ATTACHMENT A

INSTRUMENTED SYSTEMS USED IN SAFETY SIGNIFICANT AND HAZARDOUS PROCESSES DESIGN GUIDANCE (PROGRAMMATIC AND FACILITY)

TABLE OF CONTENTS

RECORD OF REVISIONS

Rev	Date	Description	POC	OIC
0	11/17/03	Initial issue.	Mel Burnett, FWO-DECS	Gurinder Grewal, FWO-DO
1	10/27/06	Administrative changes only. Organization and contract reference updates from LANS transition. IMP and ISD number changes based on new Conduct of Engineering IMP 341. Other administrative changes.	Mike Clemmons, *FM&E-DES*	Kirk Christensen, *CENG*
2	09/29/14	Administrative change. Changed from Appendix to Attachment.	Allen Hayward, *ES-EPD*	Lawrence Goen, *ES-DO*

RESPONSIBLE THE I&C STANDARDS POC
for upkeep, interpretation, and variance issues

Section D3060/F1050 App A	**Instrumentation & Controls POC/Committee**

1.0 PURPOSE

This appendix provides guidance for the development of performance attributes and design criteria for electrical/electronic/and programmable electronic systems classified as safety significant or protection layers for hazardous processes. The development of design criteria for these systems is based on the ANSI/ISA 84.01-1996 Standard. ISA 84.01 provides a performance based graded approach to the design of safety instrumented systems.

2.0 SCOPE

The guidance presented in this appendix applies only to systems that (1) are identified as a nuclear Safety Significant system, a non-nuclear system that would be considered Safety Significant using the definition in Section 3.0 below, or a safety-related ML-2 system, and (2) require instrumented systems to perform the safety function. Operator actions in response to process alarms that place a process in a safe state in order to prevent or mitigate a safety significant risk are covered within this appendix. The appendix does not cover the methods or procedures to be used to conduct a hazard analysis, perform a risk assessment, develop a risk/consequence based matrix, identify functional classifications, or identify means to be used to prevent and/or mitigate any hazards identified.

3.0 ACRONYMS AND DEFINITIONS

3.1 ACRONYMS

AC – Administrative Control

ANS – American Nuclear Society

BPCS – Basic Process Control System

DCS – Distributed Control System

FM – Factory Mutual

IPL – Independent Protection Layer

ISA – Instrument Society of America

LOC – Level of Control

LOPA – Layer of Protection Analysis

ML – Management Level

PFD – Probability of Failure on Demand

PHA – Process Hazards Analysis

RFI – Radio Frequency Interference

RRF – Risk Reduction Factor

SIL – Safety Integrity Level

SIS – Safety Instrumented System

SS – Safety Significant

SSCs – Systems, Structures and Components

SSIS – Safety Significant Instrumented System.

TSR – Technical Safety Requirement

TUV – Technischer Uberwachungs-Verein (Technical Inspection Association of Germany)

3.2 DEFINITIONS

Administrative Control – Provision relating to organization and management, procedures, record keeping, assessment, and reporting necessary to ensure the safe operation of the facility.

Analytical Limit – Limit of a measured or calculated process parameter established by the safety or hazards analysis to ensure that a safety limit is not exceeded.

Backfit Analysis – The process by which an existing SSC is evaluated to determine if it is adequate to perform its upgraded safety function in terms of newly established requirements and safety analyses. Backfit consists of a design assessment and if needed a cost benefit assessment.

Basic Process Control System (BPCS) – A system that responds to the input signals from the process, its associated equipment, other programmable systems and/or an operator and generates outputs signals causing the process and its associated equipment to operate in the desired manner but does not perform any safety instrumented functions.

Common Cause Failure – A single event that causes failure in multiple elements of a system. The initiating event may be either internal or external to the system.

Design Agency – The organization performing the detailed design and analysis of a project or modification.

Design Authority – The person or group responsible for the final acceptability of and changes to the design of a system or component and its technical baseline.

Fail-Dangerous Fault – A failure in a system or component that will result in the system/component not performing its safety function.

Fail-Safe – Fail-safe means that on loss of motive force (electrical power, air supply, hydraulics, etc.) the system will go to a safe state and remain in this safe state.

Functional Classification – A graded classification system used to determine minimum requirements for SSCs. The Functional Classifications in order of precedence are ML-1 or Safety Class, ML-2 or Safety Significant, and ML-3 or General Service.

Independent Protection Layer (IPL) – A system, structure, component, or administrative control that acts to prevent or mitigate a safety significant hazardous event. Independent Protection Layers are sufficiently independent so that the failure of one IPL will not cause the failure of another IPL that is credited with preventing or mitigating the same event.

Layer of Protection Analysis (LOPA) – A Layer of Protection Analysis is a variation of event tree analysis where only two outcomes are considered. The possible outcomes are either failure (PFD) or successful operation.

Level of Control (LOC) – One or more structures, systems, components, administrative controls, or inherent features (e.g. chemical properties, gravity, physical constants, underground location), which can be readily expected to act to prevent or mitigate a hazardous event.

Management Level 2 (ML-2) – Selective application of applicable codes, standards, procedural controls, verification activities, documentation requirements, and formalized maintenance program (i.e., certain elements may require extensive controls, while others may only require limited control measures). Could include facility work that may require independent review, management approval, and verification of design outputs, surveillance during procurement, fabrication, installation, assembly, and construction.

Probability of Failure on Demand (PFD) – A value that indicates the probability of a system failing to respond to an event for which it is designed. The average probability of a system failing to respond to a demand in a specified time interval is referred to as PFDavg.

Risk Reduction Factor (RRF) – The inverse of Probability of Failure on Demand (1/PFD). The risk reduction factor is a numeric value identifying the amount of reduction or lessening of the likelihood of an event occurring.

Safety Integrity Level (SIL) – One of three possible discrete integrity levels (SIL 1, SIL 2, and SIL 3) of Safety Significant Instrumented Systems. SILs are defined in terms of Probability of Failure on Demand (PFD) (see Table 3.1).[1]

Table 3.1 — Safety Integrity Level (SIL)

Safety Integrity Level (SIL)	Probability of Failure on Demand Average Range (PFD avg)
1	10^{-1} to 10^{-2}
2	10^{-2} to 10^{-3}
3	10^{-3} to 10^{-4}

Safety-Related – A term meaning safety class, safety significant, and those ML-1 and ML-2 SSCs that could potentially impact public or worker safety or the environment in the same way as safety class or safety significant systems respectively.

Safety Significant (SS) – Structures, Systems, and Components that are not designated as Safety-Class SSCs but whose preventive or mitigative function is a major contributor to defense in depth and/or worker safety as determined from safety analyses. [10 CFR 830]

As a general rule of thumb, Safety-Significant SSC designations based on worker safety are limited to those Systems, Structures, or Components whose failure is estimated to result in a prompt worker fatality or serious injuries or significant radiological or chemical exposures to workers. The term, serious injuries, as used in this definition, refers to medical treatment for immediately life-threatening or permanently disabling injuries (e.g., loss of eye, loss of limb).

Safety Significant Functions – SS functions are those functions that have been classified as either SS or ML-2 through the hazards analysis and graded approach.

Safety Significant Hazardous Event – An event involving a source of danger (i.e. material, energy source, or operation) with the potential to cause illness, injury, or death to personnel or damage to a facility or to the environment that has a functional classification of SS or ML-2.

Safety Significant Instrumented System (SSIS) – An SS system, a safety-related ML-2 system, or a 29 CFR 1910.119 hazardous process independent protection layer that requires instrumentation, logic devices and final control elements to monitor and detect an SS/ML-2

1 From ANSI/ISA-S84.01-1996 “Application of Safety Instrumented Systems for the Process Industries”.

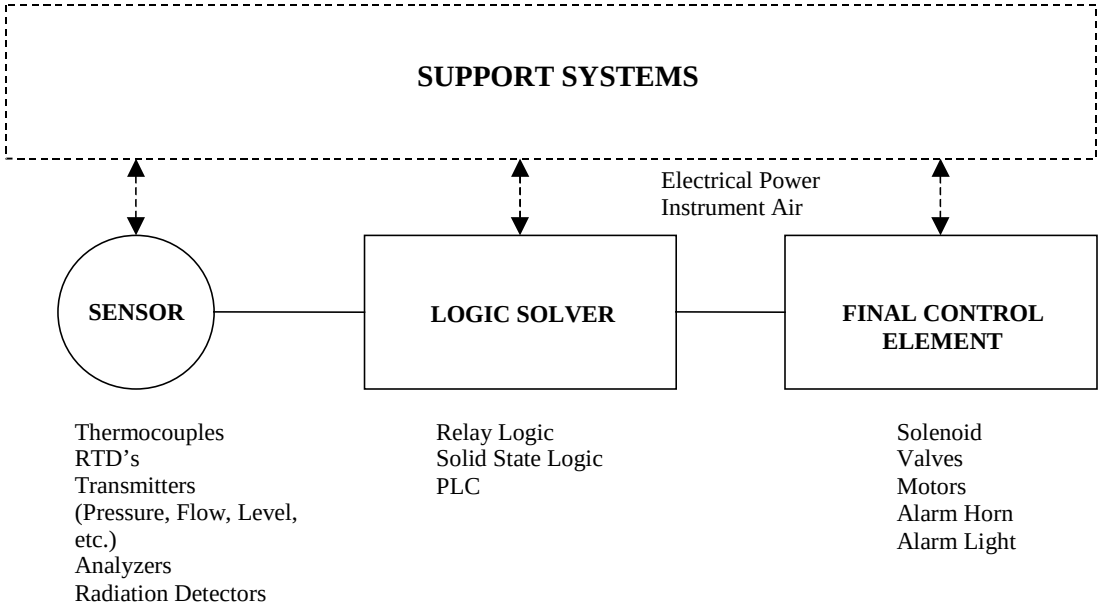
event, and which will result in automatic or operator action that will bring the facility or process system to a safe state.

TUV – A German based certification organization that provides certification services to manufacturers of safety instrumentation and safety systems.

4.0 SYSTEM ARCHITECTURE

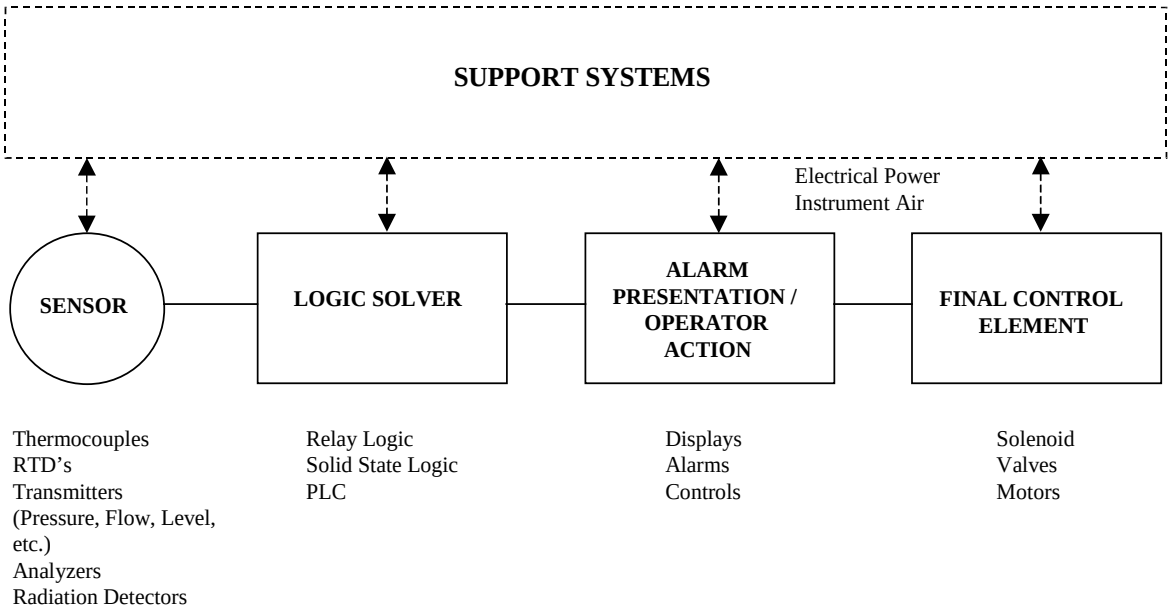
A. A Safety Significant Instrumented System (SSIS) generally consists of three parts. The first part of an SSIS is the sensor(s), which monitors one or more process parameters over a specified range to detect the initiation of a safety significant event. The second part of an SSIS is the logic solver(s), which receives input from the sensor(s) and provides logic and/or math functions to generate a safety (SS) output signal to a final control element(s). The third part of an SSIS is the final control element(s) that performs the actual safety significant action. Figure 1 below provides a block diagram of an automatic SSIS. The listing of components shown in the figure for each part of an SSIS is given to provide examples and is not meant to be a complete listing.

Figure 1: SSIS Block Diagram – Automatic Actuation



B. An operator can be included in an SSIS where operator actions are required to bring the facility or process system to a safe state. Figure 2 below provides a block diagram of an SSIS that includes operator action. The listing of components shown in the figure is given to provide examples and is not meant to be a complete listing.

Figure 2: SSIS Block Diagram – Operator Action

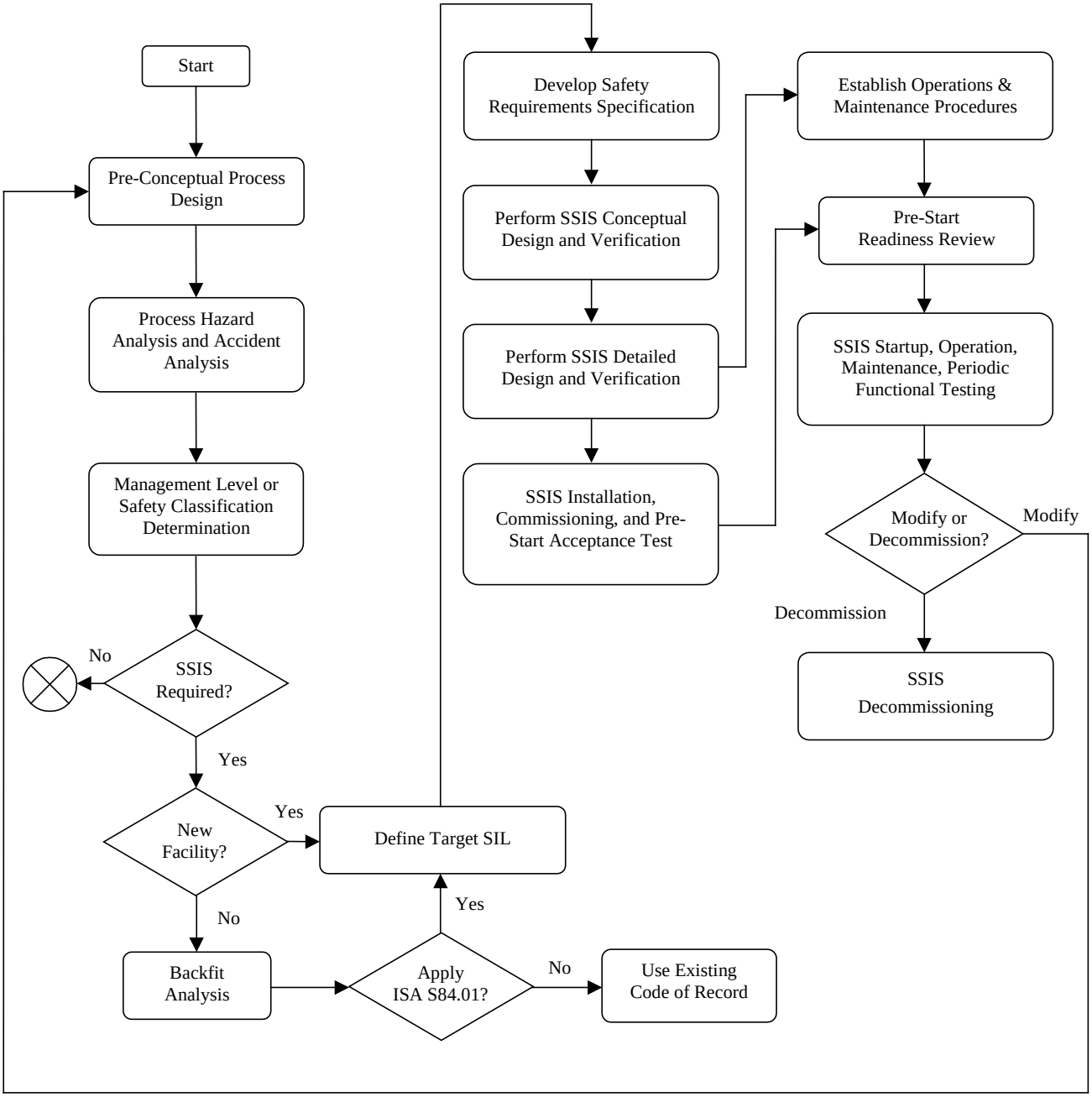


5.0 SYSTEM BOUNDARIES / CONSTRAINTS

A. The SSIS includes all elements from the sensor to the final control element(s) that are required to perform the safety significant function, including inputs, outputs, support systems (e.g., electrical power, instrument air, ventilation, etc.), and logic solvers. Also included is hardware and software, including communication links, which are required to perform the safety significant function. Portions of the system that are not required to perform the safety significant functions and have no potential adverse impact on the performance of the safety significant functions are not considered part of the SSIS. These non-SS portions are not subject to the same design guidelines defined for the safety significant portions.

6.0 SSIS LIFE CYCLE

A. ISA Standard 84.01 provides a Safety Life Cycle that covers the SSIS activities from initial conception through decommissioning. The following figure (Figure 1) depicts the SSIS life cycle approach.


Start
Pre-Conceptual Process Design
Process Hazard Analysis and Accident Analysis
Management Level or Safety Classification Determination
SSIS Required?
No
Yes
New Facility?
Yes
Define Target SIL
No
Backfit Analysis
Apply ISA S84.01?
Yes
No
Use Existing Code of Record
Develop Safety Requirements Specification
Perform SSIS Conceptual Design and Verification
Perform SSIS Detailed Design and Verification
SSIS Installation, Commissioning, and Pre-Start Acceptance Test
Establish Operations & Maintenance Procedures
Pre-Start Readiness Review
SSIS Startup, Operation, Maintenance, Periodic Functional Testing
Modify or Decommission?
Modify
Decommission
SSIS Decommissioning

7.0 DESIGN INPUTS

A. The design requirement for the SSIS is established through the determination of a target Safety Integrity Level (SIL). The SIL defines the level of performance needed by the SSIS to reduce the likelihood or consequences of a hazardous event to an acceptable level. There are three SILs defined by ISA 84.01 (SIL-1, 2 & 3). The higher the SIL number the more likely the SSIS will be available to prevent or mitigate an SS event. The SIL performance requirements in terms of probability of failure on demand (PFD) average and risk reduction factor (RRF) are listed as follows:

SIL-1	PFD: 10^{-1} to 10^{-2}	RRF: 10 to 100
SIL-2	PFD: 10^{-2} to 10^{-3}	RRF: 100 to 1000
SIL-3	PFD: 10^{-3} to 10^{-4}	RRF: 1000 to 10,000

A methodology for determining the Safety Integrity Level for an SSIS is provided in Appendix A.

B. Once the SIL level is established, the next step is to develop the Safety Requirements Specification for the SSIS design. Each SS function is generally unique and requires the identification of a specific set of performance requirements. The performance attributes should be identified and documented for each SS function and be provided by the Design Authority to the Design Agency. The following list of design input information should be considered along with information outlined in ANSI / ISA 84.01, Section 5, during the design of an SSIS or designated hazardous process protection layer:

1. Identification of the safety function. Define the state of the process. The complete description of the safety function should be provided including requirements such as the maximum allowed shutoff valve leakage. If the safe state involves sequencing, then the required sequencing should be identified.
2. Required modes of operation.
3. Target SIL of the SSIS.
4. The required operating range and analytical safety limit of the system should be specified.
5. The response time required of the system, including time for operator action, from the detection of a hazardous event to the completion of the final control element action should be specified.
6. Environmental / Seismic design requirements.
7. Desired system functional test interval.
8. Maximum acceptable nuisance/spurious trip rate.
9. Need for bypasses, manual trip or reset action by operator should be identified.
10. Interfaces to other system. This would include ‘status’ inputs/outputs to/from other systems.

C. The Design Authority should ensure that the Safety Requirements Specification for the SS function is available to the system designers at the start of the SSIS design. If a single technical agency is responsible for the total system implementation of the function, these inputs can be quantified for the overall function. However, if the design of the system is being performed through a number of technical agencies, the design input for the probability of failure on demand (PFD) and time response must be quantified for that portion of the design that each technical agency is responsible to complete. Examples for specifying these inputs amongst the different technical agencies are provided as follows:

1. Response Time Example:

   The response time requirement for an SSIS has been identified as less than 30 seconds. The design of the sensors and logic solver has been assigned to one design agency and the design of the final control element (valve) has been assigned to a different technical agency. In meeting the required response time, the sensor and logic solver portion of the SSIS should be assigned a response time (e.g., less than 10 seconds) and the final control element should be assigned a response time (e.g., less than 15 seconds). This will allow the SSIS to meet its overall specification.

2. PFD Example:

   The PFD requirement for an SSIS has been identified as less than 10^{-2} (SIL-2). The PFD for the entire SSIS is the sum of the individual PFDs of the sensor, logic solver, and final control element. The design of the sensors and logic solver has been assigned to one design agency and the design of the final control element (valve) has been assigned to a different design agency. In meeting the required PFD, the sensor and logic solver portion of the SSIS should be assigned a PFD (e.g., less than 2×10^{-3}) and the final control element should be assigned a PFD (e.g., less than 5×10^{-3}). The summation of these two PFDs (7×10^{-3}) will satisfy the system level requirement of less than 10^{-2}. This will allow the SSIS to meet its overall specification.

D. A checklist is provided in Appendix B that should be used as guidance in identifying design inputs, performing the design, and assessing the adequacy of the design. Not all items on the checklist are applicable for every SSIS and the checklist is not intended to cover all design considerations for all possible configurations. Furthermore, the checklist should not be a substitute for engineering judgement and good engineering practices, and strict adherence to the checklist does not necessarily guarantee a satisfactory design. However, judicious use of the list will increase the probability that a good design will be executed.

8.0 DESIGN CRITERIA

A. Design criteria and guidelines will vary according to the specific system function and the required SIL level. ANSI / ISA 84.01, Annex B – SIS Design Considerations, provides guidance that should be considered in establishing the design criteria that is necessary to meet the SIL requirement of a particular SSIS.

B. Systems should be designed so that the most probable failure modes of a system will increase the likelihood of a safe condition for the function. Additionally, systems should be designed as fail-safe. Appendix 2 of the I&C chapter provides guidance for the fail-safe design of process control loops. Note, however, that a system designed as fail-safe does not necessarily mean that any and all possible failures will result in the system going to a predetermined safe state.

C. The safety significant functions of the system should not be interrupted or compromised by any non-safety significant functions performed by the system or by any other system.

D. As indicated by ANSI / ISA 84.01, Section 7.4.1.3, safety signals should be hard wired and not multiplexed between the logic solver and field devices (sensor, final control element). Multiplexed signals (e.g., networks, data highways) can be used from a logic solver (e.g., PLC) to an alarm device if located in a manned area and operator action is required for the SSIS. Documentation of this configuration must demonstrate that the application meets the design criteria (PFD) for the function.

E. Guidance on routing of safety significant wiring can be found in the I&C Chapter, Section 11.2.

F. The human-machine interface should be designed in accordance with the requirements defined by the Design Authority. The applicable criteria found in the I&C Chapter, Section 10.0, and guidance provided in Appendix 5 should be considered in the design.

G. An indication that the SSIS has performed the safety function should be provided to the operator. Indications that the SSIS has detected a full or partial system failure (trouble alarm) should also be provided to the operator.

H. Systems that provide motive force (e.g., electrical power, instrument air) should be included as part of the SSIS evaluation only where they are required to complete the SS function.

I. A certification should be provided for any safety PLC used in an SSIS. TUV and FM provide certification for components used in safety instrumented systems in the process industry. Note, however, that not all components certified to the same safety level (PFD) are equivalent. The certification reports will list restrictions on the operating conditions and the configuration of the components in order to achieve a specific PFD or SIL level. A certification report must be reviewed in its entirety to assure that components can be used in the selected design configuration to achieve the target SIL for the SSIS.

J. As identified in Section 7.0, Item D, a checklist is provided in Appendix B that should be considered during the design process. An additional checklist for generic I&C systems is contained in Appendix C of the I&C chapter. This checklist should also be considered and used, as appropriate.

9.0 DESIGN VERIFICATION

A. The required probability of failure on demand (PFD) is one of the key attributes that should be specified for safety significant functions through the SIL evaluation process. It is essential that the PFD of the SSIS be verified to assure that the SSIS as designed, installed, operated and maintained meets the target SIL specified for the system. The verification of the SSIS PFD should be conducted during the conceptual design in order to develop the SSIS design and at the end of the detailed design.

B. The PFD of an SSIS should be verified by the application of Reliability Block Diagrams, Fault Tree Analysis, or Markov Models. Fault Tree Analysis is the preferred method for determining the PFD of the installed SSIS. Further guidance on the analysis of an SSIS can be obtained from draft ISA technical report TR84.00.02.

C. An analysis team knowledgeable of the design being evaluated and ISA 84.01 should be convened to initiate the Fault Tree Analysis. The team typically consists of Design Agency, Design Authority, Safety Analysis engineers and a Fault Tree analyst. The team should agree on fault mechanisms, common mode failures, appropriate assumptions, etc., to be used to complete a preliminary Engineering Calculation based on the preliminary design of the SSIS. Other tools may be used to evaluate the PFD of the preliminary design. When the detailed design is complete, the team should reconvene to confirm the Calculation based on the final detailed design.

D. Once an Engineering Calculation is completed for a final SSIS design, the calculation is maintained as a supporting document to the Authorization Basis for the facility.

E. At the end of the detailed design phase the trip setpoint for the SSIS should be calculated. ANSI/ISA 67.04.01 should be used to establish the required trip setpoint of the safety function. The actual calibrated setpoint should provide sufficient allowance between the analytical limit and the calibrated instrument trip setpoint to account for uncertainties and dynamic responses.

10.0 SYSTEM ADEQUACY ANALYSIS

A. When an existing instrumented system is to be upgraded to Safety Significant / ML-2, the Design Authority refers to the System Adequacy Analysis for the system under consideration. This process establishes whether the instrumented system will meet the specific design, maintenance, and performance requirements of a Safety Significant System. If it is determined from the System Adequacy Analysis that a design modification is necessary to justify the upgrade of the system to an SSIS, the Design Authority initiates the ISA 84.01 process. See also AP-341-515, System Adequacy Analysis.

Attachment 1: Safety Integrity Level Assignment Methodology

This methodology defines the necessary steps for assigning a target Safety Integrity Level (SIL) to Safety Significant Instrumented Systems. The methodology is based on a frequency and consequence ranking matrix recognized by DOE-STD-3009 and further developed through the LANL Hazard Analysis Technical Methodology Manual. The calculation of the target SIL is based on the credit taken for the SSIS to reduce the likelihood or consequence of the hazardous event to an acceptable level.

AP-341-502 Management Level Determination for Structures, System, and Components defines key factors within the ML-2 listing for Safety and Health that identify SS functions required to satisfy public safety, worker safety, and defense in depth at LANL. Key factors that identify SS functions required to protect the environment are provided within the ML-2 listing for Environmental Consequences. The SS functions are satisfied through control features, which can either be engineered systems, administrative controls, or passive controls. Safety Significant Instrumented Systems (SSISs) are a subset of design features that may be designated to provide an SS function to prevent or mitigate a hazardous condition or event. This methodology is only concerned with assigning SIL levels for SSISs.

The SIL level of an SSIS cannot be determined without looking at all of the SS SSCs and administrative controls that may be credited with providing the safety function to prevent or mitigate a specific hazardous event. This methodology assesses the required risk reduction for the SS hazardous event. In some cases, the SSIS alone is required to provide the entire risk reduction for the hazardous event. In other cases, the SSIS in combination with other credited design features and controls provides the required risk reduction. The quality of the SSIS design that is required to reduce the overall risk of the hazardous event to an acceptable level is based on the risk reduction provided by all of the credited design features and controls.

As established within AP-341-502, SS functions are identified through the following Key Factors:

Factor 1	SSC is designated as Safety Significant per DOE-STD-3009-94.
Factor 2	SSC failure could cause the failure of another Safety Significant SSC or prevent it from performing its required function.
Factor 3	SSC is required to support another Safety Significant SSC.
Factor 4	SSC failure could cause or allow release of radioactive material with a potential radiological dose less than 25 rem or releases of chemicals with a potential does less than ERPG-2 per DOE-STD-3009-94 at the site boundary.
Factor 5	SSC provides defense in depth, backup, or redundancy to a Safety Class SSC.
Factor 6	SSC failure could result in death or serious (disabling) injury or illness to a worker.
Factor 7	SSC failure could result in minor injury, irritation, annoyance, or illness to a member of the public.
Factor 8	SSC failure could cause or allow severe long-term damage to the environment within Laboratory boundaries.
Factor 9	SSC failure could cause or allow damage to commercial resources such as agricultural, recreational, or business properties.

SIL Assignment for SS Key Factors 1, 4, 6, 7, 8 & 9

For Factors 1, 4, 6, 7, 8 and 9 functions are classified SS based on the results of a Hazard Analysis (HA). The HA identifies abnormal occurrences and potential accident scenarios that could cause harm to the public, worker, or environment and determines the unmitigated consequences and expected frequency of each particular event. The unmitigated consequences are generally established through a quantitative analysis for nuclear and chemical hazards and through qualitative analysis for other hazards (e.g., high explosives). The unmitigated event frequency is generally established through a qualitative process that is based primarily on engineering judgement.

Once the unmitigated consequences and frequency have been established, the events are assigned to a "bin" of a frequency-consequence risk matrix to assess the relative risk. The method of risk binning allows for attention to be focused on those events that pose the greatest risk to the public, workers, and the environment. The figures on the following pages are representations of the frequency-consequence risk matrices developed by LANL for the public and the worker as identified within the LANL Hazard Analysis Technical Methodology Manual.

Figure A1: Public Hazard Risk Matrix

Likelihood → **Consequence ↓**	**Frequent** (Expected) $> 10^{0}$/yr.	**Probable** (Likely) $< 10^{0}$/yr. to $> 10^{-2}$/yr.	**Occasional** (Unlikely) $< 10^{-2}$/yr. to $> 10^{-4}$/yr.	**Improbable** (Extremely Unlikely) $< 10^{-4}$/yr. to $> 10^{-6}$/yr.	**Remote** (Beyond Extremely Unlikely) $< 10^{-6}$/yr.
High > 25 Rem TEDE > ERPG-2	**1**	**1**	**2**	**2**	**3**
Medium From > 5 Rem to < 25 Rem From > ERPG-1 to < ERPG-2	**1**	**2**	**2**	**3**	**3**
Low From > 0.1 Rem to < 5 Rem From Measurable to < ERPG-1	**1**	**2**	**3**	**3**	**4**
Negligible < 0.1 Rem < Measurable	**3**	**3**	**3**	**4**	**4**
None	**4**	**4**	**4**	**4**	**4**

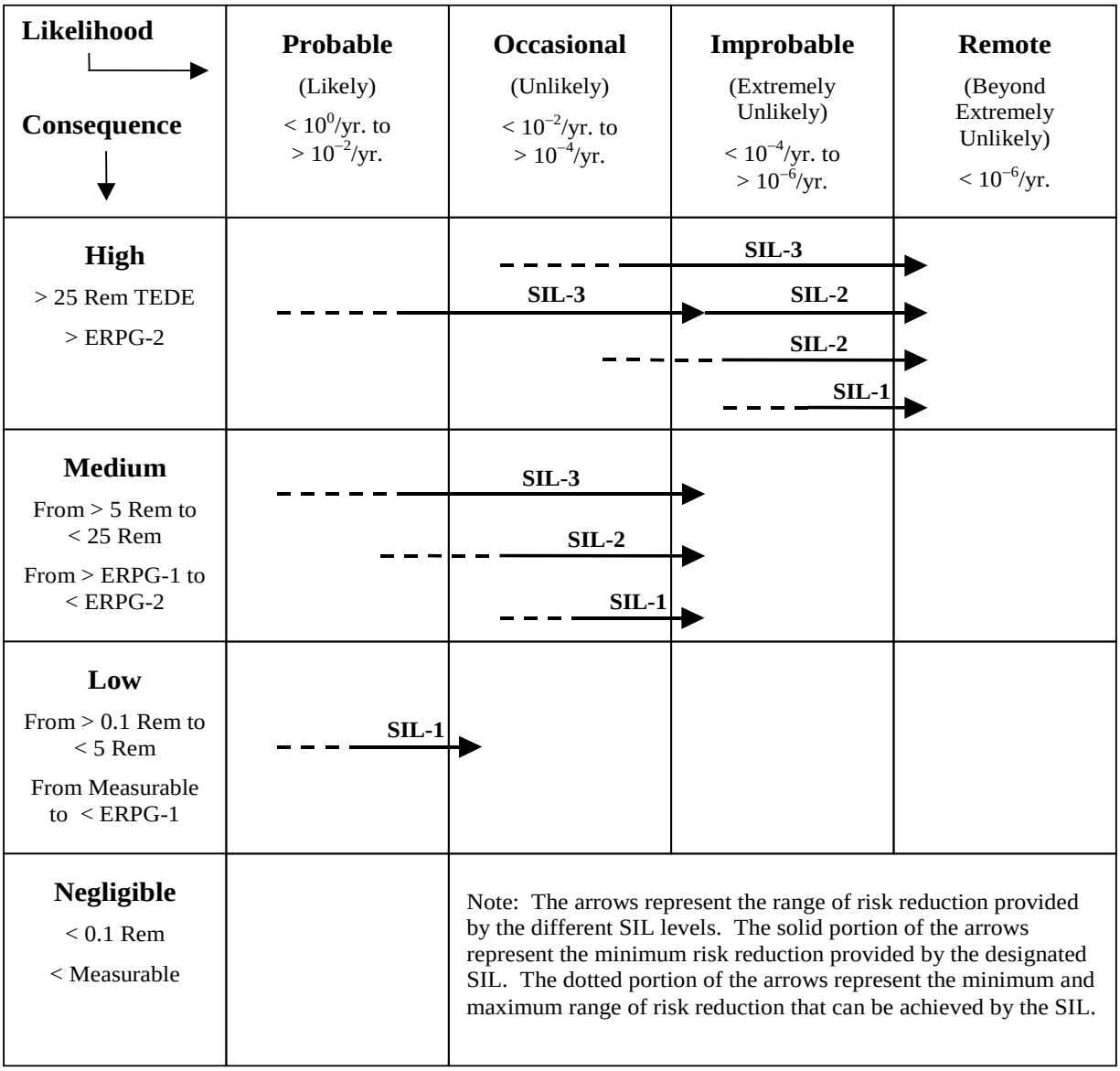
Figure A2: Worker Hazard Risk Matrix

Likelihood → / Consequence ↓	**Frequent** (Expected) $> 10^{0}$/yr.	**Probable** (Likely) $< 10^{0}$/yr. to $> 10^{-2}$/yr.	**Occasional** (Unlikely) $< 10^{-2}$/yr. to $> 10^{-4}$/yr.	**Improbable** (Extremely Unlikely) $< 10^{-4}$/yr. to $> 10^{-6}$/yr.	**Remote** (Beyond Extremely Unlikely) $< 10^{-6}$/yr.
High Immediate Health Effects or Loss of Life	**1**	**1**	**2**	**2**	**3**
Medium Long-term Health Effects, Disability, or Severe Injury (non life threatening)	**1**	**1**	**2**	**3**	**4**
Low Lost-time Injury but No Disability (work restriction)	**1**	**2**	**3**	**4**	**4**
Negligible Minor Injury with No Disability and No Work Restriction	**2**	**3**	**4**	**4**	**4**
None	**4**	**4**	**4**	**4**	**4**

Identifying Risk Reduction Goals

The hazard analysis provides the assigned risk-bin for a postulated accident scenario that require SS controls and identifies all of the control features that are credited with preventing or mitigating the SS hazardous event. The objective of SSCs and Administrative Controls (ACs) identified as SS control features are to reduce the consequences and/or frequency of the event in order to reduce the relative risk. The design of an SSIS is considered to provide adequate prevention or mitigation for an event if the risk reduction provided by the SSIS alone or the SSIS is combination with other SS features reduces the risk by an acceptable margin. The risk reduction provided by an SSIS designed to one of the three SILs is graphically illustrated on the following Risk Binning Matrix.

Figure A3: SIL Reduction Risk Binning Matrix



Determination of a Target SIL for an SSIS using a Layer of Protection Analysis (LOPA)

Each of the protective features identified within the hazard analysis as a primary (1st Level of Control) is considered a layer of protection. The hazard analysis process should quantify the expected effectiveness of the layers of protection that are not SSISs in terms of Probability of Failure on Demand (PFD) or availability. If the hazard analysis does not quantify the required PFD or availability of a credited SS system or control, then this must be determined separately before the SSIS SIL can be assigned. Where a system already exists and has been designated as a preventive or mitigation feature, verification of its safety availability is required to determine its effective PFD.

A Layer of Protection Analysis (LOPA) is used to determine the required SIL of the SSIS. A LOPA is a form of risk assessment, similar to that of an event tree analysis, in which two outcomes are considered, failure (PFD) or successful operation. The frequency of the unmitigated hazardous event in question is the stating point of the LOPA. If the hazard analysis process identifies a specific event frequency for a hazard, then this value should be used in the LOPA calculation. However, where a qualitative analysis provides the unmitigated event frequency in terms of Probable, Occasional, or Improbable, the midpoint of the frequency range for the respective bin should be used as listed below, providing that the anlaysis is conservative.

Probable (Likely)	10^{-1}/yr
Occasional (Unlikely)	10^{-3}/yr
Improbable (Extremely Unlikely)	10^{-5}/yr

A Basic Process Control System (BPCS) may be used, in combination with the assigned unmitigated event frequency, to calculate a mitigated event frequency for an SS hazardous event. However, the following conditions must be met to allow the inclusion of the BPCS in the event frequency calculation:

1. The failure of the BPCS is not the initiating or contributing cause of the event.
2. The BPCS must be designed to function during the event, including the environmental conditions for which it is credited for operation.
3. A risk reduction factor claimed for the BPCS must be ten or less (PFD $\geq 10^{-1}$).
4. SSCs that monitor initial conditions and are credited in a LOPA analysis for reducing or establishing the initial event frequency cannot be a part of a BPCS that is also credited in the LOPA analysis. BPCS must be independent of the event initiator or other Layers of Protection.

Once the event frequency has been established, the LOPA process consists of the identification of each Independent Protection Layer (IPL) and an evaluation into the effectiveness that each has in preventing and/or mitigating the SS or designated ML-2 hazardous event. Independent Protection Layers (IPLs) may include but are not limited to: (1) design features such as siting, containment, confinement, and shielding, (2) administrative controls that restrict deviations from safe operations through operating procedures or limiting conditions of operation, (3) mechanical or process systems, and (4) an SSIS. Note: Administrative controls require consideration of the human interface in sensing conditions and performing functions.

General rules for IPLs:

1. The IPL must be designed to prevent an SS hazardous event, or mitigate the consequences of such an event to an acceptable level.
2. A system, structure, component that is classified as safety class or safety significant, TSR administrative control, or other SSC that is adequately identified and controlled in the requirements of the Authorization Basis of a facility can be considered as an IPL.
3. The IPL is designed to perform a safety function during normal, abnormal and design basis accident environmental conditions for which it is required to operate.
4. IPLs must be sufficiently independent so that the failure of one IPL does not adversely affect the probability of failure of another IPL.

If some combination of components or systems is required to function together to protect a worker or the public, they should be considered as one IPL. Thus, if it takes two out of three components to function or a series of components to operate to protect a worker, then the combination of SSCs will constitute one IPL. The IPL may not by itself reduce the risk of the hazardous event occurring to an acceptable level, but it will prevent or mitigate the event to an acceptable level when it works.

Given that the IPL design follows the above rules, then the SS hazardous event and the IPL failure can be treated as statistically independent occurrences. Thus, both the hazardous event and a failure of all IPLs must occur before there is an unacceptable result. If any of the IPLs function, then the event will be prevented or mitigated to an acceptable level.

LOPA is based on calculating the probability of a series of independent events occurring. The event must occur and all IPLs must fail in order for the hazardous event to affect the workers or public. As an example probability calculation, the probability of failure (likelihood) of getting three IPLs (A, B, and C) to fail is shown below (three input AND gate):

$$P(A \cap B \cap C) = P(A) \times P(B) \times P(C)$$

$\cap \equiv$ Symbol for AND
P(Z) is the PFD of IPL (Z)

The goal of an IPL is to prevent a hazardous event from occurring or mitigate the hazardous event to an acceptable level. Whether the IPL is designed to prevent or mitigate the event, the PFD of the IPL is used in the LOPA calculation. The probability of the undesired consequence is based on the product of the unmitigated event frequency and all of the PFDs of the separate independent protection layers.

The SSIS SIL calculated from the LOPA analysis should provide the capability of a one-half decade risk reduction beyond the minimum risk reduction required to reduce the likelihood of the event by an acceptable margin. The one-half decade risk reduction, beyond that minimally required to place the event into an acceptable risk bin, provides a degree of assurance against uncertainties in event frequencies, component failure rates, and other terms used in the calculation to verify the target SSIS SIL.

Sample SIL Determinations

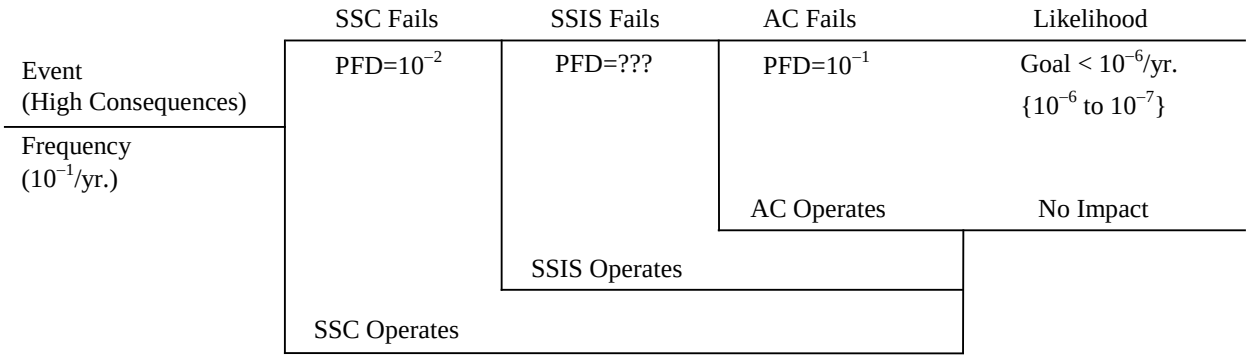
Included below are examples of the use of a LOPA to assign SSIS SIL levels. The order of the IPLs in a LOPA diagram is unimportant to the calculation of the required SIL level.

As can be seen in the example calculations, Administrative Controls are one of the layers of protection that can be taken credit for in a LOPA analysis. Administrative Controls are assigned for the programs and administrative requirements that ensure that the basic facility conditions assumed in the analysis do exist (e.g, minimum staffing limits and established inventory control programs). Administrative Controls are also assigned to procedural or program controls or equipment that perform a passive function that the operator does not directly control (e.g., inventory control based on records of installed measurement equipment or passive barriers credited in the accident analysis).

Example 1

The following is a target SIL determination for a hazardous event that is anticipated with high consequences. The design uses three Independent Protection Layers (IPLs) to reduce the likelihood of the event to less than 10^{-6}/yr.

Unmitigated Hazardous Event	IPL-1 (SSC)	IPL-2 (SSIS)	IPL-3 (AC)	Unacceptable Consequence Likelihood



Calculation:

Frequency × PFD_{IPL-1} × PFD_{IPL-2} × PFD_{IPL-3}	<	10^{-6}/yr.
(10^{-1}/yr.) × (10^{-2}) × PFD_{IPL-2} × 10^{-1}	<	10^{-6}/yr.
PFD_{IPL-2} × 10^{-4}/yr.	<	10^{-6}/yr.
PFD_{IPL-2}	<	10^{-2}/yr.

Thus, the SSIS (IPL-2) should be designed as a SIL-2 (PFD: 10^{-2} to 10^{-3}). A SIL-2 SSIS, in combination with the other IPLs, has the capability to reduce the likelihood of the unacceptable consequences for this event to 10^{-7}/yr.

Example 2

The following is a target SIL determination for a hazardous event that is unlikely with medium consequences. The design uses only one Independent Protection Layer (IPL) to reduce the likelihood of the event to less than 10^{-4}/yr.

Unmitigated Hazardous Event	IPL-1 (SSIS Alarm System / Operator Action)	Unacceptable Consequence Likelihood
	SSIS Alarm System Fails	Likelihood
Event (Medium Consequence) Frequency (10^{-3}/yr.)	PFD=???	Goal < 10^{-4}/yr. {10^{-4} to 10^{-5}}
	SSIS Alarm System Operates	No Impact

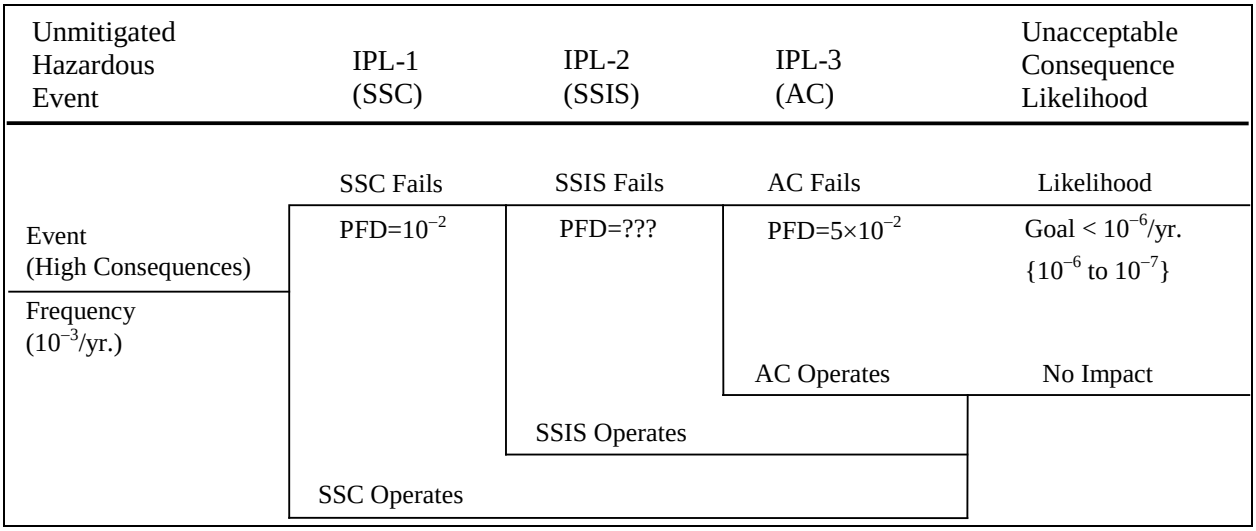
Calculation:

$$\text{Frequency} \times PFD_{IPL\text{-}1} < 10^{-6}\text{/yr.}$$
$$(10^{-3}\text{/yr.}) \times PFD_{IPL\text{-}1} < 10^{-6}\text{/yr.}$$
$$PFD_{IPL\text{-}1} < 10^{-1}\text{/yr.}$$

Thus, the SSIS (IPL-1) should be designed as a SIL-1 (PFD: 10^{-1} to 10^{-2}). A SIL-1 SSIS has the capability to reduce the likelihood of the unacceptable consequences for this event to 10^{-5}/yr.

Example 3

The following is a target SIL determination for a hazardous event that is unlikely with high consequences. The design uses three Independent Protection Layers (IPLs) to reduce the likelihood of the event to less than 10^{-6}/yr.



Calculation:

$\text{Frequency} \times \text{PFD}_{\text{IPL-1}} \times \text{PFD}_{\text{IPL-2}} \times \text{PFD}_{\text{IPL-3}}$	<	10^{-6}/yr.
$(10^{-3}\text{/yr.}) \times (10^{-2}) \times \text{PFD}_{\text{IPL-2}} \times (5\times10^{-2})$	<	10^{-6}/yr.
$\text{PFD}_{\text{IPL-2}} \times (5\times10^{-7}\text{/yr.})$	<	10^{-6}/yr.
5×10^{-7}/yr.	<	10^{-6}/yr.

The SSIS providing the IPL-2 in this example is not required because IPL-1 and IPL-3 provide a combined risk reduction factor in conjunction with the event frequency that achieves the goal of reducing the likelihood of the event. If IPL-1 (SSC) were an instrumented system it would be designated as an SSIS.

Example 4

The following is a target SIL determination for a hazardous event that is anticipated with high consequences. The design takes credit for the operation of the Basic Process Control System (BPCS), which if operating would prevent the event condition from occurring, in addition to two Independent Protection Layers (IPLs) to reduce the likelihood of the event to less than 10^{-6}/yr.

Unmitigated Hazardous Event	BPCS Event Mitigation	IPL-1 (SSC)	IPL-2 (SSIS)	Unacceptable Consequence Likelihood
		SSC Fails	SSIS Fails	Likelihood
Event (High Consequences)	BPCS Fails	PFD=10^{-2}	PFD=???	Goal < 10^{-6}/yr. {10^{-6} to 10^{-7}}
Frequency (10^{-1}/yr.)	PFD=10^{-1}			
			SSIS Operates	No Impact
		SSC Operates		

Calculation:

$\text{Frequency} \times \text{PFD}_{\text{BPCS}} \times \text{PFD}_{\text{IPL-1}} \times \text{PFD}_{\text{IPL-2}}$	<	10^{-6}/yr.
$(10^{-1}\text{/yr.}) \times (10^{-1}) \times (10^{-2}) \times \text{PFD}_{\text{IPL-2}}$	<	10^{-6}/yr.
$\text{PFD}_{\text{IPL-2}} \times (10^{-4}\text{/yr.})$	<	10^{-6}/yr.
$\text{PFD}_{\text{IPL-2}}$	<	10^{-2}/yr.

Thus, the SSIS (IPL-2) should be designed as a SIL-2 (PFD: 10^{-2} to 10^{-3}). A SIL-2 SSIS, in combination with IPL-1, has the capability to reduce the likelihood of the unacceptable consequences for this event to 10^{-7}/yr.

SIL Assignment for SS Key Factors 2 & 3

A SIL is not assigned to an SS system that provides a supporting function to or enables the performance of another ML-1, SC, ML-2, or SS safety system. However, support systems (e.g., electrical power, instrument air, cooling water, ventilation) do have a strong influence on SSIS performance. Ultimately, the support systems may determine whether or not the SSIS meets its target SIL. Nonetheless, SILs are assigned only to SSISs, not to support systems.

Although support systems to ML-2 or SS systems are not assigned a SIL, the PFD of the support system is generally required to determine the PFD of the overall SSIS system. The support system availability may have a significant impact on whether or not the SSIS will achieve its targeted SIL.

The PFD of a support system is also used in calculations to determine the PFD of non-SSIS systems for which it supports, where the non-SSIS functions may be credited in a LOPA analysis.

SIL Assignment for SS Key Factor 5

The Hazards Analysis process results in a minimum number of LOCs that are necessary for the protection of workers and the public. Additional LOCs (2nd and 3rd Levels of Control) may also be selected so that no one layer of protection is completely relied on to prevent or mitigate a hazardous event. An SSIS may be selected as an additional LOC if the system functions as defense in depth, backup, or redundant to a function designated as SC.

The LANL Hazards Analysis Technical Methodology Handbook provides criteria to aide in the selection of LOCs. This criteria specifies that preventive controls should be selected over mitigation controls. A preventive first level LOC is generally required to reduce the frequency of the event in order to reduce the relative risk. Where an SSIS LOC is providing a second or third LOC for a preventive system, then the SSIS should be designed to meet SIL-1 requirements as a minimum. A SIL-1 SSIS is an independent safety protection layer that can be readily expected to mitigate or prevent an unwanted event.

If the SSIS is providing a second LOC for an existing primary (1st LOC) ‘mitigation’ system, additional consideration should be provided in determining the required SIL. An SSIS that provides the second LOC for a mitigation system should be designed to meet SIL-1 requirements as a minimum, and if possible should prevent the hazardous event. For a ‘Probable’ event, where a preventative SSIS can be selected as an additional LOC for a mitigation primary LOC, a SIL-2 or SIL-3 SSIS should be considered.

Attachment 2: Safety Significant Instrumented System Checklist

Design Input

Safety Significant (SS) Design Input

1.	Has the Hazard Analysis identified the consequence and event frequency for each SS function?	☐ Yes	☐ No	☐ N/A
2.	Has the Safety Integrity Level been assigned for each SS function?	☐ Yes	☐ No	☐ N/A
3.	Has a time response been assigned for each SS function?	☐ Yes	☐ No	☐ N/A
4.	Has a setpoint and range been assigned for each SSIS process parameter?	☐ Yes	☐ No	☐ N/A

Conceptual Design

1.	Has the Safety Integrity Level been verified for each SS function?	☐ Yes	☐ No	☐ N/A
2.	Did an independent assessor review the conceptual design? Note: An independent assessor is considered to be any qualified individual competent enough to have prepared the design but sufficiently independent such that they are not verifying their own design.	☐ Yes	☐ No	☐ N/A

Detailed Design

Operator Interface

1.	Are controls and displays adequate, effective, and suitable for operator tasks?	☐ Yes	☐ No	☐ N/A
2.	Is the SSIS operation consistent with existing systems, established conventions and operator experience?	☐ Yes	☐ No	☐ N/A
3.	Do separate displays present consistent information?	☐ Yes	☐ No	☐ N/A
4.	Does the indication at the operator display show information that is consistent with the related control action or process response to a control or safety action?	☐ Yes	☐ No	☐ N/A
5.	Is displayed information readable, concise, complete, and usable without extrapolation?	☐ Yes	☐ No	☐ N/A
6.	Is adequate information about normal and upset conditions displayed?	☐ Yes	☐ No	☐ N/A
7.	Is display failure readily apparent?	☐ Yes	☐ No	☐ N/A
8.	Are instruments located at recommended height and reach limits?	☐ Yes	☐ No	☐ N/A
9.	Are critical alarms obvious to an operator?	☐ Yes	☐ No	☐ N/A
10.	Are related controls, displays, and alarms grouped together?	☐ Yes	☐ No	☐ N/A
11.	Is manual initiation of the SSIS provided?	☐ Yes	☐ No	☐ N/A

12. Is the possibility of accidental operator activation of SSIS initiation minimized?	☐ Yes	☐ No	☐ N/A
13. Does the SSIS require a manual reset to clear the SSIS interlock and resume operations?	☐ Yes	☐ No	☐ N/A
14. Is the SSIS in an area that requires frequent operator attention?	☐ Yes	☐ No	☐ N/A
15. Do displays support operator task requirements in terms of range, precision and accuracy?			
16. Are normal operating ranges and alarm setpoints clearly identified?	☐ Yes	☐ No	☐ N/A

Sensors

1. Is sensor redundancy employed?	☐ Yes	☐ No	☐ N/A
2. If identical redundancy is employed, has the potential for common cause failure been adequately addressed?	☐ Yes	☐ No	☐ N/A
3. Are redundant sensors installed with adequate physical separation?	☐ Yes	☐ No	☐ N/A
4. Does each sensor have dedicated wiring to the SSIS I/O modules?	☐ Yes	☐ No	☐ N/A
5. Does each sensor have a dedicated process tap?	☐ Yes	☐ No	☐ N/A
6. Does the configuration allow each sensor to be independently proof tested?	☐ Yes	☐ No	☐ N/A
7. Can redundant sensors be tested or maintained without reducing the integrity of the SSIS?	☐ Yes	☐ No	☐ N/A
8. Is diversity used?	☐ Yes	☐ No	☐ N/A
8.1 Are diverse parameters measured?	☐ Yes	☐ No	☐ N/A
8.2 Are diverse means of processing specified?	☐ Yes	☐ No	☐ N/A
9. Is there sufficient independence of hardware manufacturer?	☐ Yes	☐ No	☐ N/A
10. Is there sufficient independence of hardware test methods?	☐ Yes	☐ No	☐ N/A
11. Are sensor/instrument sensing lines adequately purged or heat traced to prevent plugging?	☐ Yes	☐ No	☐ N/A
12. Are SSIS sensors clearly identified by some means (tagging, paint, etc) as components of the SSIS?	☐ Yes	☐ No	☐ N/A
13. Has the mean time to dangerous failure rate been determined for each sensor?	☐ Yes	☐ No	☐ N/A

Logic Solver

1. Does the logic solver have methods to protect against fail-dangerous faults?	☐ Yes	☐ No	☐ N/A
2. Is the logic solver a fault-tolerant device?	☐ Yes	☐ No	☐ N/A
3. Is the logic solver separated from the Basic Process Control System?	☐ Yes	☐ No	☐ N/A
4. Are all SS functions combined in a single logic solver?	☐ Yes	☐ No	☐ N/A
5. Is the logic solver TUV or FM certified for the application?	☐ Yes	☐ No	☐ N/A

6.	Is the application software protected from unauthorized charges?	☐ Yes	☐ No	☐ N/A
7.	Has the mean time to dangerous failure been determined for the logic solver?	☐ Yes	☐ No	☐ N/A

Application Software

1.	Is the final program verified through factory acceptance testing that includes fault simulation?	☐ Yes	☐ No	☐ N/A
2.	Is the final program verified through complete site acceptance testing that includes verification of startup, operation, and testing algorithms?	☐ Yes	☐ No	☐ N/A
3.	Has software met design criteria?	☐ Yes	☐ No	☐ N/A

Actuators

1.	Are backup power sources provided?	☐ Yes	☐ No	☐ N/A
2.	Are manual actuators safely and easily accessible?	☐ Yes	☐ No	☐ N/A

Final Elements

1.	Have the final elements been checked to ensure proper sizing and application?	☐ Yes	☐ No	☐ N/A
2.	Have the final elements been checked to ensure that the devices achieve the fail-safe condition?	☐ Yes	☐ No	☐ N/A
3.	Has the mean time to dangerous failure rate been determined for each final element?	☐ Yes	☐ No	☐ N/A

Process Connections

1.	Are process connections properly installed to prevent process fouling?	☐ Yes	☐ No	☐ N/A
2.	Are process connections installed correctly for the device type and process?	☐ Yes	☐ No	☐ N/A
3.	Are sensor process isolation valves associated with the SSIS properly marked?	☐ Yes	☐ No	☐ N/A

Electrical Connections/Conduit/Wire-Trays/Junction Boxes

1.	Are electrical connections properly made and inspected?	☐ Yes	☐ No	☐ N/A
2.	Are all SSIS conduits/wire-trays properly marked?	☐ Yes	☐ No	☐ N/A
3.	Are all SSIS conduits/wire-trays adequately segregated from non-SSIS conduits/wire-trays?	☐ Yes	☐ No	☐ N/A
4.	Are all conduit covers and gaskets in place?	☐ Yes	☐ No	☐ N/A
5.	Are all seals poured?	☐ Yes	☐ No	☐ N/A
6.	Are all SSIS junction boxes properly marked?	☐ Yes	☐ No	☐ N/A
7.	Are all SSIS terminations in shared junction boxes adequately segregated from non-SSIS terminations?	☐ Yes	☐ No	☐ N/A

8. Is the electrical power source reliable?	☐ Yes	☐ No	☐ N/A
9. Have the consequences of loss of instrument power been considered?	☐ Yes	☐ No	☐ N/A
10. Is there an Uninterruptible Power Supply (UPS) for the SSIS?	☐ Yes	☐ No	☐ N/A
10.1Is it periodically tested?	☐ Yes	☐ No	☐ N/A
11. Are primary and backup supplies powered from independent busses?	☐ Yes	☐ No	☐ N/A
12. Can redundant supplies be taken out of service for maintenance without interrupting SSIS operation?	☐ Yes	☐ No	☐ N/A
13. Is the SSIS properly grounded?	☐ Yes	☐ No	☐ N/A
14. Is the SSIS hardware consistent with the area electrical classification?	☐ Yes	☐ No	☐ N/A
15. Are the power supplies adequately protected from ground faults or other voltage disturbances?	☐ Yes	☐ No	☐ N/A

Pneumatic Supply

1. Is the pneumatic supply source clean and reliable?	☐ Yes	☐ No	☐ N/A
2. Have the consequences of loss of pneumatic supply been considered?	☐ Yes	☐ No	☐ N/A
3. Have the consequences of over-pressure of the pneumatic supply been considered?	☐ Yes	☐ No	☐ N/A

Hydraulic Supply

1. Is the hydraulic supply source clean and reliable?	☐ Yes	☐ No	☐ N/A
2. Have the consequences of loss of hydraulic power been considered?	☐ Yes	☐ No	☐ N/A
3. Have the consequences of over-pressure of the hydraulic power been considered?	☐ Yes	☐ No	☐ N/A

Environmental

1. Have the effects of RFI on the SSIS devices been considered?	☐ Yes	☐ No	☐ N/A
2. Are the devices being used within the manufacturer's environmental specifications?	☐ Yes	☐ No	☐ N/A
3. Have sources of excessive vibration been eliminated or mitigated?	☐ Yes	☐ No	☐ N/A
4. Have sources of excessive temperature been eliminated or mitigated?	☐ Yes	☐ No	☐ N/A
5. Have all SSIS seismic requirements been achieved?	☐ Yes	☐ No	☐ N/A
6. Have the effects of the total integrated radiation does on components been considered?	☐ Yes	☐ No	☐ N/A
7. Have all SSIS component environmental requirements been achieved?	☐ Yes	☐ No	☐ N/A

Installation / Operation

Installation

1.	Have external causes of common cause failure been identified (e.g., fire, vehicle impact, lightning, etc.)?	☐ Yes	☐ No	☐ N/A
2.	Is the SSIS segregated from other systems to minimize the probability of external influences causing a simultaneous failure of the systems?	☐ Yes	☐ No	☐ N/A
3.	Is there sufficient separation in the installation of diverse equipment?	☐ Yes	☐ No	☐ N/A

Operation

1.	Are operators provided separate, specific SS procedures?	☐ Yes	☐ No	☐ N/A
2.	Are operators provided specific training relative to the SS system?	☐ Yes	☐ No	☐ N/A
3.	Are operators being evaluated for competency in SS operation on a regular basis?	☐ Yes	☐ No	☐ N/A

Testing / Maintenance

Testing

1.	Does the periodic test interval for the SSIS and components meet the SIL verification assumptions?	☐ Yes	☐ No	☐ N/A
2.	If a component fails under test, is the failure cause established to identify manufacturing or design defects?	☐ Yes	☐ No	☐ N/A
3.	If a redundant element fails, do procedures require the inspection of other elements for similar faults?	☐ Yes	☐ No	☐ N/A
4.	Is there adequate independence of testing methods for diverse systems?	☐ Yes	☐ No	☐ N/A

Maintenance

1.	Are maintenance bypasses alarmed to the control room?	☐ Yes	☐ No	☐ N/A
2.	Are operators trained on what to monitor when maintenance bypasses are used?	☐ Yes	☐ No	☐ N/A