cognizant engineer or enrichment process expert.

A description of the ISA Team, their areas of expertise, qualifications and experience is provided below.

ISA Team Member	Experience and Qualifications
Michael Kennedy, ISA Manager and Team Leader	Over 29 years experience in nuclear safety analyses and risk assessment. Advanced degrees in Nuclear Engineering. Completed ISA Team Leader training course.
Richard Turcotte, Team Leader	Over 25 years experience providing engineering and risk assessment support for nuclear plants. Significant experience in probabilistic risk assessment. Degreed Mechanical Engineer. Completed ISA Team Leader training course.
Melvin Gmyrek, Team Leader	Over 30 years experience in nuclear facility operations. Has held a number of reactor operator licenses and held positions as Senior Reactor Operator, shift supervisor and operations manager. Completed ISA Team Leader training course.
David Pepe, Scribe	Over 26 years experience in providing engineering and risk assessment support on nuclear facilities. Significant experience in probabilistic risk assessment. Degreed Nuclear Engineer. Completed ISA Team Leader training course.

ISA Team Member	Experience and Qualifications
Scott Tyler, Chemical/Fire Safety	Over 17 years experience in fire and chemical safety on nuclear and non-nuclear facilities. Experienced in process hazard and consequence analysis. Degreed engineer in Fire Protection and Safety Engineering Technology and a registered Professional Fire Protection Engineer.
Richard Dible, Fire Safety	Over 19 years experience in fire protection and analysis. Degreed engineer in Fire Protection and Safety Engineering.
Douglas Setzer, Chemical/Fire Safety	Over 16 years experience in design and analysis in chemical and fire safety. Experienced in process hazard and consequence analysis. Degreed engineer in Mechanical and Chemical engineering. Registered Professional Fire Protection Engineer.
Kevin Morrissey, Criticality Safety	Over 24 years of nuclear industry experience, including particle transport methods, nuclear criticality, activation analysis and reactor physics.
Mark Strum, Radiological Safety	Over 30 years of nuclear utility experience performing radiological assessments supporting the design, licensing and operation of both PWR and BWR nuclear power plant facilities. Degreed nuclear engineer with an advanced degree in Radiological Sciences and Protection.
Chris Andrews, Process Expert	Over 30 years experience in the licensing, engineering and safety analysis of gas centrifuge enrichment technology. Senior Manager responsible for safety analysis and licensing for Urenco. Degree in Physics. Professional Engineer. Completed ISA Team Leader training course.
Allan Brown, Process Expert	Over 26 years experience in the design, operations, start-up, decommissioning of gas centrifuge enrichment facilities. Design Manager with responsibility for the NEF for Urenco. Degree in Physics.
Jan Kleissen, Operations Expert	Over 30 years experience in the operation and start-up of gas centrifuge enrichment plants. Production Manager at the Almelo SP-5 plant. The NEF is based on the SP-5 design. Degreed engineer.
Edwin Mulder, Operations Expert	Over four years experience in operations of gas centrifuge enrichment plant.

ISA Team Member	Experience and Qualifications
Herald Voschezang, Operations Expert	Over 19 years of experience with Urenco, predominantly in operations of gas centrifuge enrichment plants. Commissioning Manager of the Almelo SP-5 plant. The NEF is based on the SP-5 design. Degreed engineer.
Randy Campbell, Facility Engineering	Over 25 years experience in engineering, design and construction in the power (nuclear and fossil), chemicals, automotive and other various industries and 12 years nuclear experience. Degreed Mechanical Engineer.

Classified ISA Team Member	Experience and Qualifications
Andrew Pilkington, Team Leader/Risk Analysis	Over 14 years experience in nuclear and non-nuclear facility risk assessment. Significant experience in the risk assessment of gas centrifuge enrichment facilities. Knowledgeable in the HAZOP methodology. Degreed engineer.
Tony Duff, Scribe/Risk Analysis	Over 13 years experience in nuclear facility risk assessment. Most recent experience in gas centrifuge enrichment facility risk assessment. Degree in Applied Physics.
Chris Andrews, Process Safety	Over 30 years experience in the licensing, engineering and safety analysis of gas centrifuge enrichment technology. Senior Manager responsible for safety analysis and licensing for Urenco. Degree in Physics. Professional Engineer. Completed ISA Team Leader training course.
Edwin Mulder, Operations Expert	Over four years experience in operations of gas centrifuge enrichment plant.
Philip Hale, Lead Engineer	Over 21 years experience in mechanical and process design engineering on gas centrifuge enrichment facilities. Lead design engineer for the NEF. Advanced degree in Mechanical Engineering.
Owen Parry, Criticality	Over 20 years experience in gas centrifuge technology. Most recent experience is in the criticality analysis related to gas centrifuge enrichment facilities. Degree in Chemistry and Doctoral degree in Physics.

Classified ISA Team Member	Experience and Qualifications
Ian Forrest, Dump Systems	Over 27 years experience in design engineering. Presently package manager for work associated with development and qualification of Dump Systems, and providing related support for plant and projects. Degreed Mechanical Engineer.
Alan Coles, Fire Safety	Over 36 years experience in fire protection and fire safety.
Heather Tur, Test Facilities	Over 32 years experience in centrifuge research and development and centrifuge test facility operations.
Ian Crombie, Test Facilities	Over 20 years experience in design engineering related to gas centrifuge enrichment plant. Most recently involved in the NEF design.
Herald Voschezang, Operations Expert	Over 19 years of experience with Urenco, predominantly in operations of gas centrifuge enrichment plants. Commissioning Manager of the Almelo SP-5 plant. The NEF is based on the SP-5 design. Degreed engineer.
Stephen Thomas, Process Design Engineer	Over 25 years of experience. Approximately 10 years of centrifuge plant design experience. Design support for NEF design.

The management commitments related to the conduct and maintenance of the ISA are described in Section 3.1.8.2, Integrated Safety Analysis. Training and qualifications of individuals responsible for maintaining the ISA are described in Section 11.3, Training and Qualifications, and Section 2.2, Key Management Positions.

3.1.3 Selection of Quantitative Standards

Uranium hexafluoride (UF_6) is the only chemical of concern that will be used at the facility. For licensed material or hazardous chemicals produced from licensed materials, chemicals of concern are those that, in the event of release have the potential to exceed concentrations defined in 10 CFR Part 70 (CFR, 2003b). UF_6 represents a health hazard to facility workers and the public if released to atmosphere due to the radiological and toxicological properties of two byproducts – hydrogen fluoride (HF) and uranyl fluoride (UO_2F_2) – which are generated when UF_6 is released and reacts with water vapor in the air.

Criteria for evaluating potential releases and characterizing their consequences as either “high” or “intermediate” for members of the public and facility workers are presented in Table 3.1-3, Consequence Severity Categories Based on 10 CFR 70.61 and Table 3.1-4, Chemical Dose Information. Methodologies for the development of the chemical dose criteria are contained in Chapter 6, Chemical Process Safety.

3.1.4 Hazards Analyzed

The hazards of concern for this facility are all related to either a loss of confinement (of UF_6) or criticality. All of the consequences of concern are the result of initiating events due to hazards that would result in accidents of these types. The initiating events considered for this facility are the result of failures in process components, human error or misoperation including maintenance activities, fires (external to the process), and external events (e.g., severe weather, seismic, transportation and industrial hazards). These initiating events or potential causes could result in a loss of enrichment system containment or criticality. In general, the loss of confinement would initially result in an in-leakage of air because the systems are at sub-atmospheric pressure. Moisture in the air would react with the UF_6 forming UO_2F_2 and HF as by-products. The HF, which would be in a gaseous form, could be transported through the facility and ultimately beyond the site boundary. HF is a toxic chemical with the potential to cause harm to the plant workers or the public.

A criticality event, if one should occur, is a potential source of damaging energy and would result in the release of prompt gamma rays and airborne fission products. The gamma rays and airborne fission products result in direct radiation and chemical/radiological inhalation dose exposure to plant workers and the public. Each portion of the plant, system, or component that may possibly contain enriched uranium is designed with criticality safety as an objective. Where there is a potential for significant in-process accumulations of enriched uranium, the plant design includes multiple features to minimize the possibilities for breakdown of criticality control features. The Nuclear Criticality Safety program is described in Chapter 5, Nuclear Criticality Safety.

Nuclear criticality safety is evaluated for the design features of the plant system or component and for the operating practices that relate to maintaining criticality safety. The evaluation of individual systems or components and their interaction with other systems or components containing enriched uranium is performed to assure the criticality safety criteria are met. The nuclear criticality safety analyses in Chapter 5, and the safe values in Table 5.1-1, Safe Values for Uniform Aqueous Solution of Enriched UO_2F_2, provide a basis for the plant design and criticality hazards identifications performed as part of the ISA.

3.1.5 Criticality Monitoring and Alarms

The facility is provided with a Criticality Accident Alarm System (CAAS) as required by 10 CFR 70.24, Criticality accident requirements (CFR, 2003d). Areas where Special Nuclear Material (SNM) is handled, used, or stored in amounts at or above the 10 CFR 70.24 (CFR, 2003d) mass limits are provided with CAAS coverage.

The CAAS is designed, installed, and maintained in accordance with ANSI/ANS-8.3-1997 Criticality Accident Alarm System (ANSI, 1997) as modified by Regulatory Guide 3.71, Nuclear Criticality Safety Standards Fuels and Material Facilities (NRC, 1998).

CAAS coverage consists of an overlapping detection layout, where all required covered areas are monitored by a minimum of a pair (2) of gamma detectors. Detectors trip based on both steady radiation rate and time integrated total radiation dose levels. The detectors have a stated trigger response of 1mGy/hr (0.1 rad/hr) as a gamma radiation rate meter detector. Based on this design and the guidance provided in Appendix B of ANSI/ANS-8.3 (ANSI, 1997), the radius of detection must be less than 106 m (348 ft). Because of building steel spacing and equipment arrangement as well as a desire to maintain a factor of two safety margin, a radius of detection of 40 m (131 ft) is used in the design. This ensures that the CAAS is capable of detecting a criticality that produces an absorbed dose in soft tissue of 0.2 Gy (20 rads) of combined neutron and gamma radiation at an unshielded distance of 2 m (6.6 ft) from the reacting material within one minute. The CAAS will be uniform throughout the facility for the type of radiation detected, the mode of detection, the alarm signal, and the system dependability. The CAAS, if tripped, will automatically initiate a clearly audible signal in areas that must be evacuated.

The CAAS is provided with emergency power and is designed to remain operational during credible events or conditions, including fire, explosion, corrosive atmosphere, or seismic shock (equivalent to the site-specific design-basis earthquake or the equivalent value specified by the uniform building code).

Whenever the CAAS is not functional, compensatory measures, such as limiting access and restricting SNM movement, will be implemented. Should the CAAS coverage be lost and not restored within a specified number of hours, the operations will be rendered safe (by shutdown and quarantine) if necessary. Onsite guidance is provided and is based on process-specific considerations that consider applicable risk trade-off of the duration of reliance on compensatory measures versus the risk associated with process upset in shutdown.

The Emergency Plan for the NEF provides requirements for emergency response activities that cover criticality events.

3.1.6 Fire Hazards Analysis

Fire Hazards Analyses (FHAs) are conducted for the processing buildings located within the site boundary. The FHA evaluates the facility design with respect to fire safety codes, and ensures that the facility is designed and operated such that there is acceptable risk for postulated fire accident scenarios. The Fire Safety Program is described in Chapter 7, Fire Safety.

The results of the FHA have been used to identify potential fire initiators and accident sequences leading to radiological consequences or toxic chemical consequences. The FHA is a fundamental input for evaluating fire hazards in the ISA.

3.1.7 Baseline Design Criteria

10 CFR 70.64 (CFR, 2003e) specifies baseline design criteria (BDC) that must be used for new facilities. The ISA accident sequences for the credible high and intermediate consequence events for the NEF have defined the design basis events. The IROFS for these events and safety parameter limits ensure that the associated BDC are satisfied. IROFS safety parameter limits are available in the ISA documentation. These BDC have been used as bases for the design of the NEF. After each BDC, the Chapters or sections of the license application are provided that outline the details on how the facility design or operation conforms to the baseline design criteria.

A. Quality Standards and Records.

Structures, systems, and components (SSCs) that are determined to have safety significance are designed, fabricated, erected, and tested in accordance with the quality assurance criteria set forth in Appendix B to 10 CFR Part 50 (CFR, 2003f). Appropriate records of the design, fabrication, erection, procurement and testing of SSCs which are determined to have safety significance are maintained throughout the life of the facility. A safety function is a function performed by a SSC that prevents a release of UF_6 to the environment that could result in a dose to a member of the public of at least the limits provided in Section 3.1.3, Selection of Quantitative Standards. An SSC that performs a safety function is designated as an “item relied on for safety” (IROFS).

The LES QA Program Description is provided in Appendix A to Chapter 11, Management Measures. The Management Measures applicable to IROFS are discussed in Chapter 11, Management Measures.

B. Natural Phenomena Hazards.

Structures, systems, and components that are determined to have safety significance (IROFS) are designed to withstand the effects of, and be compatible with, the environmental conditions associated with operation, maintenance, shutdown, testing, and accidents for which the IROFS are required to function.

Natural phenomena hazards are identified in Section 3.2, Site Description.

C. Fire Protection.

Structures, systems, and components that are determined to have safety significance (IROFS) are designed and located so that they can continue to perform their safety functions effectively under credible fire and explosion exposure conditions. Non-combustible and heat resistant materials are used wherever practical throughout the facility, particularly in locations vital to the control of hazardous materials and to the maintenance of safety control functions. IEEE-383 (ANSI/IEEE, 1974) fire resistant cabling shall be used for all uranic material system power, instrumentation and control circuits. Fire detection, alarm, and suppression systems are designed and provided with sufficient capacity and capability to minimize the adverse effects of fires and explosion on IROFS. The design includes provisions to protect against adverse effects that might result from either the operation or the failure of the fire suppression system.

See Chapter 7, Fire Safety, for a description of the fire safety program and a description of the Fire Protection System.

D. Environmental and Dynamic Effects.

Structures, systems, and components that are determined to have safety significance (IROFS) are protected against dynamic effects, including effects of missiles and discharging fluids, that may result from natural phenomena, accidents at nearby industrial, military, or transportation facilities, equipment failure, and other similar events and conditions both inside and outside the facility.

E. Chemical Protection.

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.

See Chapter 6, Chemical Process Safety.

F. Emergency Capability.

Structures, systems, and components that are required to support the Emergency Plan must be designed for emergencies. The design must provide for accessibility to the equipment of onsite and available offsite emergency facilities and services such as hospitals, fire and police departments, ambulance service, and other emergency agencies.

This is described in the Emergency Plan for the NEF.

G. Utility Services.

Onsite utility service systems required to support IROFS shall be provided. Each utility service system required to support IROFS shall provide for the meeting of safety demands under normal and abnormal conditions.

Utility systems are described in Section 3.5, Utility and Support Systems.

H. Inspection, Testing, and Maintenance.

Structures, systems and components that are determined to have safety significance (IROFS) must be designed to permit inspection, maintenance, and testing.

I. Criticality Control.

Safety Margins

The design of process and storage systems shall include demonstrable margins of safety for the nuclear criticality parameters that are commensurate with the uncertainties in the process and storage conditions, in the data and methods used in calculations, and in the nature of the immediate environment under accident conditions. All process and storage systems should be designed and maintained with sufficient factors of safety to require at least two unlikely, independent, and concurrent changes in process conditions before a criticality accident is possible.

Criticality safety is described in Chapter 5, Nuclear Criticality Safety.

Methods of Control

The major controlling parameters used in the facility are enrichment control, geometry control, moderation control and/or limitations on the mass as a function of enrichment.

Criticality control methods are described in more detail in Chapter 5, Nuclear Criticality Safety.

Neutron Absorbers

Neutron absorbers are not needed and are not used at the NEF.

See Chapter 5, Nuclear Criticality Safety, for additional information on how this BDC is incorporated into the design of the facility.

J. Instrumentation and Controls.

Instrumentation and control systems shall be provided to monitor variables and operating systems that are significant to safety over anticipated ranges for normal operation, for abnormal operation, for accident conditions, and for safe shutdown. These systems shall ensure adequate safety of process and utility service operations in connection with their safety function. The variables and systems that require constant surveillance and control include process systems having safety significance, the overall confinement system, confinement barriers and their associated systems, and other systems that affect the overall safety of the plant. Controls shall be provided to maintain these variables and systems within the prescribed operating ranges under all normal conditions. Instrumentation and control systems shall be designed to fail into a safe state or to assume a state demonstrated to be acceptable on some other basis if conditions such as disconnection, loss of energy or motive power, or adverse environments are experienced.

For hardware IROFS involving instrumentation that provides automatic prevention or mitigation of events, status and operation will be monitored by the plant control system (PCS) by means of an alarm. This alarm will be provided by an isolated, hardwired digital signal from the associated IROFS to the PCS programmable logic controller (PLC). This signal will only be directed from the associated IROFS to the PCS PLC. The required isolation is provided at the IROFS hardware interface in the process equipment for the connections to the PCS PLC. Consistent with IEEE-279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations” (IEEE, 1971), the isolation devices will be classified as part of the IROFS boundary and will be designed such that no credible failure at the output of the isolation device shall prevent the associated IROFS from meeting its specified safety function.

K. Defense-in-Depth Practices.

The facility and system designs are based on defense-in-depth practices. The design incorporates a preference for engineered controls over administrative controls to increase overall system reliability. For criticality safety, the engineered controls preference is for use of passive engineered controls over active engineered controls. The design also incorporates features that enhance safety by reducing challenges to items relied on for safety. Facility and system IROFS are identified in Section 3.8, IROFS. The process systems are described in Section 3.4, Enrichment and Other Process Systems. The utility and support systems are described in Section 3.5, Utility and Support Systems. In addition to identifying the IROFS associated with each system, the system descriptions also identify the additional design and safety features (considerations) that provide defense-in-depth.

3.1.8 Safety Program Commitments

This section presents the commitments pertaining to the facility’s safety program including the performance of an ISA. 10 CFR Part 70 (CFR, 2003b) contains a number of specific safety program requirements related to the integrated safety analysis (ISA). These include the primary requirements that an ISA be conducted, and that it evaluate and show that the facility complies with the performance requirements of 10 CFR 70.61 (CFR, 2003c).

The commitments for each of the three elements of the safety program defined in 10 CFR 70.62(a) (CFR, 2003g) are addressed below.

3.1.8.1 Process Safety Information

A. LES has compiled and maintains up-to-date documentation of process safety information. Written process-safety information is used in updating the ISA and in identifying and understanding the hazards associated with the processes. The compilation of written process-safety information includes information pertaining to:

1. The hazards of all materials used or produced in the process, which includes information on chemical and physical properties such as are included on Material Safety Data Sheets meeting the requirements of 29 CFR 1910.1200(g) (CFR, 2003h).

2. Technology of the process which includes block flow diagrams or simplified process flow diagrams, a brief outline of the process chemistry, safe upper and lower limits for controlled parameters (e.g., temperature, pressure, flow, and concentration), and evaluation of the health and safety consequences of process deviations.

3. Equipment used in the process including general information on topics such as the materials of construction, piping and instrumentation diagrams (P&IDs), ventilation, design codes and standards employed, material and energy balances, IROFS (e.g., interlocks, detection, or suppression systems), electrical classification, and relief system design and design basis.

The process-safety information described above is maintained up-to-date by the configuration management program described in Section 11.1, Configuration Management.

B. LES has developed procedures and criteria for changing the ISA. This includes implementation of a facility change mechanism that meets the requirements of 10 CFR 70.72 (CFR, 2003i).

The development and implementation of procedures is described in Section 11.4, Procedures Development and Implementation.

C. LES uses personnel with the appropriate experience and expertise in engineering and process operations to maintain the ISA. The ISA Team for the various processes consists of individuals who are knowledgeable in the ISA method(s) and the operation, hazards, and safety design criteria of the particular process.

The ISA Team for the initial ISA development is described in Section 3.1.2, ISA Team. Training and qualifications of individuals responsible for maintaining the ISA are described in Section 11.3, Training and Qualifications, and Section 2.2, Key Management Positions.

3.1.8.2 Integrated Safety Analysis

A. LES has conducted an ISA for each process, such that it identifies (i) radiological hazards, (ii) chemical hazards that could increase radiological risk, (iii) facility hazards that could increase radiological risk, (iv) potential accident sequences, (v) consequences and likelihood of each accident sequence and (vi) IROFS including the assumptions and conditions under which they support compliance with the performance requirements of 10 CFR 70.61 (CFR, 2003c).

The results of the ISA are presented in Section 3.6, Process Hazards; Section 3.7, General Types of Accident Sequences, and Section 3.8, IROFS.

B. LES has implemented programs to maintain the ISA and supporting documentation so that it is accurate and up-to-date. Changes to the ISA Summary are submitted to the NRC, in accordance with 10 CFR 70.72(d)(1) and (3) (CFR, 2003i). The ISA update process accounts for any changes made to the facility or its processes. This update will also verify that initiating event frequencies and IROFS reliability values assumed in the ISA remain valid. Any changes required to the ISA as a result of the update process will be included in a revision to the ISA. Management policies, organizational responsibilities, revision time frame, and procedures to perform and approve revisions to the ISA are outlined in Chapter 11.0, Management Measures. Evaluation of any facility changes or changes in the process safety information that may alter the parameters of an accident sequence is by the ISA method(s) as described in the ISA Summary Document. For any revisions to the ISA, personnel having qualifications similar to those of ISA team members who conducted the original ISA are used.

C. Personnel used to update and maintain the ISA and ISA Summary are trained in the ISA method(s) and are suitably qualified. Training and Qualification of personnel used to update or maintain the ISA are described in Section 11.3, Training and Qualifications.

D. Proposed changes to the facility or its operations are evaluated by the ISA method(s) described in Section 3.1, General ISA Information. New or additional IROFS and appropriate management measures are designated as required. The adequacy of existing IROFS and associated management measures are promptly evaluated to determine if they are impacted by changes to the facility and/or its processes. If a proposed change results in a new type of accident sequence or increases the consequences or likelihood of a previously analyzed accident sequence within the context of 10 CFR 70.61 (CFR, 2003c), the adequacy of existing IROFS and associated management measures are promptly evaluated and the necessary changes are made, if required.

E. Unacceptable performance deficiencies associated with IROFS are addressed that are identified through updates to the ISA.

F. Written procedures are maintained on site. Section 11.4, Procedures Development and Implementation, discusses the procedures program.

G. All IROFS are maintained so that they are available and reliable when needed.

3.1.8.3 Management Measures

Management measures are functions applied to IROFS, and any items that may affect the function of IROFS. IROFS management measures ensure compliance with the performance requirements assumed in the ISA documentation. The measures are applied to particular structures, systems, equipment, components, and activities of personnel, and may be graded commensurate with the reduction of the risk attributable to that IROFS. The IROFS management measures shall ensure that these structures, systems, equipment, components, and activities of personnel within the identified IROFS boundary are designed, implemented, and maintained, as necessary, to ensure they are available and reliable to perform their function when needed, to comply with the performance requirements assumed in the ISA documentation.

The following types of management measures are required by the 10 CFR 70.4 definition of management measures. The description for each management measure reflects the general requirements applicable to each IROFS. Any management measure that deviates from the general requirements described in this section, which are consistent with the performance requirements assumed in the ISA documentation, are discussed in Section 3.8.3, Basis for Enhanced or High Availability Failure Probability Index Number. A cross reference from the associated IROFS in Table 3.8-1 to the applicable subsection is provided in Table 3.8-1.

Additional detail regarding implementation of management measures for IROFS, and any items that may affect the function of IROFS (as well as non-IROFS management measures), is found in Chapter 11.

Configuration Management

The configuration management program is required by 10 CFR 70.72 and establishes a system to evaluate, implement, and track each change to the site, structures, processes, systems, equipment, components, computer programs, and activities of personnel. Configuration management of IROFS, and any items that may affect the function of IROFS, is applied to all items identified within the scope of the IROFS boundary. Any change to structures, systems, equipment, components, and activities of personnel within the identified IROFS boundary must be evaluated before the change is implemented. If the change requires an amendment to the License, Nuclear Regulatory Commission approval is required prior to implementation.

Maintenance

Maintenance of IROFS, and any items that may affect the function of IROFS, encompasses planned surveillance testing and preventative maintenance, as well as unplanned corrective maintenance. Implementation of approved configuration management changes to hardware is also generally performed as a planned maintenance function.

Planned surveillance testing (e.g., functional/performance testing, instrument calibrations) monitors the integrity and capability of IROFS, and any items that may affect the function of IROFS, to ensure they are available and reliable to perform their function when needed, to comply with the performance requirements assumed in the ISA documentation. All necessary periodic surveillance testing is performed on an annual frequency (any exceptions credited within the ISA are discussed in Section 3.8.3).

Planned preventative maintenance (PM) includes periodic refurbishment, partial or complete overhaul, or replacement of IROFS, as necessary, to ensure the continued availability and reliability of the safety function assumed in the ISA documentation. In determining the frequency of any PM, consideration is given to appropriately balancing the objective of preventing failures through maintenance, against the objective of minimizing unavailability of IROFS because of PM. In addition, feedback from PM and corrective maintenance and the results of incident investigations and identified root causes are used, as appropriate, to modify the frequency or scope of PM.

Planned maintenance on IROFS, or any items that may affect the function of IROFS, that do not have redundant functions available, will provide for compensatory measures to be put into place to ensure that the IROFS function is performed until it is put back into service.

Corrective maintenance involves repair or replacement of equipment that has unexpectedly degraded or failed. Corrective maintenance restores the equipment to acceptable performance through a planned, systematic, controlled, and documented approach for the repair and replacement activities.

Following any maintenance on IROFS, and before returning an IROFS to operational status, functional testing of the IROFS, as necessary, is performed to ensure the IROFS is capable of performing its intended safety function.

Training and Qualifications

IROFS, and any items that may affect the function of IROFS, require that personnel involved at each level (from design through and including any assumed process implementation steps or actions) have and maintain the appropriate training and qualifications. Employees are provided with formal training to establish the knowledge foundation and on-the-job training to develop work performance skills. For process implemented steps or actions, a needs/job analysis is performed and tasks are identified to ensure that appropriate training is provided to personnel working on tasks related to IROFS. Minimum training requirements are developed for those positions whose activities are relied on for safety. Initial identification of job-specific training requirements is based on experience. Entry-level criteria (e.g., education, technical background, and/or experience) for these positions are contained in position descriptions.

Qualification is indicated by successful completion of prescribed training, demonstration of the ability to perform assigned tasks, and where required by regulation, maintaining a current and valid license or certification.

Continuing training is provided, as required, to maintain proficiency in specific knowledge and skill related activities. For all IROFS, and any items that may affect the function of IROFS, involving process implemented steps or actions, annual refresher training or requalification is required (any exceptions credited within the ISA are discussed in Section 3.8.3).

Procedures

All activities involving IROFS, and any items that may affect the function of IROFS, are conducted in accordance with approved procedures. Each of the other IROFS management measures (e.g., configuration management, maintenance, training) is implemented via approved procedures. These procedures are intended to provide a pre-planned method of conducting the activity in order to eliminate errors due to on-the-spot analysis and judgments.

All procedures are sufficiently detailed that qualified individuals can perform the required functions without direct supervision. However, written procedures cannot address all contingencies and operating conditions. Therefore, they contain a degree of flexibility appropriate to the activities being performed. Procedural guidance exists to identify the manner in which procedures are to be implemented. For example, routine procedural actions may not require the procedure to be present during implementation of the actions, while complex jobs, or checking with numerous sequences may require valve alignment checks, approved operator aids, or in-hand procedures that are referenced directly when the job is conducted.

To support the requirement to minimize challenges to IROFS, and any items that may affect the function of IROFS, specific procedures for abnormal events are also provided. These procedures are based on a sequence of observations and actions to prevent or mitigate the consequences of an abnormal situation.

Audits and Assessments

Audits are focused on verifying compliance with regulatory and procedural requirements and licensing commitments. Assessments are focused on effectiveness of activities and ensuring that IROFS are reliable and are available to perform their intended safety functions as documented in the ISA. The frequency of audits and assessments is based upon the status and safety importance of the activities being performed and upon work history. However, at a minimum, all activities associated with maintaining IROFS will be audited or assessed on an annual basis (any exceptions credited within the ISA are discussed in Section 3.8.3).

Incident Investigations

Incident investigations are conducted within the Corrective Action Program (CAP). Incidents associated with IROFS, and any items that may affect the function of IROFS, encompass a range of items, including (a) processes that behave in unexpected ways, (b) procedural activities not performed in accordance with the approved procedure, (c) discovered deficiency, degradation, or non-conformance with an IROFS, or any items that may affect the function of IROFS. Additionally, audit and assessment results are tracked in the Corrective Action Program.

Feedback from the results of incident investigations and identified root causes are used, as appropriate, to modify management measures to provided continued assurance that the reliability and availability of IROFS remain consistent with the performance requirements assumed in the ISA documentation.

Records Management

All records associated with IROFS, and any items that may affect the function of IROFS, shall be managed in a controlled and systematic manner in order to provide identifiable and retrievable documentation. Applicable design specifications, procurement documents, or other documents specify the QA records to be generated by, supplied to, or held, in accordance with approved procedures are included.

Other Quality Assurance Elements

Chapter 11 identifies specifics of various other quality assurance elements. Any other quality assurance element associated with IROFS, or any items that may affect the function of IROFS, that is required to ensure the IROFS is available and reliable to perform the function when needed to comply with the performance requirements assumed in the ISA documentation, will be listed in Table 3.8-1 and discussed in Section 3.8.3.

3.1.9 References

ANSI/IEEE, 1974. IEEE Standard for Type Test of Class 1E Electrical Cables, Field Splices, and Connections for Nuclear Power Generating Stations, ANSI/IEEE-383-1974, American National Standards Institute/Institute of Electrical and Electronics Engineers, 1974.

ANSI, 1997. Criticality Accident Alarm System, ANSI/ANS-8.3-1997, American National Standards Institute/American Nuclear Society, 1997.

CFR, 2003a. Title 10, Code of Federal Regulations, Section 70.65, Additional content of applications, 2003.

CRF, 2003b. Title 10, Code of Federal Regulations, Part 70, Domestic Licensing of Special Nuclear Material, 2003.

CFR, 2003c. Title 10, Code of Federal Regulations, Section 70.61, Performance requirements, 2003.

CFR, 2003d. Title 10, Code of Federal Regulations, Section 70.24, Criticality accident requirements, 2003.

CFR, 2003e. Title 10, Code of Federal Regulations, Section 70.64, Requirements for new facilities or new processes at existing facilities, 2003.

CFR, 2003f. Title 10, Code of Federal Regulations, Part 50, Appendix B, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants, 2003.

CFR, 2003g. Title 10, Code of Federal Regulations, Section 70.62, Safety program and integrated safety analysis, 2003.

CFR, 2003h. Title 29, Code of Federal Regulations, Section 1910, Occupational Safety and Health Standards, 2003.

CFR, 2003i. Title 10, Code of Federal Regulations, Section 70.72, Facility changes and change process, 2003.

IEEE, 1971. Criteria for Protection Systems for Nuclear Power Generating Stations, IEEE-279, 1971, Institute of Electrical and Electronics Engineers, 1971.

LES, 1993. Claiborne Enrichment Center Safety Analysis Report, Louisiana Energy Services, December 1993.

NRC, 1998. Nuclear Criticality Safety Standards for Fuels and Materials Facilities, Regulatory Guide 3.71, Nuclear Regulatory Commission, August 1998.

NRC, 2001. Integrated Safety Analysis Guidance Document, NUREG-1513, U.S. Nuclear Regulatory Commission, May 2001.

NRC, 2002. Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility, NUREG-1520, U.S. Nuclear Regulatory Commission, March 2002.

TABLES

Table 3.1-1 HAZOP Guidewords

UF_6 PROCESS GUIDEWORDS			
Less Heat	Corrosion	Maintenance	No Flow
More Heat	Loss of Services	Criticality	Reverse Flow
Less Pressure	Toxicity	Effluents/Waste	Less Uranium
More Pressure	Contamination	Internal Missile	More Uranium
Impact/Drop	Loss of Containment	Less Flow	Light Gas
Fire (Process, internal, other)	Radiation	More Flow	External Event
NON UF_6 PROCESS GUIDEWORDS			
High Flow	Low Pressure	Impact/Drop	More Uranium
Low Flow	High Temperature	Corrosion	External Event
No Flow	Low Temperature	Loss of Services	Startup
Reverse Flow	Fire	Toxicity	Shutdown
High Level	High Contamination	Radiation	Internal Missile
Low Level	Rupture	Maintenance	
High Pressure	Loss of Containment	Criticality	
No Flow			
EXTERNAL EVENTS POTENTIAL CAUSES			
Construction on Site	Hurricane	Seismic	Transport Hazard Off-Site
Flooding	Industrial Hazard Off-site	Tornado	External Fire
Airplane	Snow/Ice	Local Intense Precipitation	

Table 3.1-2 ISA HAZOP Table Sample Format

Page 1 of 1

ISA HAZOP NODE:		**DESCRIPTION :**			**DATE:**	**PAGE:**
GUIDEWORD	**HAZARD**	**CAUSE**	**CONSEQUENCE**	**SAFEGUARDS**	**MITIGATING FACTORS**	**COMMENTS**

Table 3.1-3 Consequence Severity Categories Based on 10 CFR 70.61

	Workers	Offsite Public	Environment
Category 3 High Consequence	*RD>1 Sievert (Sv) (100 rem) **CD>AEGL-3	RD>0.25 Sv (25 rem) 30 mg sol U intake CD>AEGL-2	–
Category 2 Intermediate Consequence	0.25 Sv (25 rem) <RD≤ 1 Sv (100 rem) AEGL-2 <CD≤ AEGL-3	0.05 Sv (5 rem) < RD≤ 0.25 Sv (25 rem) AEGL-1 <CD≤ AEGL-2	Radioactive release > 5000 x Table 2 Appendix B of 10 CFR Part 20
Category 1 Low Consequence	Accidents of lower radiological and chemical exposures than those above in this column	Accidents of lower radiological and chemical exposures than those above in this column	Radioactive releases with lower effects than those referenced above in this column

Note:

* RD: Radiation Dose
**CD: Chemical Dose

Table 3.1-4 Chemical Dose Information

	High Consequence (Category 3)	**Intermediate Consequence (Category 2)**
Worker (local) (1-min exposure)	> 40 mg U intake > 1,300 mg HF/m^3	> 10 mg U intake > 137 mg HF/m^3
Worker (elsewhere in room) (2.5-min exposure)	Note 1 Note 2	> 30 mg U/m^3 Note 2
Worker (elsewhere in room) (5-min exposure)	> 298 mg U/m^3 > 175 mg HF/m^3	> 24 mg U/m^3 > 98 mg HF/m^3
Outside Controlled Area (30-min exposure)	> 13 mg U/m^3 > 28 mg HF/m^3	> 2.4 mg U/m^3 > 0.8 mg HF/m^3

Notes:

1. Use the conservative 5-minute exposure value for uranium.
2. Use the conservative 5-minute exposure value for hydrogen fluoride.

Table 3.1-5 Likelihood Categories Based on 10 CFR 70.61
Page 1 of 1

	Likelihood Category	Probability of Occurrence*
Not Unlikely	3	More than 10^{-4} per-event per-year
Unlikely	2	Between 10^{-4} and 10^{-5} per-event per-year
Highly Unlikely	1	Less than 10^{-5} per-event per-year

*Based on approximate order-of-magnitude ranges

Table 3.1-6 Risk Matrix with Risk Index Values

Severity of Consequences	Likelihood of Occurrence		
	Likelihood Category 1 Highly Unlikely (1)	Likelihood Category 2 Unlikely (2)	Likelihood Category 3 Not Unlikely (3)
Consequence Category 3 High (3)	Acceptable Risk 3	Unacceptable Risk 6	Unacceptable Risk 9
Consequence Category 2 Intermediate (2)	Acceptable Risk 2	Acceptable Risk 4	Unacceptable Risk 6
Consequence Category 1 Low (1)	Acceptable Risk 1	Acceptable Risk 2	Acceptable Risk 3

Table 3.1-7 (Not Used)

Table 3.1-8 Determination of Likelihood Category

Likelihood Category	Likelihood Index T (= sum of index numbers)
1	$T \leq -5$
2	$-5 < T \leq -4$
3	$-4 < T$

Table 3.1-9 Failure Frequency Index Numbers

Frequency Index No.	Based On Evidence	Based On Type Of IROFS**	Comments
-6*	External event with freq. < 10^{-6} /yr		If initiating event, no IROFS needed.
-4*	No failures in 30 years for hundreds of similar IROFS in industry	Exceptionally robust passive engineered IROFS (PEC), or an inherently safe process, or two independent active engineered IROFS (AECs), PECs, or enhanced admin. IROFS	Rarely can be justified by evidence. Further, most types of single IROFS have been observed to fail
-3*	No failures in 30 years for tens of similar IROFS in industry	A single IROFS with redundant parts, each a PEC or AEC	
-2*	No failure of this type in this facility in 30 years	A single PEC	
-1*	A few failures may occur during facility lifetime	A single AEC, an enhanced admin. IROFS, an admin. IROFS with large margin, or a redundant admin. IROFS	
0	Failures occur every 1 to 3 years	A single administrative IROFS	
1	Several occurrences per year	Frequent event, inadequate IROFS	Not for IROFS, just initiating events
2	Occurs every week or more often	Very frequent event, inadequate IROFS	Not for IROFS, just initiating events

*Indices less than (more negative than) –1 should not be assigned to IROFS unless the configuration management, auditing, and other management measures are of high quality, because, without these measures, the IROFS may be changed or not maintained.

**The index value assigned to an IROFS of a given type in column 3 may be one value higher or lower than the value given in column 1. Criteria justifying assignment of the lower (more negative) value should be given in the narrative describing ISA methods. Exceptions require individual justification.

Table 3.1-10 Failure Probability Index Numbers

Probability Index No.	Probability of Failure on Demand	Based on Type of IROFS	Comments
-6*	10^{-6}		If initiating event, no IROFS needed.
-4 or -5*	10^{-4} - 10^{-5}	Exceptionally robust passive engineered IROFS (PEC), or an inherently safe process, or two redundant IROFS more robust than simple admin. IROFS (AEC, PEC, or enhanced admin.)	Can rarely be justified by evidence. Most types of single IROFS have been observed to fail
-3 or -4*	10^{-3} - 10^{-4}	A single passive engineered IROFS (PEC) or an active engineered IROFS (AEC) with high availability	
-2 or -3*	10^{-2} - 10^{-3}	A single active engineered IROFS, or an enhanced admin. IROFS, or an admin. IROFS for routine planned operations	
-1 or -2	10^{-1} - 10^{-2}	An admin. IROFS that must be performed in response to a rare unplanned demand	

*Indices less than (more negative than) –1 should not be assigned to IROFS unless the configuration management, auditing, and other management measures are of high quality, because, without these measures, the IROFS may be changed or not maintained.

Table 3.1-11 Failure Duration Index Numbers

Duration Index No.	Avg. Failure Duration	Duration in Years	Comments
1	More than 3 yrs	10	
0	1 yr	1	
-1	1 mo	0.1	Formal monitoring to justify indices less than -1
-2	A few days	0.01	
-3	8 hrs	0.001	
-4	1 hr	10^{-4}	
-5	5 min	10^{-5}	