TS

NOT MEASUREMENT SENSITIVE

DOE-STD-1195-2011
April 2011

DOE STANDARD

DESIGN OF SAFETY SIGNIFICANT SAFETY INSTRUMENTED SYSTEMS USED AT DOE NONREACTOR NUCLEAR FACILITIES

U.S. Department of Energy
Washington, D.C. 20585

AREA SAFT

FOREWORD

Safety instrumented systems (SIS) that include both analog and digital control systems are widely used in many industries, including in commercial nuclear power plants, for safety-related applications. SISs are also used in the U.S. Department of Energy's (DOE) nonreactor nuclear facilities for various safety controls, including safety class (SC) and safety significant (SS) controls. Although use of the SIS technology and, more specifically, computer-based digital controls, can improve performance and safety, it can also introduce complexities, such as failure modes, that are not readily detectable.

DOE requirements and guidance for structures, systems, and components used in SC and SS applications are contained in the following DOE Orders: DOE O 420.1B, Chg 1, *Facility Safety*, along with its associated guide, DOE G 420.1-1, *Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria Guide for Use with DOE 420.1, Facility Safety*; and DOE O 414.1C, *Quality Assurance*. This standard focuses on SISs utilized in SS applications and illustrates how a widely-used process industry standard, American National Standards Institute /International Society of Automation (ANSI/ISA) 84.00.01-2004, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector,* can be utilized to support reliable designs. SISs utilized in SC applications are designed in accordance with nuclear industry standards with additional guidance provided in DOE G 420.1-1. Beneficial comments (recommendations, additions, deletions) and any pertinent data that may improve this document shall be sent to:

U.S. Department of Energy
Office of Nuclear Safety Policy and Assistance (HS-21)
1000 Independence Avenue SW
Washington, DC 20585.

DOE technical standards, such as this, do not establish requirements. However, all or part of the provisions within this DOE technical standard shall be implemented under the following circumstances:

- The provisions are explicitly stated to be requirements in a DOE requirements document; or

- The organization makes a commitment to meet a standard 1) in a contract, or 2) in an implementation plan or program plan of a DOE requirements document.

Throughout this standard, the word "shall" is used to denote actions that must be performed if the objectives of this standard are to be met. If the provisions in this standard are made requirements through one of the two ways discussed above, then the "shall" statements become requirements. It is not appropriate to consider that "should" statements would automatically be converted to "shall" statements, as this action would violate the consensus process used to approve this standard.

Intentionally Blank

TABLE OF CONTENTS

1. INTRODUCTION

This standard provides requirements and guidance for the design, procurement, installation, testing, maintenance, operation, and quality assurance of safety instrumented systems (SIS) that may be used at Department of Energy (DOE) nonreactor nuclear facilities for safety significant (SS) functions.

The focus of this standard is on how the process industry standard, American National Standards Institute/International Society of Automation (ANSI/ISA) 84.00.01-2004, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector,* can be utilized to support design of reliable SS SISs.

1.1 Scope

This standard covers SS SISs that contain analog or digital components. Those analog or digital components include: switches, electrical relays, analog transmitters, computer-based systems consisting of embedded hardware and software components (such as programmable logic controllers, smart transmitters with built-in logic functions, and microprocessor-based monitoring systems), and final control devices. In essence, an SIS is composed of any combination of sensors, logic solvers, and final elements.

This standard is not intended to be used as the sole source of information to develop design requirements for specific applications. Other requirements and specifications, such as those found in DOE Order (O) 420.1B, Chg 1, *Facility Safety*, and DOE O 414.1C, *Quality Assurance* (and their associated guides) should also be consulted, as appropriate. In addition, recognized national and international standards, as well as the Nuclear Regulatory Commission's regulatory guides, should also be consulted, as appropriate.

This standard uses a set of hazard controls identified in a nuclear facility's documented safety analysis (DSA) to support identification of SIS reliability targets. The standard is not to be used to evaluate the adequacy of the set of hazard controls established in the DSA.

1.2 Applicability

This standard is applicable to SS SISs identified in the safety basis documents (Conceptual Safety Design Report [CSDR], Preliminary Safety Design Report [PSDR], and Preliminary Documented Safety Analysis [PDSA]) for new nonreactor nuclear facilities and for major modifications as defined in 10 CFR Part 830.3, *Nuclear Safety Management, Definitions*, for existing Hazard Category 1, 2 and 3 nonreactor nuclear facilities.

This standard is not applicable to safety class (SC) SISs.

This standard may also be useful to support design of SISs for facilities other than Hazard Category 1, 2 and 3 nonreactor nuclear facilities.

1.3 Background

SISs are widely used in many process industries and commercial nuclear power plants for safety-related functions. SISs are also used in DOE nonreactor nuclear facilities for various safety controls such as safety interlocks and process alarms.

Some SISs utilize programmable electronic technology (i.e., computer-based control systems), which has the capability of improving performance and safety, but also introduces complexity in failure modes that are not as readily predicted or understood, and may cause common mode failures that are difficult to detect. A primary concern is that a design that uses the same or shared hardware, software (including embedded software), and data may be susceptible to a common-cause or common-mode failure due to software errors, hardware failures, or combinations thereof, thus defeating the defense-in-depth/layer-of-protection concept implemented in the design. In addition, DOE did not have a standard method for determining the safety integrity level (SIL) for SISs that would account for defense-in-depth/layer-of protection concept in the design.

SS structures, systems, and components (SSC), whose preventive or mitigative function is a major contributor to defense-in-depth and/or worker safety as determined by safety analyses, should be designed to ensure that failures in one layer will not propagate to or affect other protection layers. This standard for SS SISs emphasizes quality, independence, and SIS reliability as protection against common-cause failures within and between protection layers. Equally important in preventing the propagation of common-cause failures is the application of sound software quality assurance practices throughout the software life cycle to ensure reliable software.

DOE has evaluated the chemical industry's approaches and practices, and this standard was developed using (ANSI/ISA) 84.00.01-2004.

1.4 Contents of Standard

Section 2 provides requirements for SISs, with Section 2.1 providing general requirements and identifying two industry standards options for SIS design, and Sections 2.2 through 2.9 identifying detailed requirements.

Appendices A through I provide the following guidance or requirements related to ANSI/ISA 84.00.01-2004 implementation.

- Appendix A provides a general overview of ANSI/ISA 84.00.01-2004.
- Appendix B provides requirements of the approved method for the determination of SILs.
- Appendix C provides guidance on SIL verification.
- Appendix D provides an example of SIL determination and verification.
- Appendix E provides guidance for obtaining failure rate data.
- Appendix F provides guidance related to quality assurance for safety software used in SISs.
- Appendix G provides guidance on human factors engineering.
- Appendices H and I provide references, abbreviations, acronyms, and definitions.

1.5 Users

The users of this standard should include personnel from various organizations including project management, engineering and design, procurement, and operations and maintenance.

2. REQUIREMENTS AND IMPLEMENTATION GUIDANCE

2.1 General Requirements

General requirements for SSCs, including SISs, used in SC and SS applications are contained in DOE O 420.1B, Chg1, *Facility Safety*, with implementation guidance provided in the associated guide, DOE G 420.1-1, *Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria Guide for Use with DOE O 420.1, Facility Safety*.

Additionally, DOE-STD-1189, *Integration of Safety into the Design Process*, provides certain general requirements (e.g., seismic design). For SSCs associated with facilities/modifications under the purview of DOE G 420.1-1 and/or DOE-STD-1189 should be used, if required, and as applicable, for guidance on environmental and seismic qualification requirements.

DOE O 420.1B, Chg 1, Chapter I, states that the safety SSCs and safety software must be designed, commensurate with the importance of the safety functions performed, to perform their safety functions when called upon, and to meet the quality assurance program requirements of 10 CFR 830, Subpart A, *Quality Assurance Requirements,* and DOE O 414.1C or its successor directives, as applicable. That statement supports a graded approach to design and reliability of an SIS based on the importance of its safety function. Either of the following two approaches for an SS SIS design should be utilized.

Use of Commercial Nuclear Standards (Used for SC SISs)

To achieve the required reliability, the design can utilize industry standards developed for commercial nuclear power plant design for safety-related systems. These standards are listed in DOE G 420.1-1 for SC instrumentation and control systems. However, the listed standards include some design requirements that are unwarranted for the design of SS SISs used in DOE nonreactor nuclear facilities (e.g., the application of nuclear power industry standards call for single-failure-proof designs, when other options to achieve adequate reliability might be more appropriate and cost effective).

Use of Process Industry Standards

An appropriate alternative means for meeting the reliability requirements for SS SISs is to utilize the processes outlined in ANSI/ISA 84.00.01-2004 – Part 1, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements.* ANSI/ISA 84.00.01-2004 is used by the process industries for designing reliable SISs that are commensurate with the level of hazard mitigation or prevention strategy.

Appendices A, C, and D of this standard provide specific information on the use of ANSI/ISA 84.00.01-2004, whereas Appendix B provides an approved method for SIL determination. Appendices E through G provide additional information to support the design process. To support implementation of ISA 84.00.01-2004, DOE Order requirements and practices for

performing hazards analysis, selection of hazard controls, quality assurance, qualification of personnel, testing and maintenance shall be used.

2.2 Quality Assurance for Safety Software used in SISs

2.2.1 Introduction

This section provides guidance on an approach to meet the objectives of ISA 84.00.01-2004, Part 1, Clause 12, *Requirements for application software, including selection criteria for utility software*, for achieving an acceptable level of assurance that SS SIS components that use software will execute the required safety functions within the system/application and operational environment. This section draws on the requirements of DOE O 414.1C and guidance provided in DOE G 414.1-4, *Safety Software Guide for use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance*.

2.2.2 Background

Three major types of software are used in SISs:

- Embedded software (normally provided by a vendor of programmable electronic systems);
- Utility software (i.e., software supplied by a vendor that is used to develop and verify application software); and
- Application software developed for the specified safety functions (normally the responsibility of the end-user or process system designers for the SIS).

An SS SIS may have any combination of software stated above. Each programmable electronic system (e.g., the logic solver), may have hardware and software components that can be divided into embedded software and application software.

2.2.3 Requirements and Guidance

Quality assurance (QA) requirements for software development shall be controlled in accordance with the contractor's QA process, which shall meet the DOE's QA requirements (10 CFR 830, Subpart A and DOE O 414.1C, as appropriate).

Appendix F provides relevant details for software quality assurance activities, as discussed in DOE G 414.1-4 and in ANSI/ISA 84.00.01-2004 and other industry practices.

2.3 Commercial Grade Dedication

2.3.1 Introduction

Commercial Grade Dedication (CGD) may be used to approve the selection of components and subsystems in an SIS in lieu of the ANSI/ISA 84.00.01-2004, Part 1, Clause 11.5, methodology of acceptance by qualification to IEC 61508, *Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-Related Systems* and/or "prior use."

ASME Nuclear Quality Assurance (NQA)-1, *Quality Assurance Requirements for Nuclear Facility Applications,* provides details of the CGD process. The goal of CGD is to provide a

reasonable assurance that an item procured will perform its intended safety function, as specified by design requirements.

2.3.2 Critical Characteristics for Commercial Grade Dedication:

The following critical characteristics, as appropriate, should be addressed when assessing the acceptability of an SIS that utilizes software for meeting the design attributes.

a. Failure rate of an item such as:
   - unsafe/dangerous failure rate (detected and undetected); or,
   - safe failure rate (spurious trip rate)
b. Safe failure state, and safe recovery
c. Environmental design constraints
d. Software critical characteristics (e.g., build date, release name, part or catalog number, traceability matrix, etc.)
e. Diagnostic coverage
f. Response time
g. Accuracy
h. Isolation capability of component/system from non-safety interfaces (i.e., communication inputs and outputs)
i. Unused and unintended or prohibited functions
j. Supplier catalog and part number
k. Supplier technical manual and product specification
l. Conformance to national codes and standards

The above list is not all inclusive. Users should develop the list for specific SS SIS design requirements.

2.4 Setpoint Development

SS SIS setpoint development, including indications and alarms, shall follow the requirements of ANSI/ISA 67.04.01, *Setpoints for Nuclear Safety-Related Instrumentation.*

2.5 Power

Power sources (i.e., electric power or instrument air) shall be provided with backup power sufficient to fulfill the requirements of the SIS safety function, except in cases where the design is fail-safe on loss of power.

2.6 SIS Life-Cycle Management Process

A key aspect of the implementation of ANSI/ISA 84.00.01-2004 is effective control over each stage of the SIS life cycle to ensure proper initial design, proper installation, effective operation

and maintenance, and configuration control. The processes for performing the life-cycle management for SIS should be defined, including identifying the organization(s) responsible for implementing them. Appendix A provides additional details on the SIS life-cycle process. The life-cycle stages outlined in ANSI/ISA 84.00.01-2004 can be fulfilled by conformance to the ANSI/ISA 84.00.01-2004 requirements or by conformance to DOE orders, manuals, standards, and guides that provide equivalent processes and methods for the life-cycle stages of the safety instrumented functions.

2.7 Human Factors Engineering

ANSI/ISA 84.00.01-2004, Part I, Clause 11.2.6 requires that the design of SIS take into account human-machine interfaces and their limitations, and follow good human factors engineering (HFE) practices. HFE involves diverse areas (e.g., information display, user-system interaction, alarm management, operator response, control room design, and system maintainability), which affect all aspects of a system's development and modification. Appendix G gives an overview of how HFE should apply in the SIS life cycle. An HFE Plan should be developed for the SS SIS, defining the required participants and human factors activities, including the documentation, review, and approval of each activity.

Details of the HFE Plan should be developed in accordance with DOE G 420.1-1, guided or supplemented by information in NUREG 0700, *Human-System Interface Design Review Guidelines*, ANSI/ISA 18.2, *Management of Alarm Systems for the Process Industries*, and other HFE references given in Table G-1.

The HFE process should follow applicable requirements of DOE O 414.1C for software and hardware configuration controls.

2.8 Security

This standard does not provide details of security requirements for SIS design. The SS SISs shall be secured from electronic vulnerabilities, including unauthorized and/or inappropriate access that may harm system integrity and safety.

The SS SIS design development process should address the potential security vulnerabilities in each phase of the system life cycle, and the requirements should be commensurate with risk and magnitude of harm resulting from unauthorized and inappropriate access, use, disclosure, disruption, or destruction of the system.

ANSI/ISA 84.00.01-2004, Clause 11.7.2.2, provides some basic access security protection measures. Users should consult applicable DOE requirements and other industry standards to ensure the design meets the security requirements.

2.9 Instrumented System Applications not Covered by ANSI/ISA 84.00.01-2004

ANSI/ISA 84.00.01-2004, Part 1, design methodology should not be used for instrumented systems in the following applications because they are more appropriately covered by other industry standards such as National Fire Protection Association (NFPA) standards and American Nuclear Society 8.3, Criticality Accident Alarm Systems. Users should judge whether the SS SISs are more appropriately covered by any other industry standards. DOE G 420.1-1 identifies the standards that would be applied to systems such as:

a. Evacuation alarms (e.g., nuclear incident monitors, fire alarms, and public address systems);

b. Fire protection/detection systems (covered by NFPA standards); and

c. Support systems (e.g., electrical power systems, instrument air systems).

APPENDIX A. OVERVIEW OF ANSI/ISA 84.00.01-2004

A.1 Purpose

This appendix provides an overview of American National Standards Institute/International Society of Automation (ANSI/ISA) 84.00.01-2004, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*. It describes a life-cycle approach that is useful in the implementation of this process industry standard at the Department of Energy (DOE).

A.2 Background

Several national and international bodies have developed and published standards and guidelines to enable application of Electrical/Electronic/Programmable Electronic Systems technology in safety systems. Efforts are continuing to further the understanding of the safety application concepts, improve the standards and guidelines, and be responsive to new process needs and technology developments. Examples of standards that are currently published and widely used by the process industries for safety applications are listed below.

ANSI/ISA 84.00.01-2004, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector* - Parts 1, 2, and 3 and the Technical reports in the ISA TR84.00.xx series.

International Electrotechnical Commission 61511, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector* - Parts 1, 2, and 3. IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.* (This standard is primarily applicable to vendor-manufactured products.)

The ANSI/ISA 84.00.01-2004 approach provides coverage of the safety system full life cycle to account for the many deficiencies identified in the evaluations of past industry methods and approaches.

A.3 ANSI/ISA 84.00.01-2004 Life-Cycle Approach

The elements in the life cycle are hazards identification, safety requirements specification, design, installation, startup testing, management of change, operational testing, maintenance, operation, modification, and decommissioning of safety instrumented systems (SIS). The life cycle also includes retention of the original documentation, including design criteria, procurement specification, commercial grade dedication files, and other relevant information for the life of the affected systems. Management of changes is applied in all steps of the life cycle. This life-cycle approach is directed toward reducing the risks inherent in process facility operations. The ANSI/ISA 84.00.01-2004 approach can be summarized into five steps as depicted in Figure A.3-1: Life-Cycle Steps for Safety Instrumented Systems.

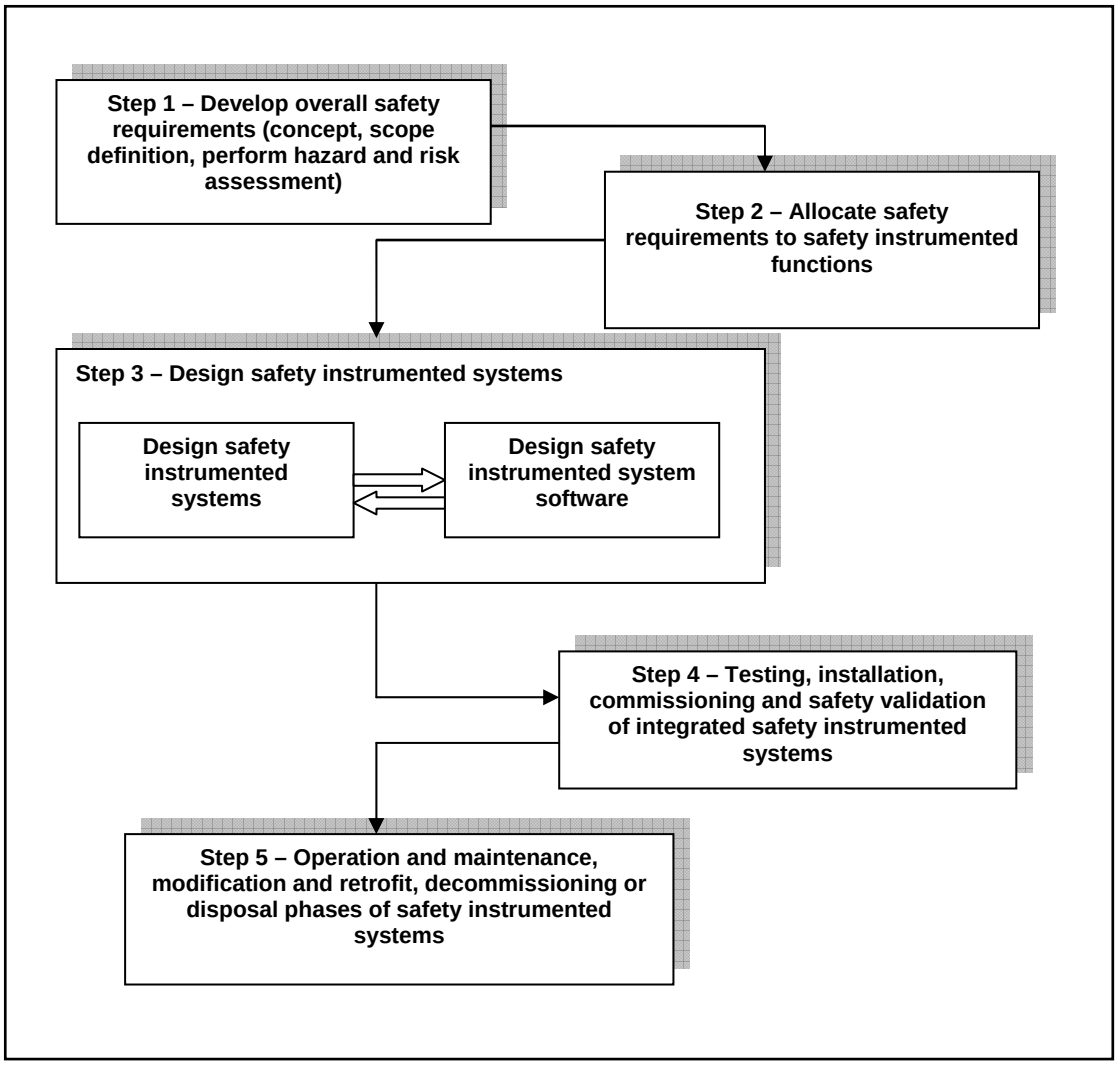

Figure A.3-1: Life-Cycle Steps for Safety Instrumented Systems

Step 1: Develop overall safety requirements

This initial phase focuses on how much risk reduction will be required throughout the life cycle of the SIS. Some level of residual risk will always exist. The purpose of any safety system is to reduce the identified risk to an acceptable level as defined in the safety basis documentation.

Following the establishment of the conceptual requirements and scope definition, ANSI/ISA 84.00.01-2004 begins with a requirement to perform a hazard analysis, identification of hazards and associated risks. The safety functions that are required to reduce the identified risks to an acceptable level are determined during this phase. (See Appendix B for application at DOE facilities.)

Step 2: Allocate safety requirements to safety instrumented functions

Acceptable risk is achieved by allocating safety requirements to various safety functions. The safety functions are then allocated to different systems, such as safety class/safety significant (SC/SS) mechanical or process systems, design features, SC or SS SISs, and other external hazard controls. When a safety function is allocated to an SIS, it is called a safety instrumented function (SIF). The allocation process also includes assigning a safety integrity level (SIL) to the SS SIF, which corresponds to the amount of risk reduction determined to be necessary in the hazard and risk analysis.

SILs can be expressed as either risk reduction factors (RRF) or as a probability of failure on demand-average (PFDavg). SILs have four discrete performance ranges and two kinds of controls; namely, those that respond "on demand" and those for "continuous demand." The SIL is related to the average probability of the SIS failing when demanded to perform its safety function. In either case, ANSI/ISA 84.00.01-2004 applies. Since the majority of DOE safety controls are of the "on demand" mode of operation, this is the focus of this standard. The SIL performance requirements in terms of the PFDavg and RRF are listed in Table A.3-1: SIL Level and Performance Ranges for On-Demand Mode below.

Table A.3-1: SIL Level and Performance Ranges for On-Demand Mode

SIL Level Designation	Probability of Failure On Demand-average (PFDavg)	Risk Reduction Factor (RRF)
SIL-1	$< 10^{-1}$ to $\geq 10^{-2}$ PFDavg	> 10 to ≤ 100 RRF
SIL-2	$< 10^{-2}$ to $\geq 10^{-3}$ PFDavg	> 100 to ≤ 1000 RRF
SIL-3	$< 10^{-3}$ to $\geq 10^{-4}$ PFDavg	> 1000 to ≤ 10,000 RRF
SIL-4	$< 10^{-4}$ to $\geq 10^{-5}$ PFDavg	> 10,000 to ≤ 100,000 RRF

SIL-1 represents the lowest risk-reduction level of performance; SIL-4 represents the highest risk-reduction level of performance. SIL-4 is not used in the process industry sector because it requires elaborate systems and is difficult to support because of the high level of reliability required of the hardware. SIL-4 systems are not expected to be used for SS controls in DOE facilities.

A number of methods (qualitative and quantitative) are available for assigning the SIL. Qualitative methods may be appropriate when the risk, implementing design, and the hardware are not well understood. Quantitative methods, such as fault tree or event tree analysis, should be used when the design and hardware are well understood and supporting data are available. Quantitative methods are required for verification that the final design and its installation meet the assigned SIL. Assigning the SIL links the design integrity of the SIS to the required level of risk reduction, and thereby closes the gap between the hazard analysis and safe process operation.

ANSI/ISA 84.00.01-2004 provides several methods for determining SIL, such as Layer of Protection Analysis, which uses frequency of the event as a basis, or Safety Layer Matrix, which uses available information of independent protection layers (IPLs) as a basis for selection of SIL for the SIS. For DOE's application, the accepted methodology is a deterministic method using the number of IPLs credited by hazard analysis (per DOE-STD-3009, *Preparation Guide for*

U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analysis and DOE-STD-1189, *Integration of Safety Into the Design Process*). The DOE deterministic methodology is discussed in Appendix B.

Step 3: Design the SIS and safety software

The SIL establishes a minimum required performance for the SIS, as measured by the PFDavg or RRF. The factors that affect the PFDavg or RRF are:

a. Component failure rate;
b. Redundancy/diversity of systems and components;
c. Voting (e.g., one-out-of-two or two-out-of-four logic);
d. Testing frequency;
e. Diagnostic coverage (e.g., on-line testing, monitoring of component and system performance, and monitoring of various failure modes);
f. Common cause failure (e.g., design, human factors, manufacturing, and software);
g. Human factors;
h. Technology (e.g., digital vs. analog); and
i. Software integrity (e.g., diversity, failure detection by on-line monitoring, etc.).

The user should design the SIS with hardware and software components considering the above factors to achieve the PFDavg or RRF related to the target SIL. The target SIL is an objective of design process decisions, component specification and procurement to ensure that the design is consistent with the target SIL. The design is verified at the end of the detailed design process to ensure that the design as installed and tested can achieve the assigned PFDavg or RRF.

Step 4: Testing, installation, commissioning, and safety validation of SIS

Testing is performed throughout the installation stages to enable validation and verification that SIS requirements are met. This phase of the life cycle addresses the policy that will be applied for the following:

a. Integration of software and hardware;
b. Types of testing to be performed and data required to demonstrate functional adequacy and acceptance;
c. Environment necessary for conducting testing along with the configuration that exists for testing;
d. Test criteria for which data will be collected and used to judge acceptability;
e. Physical locations (factory or site) for which the test will be performed;
f. Personnel requirements and qualifications required for performing the various activities related to the validation and verification functions; and
g. Process for documenting and dispositioning non-conformances.

In Step 4, the SIS design is validated in its “as installed” configuration as achieving its assigned SIL.

Step 5: Operation and maintenance, modification and retrofit, decommissioning or disposal phases of SISs

Long-term preservation of an SIS through startup, operation, maintenance, and management of change activities is as important as initial design and installation phases. The SIL is not just a design parameter; it is also an operational parameter. The selection made during conceptual or preliminary design phases, including design configuration, testing frequency, and so on, is maintained throughout the life of the facility. Therefore, it is essential that management of system change be maintained to ensure preservation of the SIS.

APPENDIX B. SAFETY INTEGRITY LEVEL DETERMINATION METHODOLOGY

B.1 Purpose

This appendix establishes a method for determining the appropriate safety integrity level (SIL) for safety significant (SS) safety instrumented function (SIF) for DOE nonreactor nuclear facilities. The target SIL provides design input to an SS safety instrumented system (SIS) that is credited with reducing the risk of a hazardous event by itself or in combination with other features to an acceptable level, as defined in the safety basis documentation. The SIL determination methodology defined in this appendix shall not be used as an input or requirement to hazard/safety analysis, classification of Safety, Systems, and Components (SSC) as safety class (SC) or SS, or crediting of SSCs, specific administrative controls (SAC), or administrative controls (AC) to prevent or mitigate hazardous conditions.

ANSI/ISA 84.00.01-2004, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector,* leaves it up to the user to determine the level of performance (i.e., SIL) that is needed to achieve the user's process safety objectives. There are a number of recognized methods, which include, but are not limited to, deterministic, Layers of Protection Analysis, and Safety Layer Matrix (SLM). A deterministic methodology (a modified SLM methodology), is the approved method for applying the ANSI/ISA 84.00.01-2004 approach in this standard. The basis for this modified SLM methodology is that the safety classifications of SSCs are based on documented safety analyses (DSAs), and, therefore, likelihoods and consequences do not have any further role in SIL determination.

B.2 SIL Determination and Independent Protection Layers

The SIL Determination Methodology (Figure B.2-1) is a qualitative approach to determine the SIL of the last SS SIS credited with preventing or mitigating a hazardous event by assessing the total number of Independent Protection Layers (IPLs) credited with protecting the worker or public from this event.

Figure B.2-1 is used solely to determine the SIL of an SS SIS after it has been classified as SS. It is not to be used to determine whether an SSC is classified as SC or SS and should not be used to determine the required number of IPLs.

Number of IPLs		
	3	SIL-1
	2	SIL-2 (1)(2)
	1	SIL-2 (1)(2)

Figure B.2-1: SIL Determination Methodology

Note 1: When an event may result in a prompt public fatality or multiple prompt collocated worker fatalities (due to chemical releases; see Appendix B of

DOE-STD-1189, *Integration of Safety Into the Design Process*), the design authority should consider increasing the SIL number of the SIS by one or credit an additional IPL.

Note 2: When an event (non-criticality) is not expected to result in a facility worker or collocated worker prompt fatality or serious injuries or significant radiological or chemical exposures (see Appendices B and C of DOE-STD-1189), the design authority may consider decreasing the SIL number of the SIS to SIL-1.

IPLs shall meet the following general requirements:

- The IPL shall be designed to prevent an event or to mitigate the consequences of an event to a level that is supported by safety basis documents;
- The IPL safety function shall be identified and documented in the safety basis documents of a facility;
- The IPL shall be designed to perform its safety function during normal, abnormal, and design basis accident environmental conditions for which it is required to function; and
- The IPL shall be sufficiently independent so that the failure of one IPL, or of a component or subsystem of an IPL, does not adversely affect the probability of failure of another IPL credited for the same event.

An IPL shall be independent from the initiating cause of the SS event. A process system (e.g., ventilation, cooling water) that is not functionally classified as SS or SC should only be identified as an IPL if its functions are implemented for the purposes of risk reduction, and if its components and the basic process control system (BPCS) are independent from the initiating event. This IPL should be maintained in a maintenance/surveillance program and should have a limiting condition of operation (LCO).

If some combination of components or systems is required to function together to protect a worker or the public, they shall be considered as one IPL. Thus, if two out of three components are needed to complete the SS function of a series of components that must function together to protect a worker, then the combination of components shall constitute one IPL.

Selection of IPLs and the justification for SIL determination for an SS SIS shall be documented in the DSA.

B.2.1 Independent Protection Layer Identification

The identification of IPLs by the hazard analysis is used as input to SIL determination. As shown in Figure B.2-1, the number of IPLs credited for a hazardous event will determine the SIL of an SIS. Safety functions, controls, and programs that can be credited as IPLs are as follows:

- **Credited passive safety design features:** Each passive safety design feature may be credited as two IPLs if it is controlled under a documented configuration management program and subject to periodic surveillance, if required, that confirms and documents that the SSC will perform its intended safety function.

- **Specific administrative control (SAC):** SACs that can be directly credited with preventing or mitigating an event to a level as defined in the safety basis documentation. Only one SAC shall be credited in the SIL determination for a specific hazardous event.

- **Administrative control programs (AC):** AC programs should be credited in the SIL determination only for the protection of in-facility workers or for protection against criticality accidents. The AC shall be identified in the Technical Safety Requirements as being important to risk reduction for specific accidents. Only one AC shall be credited in the SIL determination for a specific hazardous event.

- **Safety Significant systems:** Process systems classified as SS (e.g., ventilation systems, cooling systems) can be credited when they provide protection against the same set of hazards/accidents as the SIS being evaluated. They may be credited as two IPLs if a calculation of their safety unavailability in terms of the average probability of failure on demand (PFDavg) is less than 10^{-2} or the RRF is greater than 100.

- **Safety Class systems:** An SC system that is credited with providing protection against the same set of hazards/accidents as the SIS being evaluated may be credited as two IPLs. An associated defense-in-depth SS control for an SC control may be credited as a separate IPL if it is independent of the SC system.

- **The SIS whose SIL is being determined:** An SIS whose SIL is being determined is also credited as an IPL.

B.2.2 Application of the SIL Determination Methodology

This section describes how the SIL Determination Methodology shown in Figure B.2-1 can be used to determine the SIL for an SIS for protection from an event impacting a collocated worker.

If only two IPLs are credited in the hazard analysis for this event, and one of them is a SS SIS, the SS SIS target SIL is SIL-2. If three or more IPLs are credited for this scenario, the SS SIS would have a target SIL of SIL-1.

In a situation in which two SS SISs are credited with preventing or mitigating the same event, one of the SS SISs may be assigned as SIL-1. The second SS SIS shall have its SIL determined by Figure B.2-1. Both SS SISs can be credited if they meet the requirements listed in Sections B.2 and B.2.1.

If an instrumented system has been classified as SS during the hazard analysis and functional classification process, then, regardless of the number of IPLs credited, it shall have a target SIL of no less than SIL-1. The SIL determination methodology shall not be used by itself to reduce the classification of an SS SIS to non-safety significant. A more detailed example utilizing a specific SIS is provided in Appendix D.

APPENDIX C. SAFETY INTEGRITY LEVEL VERIFICATION GUIDANCE

C.1 Purpose

This appendix provides guidance on safety integrity level (SIL) verification calculations that are required in Section 11.9.1 of ANSI/ISA 84.00.01-2004, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*. In particular, this appendix provides additional clarification and information for some calculation techniques that are not addressed in ISA TR84.00.02, *Safety Instrumented Functions (SIF) — Safety Integrity Level (SIL) Evaluation Techniques.*

C.2 SIL Verification Calculation Content

The SIL verification calculation should include details on input data, the safety significant (SS) SIF, and the SS safety instrumented system (SIS) description that should be met. The information described below for SIL verification calculations is necessary for developing or reviewing the calculation, as well as for adequate understanding of the SS SIS and the risk reduction that it provides.

C.2.1 Input Data

1. The source of failure rate data and the periodic surveillance and test frequencies for components of the SS SIS should be documented.

2. Where facility documents, such as a Technical Safety Requirements (TSR) or Documented Safety Analysis/safety basis documents, allow a grace period (e.g., test frequencies may be extended up to 25 percent without prior approval) for calibration and test frequencies, this grace period should be added to the test/calibration frequencies to prevent unanalyzed conditions.

3. Input data, such as periodic test frequencies and trip setpoints, should be in the safety basis documents.

4. Components that are certified for process safety under the International Electrotechnical Commission (IEC) 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems,* are supplied with a vendor safety manual. The vendor safety manual should be referenced. The vendor safety manual may list restrictions on the operating conditions and configuration of components in order to achieve a specific average probability of failure on demand (PFDavg) or SIL compliance. The vendor safety manual should be reviewed in its entirety to ensure that a component can be used in the selected design configuration and environment to achieve the target SIL.

5. The failure modes on loss of motive force should be documented for each of the SS SIS components.

6. When support systems (e.g., electrical power, instrument air) are required to complete the SS SIS, their availability should be determined so that it can be included in the verification calculation.

7. Operator errors should be included in the SIL verification calculation when an operator action is required to respond to an alarm or indication to accomplish the SS SIF. To credit operator action either the alarm/indication should be in (1) a continuously-manned control room, or (2) a remote area that has a mandated periodic surveillance. The source of operator error data should be documented.

8. Components that do not have an assigned test or calibration frequency, but the availability of which contributes to the overall functionality of the SS SIS, should be assigned a test interval equivalent to the "mission time" of the process. The mission time is the life of the process being performed or the period of time that a component will be in service before it is replaced.

C.2.2 SS SIF Description

A complete description of the SS SIF addressed should be included in the SIL verification calculation. The description should include the required SIL for the function, and the required modes of operation for the SS SIF.

A description of any manual (operator) actions that are required to complete the safety function should be identified. The performance requirements for the SS SIF (e.g., response times, maximum valve leakage) should be identified. The required operating range and analytical safety limit of the SS SIF should be identified. References to the safety documents that describe the SS function and its performance requirements should be provided.

C.2.3 SS SIS Components Identification

All of the SS components (e.g., sensors, logic solvers, final control elements) of the system, a description of their safety functions in the system, and a sketch and/or reference drawing(s) (e.g., piping and instrumentation diagram, schematic, loop diagram, logic diagram, or description) for the system should be identified. A description of SS SIS interfaces from/to support systems and non-safety operator information systems should also be included.

C.3. SIL Verification Calculation Guidance

The ISA technical report, ISA TR84.00.02, provides guidance on SIL verification calculations. A SIL verification calculation for a SS SIF is normally performed using simplified equations (ref. ISA TR84.00.02-2002 – Part 2) or fault tree analysis (ref. ISA TR84.00.02-2002 – Part 3).

C.3.1 Common Cause Failure

Common Cause Failures (CCF) can be either safe detected or undetected, or dangerous detected or undetected. The SIL verification calculation is concerned only with dangerous undetected failures. CCFs are influenced by physical and electrical separation, diversity, and the robustness of design of the component (ability to withstand environmental stressors). ANSI/ISA 84.00.01-2004 uses the beta factor method to model common cause failures (see ISA TR84.00.02) in a single SS SIS with redundant components. The beta factor normally falls within the range of 0 to 10 percent. When good engineering design is followed, the beta factor will generally fall within the range of 0 to 5 percent (Ref. ISA TR84.00.04 –Part 1).

When physical and electrical separation is provided consistent with the intent of IEEE 384, *Standard Criteria for Independence of Class 1E Equipment and Circuits*, for two or more diverse

SS SISs that are IPLs for a specific hazardous event, they may be considered as independent, and the addition of a CCF factor into the SIL verification calculation is not recommended.

A CCF factor should be included in the SIL verification calculation of an SS SIS when it is credited with another SS SIS IPL to reduce the risk of a specific hazardous event to a level defined in the safety basis documentation, and the SS SISs have identical or similarly functioning components in any of the subparts of the systems (i.e., sensors, logic solvers, final control elements), and when physical and electrical separation between SS SIS IPLs is not maintained.

For example, if both SS SISs for a hazard event use identical valves as the final control element to shut off flow, then a beta factor times the PFDavg of the valve should be added to the final PFDavg value in at least one of the SS SIS SIL verification calculations. If an individual SS SIS has redundant architecture within a subpart (e.g., 1oo2 valves or 2oo3 sensors) and has included a beta factor to address this architecture, then no additional beta factor is recommended for using identical components in similar SS SIS IPLs for a specific event because a beta factor is already addressed in the SS SIS SIL verification calculation of one of the IPLs.

The following CCF term should be added to the total PFDavg of the SIL verification calculation for each component/subsystem that is identical between two or more SS SISs credited for a single hazard.

$$CCF = \beta \times \lambda \times (TI/2)$$

β is the fraction of failures that impact more than one component/subsystem in a redundant configuration.

λ is the undetected dangerous failure rate of the component/subsystem.

TI is the time interval between functional tests of the component/subsystem.

C.3.2 Systematic Failure

Systematic failures (e.g., human design errors, software failures, programmatic failures) are generally not to be included in the verification calculation if they are adequately addressed by procedures. For example, if software development meets the intent of ANSI/ISA 84.00.01-2004, Part 1, Section 12, then software failures should not be included in the SIL verification calculation.

C.3.3 Converting Per Demand Failures into Failure Rate

Some mechanical components (valves/relays) have their failure described as “failures/demand” versus a failure rate (λ) “failures/hour.” This failure/demand value may be used in the fault tree or simplified equation as the PFDavg for that component. When it is desired to take credit for the periodic testing of these components, the failure/demand can be converted to a failure rate. The conversion from failure data given in failures/demand to a failure rate should only be done for hardware failures. Human failure rates given in failures/demand cannot be converted into failures/hour.

A conversion example using a hardware failure of 5.0 E-03/demand for an anticipated hazard is shown below. The demand rate in this equation is the quantitative or qualitative value for the frequency of the hazard. When the hazard frequency has been qualitatively defined as "Anticipated," "Unlikely," or "Extremely Unlikely," the calculation should use a demand rate of once per year. Conversion from a per demand value to a failure rate (λ) is not recommended when the hazard rate is less than once per year.

$$\lambda = \text{PFD} \times \text{Demand Rate}$$

$$\lambda = \text{failure/demand} \times \text{demand/hours}$$

$$\lambda = (5.00\text{E-}03/\text{demand}) \times (\text{demand}/8760 \text{ hours})$$

$$\lambda = 5.7 \text{ E-}07/\text{hour}$$

C.3.4 Dangerous Detected Failures

Dangerous detected failures should be managed. If a dangerous failure is detected either automatically (diagnostic alarm) or through periodic surveillance, some action should be taken to either: (1) restore the device to full operability within the allowed mean time to repair (MTTR); (2) place that device or system in a safe/tripped state; or, (3) provide compensatory measures. If none of the actions described above is taken, the dangerous detected failure should be treated as a dangerous undetected failure as far as the verification calculation is concerned.

C.4. Spurious Trips

ISA 84.00.01-2004 Part 1, Section 10.3.1, requires the identification of the maximum allowable spurious trip rate for a SIF. This value in terms of a spurious trip rate or mean time to fail spurious ($MTTF^{spurious}$) is a key design feature which establishes the required reliability of the SIF. A system that requires a high availability may require redundancy of field devices that are voted in a 1 out of 2 (1oo2) or 2oo3 configuration regardless of the SIL value. Evaluation techniques for $MTTF^{spurious}$ can be found in ISA TR84.00.02.

APPENDIX D. ILLUSTRATION OF A SAFETY INTEGRITY LEVEL DETERMINATION AND SAFETY INTEGRITY LEVEL VERIFICATION CALCULATION[1]

D.1 Purpose

This appendix is intended to provide an example of a safety significant (SS) safety instrumented system (SIS) and to show the activities appropriate to two stages in the safety life cycle: safety integrity level (SIL) determination and SIL verification calculation. The entire safety life cycle consists of all of the activities involved in the implementation of safety instrumented function (SIF), starting at project conception and ending with decommissioning. The example in this appendix illustrates the determination of an SIL based on the hazard analysis and SIF description. The example also includes the SIL verification calculation performed to confirm that the design, operation, and testing of the SS SIS meets the designated SIL.

Note: The design, SIL determination, and verification are for illustrative purposes only. The values (failure rates, test frequencies, beta factors) used in the SIL verification calculation were developed for this example only and are not to be construed as valid for any other calculation.

D.2 SIL Determination of an Example SS SIS

D.2.1 Hazard Description (Example)

The liquid aqueous waste solutions from separations processes are concentrated in batch evaporators. The solution is heated to the boiling point by condensing steam in the evaporator coils. The steam pressure in the coils is maintained between 14 psig and 24 psig at saturated conditions. In a typical batch process, the evaporator pot is filled with process waste solution to a predetermined level to cover the heating coils. The solution is heated to boiling. As the solution is heated, it begins to circulate through the evaporator pot draft tube from the bottom to the top. This flow is created by natural heat convection and engineering design. As the solution is boiled, the vapors flow upward to the condenser. Feed flow from the evaporator feed tank must be started at this time to maintain the evaporator pot liquid level. The formation of an organic layer above the aqueous layer is possible.

When tributyl phosphate (TBP) and nitric acid are mixed and heated, the TBP starts to decompose. Although a heat source is required to initiate the rapid initial reactions, at some point, the reaction generates enough heat and pressure to sustain the reaction without an external heat source. This is the autocatalytic or runaway reaction initiation temperature. In this example, a potential exists for an uncontrolled reaction between TBP and nitric acid that could result in a significant release of radioactive material.

A hazard analysis was performed that identified the need for SS control(s). The hazard is anticipated and has a consequence that exceeds evaluation guidelines to the collocated worker.

---

[1] Appendix D is included for information only. All the conditions presented are representative and may need modification to ensure their suitability to any specific application.

D.2.2 SS SIF Description (Example)

An interlock is provided to close the steam shutoff valve to the evaporator coils prior to reaching the autocatalytic temperature in the evaporator's liquid aqueous waste solution. The steam shutoff valve must close within (to be determined) seconds.

D.2.3 SIL Determination (Example)

The SIL determination is made by considering the type and number of independent protection layers (IPL) that are provided to prevent or mitigate the hazardous event in question. Appendix B of this standard provides details on the SIL determination methodology and how it is to be applied.

The following describes the IPLs selected for the evaporator used as the example.

Two IPLs were considered to prevent a TBP-nitric acid reaction. These IPLs either limit the temperature or prevent large accumulations of TBP in a single vessel. The methods used to implement these basic approaches include the following:

1. Limit the mass of TBP (organics) present, and

2. Prevent mixtures of TBP and nitric acid from reaching high temperature by controlling the heat sources.

The hazard analysis has determined that the event exceeds evaluation guidelines to collocated workers. SS controls are required to prevent the event. The following controls (IPLs) were selected:

IPL#1 — A specific administrative control (SAC) requires a periodic inspection (to be completed annually) of the feed tank for a continuous layer of organic. If a continuous layer of organic is detected, it shall be removed by flushing or skimming. This allows detection and removal of the organic to limit the mass of TBP present; and,

IPL#2 — A high temperature-steam flow interlock is credited as an SS feature to prevent exceeding the autocatalytic reaction temperature. Two IPLs are credited for this event: the SAC and the SS SIS temperature. With two IPLs credited, the SS SIS (temperature interlock) is required to be SIL-2 per the Figure D.2.3-1: SIL Determination Methodology shown below.

Number of IPLs	3	SIL-1
	2	SIL-2[(1)(2)]
	1	SIL-2[(1)(2)]

Figure D.2.3-1: SIL Determination Methodology

Note 1: When an event may result in a prompt public fatality, or multiple prompt collocated worker fatalities (due to chemical releases; see Appendix B of DOE-STD-1189, *Integration of Safety Into the Design Process*), the design authority should consider increasing the SIL number of the SIS by one or credit an additional IPL.

Note 2: When an event (non-criticality) is not expected to result in a facility worker or collocated worker prompt fatality, or serious injuries, or significant radiological or chemical exposures (see Appendices B and C of DOE-STD-1189), the design authority may consider decreasing the SIL number of the SIS to SIL-1.

D.2.3.1 SS SIS Description

The high temperature steam flow interlock for the batch evaporator (see Figure D.2.3.1-1: Evaporator Temperature Interlock) consists of sensors (two temperature elements/transmitters), logic solver (safety programmable logic controller [PLC]), and final control elements (solenoid and isolation valves). Temperature control is provided by temperature element, or TE-1, the Digital Control System (DCS), and the flow control valve (FCV). When a high temperature is sensed by one-out-of-two (1oo2) temperature devices (TE-2 and TE-3), the interlock prevents the evaporator from reaching the runaway initiation temperature. The temperature interlock will shut off the steam to the heating coils by deenergizing the solenoid valve (SV), thus closing the steam isolation valve (FV). The isolation valve has no leakage classification requirements. The shutoff capability of the isolation valve is tested periodically by verifying temperature drop after the valve is shut.

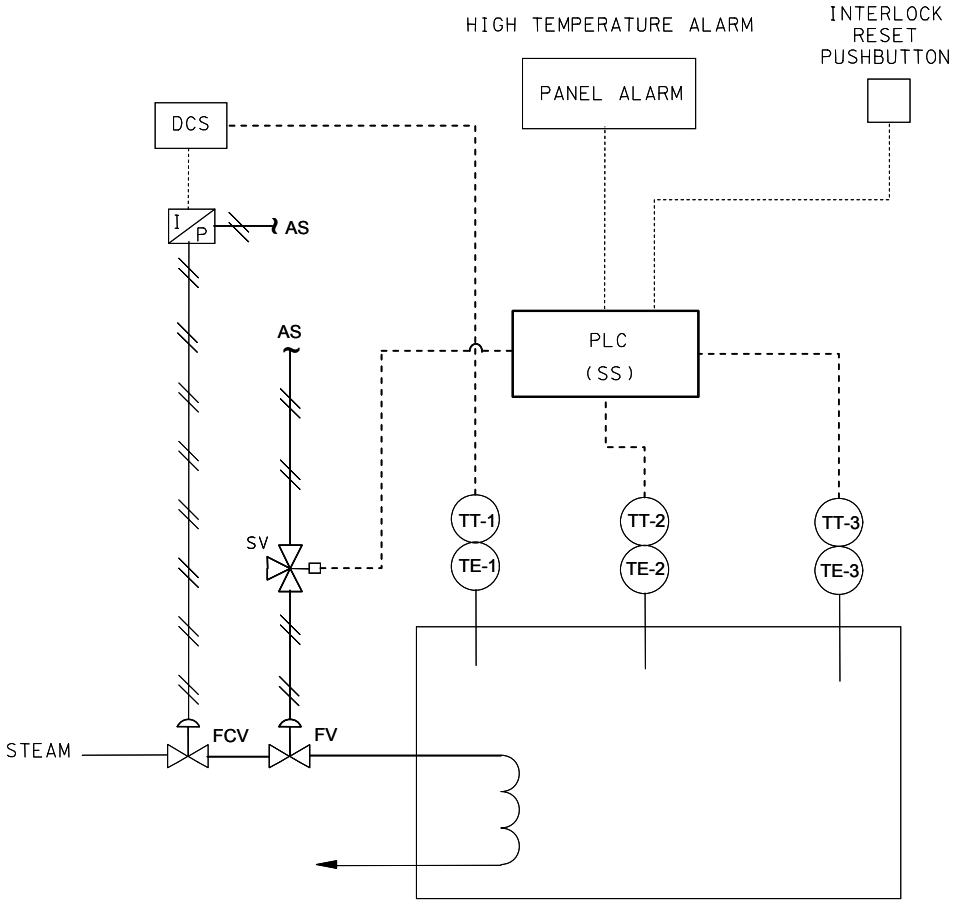

Figure D.2.3.1-1: Evaporator Temperature Interlock

The SV fails in the closed position (vents air from the FV on loss of signal or loss of instrument air) (fail safe). The FV closes on loss of instrument air (fail safe). SS temperature transmitters (TT-2 and TT-3) are reverse acting so that a low signal or loss of signal initiates the interlock. The PLC is programmed to detect a “hi-hi” signal or loss of signal from the temperature transmitters and initiate the temperature interlock.

Hardware Fault Tolerance

> An SIL-2 design requires a minimum hardware fault tolerance of 1 for sensors and final elements (See ANSI/ISA 84.00 -2004, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector* - Part 1, Section 11.4.4).

To meet this requirement for the sensors, the design employed redundant temperature elements (TE-2, TE-3) and temperature transmitters (TT-2, TT-3).

The SS PLC uses an internal triple modular redundant configuration. It is certified as SIL-3 compliant in a non-redundant configuration that exceeds the requirements for SIL-2 design.

The SV and the FV function together as the final element. The solenoid valve is certified as SIL-2 compliant in a non-redundant configuration. Based on “prior use,” and other attributes stated in ANSI/ISA 84.00.01-2004 – Part 1, Sections 11.4.4 and 11.5.3, the hardware fault

tolerance for the steam isolation valve was reduced to zero. Therefore, a single isolation valve is adequate for the SIL-2 design.

D.2.3.2 SIL Verification Calculation

The purpose of the SIL verification calculation is to demonstrate by analysis that the design of an SS SIS meets the integrity requirement specified by its SIL determination.

Technical Safety Requirements (TSR) allow a grace period for loop and calibration testing to be extended by 25 percent without an engineering review. To account for this allowance, all test frequencies (τ) will be multiplied by a factor of 1.25.

SENSOR (S) FAILURES

Resistance Temperature Element (RTD) Failure (TE-2, TE-3)

Failure data was obtained from the facility owner's database (λ = 1.0E-06/h). The temperature elements are replaced on an 18-month cycle when the thermowells are replaced due to corrosion concerns. The failure of an RTD would be corrected at the time the RTD is changed out (18 months). TSRs allow the change-out period to be extended by 25 percent without an engineering review.

τ = mission time or the periodic functional test period

τ = (1.5 yr) (8760 hours/yr) (1.25)

τ = 16,425 hours

$\mathbf{PFDavg_{(TE)}} = 0.5\lambda\tau$

$\mathbf{PFDavg_{(TE)}} = (0.5)(1.0E\text{-}06)(16{,}425) = 8.2E\text{-}03$

Temperature Transmitter Failure (TT-2, TT-3)

Failure data was provided by the vendor (λ = 9.8E-08/h). The test interval per TSR for the instrument loop test of the interlock is once every 90 days (2160 hrs) 2160 hrs x 1.25 = 2700 hours (τ = 2700 hours).

$\mathbf{PFDavg_{(TT)}} = 0.5\lambda\tau$

$\mathbf{PFDavg_{(TT)}} = (0.5)(9.8E\text{-}08)(2700) = 1.3E\text{-}04$

The PFDavg of the temperature element and transmitter series combination is calculated below:

$\mathbf{PFDavg_{(TE/TT)}} = PFDavg(TE) + PFDavg(TT)$

$\mathbf{PFDavg_{(TE/TT)}} = 8.2E\text{-}03 + 1.3E\text{-}04 = 8.3E\text{-}03$

Beta Factor

Since redundant temperature elements and temperature transmitters were used to meet the hardware fault tolerance requirement for a SIL-2 system, a beta factor was included. A very conservative beta factor of 10 percent was used in this example. A lesser beta factor would be justifiable based on environmental stressors and the physical and electrical separation provided by the design.

Sensor PFDavg(s)

The $\mathbf{PFDavg_{(S)}}$ equation for the TE/TT sensor devices in a one-out-of-two (1oo2) arrangement is:

$$\mathbf{PFDavg_{(S)}} = [PFDavg(_{TE/TT})]^2 + \beta \times PFDavg(_{TE/TT})$$

$$\mathbf{PFDavg_{(S)}} = 6.9E\text{-}05 + (0.1) \times 8.3E\text{-}03$$

$$\mathbf{PFDavg_{(S)}} = 9.0E\text{-}04$$

LOGIC SOLVER (LS) FAILURES

PLC Failure

Probability of failure on demand is provided by the vendor as (PFD = 5.5E-05).

$$\mathbf{PFDavg_{(LS)}} = 5.5E\text{-}05$$

FINAL CONTROL ELEMENT (FE) FAILURES

Solenoid Valve (SV) Failure

The solenoid valve has been certified as SIL-2 compliant. Failure data was obtained from the vendor (λ = 4.0 E-7/d). To convert a "per demand rate of failure" to a "per hour rate of failure," a demand rate (hazard event frequency) of once per year is used. Therefore:

λ = PFD * Demand Rate

λ = failure/demand * demand/hours

λ = (4.0E-07/demand) * (demand/8,760 hours)

λ = 4.6 E-11/hour

The test interval per TSR for the instrument loop test is once every 90 days (2160 hrs) x 1.25 = 2,700 hours (τ = 2,700 hours).

$$\mathbf{PFDavg_{(SV)}} = 0 .5\lambda\tau$$

$$\mathbf{PFDavg_{(SV)}} = (0.5)\ (4.6E\text{-}11/h)\ (2{,}700h) = 6.2E\text{-}08$$

Steam Valve (FV) Failure

Because no vendor-specific data are available, site generic failure data for a control valve failing to close is used (λ = 3.0 E-6/h). The test interval per the TSR for the instrument loop test is once every 90 days (2,160 hrs) x 1.25 = 2,700 hours (τ = 2,700 hours).

$\mathbf{PFDavg_{(FV)}} = 0.5\ \lambda\tau = (0.5)\ (3.0\ E\text{-}6/h)\ (2700h) = 4.0E\text{-}03$

Final Control Element (FE) PFDavg

$\mathbf{PFDavg_{(FE)}} = PFDavg_{(SV)} + PFDavg_{(FV)}$

$\mathbf{PFDavg_{(FE)}} = 6.2E\text{-}08 + 4.0E\text{-}03 = 4.0E\text{-}03$

SYSTEM (SIS) PFDavg

$\mathbf{PFDavg\ _{(SIS)}} = PFDavg_{(S)} + PFDavg_{(LS)} + PFDavg_{(FE)}$

$\mathbf{PFDavg\ _{(SIS)}} = 9.0E\text{-}04 + 5.5E\text{-}05 + 4.0E\text{-}03$

$\mathbf{PFDavg\ _{(SIS)}} = 5.0E\text{-}03$

The required SIL for this example was SIL-2. The accepted PFDavg range for SIL-2 is $<10^{-2}$ to $\geq 10^{-3}$. The calculated PFDavg for the SS SIS is 5.0E-03.

$\mathbf{RRF_{(SIS)}} = 1/PFDavg_{(SIS)} = 200$

APPENDIX E. FAILURE RATE DATA[2]

E.1 Failure Rate Data

American National Standards Institute/International Society of Automation (ANSI/ISA) 84.00.01-2004, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector,* requires the user to verify that the average probability of failure on demand (PFDavg) of the safety significant (SS) safety instrumented system (SIS) as designed, operated, and tested meets its safety integrity level (SIL). One of the key factors in the calculation of PFDavg is the failure rate of the components comprising the SS SIS.

Failure rate database use is common in the process industry sector when complying with ANSI/ISA 84.00.01-2004 – Part 1. The databases that provide a relative probability of failure for component types (e.g., level transmitters, pressure transmitters, analyzers, relays, breakers, pumps, motors, valves) are obtained from various industry sectors. In virtually all cases, these industrial databases turn out to be more conservative than product-specific data or user-specific data. Although some of the databases have not been updated recently, their data can be used in SIL verification calculations based on the conservatism of their failure rate values and the improved reliability, on average, of newer equipment.

The ANSI/ISA 84.00.01-2004 requirements for hardware fault tolerance (HFT) for SIL-2 and SIL-3 systems will drive redundancy and guard against the underestimation of equipment failure rates adversely affecting system-level safety unavailability (PFDavg). In addition, the ANSI/ISA 84.00.01-2004 requirement for performance monitoring will detect those cases in which the failure rate of a device was underestimated, or it proved unsuitable in a particular process application. HFT requirements and performance monitoring, in combination with failure rate databases, provide assurance that the design and operation of the SIS will be in compliance with the target SIL.

Failure rate data can be obtained from the sources listed below.

E.1.1 Industrial Databases

1. Offshore Reliability Data (OREDA)
2. Reliability Analysis Center
    a. EPRD-CD, Electronic Parts Reliability Data
    b. FMD-97, Failure Mode/Mechanism Distributions
    c. NPRD-CD, Non-electronic Parts Reliability Data
3. Guidelines for Process Equipment Reliability Data, with Data Tables, 1989, Center for Chemical Process Safety of American Institute of Chemical Engineers (AIChE)

[2] Appendix E is included for information only. All the conditions presented are representative and may need modification to ensure their suitability to any specific application.

4. ANSI/IEEE-Std-500, IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations, 1984

5. Reliability Data for Control and Safety Systems, 1998, SINTEF Industrial Management

6. Process Equipment Reliability Database, Center for Chemical Process Safety (CCPS), AIChE

Note 1: In addition to the above industrial databases, many consultant companies working in the chemical process safety industry have developed their own failure rate databases, combining the above data with company-specific and product-specific data.

Note 2: The list of databases above is not all inclusive. There is no intent to endorse or limit the use of comparable databases.

Industrial databases are not product-specific or application-specific; that is, they do not distinguish between harsh or mild environments, process conditions, or levels of maintenance and inspection. The data do provide a good, generally conservative estimation of equipment failure rates. Users should evaluate the expected environmental stressors on their safety devices, and, if they are expected to be above the norm, the SIS design should consider increased diagnostics and/or a factor increase in the failure rates. The source of the industrial data is an indicator of the environment in which the equipment was performing. For example, the OREDA data are primarily from the rather severe conditions of the North Sea oil rigs, and the ANSI/IEEE-Std-500 data are from the less severe environmental conditions for electrical devices in commercial nuclear power plants.

In using failure rate data, whether it is from industrial databases, product-specific data, or user-specific data, the conditions (both environmental and other stressors) in which the equipment identified in the database was required to perform should be ascertained and understood. These conditions should then be compared to the performance conditions of the equipment to be analyzed. The first choice of failure rate data should be that which comes from applications that are as near as possible to the application to be analyzed. The best practice is to consult more than one database in determining or confirming the appropriate failure rate value to be used. For any differences between the application to be analyzed and the database applications, data adjustment would be in order and may be necessary.

E.1.2 Product-Specific Data

Suppliers of components (e.g., instrumentation, programmable logic controllers, valves) used in process safety applications perform detailed analysis of their products to determine their specific probabilistic failure rate. The vendors providing equipment to the process industry sector must, by U.S. and international requirements, meet process safety requirements that are generally met by adhering to IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*. This standard establishes recommendations for the design and manufacture of components and discrete systems, including quality assurance, testing, and performance. The product-specific failure rates should be determined either by the manufacturer or a third-party certification organization. Product-specific failure rates can be determined by performing a failure modes and effects analysis (FMEA), which provides a specific failure rate for each component. In addition, the analysis should provide a

determination of safe versus dangerous failures and, where applicable, the diagnostic capabilities of the device to detect unsafe failures. Product-specific data end at the boundary of vendor equipment. Product-specific failure data do not consider process conditions or environmental factors. When using product-specific data in SIL verification calculations, the user is cautioned to include failures of process interfaces (e.g., sensor impulse line plugging).

Vendors of process safety equipment generally monitor the failures of devices after they have gone to market through contact with their users and returns of failed devices. On average, the FMEAs of a device designed for safety applications in the process industry have been found to have a lower failure rate versus the industrial databases identified in Section E.1.1.

E.1.3 User-Specific Data

Many chemical and process industry companies have developed their own failure rate databases based on their usage and applications. These data can be generic (e.g., level transmitters or control valves) or product-specific (i.e., Company ABC Model No. XYZ). When sufficient operational data exists, a user-specific database can be the most accurate because it reflects all stressors that impact a device. This includes environmental (e.g., temperature, vibration, process conditions) and operational (e.g., maintenance, testing, inspection) considerations. Caution should be taken when using data that come from multiple facilities on one site to ensure that the stressors and environmental conditions are applicable to the application to be analyzed.

E.1.4 Performance Monitoring

ANSI/ISA 84.00.01-2004 – Part 1, Section 5.2.5.3, requires the user to assess whether the observed fail-dangerous failure rates are in accordance with those used in the SIL verification calculation. To fulfill this requirement, the user should have a procedure to monitor the performance of safety devices and should periodically assess the observed failure data for comparison to that used in the SIL verification calculation.

ANSI/ISA 84.00.01-2004 – Part 1, Section 11.5, allows for the selection of safety components and subsystems based on “prior use.” Essentially, when users have experience with a device in either a safety or non-safety application, they may use that knowledge of failure modes and rates to justify application of that device in an SS SIS. In order to have the necessary data available to support “prior use,” the user should have systems/procedures in place to capture operational experience (Performance Monitoring) for devices that may be used in the future for safety applications.

APPENDIX F. QUALITY ASSURANCE FOR SAFETY SOFTWARE FOR SAFETY INSTRUMENTED SYSTEMS

This appendix provides a general discussion of the types of safety software and applicable quality assurance requirements.

F.1 Safety Software

The following types of software are used in safety instrumented systems (SIS).

Embedded software, normally provided by the vendor, is developed by a vendor and contained within the assembly of a programmable electronic device that is configured for performing a specific functional need and is not accessible for modification by the end-user. Embedded software is also referred to as firmware or system software.

Utility software, supplied by the vendor, is used to develop and verify application software. Utility software, like embedded software, is also developed by a vendor.

Application software, normally programmed by the end users, is developed for a specific application. In general, it contains logic sequences, permissives, limits, and expressions that control the appropriate input, output, calculations, and decisions necessary to meet the Safety Instrumented Function requirements. For application software, the vendor generally provides Fixed Program Language (FPL), Limited Variability Language (LVL), or Full Variability Language (FVL) programming software.

FPL is designed to limit the user to the adjustment of a few parameters; for example, range of the pressure transmitter, alarm levels, and network addresses.

LVL is designed to be comprehensible to process sector users, and provides high-level configurable program instructions, such as ladder logic or function blocks, to allow the end-user to configure the application within a strictly controlled framework or environment. LVL is widely used by the end-user for Programmable Logic Controller (PLC) application programming.

FVL is designed to be comprehensible to computer programmers and provides the capability to implement a wide variety of functions and applications.

F.2 Software and Hardware Integration

Three elements of safety software applications are as follows:

- the **sensor** (may have internal logic; the primary function is to sense and transmit data or some form of aggregated data);
- the **logic device** (the purpose is to process information variables to determine their condition relative to a trip point, calculating transfer functions, or other process specific tasks); and
- the **control element** (an actuator, for example, performs a desired function based on the output results from the sensor or logic device).

The above elements are normally integrated using a network system with software of some type, such as an embedded program. Fieldbuses are also used for communication to field devices. Software development management control principles and software life-cycle elements apply to each of the above elements to the extent that the safety case can be verified for all safety subsystems and the overall safety system.

Prior to development of application software, an SIS software requirements specification should be developed (in accordance with guidance provided in DOE G 414.1-4, *Safety Software Guide for Use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance*) that describes overall system operating requirements and functions, including applicable safety functions and safety requirements that form the safety basis for the system design. Safety software is designed to support one of the following or a combination of them.

- Isolation — Critical components are separated from each other in a manner to preclude undefined interactions. When applied to software design, the emphasis is on encapsulation, information hiding, and formal interfaces that preclude (i.e., isolate) SIS failure due to unintended software execution or malfunction.

- Independence — The stimuli for actions originate from, and are handled by, separate components. This is generally implemented by redundant components often with different designs that support a safety-related task. As applied to software, independent hardware inputs are directed to independent software modules.

- Inoperability — Abnormal conditions cause a component to become inoperable in a safe, predictable manner and before any isolation features are compromised. As applied to software design, these criteria may be implemented through comprehensive exception handling and fail-safe designs in critical components.

- Incompatibility — Components in different parts of the system cannot operate together in a satisfactory manner. To avoid incompatibility, consider that sensors, a logic device (such as a processor), and control devices may have embedded software that needs to be integrated into a networked system. The acceptability of the integration needs to be validated.

Embedded software is generally used for software/hardware integration, and fieldbus is used for networking and communication purposes. Fieldbuses used to implement safety functions should follow the design considerations listed in ISA TR84.00.06.

F.3 Safety Software Quality Assurance Work Activities

DOE G 414.1-4, *Safety Software Guide for Use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance,* identifies 10 software quality assurance (SQA) activities applicable to software development and acquisition. Table F.3-1: Crosswalk of SQA Work Processes with Acceptable Industry Implementation Guidance Standards identifies industry guidance standards available to fulfill requirements of the DOE Guide. The industry guidance standards listed in Table F.3-1 are not intended to be an exhaustive list. Other standards may be applied so long as the basis for their selection for the application is documented and is shown to be equivalent level of quality assurance as to DOE O 414.1C, *Quality Assurance.*

Table F.3-1: Crosswalk of SQA Work Processes with Acceptable Industry and Other Implementation Guidance Standards

Item	SQA Work Processes DOE G 414.1-4	Acceptable Industry Implementation Guidance Standards
1	**Sec. 5.2.1, *Software Project Management and Quality Planning*** Software project management and quality planning should involve identifying all tasks associated with the software development and procurement, including procurement of services, as described for safety software in Section 5.2.1.	• ANSI/ISA 84.00-01-2004-Part 1 (Clause 12) • ASME NQA-1-2000 and Subpart 2.7 • ANSI/IEEE STD 730, *Standard for Software Quality Assurance Plans*
2	**Sec. 5.2.2, *Software Risk Management*** The risk associated with safety software applications needs to be understood and documented. As discussed in Section 5.2.2, all apparent risks known at the time, whether large or small, should be identified, analyzed for impact and probability of occurrence, prioritized, and resolved to a level as defined in the safety basis documentation of risk to enable establishing a historical record for the life of the safety software.	• ANSI/ISA 84.00-01-2004-Part 1 (Clause 12) • ASME NQA-1-2000 and Subpart 2.7 • ANSI/IEEE STD 730, *Standard for Software Quality Assurance Plans*
3	**Sec. 5.2.3, *Software Configuration Management (SCM)*** SCM activities identify all functions and tasks required to manage the configuration of the software system, including software engineering requirements, establishing the configuration baselines to be controlled, and software configuration change control process. SCM includes (1) configuration identification, (2) configuration control, (3) configuration status accounting, and (4) configuration audits and reviews.	• ANSI/ISA 84.00-01-2004-Part 1 (Clause 12) • ASME NQA-1-2000 and Subpart 2.7 • ANSI/IEEE STD 730, *Standard for Software Quality Assurance Plans*
4	**5.2.4, *Software Procurement and Supplier Management*** This section provides essential attributes for safety software procurement that are applicable to SIS embedded software and utility software, as well as any services provided for application software development.	• ANSI/ISA 84.00-01-2004-Parts 1 (Clause 12) • ASME NQA-1-2000 and Subpart 2.7 • ANSI/IEEE-Std-730, *Standard for Software Quality Assurance Plans*

Item	SQA Work Processes DOE G 414.1-4	Acceptable Industry Implementation Guidance Standards
5	**Sec. 5.2.5, *Software Requirements Identification and Management*** SIS design basis requirements provide the foundation for the identification and management of software requirements that include functional, performance, safety requirements, design constraints, interface, installation considerations, and access control, as appropriate. The software design requirements should identify the applicable operating system, functions, interfaces, performance requirements, installation considerations, design inputs, and constraints. The requirements shall be traceable, verifiable (including acceptance criteria), consistent, and clear (unambiguous).	• ANSI/ISA 84.00-01-2004-Part 1 (Clause 12) • ASME NQA-1-2000, and Subpart 2.7 • IEEE-STD-7-4.3.2-2003, *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations* • ANSI/IEEE-STD-830-1998, *IEEE Recommended Practice for Software Requirements Specification* • ANSI/IEEE-STD-730, *Standard for Software Quality Assurance Plans*
6	**Sec. 5.2.6, *Software Design and Implementation*** For application software, the design should be documented and include, as applicable, numerical methods, mathematical models, physical models, control and logic flow, data flow, process flow, data structures, applicable relationships between data structures and process structures, and traceability requirements. The software design shall be translated into computer program(s) using the programming or design organization's programming standards and conventions.	• ANSI/ISA 84.00-01-2004–Part 1 (Clause 12) • ASME NQA-1-2000, and Subpart 2.7 • IEEE-STD-7-4.3.2-2003; *Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations* • ANSI/IEEE-STD-830-1998, *Recommended Practice for Software Requirements Specification* • ANSI/IEEE-STD-730, *Standard for Software Quality Assurance Plans*
7	**Sec. 5.2.7, *Software Safety*** The development of software applications requires identification of hazards that have the potential for defeating a safety function and the implementation of design strategies to eliminate or mitigate those hazards. Methods to mitigate the consequences of software failures should then be an integral part of the software design.	• ANSI/ISA 84.00-01-2004-Part 1 (Clause 12) • IEEE-STD-7-4.3.2-2003, *Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*

Item	SQA Work Processes DOE G 414.1-4	Acceptable Industry Implementation Guidance Standards
8	**Sec. 5.2.8, *Verification and Validation*** Verification is performed throughout the life cycle of the safety software. Validation activities are performed at the end of the software development or acquisition processes to ensure the software meets the intended requirements.	• ANSI/ISA 84.00-01-2004-Part 1 (Clause 12) • ASME NQA-1-2000 and Subpart 2.7 • ANSI/IEEE-*STD-1012, Standard for Software Verification and Validation*
9	**Sec. 5.2.9, *Software Problem Reporting and Corrective Management*** The reporting and corrective action system will cover (1) methods for documenting, evaluating, and correcting software problems; (2) an evaluation process for determining whether a reported problem is indeed a defect or an error; and (3) the roles and responsibilities for disposition of the problem reports. Procurement documents should identify the requirements for suppliers to report problems and any required responses and the method for the purchasers to report problems to the supplier.	• ANSI/ISA 84.00-01-2004-Part 1 (Clause 12) • ASME NQA-1-2000 and Subpart 2.7 • ANSI/IEEE-STD-730, *Standard for Software Quality Assurance Plans*
10	**Sec. 5.2.10, *Training of personnel in the design, development, use, and evaluation of safety software*** Training should be commensurate with the scope, complexity, and importance of the tasks and the education, experience, and proficiency of the individual.	• ANSI/ISA 84.00.01-2004, Section 5, “Management of Functional Safety” • ASME NQA-1-2000 and Subpart 2.7 • ANSI/IEEE-STD-730, *Standard for Software Quality Assurance Plans*

APPENDIX G. HUMAN FACTORS ENGINEERING

See Section 2.7 of this standard for details regarding Human Factors Engineering (HFE). Figure G-1: Application of HFE Throughout the SIS Life Cycle shows how HFE is applied throughout the safety system life cycle. Table G-1: Human Factors Standards and Guidance Documents provides information on HFE standards and guidance documents.

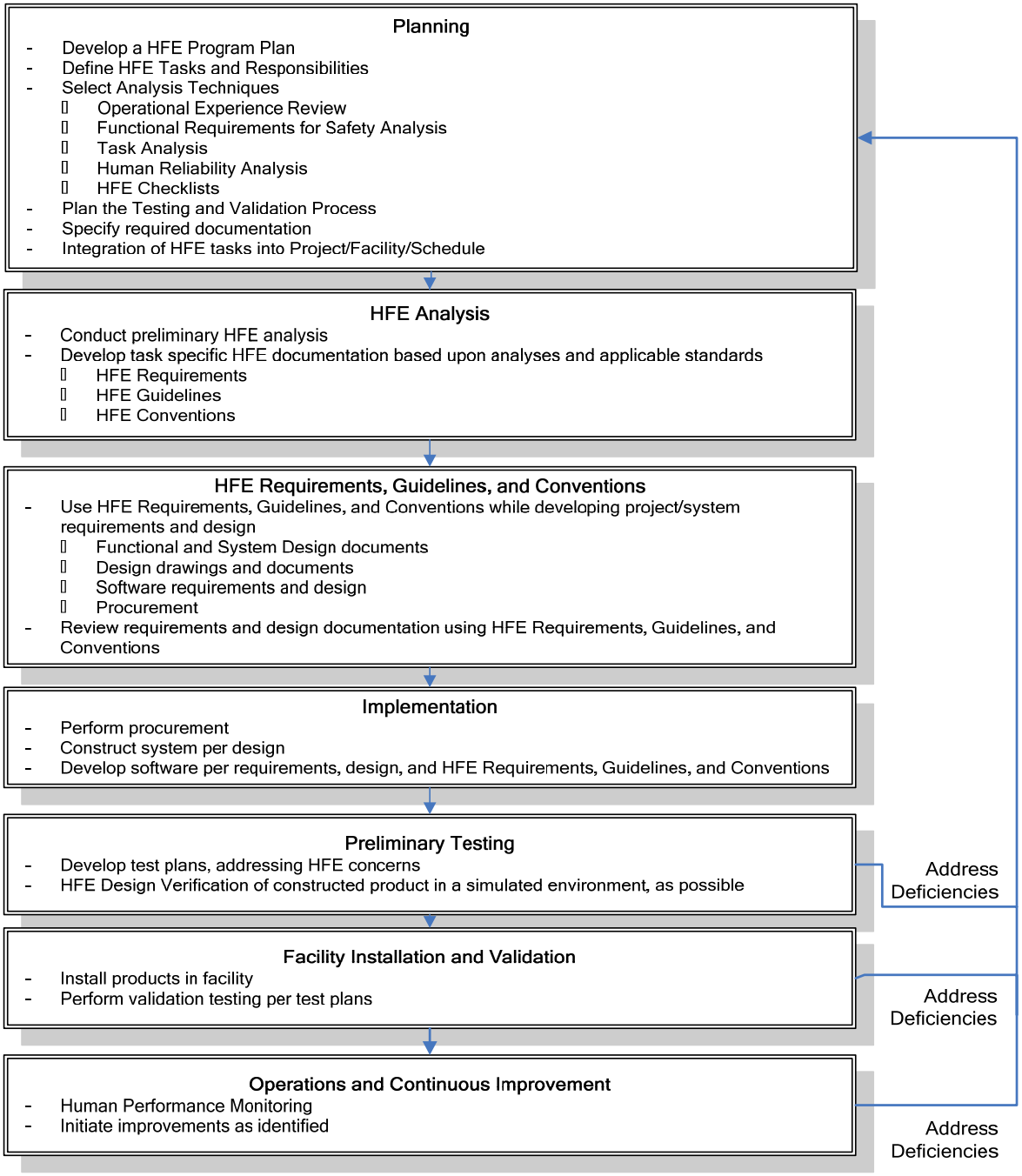

Figure G-1: Application of HFE Throughout the SIS Life Cycle

Table G-1: Human Factors Standards and Guidance Documents

HFE Phase	Standard/Document	HFE Guidance Provided
Planning	DOE-HDBK-1140-2001, *Human Factors Ergonomics Handbook for Ease of Maintenance*	Provides guidelines for ease of maintenance.
	NUREG-0711, *Human Factors Engineering Program Review Model*	Defines an approach for ensuring that the HFE aspects of a facility are developed, designed, and evaluated on the basis of a structured analysis using accepted HFE principles.
	EPRI 1008122, *Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation and Maintenance*	Provides a general analytical tool for considering system design and required operator actions. It includes a comparison of how control room operators perform control room tasks and or respond to alarm conditions in traditional analog control rooms versus a modernized control room that incorporates digital instrument and control systems.
	IEEE-STD-845, *IEEE Guide to Evaluation of Man-Machine Performance in Nuclear Power Generation Station Control Room and Other Peripheries*	Provides guidance for the selection and application of human factors techniques to carry out the following tasks: ▪ Evaluation of a given man-machine design in control rooms and other control areas to ascertain the degree of design adequacy; ▪ Determination, as needed, of changes to increase acceptability of a man-machine design; and ▪ Determination of the relative adequacy of alternative designs.

HFE Phase	Standard/Document	HFE Guidance Provided
	• ANSI/IEEE-STD-1023, Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities	Provides help in evaluating the effect that automated system actions have on the operator's understanding of process operations and the potential for operator confusion. Also, it provides general guidance to address human error and the implementation of design features to mitigate undesirable consequences associated with anticipated human errors.
HFE Analysis (Requirements, Guidelines, Conventions) and Requirements & Design	ANSI/ANS 58.8, *Time Response Design Criteria for Safety-Related Operator Actions*	Provides guidelines to be applied in determining time requirements for safety-related operator response.
	DOE-HDBK-1140-2001 (same as Planning)	(See Planning)
	DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Reports*	Provides guidance in identifying the human-machine interfaces required for ensuring safety function during normal, abnormal, and emergency operations. This guide also identifies interfaces for surveillance and maintenance of safety systems, structures, and components during normal operations.
	EPRI 1008122 (same as Planning)	(See Planning)
	ANSI/ISA 18.2, *Management of Alarm Systems for the Process Industries*	Covers all aspects of alarm management.
	MIL-STD-1472, *Department of Defense Design Criteria Standard – Human Engineering*	Presents human engineering design criteria, principles and practices to be applied in the design of systems, equipment and facilities.

HFE Phase	Standard/Document	HFE Guidance Provided
	NUREG-0700, *Human-System Interface Design Review Guidelines,* Rev. 2	Provides a comprehensive review for HFE principles and design guidelines, regardless of the platform.
Implementation	ANSI/ANS 3.5, *Nuclear Power Plant Simulators for Use in Operator Training and Examination*	Provides guidance for simulator model requirements.
Testing	NUREG-0711, *Human Factors Engineering Program Review Model,* Rev. 2	Defines an approach to ensure that the HFE aspects of the facility are developed, designed, and evaluated on the bases of a structured analysis using accepted HFE principles.
Continuous Improvement	NUREG-0711 (same as Testing)	(See Testing)

APPENDIX H. APPLICABLE DOCUMENTS

H.1 Department of Energy Directives

The following DOE Directives provide high-level requirements and guidance that are the basis for the Safety Instrumented Systems (SIS) criteria and guidance in this standard. The DOE Directives (or their successor directives) should be referred to in support of effective implementation of this standard.

- DOE O 414.1C, *Quality Assurance*
- DOE O 420.1B, Change Notice No. 1, *Facility Safety*
- DOE O 426.1, *Federal Technical Capability*
- DOE O 426.2, *Personnel Selection, Training, Qualification, and Certification Requirements for DOE Nuclear Facilities*
- DOE G 414.1-4, *Safety Software Guide for Use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance*
- DOE G 420.1-1, *Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria Guide For Use With DOE O 420.1, Facility Safety*
- DOE-HDBK-1140-2001, *Human Factor/Ergonomics Handbook for the Design for Ease of Maintenance*
- DOE-STD-1186-2004, *Specific Administrative Controls*
- DOE-STD-1189-2008, *Integration of Safety into the Design Process*
- DOE-STD-3007-2007, *Guidelines for Preparing Criticality Safety Evaluations at Department of Energy Nonreactor Nuclear Facilities*
- DOE-STD-3009-94, Change Notice No. 3, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analyses*

H.2 National and International Standards

These national and international standards should be referred to in support of effective implementation of this standard. Some of these are specifically identified for use within this standard.

- ASME NQA-1, *Quality Assurance Requirements for Nuclear Facility Applications (Version 2000, and all subsequent editions)*
- ANSI/ANS 3.5, *Nuclear Power Plant Simulators for Use in Operator Training and Examination*
- ANSI/ANS 8.3, *Criticality Accident Alarm Systems*
- ANSI/ANS 58.8, *Time Response Design Criteria for Safety-Related Operator Actions*

- ANSI/IEEE- Std -500, *IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations*
- ANSI/IEEE- Std -730, *Standard for Software Quality Assurance Plans*
- ANSI/IEEE- Std -828, *Standard for Software Configuration Management Plans*
- ANSI/IEEE- Std -829, *Standard for Software Test Documentation*
- ANSI/IEEE- Std -830, *Recommended Practice for Software Requirements Specifications*
- ANSI/IEEE-Std-1012, *Standard for Software Verification and Validation*
- ANSI/IEEE-Std-1023, *Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities*
- ANSI/IEEE-Std-1028, *Standard for Software Reviews and Audits*
- ANSI/IEEE-Std-1074, *Standard for Developing Software Life-Cycle Processes*
- ANSI/IEEE-Std-1219, *Standard for Software Maintenance*
- ANSI/IEEE-Std-1228, *Standard for Software Safety Plans*
- IEEE-Std-845, *IEEE Guide to Evaluation of Man-Machine Performance in Nuclear Power Generation Station Control Room and Other Peripheries*
- IEEE-Std 7-4.3.2, *Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*
- ANSI/ISA 18.2, *Management of Alarm Systems for the Process Industries*
- ANSI/ISA 67.01.01, *Transducer/Transmitter Installation for Nuclear Safety Applications*
- ANSI/ISA 67.04.01, *Setpoints for Nuclear Safety-Related Instrumentation*
- ANSI/ISA 84.00.01-2004 Part 1 (IEC61511-1 Mod), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements*
- ANSI/ISA 84.00.01-2004 Part 2 (IEC 61511-2 Mod), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 2: Guidelines for the Application of ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) – Informative*
- ANSI/ISA 84.00.01-2004 Part 3 (IEC 61511-3 Mod), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 3: Guidance for the Determination of the Required Safety Integrity Levels – Informative*
- ISA TR84.00.02, *Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques*

- ISA TR84.00.03, *Guidance for Testing of Process Sector Safety Instrumented Function (SIF) Implemented as or Within Safety Instrumented Systems*
- ISA TR84.00.04, *Guideline for the Implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod)*
- ISA TR84.00.06, *Safety Fieldbus Design Considerations for Process Industry Sector Applications*
- IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*
- IEC 61511, *Functional Safety – Safety Instrumented Systems for the Process Industry Sector*

H.3 Nuclear Regulatory Commission (NRC) Guidance

These NRC guidance documents should be referred to in support of effective implementation of this standard.

- NUREG-0700, Rev. 2, *Human-System Interface Design Review Guidelines*
- NUREG-0711, *Human Factors Engineering Program Review Model*
- NUREG-0800, BTP 7-14, *Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems*
- NUREG-0800, BTP 7-18, *Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems*
- NUREG-0800, BTP 7-19, *Guidance for Evaluation of Diversity and DID in Digital Computer-Based Instrumentation and Control Systems*
- NUREG-0800, BTP 7-21, *Guidance on Digital Computer Real-time Performance*
- NUREG-6090, *The PLC and its Application in Nuclear Reactor Protection Systems*
- NUREG-6303, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*
- NUREG/CR-6421, *A Proposed Acceptance Process for Commercial Off-the–Shelf (COTS) Software in Reactor Applications*
- NUREG/CR-6842, *Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants*
- NRC RG 1.152, Rev. 2, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*

H.4 Other Sources

These documents should be referred to in support of effective implementation of this standard. Some of these are specifically identified for use within this standard.

- EPRI-1008122, *Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance*
- EPRI TR-102260, *Supplemental Guidance for the Application of EPRI Report NP-5652 on the Utilization of Commercial Grade Items*
- EPRI TR-106439, *Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications*
- INPO 05-003, *Performance Objectives and Criteria – Fundamentals of Training*
- MIL-STD-1472, *Department of Defense Design Criteria Standard – Human Engineering*

APPENDIX I. ABBREVIATIONS, ACRONYMS, AND DEFINITIONS

I.1 Abbreviations and Acronyms

AC	Administrative Controls
ANSI	American National Standards Institute
BPCS	Basic Process Control System
CCF	Common Cause Failure
CGD	Commercial Grade Dedication
CSDR	Conceptual Safety Design Report
DCS	Digital Control System
DID	Defense-In-Depth
DOE	Department of Energy
DSA	Documented Safety Analysis
FCV	Flow Control Valve
FMEA	Failure Modes and Effects Analysis
FPL	Fixed Program Language
FV	Steam Isolation Valve
FVL	Full Variability Language
HFE	Human Factors Engineering
HFT	Hardware Fault Tolerance
IPL	Independent Protection Layer
IEC	International Electrotechnical Commission
ISA	International Society of Automation
LCO	Limiting Condition of Operation
LVL	Limited Variability Language
MTTF	Mean Time To Failure
NFPA	National Fire Protection Association

NRC	Nuclear Regulatory Commission
PDSA	Preliminary Documented Safety Analysis
PFDavg	Average Probability of Failure on Demand
PLC	Programmable Logic Controller
PSDR	Preliminary Safety Design Report
QA	Quality Assurance
RTD	Resistance Temperature Detector
RRF	Risk Reduction Factor
SAC	Specific Administrative Control
SC	Safety Class
SCM	Software Configuration Management
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SQA	Software Quality Assurance
SS	Safety Significant
SSC	Structures, Systems, and Components
SV	Solenoid Valve
TE	Temperature Element
TSR	Technical Safety Requirement

I.2 Definitions

The following definitions are included with this standard for convenience and clarification. Where applicable, DOE Order definitions shall take precedence over those shown in this document.

Application Software. Software which is specific to the user application. In general, it contains logic sequences, permissives, limits and expressions that control the appropriate input, output, calculations, decisions necessary to meet the safety instrumented functional requirements. [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod); Clause 3.2.81.2.1]

Basic Process Control System (BPCS). The system which responds to input signals from the process, its associated equipment, other programmable systems and/or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any safety instrumented functions with a claimed SIL ≥ 1. [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod); Clause 3.2.3]

Common-Cause Failure (CCF). A failure, which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to system failure. [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod); Clause 3.2.6.1]

Common-Mode Failure (CMF). The failure of two or more channels in the same way, causing the same erroneous result. [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), Clause 3.2.6.2]

Dedication. An acceptance process performed in accordance with this standard to provide reasonable assurance that a commercial grade item or service will successfully perform its intended safety function and, in this respect, is deemed equivalent to an item or services provided under the requirements of this Standard. [NQA-1, 2004]

Dedicating entity. The organization that performs the dedication process. [NQA-1-2004]

Demand Mode Safety Instrumented Function. When a specified action (for example, closing of a valve) is taken in response to process conditions or other demands. In the event of a dangerous failure of the safety instrumented function a potential hazard only occurs in the event of a failure in the process or the BPCS. [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), Clause 3.2.43.1]

Defense-in-Depth (DID). The design and operational philosophy that calls for multiple layers of protection to prevent and/or mitigate accidents. It may include the use of controls, multiple physical barriers, redundant safety functions, and emergency response measures.

Dangerous Failure. Failure which has the potential to put the safety instrumented system in a hazardous or fail-to-function state [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), Clause 3.2.11]

Detected. In relation to hardware failure and software faults, detected by the diagnostic tests or through normal operation. [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), Clause 3.2.13]

Diagnostic Coverage. Ratio of the detected failure to the total failure rate of the component or subsystems as detected by diagnostic tests. Diagnostic coverage does not include any faults detected by proof tests. [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), Clause 3.2.15]

Diversity. The existence of different means performing a required function. [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), Clause 3.2.16]

Embedded Software. Software that is part of the system supplied by the manufacturer and is not accessible for modification by the end-user. Embedded software is also referred to as firmware or system software. [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), Clause 3.2.81.2.2]

Electrical/Electronic/Programmable Electronic (E/E/PE). Based on electrical (E) and/or electronic (E) and/or programmable electronic (PE) technology [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), clause 3.2.17]

Failure. Termination of the ability of a functional unit to perform a required function. [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), Clause 3.2.20]

Fault. An abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function. [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) Clause 3.2.21]

Fixed Program Language (FPL). In this type of language, the user is limited to an adjustment of a few parameters (for example, range of the pressure transmitter, alarm levels, network addresses). [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), Clause 3.2.81.1.1]

Full Variability Language (FVL). This type of language is designed to be comprehensible to computer programmers and provides the capability to implement a wide variety of functions and applications. [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), Clause 3.2.81.1.3]

Independent Protection Layer (IPL). A structure, system, component, or administrative control that prevents or mitigates a safety significant hazardous event to an acceptable condition.

Layer of Protection Analysis (LOPA). LOPA is a simplified form of risk assessment. LOPA typically uses order of magnitude categories for initiating event frequency, consequence severity, and the likelihood of failure of independent protection layers (IPLs) to approximate the risk of scenario. LOPA is limited to evaluating a single cause-consequence pair as a scenario. [Ref. Chapter 2 of *Layer of Protection Analysis Simplified Process Risk Assessment* by Center for Chemical Process Safety, ISBN 0-8169-0811-7.]

Limited Variability Language (LVL). This type of language that is designed to be comprehensible to process sector users, and provides the capability to combine predefined, application-specific, library functions to implement the safety requirements specifications. A LVL provides a close functional correspondence with the functions required to achieve the application. A typical example of system LVL: standard PLC. [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), Clause 3.2.81.1.2]

Major Modification. A modification to a nuclear facility that substantially changes the existing safety basis for the facility. [10 CFR 830.3]

Programmable Electronic System (PES). System for control, protection or monitoring based on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, actuators and other output devices. [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), Clause 3.2.56]

Probability of Failure on Demand – Average (PFDavg). The PFDavg for an IPL is the average probability that, when demanded, it will <u>not</u> perform the required task. Failure to perform could be caused by:

- a component of an IPL being in a failed or unsafe state when the initiating event occurs; or
- a component failing during the performance of its task; or
- human intervention failing to be effective, etc.

[Ref. Chapter 6 of *Layer of Protection Analysis Simplified Process Risk Assessment* by Center for Chemical Process Safety, ISBN 0-8169-0811-7.]

Risk Reduction Factor (RRF). RRF is the inverse of Probability of Failure on Demand (1/PFD).

Safe Failure. Failure does not have the potential to put the safety instrumented system in a hazardous or fail-to-function state. [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), Clause 3.2.65]

Safe Failure Fraction. Faction of the overall random hardware failure rate of a device that results in either a safe failure or a detected dangerous failure. [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), Clause 3.2.65.1]

Safety Instrumented Function (SIF). Safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function. [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), Clause 3.2.71]

Safety Integrity Level (SIL). Discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to safety instrumented systems. Safety integrity level 4 is assigned the highest level of safety integrity; while safety integrity level 1 is the lowest. [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), Clause 3.2.74]

Safety Instrumented System (SIS). Instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor(s), logic solver(s), and final element(s). [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), Clause 3.2.72]

Note 1: An SIS may be either automatic or require operator action to bring the process to a safe state, or mitigate a hazard in response to an alarm or indication. An automatic SIS is composed of sensor(s), logic solver(s), and final element(s). An SIS with required operator action is composed of any combination of sensor(s), logic solver(s), alarm presentation/operator action(s), and final element(s).

Note 2: An instrumented system, classified as safety significant, that does not take action to bring the process to a safe state or mitigate a hazard to an acceptable level is not by definition an SIS and is, therefore, not covered by this standard.

Safety Life Cycle. Necessary activities involved in the implementation of safety instrumented function(s) occurring during a period of time that starts at the concept phase of a project and

finishes when all of the safety instrumented functions are no longer available for use. [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), Clause 3.2.76]

Safety Software. [For definition of Safety Software see DOE O 414.1C]

System. Set of elements, which interact according to a design; an element of a system can be another system, called a subsystem, which may be a controlling system or a controlled system and may include hardware, software, and human interaction. A person can be of a system. A system includes the sensors, the logic solvers, final elements, communication, and ancillary equipment belonging to SIS (for example, cables, tubing, and power supply). [Ref. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), Clause 3.2.84]

CONCLUDING MATERIAL

Review Activities:

DOE	**Ops Office**	**Preparing Activity:**
NA	AL	DOE-HS-21
HS	SR	
EM	ID	Project Number:
SC	NV	SAFT-0128
NE	OR	
GC	RL	
Energy CTA	CH	
NNSA CTA		

Area/Site Office	**National Laboratories**
Pantex	SRNL
Carlsbad	LANL
Princeton	LLNL
ORP	PNNL
Los Alamos	INL
Y-12	PPPL
Savannah River	ANL
Ames	Ames
Argonne	BNL
BHSO	Berkeley
BSO	Fermi
FSO	SLAC
NBL	TJNAL
PNSO	
PPPO	
SSO	
TJSO	