CHAPTER 3.0
INTEGRATED SAFETY ANALYSIS

3.0 Introduction

The Integrated Safety Analysis (ISA) identifies process hazards associated with the fuel manufacturing facility operated at Global Nuclear Fuel –Americas LLC (GNF-A), located in Wilmington, North Carolina.

The analysis determines potential accident sequences and provides reasonable assurance that adequate controls are in place to prevent and/or mitigate accidents in accordance with the performance requirements of 10 CFR Part 70.61. Items Relied On For Safety (IROFS) are identified for each accident sequence that could fail to meet the performance requirements of 10 CFR 70.61.

The primary scope of the analysis focuses on consideration of the effects of relevant hazards on radiological safety, prevention of nuclear criticality accidents, or chemical hazards directly associated with NRC-licensed radioactive material.

The ISA covers all major equipment associated with the fuel manufacturing facility. Utilities (e.g., cooling water, plant air) supporting the facility were considered only to the extent that (1) failure or improper operation of the utility systems could cause significant hazards in the facility or (2) upsets in the facility and manufacturing process systems could cause significant hazards in the utility systems.

Facility operating experience, including unusual event and incident reports, is considered in the process hazards analysis of the fuel manufacturing facility and its associated process systems. Consideration is also given to related nuclear operations at other fuel fabrication facilities. These allow the team to consider how additional problems might occur and whether similar incidents could occur again.

3.1 Integrated Safety Analysis

Integrated Safety Analysis is a systematic analysis to identify facility and external hazards and their potential for initiating accident sequences, the potential accident sequences, their likelihood and consequences, and the IROFS. Figure 3.1 provides an overall process flow diagram of the ISA methodology applied to licensed activities.

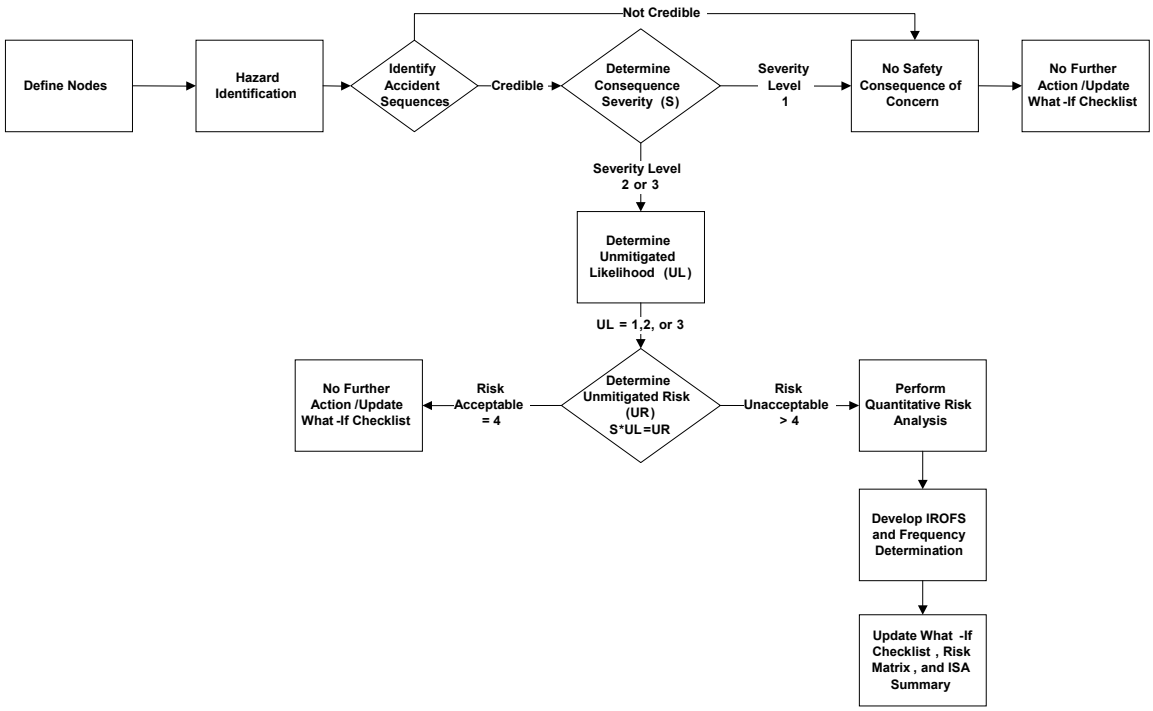

Figure 3.1 – ISA Process Flow Diagram (Typical)

3.2 Hazards and Risk Evaluation Methods used at GNF-A

To identify hazards and evaluate accident sequences, GNF-A in general uses methodologies identified in the following references: NUREG-1520 Rev. 1 (May 2010), *Standard Review Plan (SRP) for the Review of a License Application for a Fuel Cycle Facility,* NUREG-1513 (May 2001), *Integrated Safety Analysis Guidelines Document, Guidelines for Hazard Evaluation Procedures, Second Edition*, and *Layer of Protection Analysis, Simplified Process Risk Assessment.*

Several methods, which are routinely used in industry, are approved for use at GNF-A. Approved methods include the following:

- Checklist
- What-If Analysis
- Hazards and Operability Analysis (HAZOP)
- Failure Modes and Effects Analysis (FMEA)
- Fault Tree Analysis
- Event Tree Analysis
- Human Reliability Analysis
- Layer of Protection Analysis (LOPA)

One or more of these methods may be used to qualitatively analyze the hazards of the process or operation being studied. Methods such as HAZOP, what-if, checklist, or a combination of two or more of these methods are used to conduct the process hazard analyses.

Methods such as event tree analysis, fault tree analysis, human reliability analysis, and LOPA are approved for quantitatively determining the risks of a process or operation. Other methods consistent with industry or regulatory guidance, including semi-quantitative methods, may also be used. These methods can be used to determine the overall likelihood of an accident sequence previously identified during the process hazard analysis.

3.3 Conducting the Process Hazard Analysis

The focus of the process hazard analysis is to identify the hazards associated with the fuel manufacturing facility, identify credible accident sequences and their causes, and determine the unmitigated risks of these hazards. The results of the process hazard analysis are documented in the ISA reference report. GNF-A procedures require that the ISA Reference Report (also referred to as the process hazard analysis [PHA]) be maintained as a living document and supplemented with additional sections as changes are made to the facility and subsequent ISA studies are completed. Changes to the ISA PHA document are documented with an ISA Change Report and included in a Change Request.

3.3.1 Selecting the Analysis Method

GNF-A procedures require that the process hazard analysis method chosen be commensurate with the degree of complexity of the process or operation and the severity of hazards posed. Other factors to consider when selecting the analysis technique include the perceived risks associated with the process and the skill and knowledge of the personnel doing the analysis (which includes their process knowledge, experience, and knowledge of the process hazard analysis technique being used). The ISA leader selects an appropriate process hazard analysis technique, giving due consideration to these factors. Regardless of which method is used, the study must (1) include consideration of nuclear criticality, radiological, chemical/toxic, fire, and explosion hazards and (2) provide the required inputto the ISA Reference Report.

HAZOP

The ISA teams used the HAZOP analysis approach to identify and evaluate process hazards for complex systems and processes such as the uranium hexafluoride (UF_6) feed and conversion processes. This technique is a systematic method for identifying ways the process equipment can malfunction or be improperly operated, leading to undesirable conditions. The HAZOP technique is typically used to analyze complex processes and operations. This technique focuses on both safety hazards and operability issues. It may be used both during and after the process design phase. It is applicable for both continuous and batch flow processes.

HAZOP uses the synergy of an interdisciplinary team and a systematic approach to identify hazards and operability problems resulting from deviations from the process's design intent that could lead to undesirable consequences. Typically a fixed set of guide words (e.g., no/not, more, less, as well as) are combined with process parameters (e.g., flow, temperature, pressure, level) to create deviations from the design intent, which are applied to the specified points (nodes) to evaluate potential outcomes.

What-if/Checklist Analysis

This is a hybrid approach that combines the best features of what-if creative brainstorming with the discipline of checklist analysis. It depends on an experienced team. It is very effective for the simpler, straightforward processes where a high degree of resolution is not required (e.g., powder blending, pellet pressing, grinding, etc.). It can be used at every stage in the life of the process.

The what-if analysis technique is a brainstorming approach that builds on the synergy of an experienced group. While inherently not as structured as some techniques such as HAZOP, it is flexible and effective for the more simple processes (e.g., mechanical steps of assembling a fuel bundle, scanning). It can be used at every stage in the life of the process; however, analysis reliability is increased by experience.

Checklist analysis is a simple and effective technique for verifying the status of a system. It is highly disciplined and effective for verifying compliance (e.g., lockout-tagout, fall prevention, rod storage). It can be used at any stage of a process's lifetime but is dependent upon the experience and knowledge of those preparing the checklist.

3.3.2 Define the Node/Area to Be Studied

The first step of the ISA, identifying the hazards, is initiated by systematically breaking down the process system or operation being studied into well-defined sections or nodes (e.g., major vessels, columns, interconnecting process piping) in which the ins, outs and internal activity/flows can be defined, in order to allow interactions to be studied. All licensed operations are treated in this manner so that the entire facility is evaluated in a logical flow approach. This approach is also used to (1) evaluate the hazards associated with a new process or operation and (2) identify any new hazards that may result from modifications made to an existing process or operation.

In defining the node it is necessary to identify the bounding assumptions and initial conditions that the analysis will be based on. These terms are defined as follows:

Initial Conditions – Important aspects of a process and associated equipment, process operating parameters (e.g., temperature, pressure, flow rate), material throughput, and characteristics of the facility in which the process resides (e.g., design features) that establish the normal operating conditions from which the process hazard analysis is performed.

Bounding Assumptions – Identified assumptions about a process or material characteristics that bound the credible conditions of the process. These assumptions are based on the process chemistry, applicable scientific principles, facility-specific experimental data, operational history, and/or facility construction requirements. In determining the bounding assumptions for process parameters or material characteristics, no credit may be taken for controls placed on those parameters.

The bounding assumptions and initial conditions considered in the analyses shall be documented.

Preparation for the process hazard analysis begins by gathering process safety information on the process system and/or operation to be studied. Information typically used for the analysis included, but is not limited to, the following:

- Piping and instrumentation diagrams (P&IDs)
- Process flow diagrams
- Equipment arrangement drawings with general equipment layout and elevations
- Design temperatures and pressures for major process equipment and interconnected piping

- Materials of construction for major process equipment and interconnected piping
- Operating procedures for normal operations, as well as procedures for startup, shutdown, sampling, emergency shutdown, and any on-line maintenance
- Material safety data sheets (MSDSs) for any chemicals involved in the process (including any intermediate chemical reaction products) and other pertinent data for the chemicals or process chemistry (e.g., chemical reactivity hazards)
- Nuclear Safety Release/Requirements (NSR/Rs),
- Data for process alarms, interlocks, or trips
- Incident reports for the specific area being studied

3.3.3 Identify Credible Accident Sequences

The goal is to identify credible accident sequences by analyzing single initiating events. Using one or more of the approved methods, the ISA team identifies accident sequences associated with a process or operation, including possible unmitigated consequences and causes. Consequences of interest included nuclear criticality accidents, radiological material releases, radiation exposures, chemical/toxic exposures from licensed material or hazardous chemicals produced from licensed material, fires, and explosions.

As required by 10 CFR 70.62, the ISA must consider credible external events, including natural phenomena, for the potential hazardous consequences that they can cause. Natural-phenomenon events, such as hurricanes, tornadoes / high winds, seismic events, and external events, such as aircraft crashes, are addressed separately in GNF-A ISA Summary.

In considering accident sequences at this facility, it is necessary to determine those that are considered not credible and those that are credible. When conducting the process hazard analysis, the ISA team considers each accident sequence as credible, unless it can be determined to be not credible. Accident sequences that do not meet the definition of *not credible* are therefore considered *credible* and treated in accordance with 10 CFR 70.61.

Any one of the following three independent criteria is used to define an event as not credible:

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

(2) A process deviation that consists of a sequence of many unlikely events or errors for which there is no reason or motive. In determining that there is no reason for such errors, 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.

(3) Process deviations for which there is a convincing argument, based on physical laws, that they are not possible, sound engineering or technical data that the deviations are not possible, or are unquestionably extremely unlikely. The validity of the argument must not depend on any feature of the design or materials controlled by the facility's system of IROFS or management measures.

The bounding assumptions and initial conditions for the node under evaluation may also be considered when identifying credible accident sequences and initiating events. Justification that an accident sequence is not credible shall be documented.

3.3.4 Identify Accident Causes

When analyzing accident sequences, the ISA team considers process deviations, human errors, internal facility events, and credible external events. The team evaluates common mode failure and systems interaction. The team documents postulated accident sequences considered not credible. In addition to normal conditions, the team considers abnormal conditions including start-up, shutdown, maintenance, and process upsets.

3.3.5 Determine the Unmitigated Consequence Severity

For each credible accident sequence identified, the ISA team assigns a severity rank for the unmitigated consequences using the consequence severity rankings shown in Table 3.1 and documents the assigned severity rank in the ISA Reference Report. Assigning a severity rank allows each accident sequence to be categorized in terms of the performance requirements set forth in 10 CFR 70.61 (b), (c), and (d). A severity rank of 3 corresponds to "high consequences"; a severity rank of 2 corresponds to "intermediate consequences." When estimating the possible unmitigated consequences of an accident sequence, the ISA team members use plant experience, guidance from NUREG/CR-6410, *Nuclear Fuel Cycle Accident Analysis Handbook*, and their best judgment. All credible criticality accident sequences are assigned a severity ranking of 3 "high consequences".

The quantitative standards used to assess the consequence severity from chemical exposures to licensed materials or chemicals produced by licensed materials are shown in Table 3.2. The levels-of-concern values shown are derived from the EPA Acute Exposure Guideline Levels (AEGLs), based on an exposure for up to one hour for each limit. The AEGL-1, -2, and -3 values are used as the threshold concentration levels for establishing a low, intermediate, or high severity consequences as shown in Table 3.1.

The uranium hexafluoride concentration in air is not directly equivalent to soluble uranium intake. GNF-A uses worker intake quantities consistent with NRC FCSE Interim Staff Guidance ISG-14, Rev. 0 "Acute Uranium Exposure Standards for Workers", dated June 15, 2015.

Table 3.1 – Facility Consequence Severity Categories

Severity Ranking	Consequence Description		
	Workers	**Off-site Public**	**Environment**
3	• Radiological dose greater than 1 Sv (100 rem) • 400 mg soluble uranium intake • Chemical exposure greater than AEGL-3 • A criticality accident	• Radiological dose greater than 0.25 Sv (25 rem) • 30 mg soluble uranium intake • Chemical exposure greater than AEGL-2 • A criticality accident	• A criticality accident
2	• Radiological dose greater than 0.25 Sv (25 rem) but less than or equal to 1 Sv (100 rem) • 150 mg soluble uranium intake • Chemical exposure greater than AEGL-2 but less than or equal to AEGL-3	• Radiological dose greater than 0.05 Sv (5 rem) but less than or equal to 0.25 Sv (25 rem • Chemical exposure greater than AEGL-1 but less than or equal to AEGL-2	• Radioactive release greater than 5,000 times Table 2 Appendix B of 10 CFR Part 20
1	Accidents with radiological and/or chemical exposures to workers less than those above	Accidents with radiological and/or chemical exposures to the public less than those above	Radioactive releases to the environment producing effects less than those specified above

*Where Sv = Sieverts; AEGL = acute exposure guideline level

Table 3.2 –Levels of Concern (AEGL)

Chemical	AEGL 1	AEGL 2	AEGL 3
Uranium hexafluoride (UF_6)	3.6 mg/m^3	9.6 mg/m^3	36 mg/m^3
Hydrogen fluoride (HF)	1 PPM	24 PPM	44 PPM

(Note: All values shown are for 60-minute exposures)

3.3.6 Determine the Unmitigated Likelihood

The unmitigated likelihood of an accident sequence occurring is required to be determined for all credible accident sequences assigned a consequence severity of "high" or "intermediate." Unmitigated likelihood is the likelihood or frequency that the initiating event or cause of the accident sequence occurs. The team assigns an unmitigated likelihood level for each accident sequence using the defined categories in Table 3.3 and documents the assigned level in the ISA Reference Report. When assigning a likelihood category, the team uses process knowledge, accident sequence information, operating history, and manufacturers/product information to determine which category of likelihood is appropriate. For accident sequences where multiple causes have been identified, the team estimates the likelihood for the most credible cause. This helps assure that the accident sequence is screened using the most conservative estimate of risk.

Table 3.3 – Unmitigated Likelihood Categories

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

* Default selection in absence of quantitative assessment.

3.3.7 Determine the Unmitigated Risk

Credible accident sequences identified for the facility, which have the capability of producing conditions that fail to meet the performance requirements of 10 CFR 70.61 (b), (c) or (d), require IROFS to be assigned to reduce the overall risk to an acceptable level. For each credible accident sequence, the ISA team uses the unmitigated severity category rank and unmitigated likelihood level to assign an unmitigated risk level. (The unmitigated risk is determined from the product of the severity ranking and the unmitigated-likelihood level.) The ISA teams use the risk matrix in Table 3.4 to determine the unmitigated risk and document the assigned risk in the ISA Reference Report.

Table 3.4 – Unmitigated Risk Assignment Matrix

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

3.4 Conducting the Quantitative Analysis

For each accident sequence having an unmitigated risk of unacceptable, IROFS must be assigned and the overall mitigated likelihood determined for each accident sequence. Approved quantification methods include event tree analysis, fault tree analysis, human reliability analysis, LOPA, and the semi-quantitative index method. Figure 3.2 presents the steps taken to quantify the mitigated likelihood of an accident sequence. Specific details for accomplishing these steps are included in this section, including identifying the initiating events, estimating the initiating event's frequency, identifying enabling conditions and conditional events, selection of IROFS, and estimating the failure probability of each credited IROFS.

Determination of the overall likelihood for an accident sequence is documented in a Quantitative Risk Assessment (QRA) report. The purpose of these reports is to provide sufficient background and operational information to understand and examine all accident sequences that result in unacceptable risks for each accident sequence. Each QRA report provides details concerning an accident sequence's quantification, including method used, initiating-event frequency determination, enabling or conditional event probabilities, the IROFS credited to prevent or mitigate the initiating event(s) being analyzed, the failure probabilities for the credited IROFS, and the overall likelihood estimates. The QRA reports are controlled by Configuration Management and are reviewed and approved when modified as described in Subsection 3.5.1. The quantification results from each QRA are summarized in the GNF-A ISA Summary.

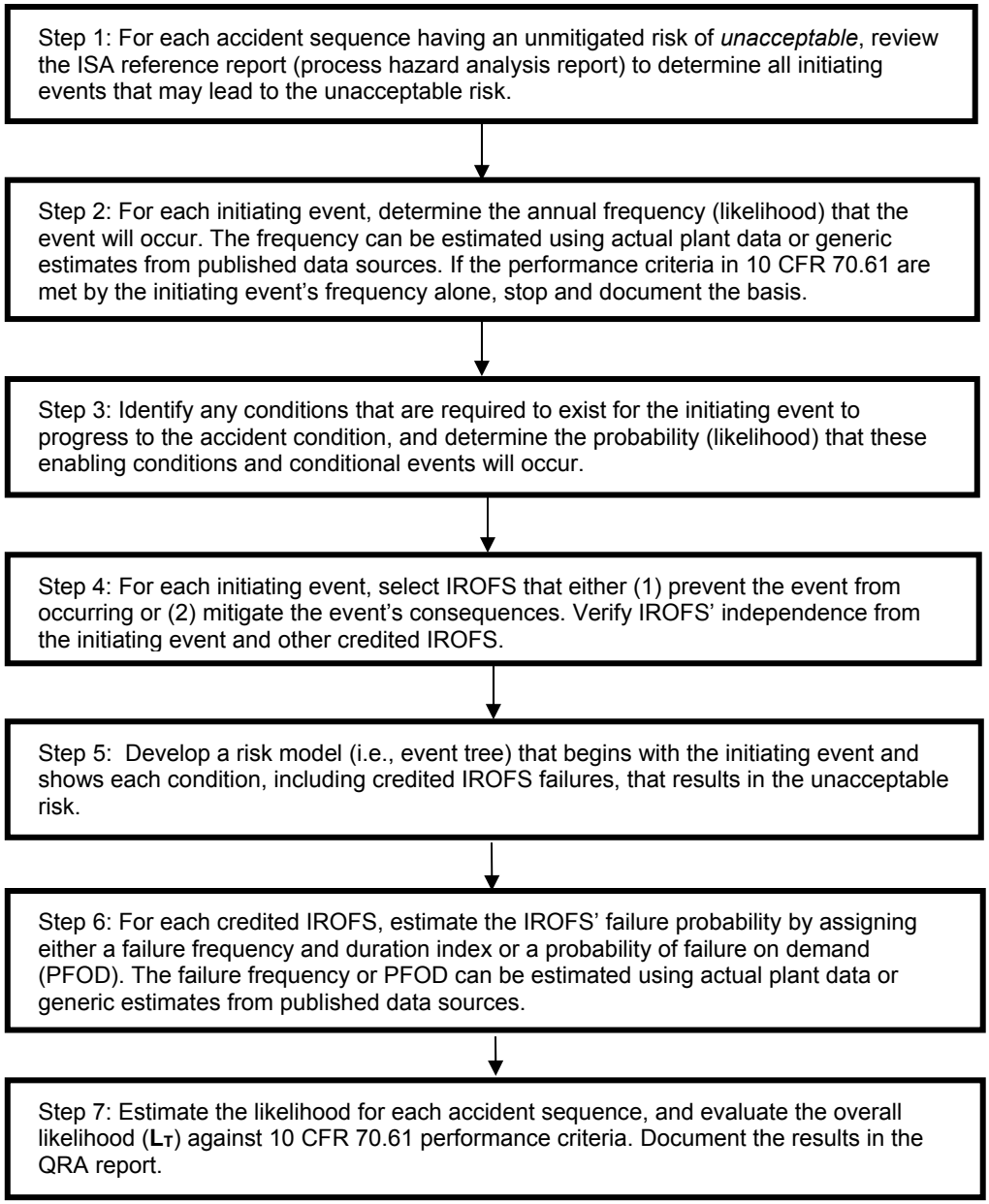

Figure 3.2 – Quantification Methodology

3.4.1 Initiating Events

For each accident sequence requiring quantification, the ISA team member responsible for quantifying the accident sequence first reviews the ISA reference report (process hazard analysis report) to determine all initiating events that may result in an unacceptable risk. The annual frequency of each initiating event is estimated using plant operational experience, industrial performance data, or index values supplied in the GNF-A ISA Summary.

3.4.2 Enabling Conditions and Conditional Events

For each accident sequence, enabling conditions and conditional events that affect the outcome of the accident sequence (i.e., conditions that affect the likelihood of the accident sequence or could mitigate the consequences to either workers or the public) are identified where appropriate.

An enabling condition does not directly cause the accident sequence, but must be present for the initiating event to proceed to the consequences described. Enabling conditions are expressed as annual probabilities, and can include such things as the mode of operation (e.g., percent of annual operational online availability).

Conditional events that affect the probability of the unacceptable risk are also identified. These can include probabilistic consideration of individual or administrative actions that would not be considered IROFS, but would affect the overall likelihood of the accident. For example, if an accident sequence involves personal injury hazards, at least one worker must be present in the affected area at the time of the event for the injury to occur. Thus, the presence of workers in the affected area is a conditional modifier for a consequence involving personal injury. Another example of a conditional event is the probability that a worker can successfully evacuate from an area given that a hazard is present.

3.4.3 IROFS Identification and Evaluation

IROFS are controls or control systems (eg. structures, systems, equipment, components, and activities of personnel) that are relied on to prevent potential accidents at a facility that could exceed the performance requirements of 10 CFR 70.61 or to mitigate their potential consequences. When selecting IROFS, the IROFS must be independent of the initiating event (i.e., occurrence of the initiating event does not cause failure of the IROFS) and other credited IROFS (i.e., failure of one IROFS does not cause failure of another IROFS).

For IROFS that use process control computer systems, such as distributed control systems (DCS) and programmable logic controllers (PLC), GNF-A uses design standards for these systems that result in IROFS with a high reliability and response capability. The architecture design standards for these control systems include the use of mechanically fail-safe final control elements where feasible, security procedures for access and changes to control-system software, separate final elements utilizing separate output modules, and independent control element sensors on separate input modules. When selecting IROFS, GNF-A follows the guidelines from LOPA using the type B methodology for IROFS that use process control computer systems. This methodology limits GNF-A to claiming no more than two IROFS in a single logic controller for any accident

sequence. All control-system IROFS are subject to the applicable management measures as described in the ISA Summary, including periodic verification of IROFS functionality.

GNF-A commits to identify IROFS as a part of the ISA and include the identification of the IROFS in the ISA Summary Report prepared and maintained for the facility. The IROFS are defined in such a way as to delineate their boundaries, to describe the characteristics of the preventive/mitigating function, and to identify the assumptions and conditions under which the IROFS is relied on.

When evaluating accident sequences, the overall likelihood of the accident sequence must be determined and the adequacy of IROFS to prevent or mitigate the accident sequence is clearly identified.

IROFS which are continuous controls may be evaluated by determination of failure frequency and duration. IROFS which are passive controls or only operate when demanded may be evaluated by determining the probability of failure on demand (PFOD). The duration term does not apply when PFOD is used.

3.4.4 Determining the Overall Likelihood

The *overall likelihood* for an accident sequence is the product of the frequency of the initiating event times the probability of any enabling conditions, times the probability of failure for each credited IROFS. Considerations include frequency of the initiating event, IROFS, enabling conditions, conditional events, time period (duration) of the IROFS failed condition prior to detection/response, IROFS testing or surveillance interval, and independence of IROFS which mitigate the progression of the accident sequence.

Several methods are approved for determining the overall likelihood for an accident sequence. Rigorous methods, such as event tree analysis, are used when the accident sequence is complex and issues such as employee evacuation, the size and location of the material release, and timing or order of IROFS failures needs to be considered. Standard quantitative risk assessment techniques were employed in assessing the overall likelihood for accident sequences using the event-tree analysis method. Overall likelihood is evaluated using limits defined in Table 3.5.

Simplified quantitative methods such as LOPA and an index method are approved for estimating an accident sequence's overall likelihood. The index value for the overall likelihood, L_T, can be determined using the following semi-quantitative equation. The index values are $\log_{10}$ values for each of the annual frequencies and probabilities, which are then summed to determine overall likelihood.

This method conforms to the GNF-A ISA methodology, the GNF-A proposed new overall likelihood methodology, and the additional refinements to the GNF-A overall likelihood methodology.

$$L_T = \lambda_{IE} + \sum_{k=1}^{k=M} P_{E,k} + [\sum_{i=1}^{i=N-1} (\lambda_{f,i} + \lambda_{(T/2+MTTR),i}) \bullet \lambda_{IND,i}] + [\lambda_{f,N} + \lambda_{T/2,N}]$$ Where,

L_T = Overall likelihood index value for the accident sequence being reviewed

Each summed index value term is the $\log_{10}$ representation of each probability or frequency where,

λ_{IE} = Index value for the probability of the initiating event occurring for the identified accident sequence (on a per-year basis, per 3.4.1).

$P_{E,k}$ = Index value for probability of the (k^{th}) enabling condition or conditional event, per 3.4.2. Enabling-condition probabilities are expressed on a per-year basis. These terms are optional.

$\lambda_{f,i}$ = Index value for the failure frequency (on a per-year basis) for an individual (i^{th}) IROFS considered in preventing or mitigating the accident sequence.

$\lambda_{(T/2+MTTR),i}$ = Index value for the duration for an individual (i^{th}) IROFS considered in preventing or mitigating the accident sequence. For functionally tested IROFS, use the sum of one-half the testing (or surveillance) interval and the mean time to repair (MTTR) or place the system in a safe configuration.

Note: For IROFS where the Probability of Failure on Demand (PFOD) is used, replace the term ($\lambda_{f,i} + \lambda_{(T/2+MTTR),i}$) with $\lambda_{PFOD,i}$, which represents the index value for the PFOD for the i^{th} IROFS.

$\lambda_{IND,i}$ = Independence factor for an individual (i^{th}) IROFS. If the failure of a particular IROFS in the identified accident sequence is not caused by, or made more likely to occur by, failure of another IROFS, independence is established, and a value of 1 is used; otherwise a value of 0 is used.

$\lambda_{f,N}$ = Index value for the failure frequency (on a per-year basis) for the final (N^{th}) IROFS considered in preventing or mitigating the accident sequence.

$\lambda_{T/2,N}$ = Index value for the duration for the N^{th} IROFS considered in preventing or mitigating the accident sequence. For functionally tested IROFS, use the sum of one-half the testing (or surveillance) interval. For the final (N^{th}) IROFS considered in preventing or mitigating the accident sequence, the mean time to repair term is excluded for *order-dependent* accident sequences, because this IROFS represents the final barrier in the accident sequence.

Qualitative indices are assigned to the initiating-event frequency, the IROFS failure frequencies and duration indices and then "combined" together with factors representing the immunity to common mode failure to assign a score to the overall (total) likelihood. The overall-likelihood index, L_T, is then evaluated against the applicable limit for the corresponding consequence category. The mitigated likelihood of the accident sequence occurring with the preventive or mitigating IROFS in-place must meet the requirements in 10 CFR 70.61, which requires that unacceptable consequences be limited (see Table 3.5 for mitigated overall likelihood limits).

Table 3.5 – Acceptance Criteria for Overall Likelihood

Index Value (L_T)*	Likelihood (per year)	Acceptance Criteria
-6.0	$\leq 1.0 \times 10^{-6}$	Acceptable for high (and intermediate) consequence accidents
-5.0	$\leq 1.0 \times 10^{-5}$	Acceptable for high (and intermediate) consequence accidents
-4.0	$\leq 1.0 \times 10^{-4}$	Acceptable for high (and intermediate) consequence accidents
-3.0	$\leq 1.0 \times 10^{-3}$	Acceptable for intermediate consequence accidents only; not acceptable for high consequence accidents
-2.0	$\leq 1.0 \times 10^{-2}$	Not acceptable for high or intermediate consequence accidents
-1.0	$\leq 1.0 \times 10^{-1}$	Not acceptable for high or intermediate consequence accidents

* L_T determined using the semi-quantitative equation in Subsection 3.4.4

3.5 ISA Management

3.5.1 ISA Change Management

As described in Chapter 11, Management Measures, a formal configuration management process, governed by written, approved practices, ensures that plant design changes do not adversely impact the ISA at GNF-A. Facility, documentation, and temporary changes are initially evaluated by a trained and approved safety reviewer to determine the potential effects to safety disciplines (criticality, radiation, chemical, industrial, fire and/or explosion), the site license and the ISA, and to assure safe implementation and operation of the change.

Changes that require NRC prior approval per 10 CFR 70.72(c) will be submitted with ISA Summary revisions, but are not implemented until NRC approval is obtained. An annual update to the ISA Summary is also submitted for implemented changes that do not require pre-approval by the NRC or otherwise affect the ISA Summary.

Changes that do not require NRC prior approval, but which may affect the ISA, require formal evaluation by the ISA team to determine the effects to any ISA documentation, including the ISA Reference Report, Quantitative Risk Assessment report(s), and the ISA Summary. ISA methods are utilized to evaluate the adequacy of existing IROFS and associated management measures, and to designate new or additional IROFS and appropriate management measures as required.Changes are evaluated to ensure they do not remove, without at least an equivalent replacement of safety function, an IROFS listed in the ISA Summary that is necessary for compliance with performance requirements.

Updates to the ISA, are issued in accordance with approved procedures. ISA updates are approved prior to operation of any change.

Unacceptable IROFS performance deficiencies will be corrected, and evaluated for potential changes that may be necessary to the ISA.

3.5.2 Training and Qualifications of ISA Teams

3.5.2.1 Process Hazard Analysis

To ensure the adequacy of the results of the ISA, the analyses are performed by teams composed of individuals with expertise in engineering and process operations and in accordance with internal procedures.

Each team consists of persons experienced and knowledgeable in the hazards that are known to exist in the study area (e.g., criticality, radiation, chemical, industrial, fire and explosion).

In addition, the team will include a cognizant engineer with experience and knowledge specific to the process being evaluated and a person directly experienced with the operations.

The team will include a Team Leader determined by management to be knowledgeable in the ISA process and procedures in use at the facility. Management may elect to augment Team Leader skills with a qualified facilitator familiar with the methods being used. The Team Leader assignment will be formally documented in writing.

3.5.2.2 Quantitative Risk Analyst

Technical or safety professionals may be assigned as approvers of a Quantitative Risk Assessment (QRA) report, after they have completed fundamental training on Risk Assessment.

3.5.3 Management Measures

Management measures ensure that IROFS are designed, implemented, and maintained, as necessary, to be available and reliable to perform their function when needed. Management measures are applied to IROFS in a graded approach based on the type and robustness of the IROFS and the accident sequences the IROFS is preventing or mitigating. The ISA Summary provides a description of the management measures to be applied to each identified IROFS.

A minimum set of management measures are assigned to a particular grouping of IROFS by the ISA Team depending on whether the IROFS are classified as sole IROFS or if they are active engineered control (AEC), passive engineered control (PEC), augmented administrative control (AAC), or administrative control (AC) IROFS.

Within each of the five general classifications of IROFS (Sole, AEC, PEC, AAC, or AC), the IROFS are then assigned specific elements of the management measures. The selection of specific management measure elements is determined by the operational organization based on consideration of the selection criteria.

All IROFS will have management measures applied. The graded approach does not allow for the application of management measures to be waived, but rather allows for varying levels of the number and type of management measures to be applied, as well as the specific elements of management measures, to provide adequate assurance, commensurate with risk, that the IROFS safety function will be met.

The selection criteria used to identify the appropriate application of management measures (or elements of a specific management measure) includes the following:

- Type of IROFS (AEC, PEC, AAC, AC)
- Number of IROFS (e.g., sole IROFS)
- Failure probability of the IROFS as identified in the quantitative risk assessment
- Failure mechanisms
- Design attributes (redundancy, separation requirements, complexity)
- Applicable codes or standards applicable to the IROFS
- Failure history
- Consequence severity (from PHA)
- Worker, public, or environmental consequences (from PHA)
- Type of risk analysis performed (qualitative, semi-quantitative, quantitative)
- Safety function
- Preventative or mitigative IROFS

The use of the graded approach in assigning management measures to IROFS is documented and provided to the ISA Team performing the ISA review.

The management measures are described in Chapter 11 and in the ISA Summary. The ISA Summary specifies the management measures assigned to each IROFS.