

SAFETY INSTRUMENTED FUNCTIONS as CRITICALITY DEFENSES

William H. Hearn
Lawrence T. Suttinger
Washington Savannah River Company
Savannah River Site, Bldg. 703-H, Aiken, SC 29808
Phone 803-208-1929 / Fax 803-208-8091
william.hearn@srs.gov
lawrence.suttinger@SRNL.doe.gov

Abstract

The objective of this paper is to share the SRS methodology for identifying the reliability requirements and documenting the expected performance of Safety Instrumented Functions (SIFs) used as criticality defenses. Nuclear Criticality SIFs are comprised of sensors, logic solvers, and final control elements, which may be either automatic or manual, to detect a process hazard and respond to prevent a criticality.

The Savannah River Site (SRS) has invoked the chemical process industry safety standard (ANSI/ISA 84.00.01)¹ for the design of safety significant instrumented systems. The ISA standard provides a graded approach to design based on the amount of risk reduction that is required of an SIF. SRS is embarking on application of this standard to nuclear criticality defenses, thus integrating criticality safety requirements with verifiable design methodology. Per the DOE G 421.1-1² discussion of the double contingency principle, guidance for a single contingency barrier includes, "The estimated probability that the control will fail (when called upon for protection) is not greater than 1 in 100 demands."

The application of this standard to nuclear criticality SIFs will provide clear requirements in terms of safety availability and testing to assure that the instrumented criticality system as designed, installed, and maintained will meet its performance requirements. The paper identifies the numerous challenges presented by this initiative and the benefits of this approach.

INTRODUCTION

Historically when a nuclear criticality SIF had been used as an active-engineered nuclear criticality barrier, it was designed using equipment procured under a QA program and installed in a fail-safe configuration. In most cases the safety instrumented function was configured as a simplex system. That is there was no redundancy of instruments or final devices that placed the process in a shutdown or safe condition. The instrumented system may have been implemented by separate, hardwired components, or in some cases they were included as part of the basic

process control system that functioned as the non-safety hardware platform for the process. Although these systems were judged to be reliable, there was no requirement to quantitatively estimate the system unavailability. These practices have supported the SRS record of ZERO inadvertent criticalities over 50+ years of handling fissile materials.

The Savannah River Site (SRS) has now adopted a safety design standard, which is used for the design and management of safety systems by the process industry, for the design of Nuclear Criticality Safety Significant Instrumented Functions. ANSI/ISA S84.01-1996³ and its successor ANSI/ISA 84.00.01-2004, Functional Safety: Safety Instrumented Systems for the Process Industry Sector¹, have been in use at SRS since 1999 for the design of instrumented systems classified as Safety Significant (SS), but not until 2007 has the ISA standard been applied to Nuclear Criticality Safety Significant Instrumented Functions. The application of the ISA Functional Safety design standard is intended to augment our safety posture rather than replace any ANS or DOE requirement for (1) the assessment for the need for an active-engineered criticality defense, or (2) the required safety unavailability of the SIF.

NUCLEAR CRITICALITY CODE REQUIREMENTS and GUIDANCE

ANSI/ANS 8.1-1998, Nuclear Criticality Safety in Operations with Fissionable Material Outside Reactors⁴, Section 4.2.2 has a requirement for a *Double Contingency Principle*. It states that, "Process designs should incorporate sufficient factors of safety to require at least two unlikely, independent, and concurrent changes in process conditions before a criticality accident is possible." Within the standard it does not further define the term 'Unlikely' with respect to a safety unavailability or probability of failure on demand.

DOE G 421.1-1, Criticality Safety Good Practices Program Guide for DOE Nonreactor Nuclear Facilities², does provide some guidance on when a barrier (One arm of a double contingency) is sufficiently unlikely to fail in terms of unavailability. Section 5.7.7.3.1, Guideline 1, provides a failure limit of no greater than 1 in 100 demands to qualify the barrier for application to the Double Contingency Principle. To put this reliability requirement in perspective, the Guide also states in 5.7.7.1, "While failure mode independence can be established, likelihood of failure cannot be well quantified ..." indicating that principal reliance is placed on the independence of barriers.

There are three basic means of control to prevent a criticality; (1) passive-engineered control, (2) active-engineered control, and (3) administrative control. A Safety Instrumented Function (SIF) is classified as an active-engineered control. A SIF is composed of instrument(s) that monitor critical process parameters, logic solver(s) that determine when a safety limit is exceeded, and final device(s) that place a process in a safe condition. Alarms systems used solely to evacuate personnel, such as a Nuclear Incident Monitor (NIM), are not considered to be SIFs since they don't actively place a process in a safe state. ANSI/ANS 8.3, Criticality Accident Alarm System⁵, is the governing standard for the design of these types of systems. Any criticality alarm or instrumentation system that does not have a safety function to actively prevent a criticality is not considered a SIF and is not covered by the ANSI/ISA 84.00.01¹ design process discussed below.

ANSI/ISA 84.00.01

ISA 84.00.01¹ is a process industry (e.g. chemical, refinery) standard for the design, installation, operation, maintenance, start-up, periodic functional testing, and management of safety instrumented systems. The standard promotes a risk-informed performance-based methodology for the life cycle management of safety systems. It provides a graded approach to design based on the risk reduction required for a particular Safety Instrumented Function. The amount of risk reduction required is not dictated by the standard, but is determined by the facility owner. Risk is a function of the frequency of occurrence of a hazardous event and the consequence of that event. Once the amount of risk reduction for a SIF is determined, the standard provides the design requirements and safety management required to meet and maintain the safety design.

The standard has four Safety Integrity Levels (SILs) which are used to provide the graded approach. The SILs are defined in terms of the average probability of failure on demand (PFDavg) or in other terms, the risk reduction factor (RRF), that the SIL provides as indicated below:

- SIL-1 RRF of 10 to 100 PFDavg 10^{-1} to 10^{-2}
- SIL-2 RRF of 100 to 1,000 PFDavg 10^{-2} to 10^{-3}
- SIL-3 RRF of 1000 to 10,000 PFDavg 10^{-3} to 10^{-4}
- SIL-4 RRF of 10,000 to 100,000 PFDavg 10^{-4} to 10^{-5}

The calculation of the safety unavailability (probability of failure on demand) of an instrumented system is much different than that for a structural or mechanical system. The simplified formula for calculating the PFDavg of a simplex SIS (no redundancy of components) is as shown below:

$$\text{PFDavg} = \lambda (\text{TI}/2)$$

λ is the dangerous failure rate of the component

TI is the test interval between periodic functional tests of the system

When calculating the PFDavg for redundant systems common cause failure must be taken into account. The equations can become more complex if other factors that would affect the PFDavg are considered such as diagnostic coverage and safe failure fraction.

SIL DETERMINATION

The ISA standard does not dictate the SIL value that has to be applied to a SIF in any given situation. The assignment of a SIL for a particular SIF is left up to the facility owner based on the risk tolerance of that owner. As an example, the location of identical process facilities in relation to environmental or population concerns will drive the acceptable risk of an accident based on the ultimate consequence.

As noted above, DOE G 421.1-1² provides guidance on the safety availability of a nuclear criticality barrier. Its requirement for a failure on demand of no more than 1 in a 100, converts to a SIL-2. As noted above, the DOE Guide provides a minimum goal for the probability of failure

on demand regardless of any qualitative or quantitative assessment of the frequency of a criticality event.

The Savannah River Site (SRS) has adopted an in-house standard for Nuclear Criticality SIL determination. SRS Engineering Standard 01703⁶, Application of ISA 84.00.01- Part 1 for SRS non-Reactor Facilities, for the design of all Safety Significant Instrumented Systems, which includes nuclear criticality instrumented systems. The standard includes the following statements for the SIL determination:

“Per the DOE G 421.1-1² discussion of the double contingency principle, guidance for a single contingency barrier includes: 5.7.7.3.1 Guideline 1: The estimated probability that the control will fail (when called upon for protection) is not greater than 1 in 100 demands. The DOE guidance is applied regardless of functional classification. To envelope this performance, an instrumented system should be designed as SIL-2. A SIL-2 SIF is defined as possessing an average probability of failure on demand (PFDavg) of 0.01 to 0.001 (RRF = 100 to 1000).

Criticality Engineering may designate a higher or lower reliability requirement for a specific SIF, based on the strength of the other credited criticality controls and the degree of independence between the SIF and those credited controls.

Application of the life cycle, structure, calculation methodology, and design philosophy presented in ANSI/ISA 84.00.01-2004¹ is appropriate for criticality safety instrumented functions with a functional classification of Production Support (PS) or General Services (GS-C). Requirement 9.4.2 of ISA 84.00.01 limits the risk reduction factor for a system implemented in a BPCS (Basic Process Control System – usually the DCS). The risk reduction factor, for a PS or GS-C function implemented within a Distributed Control System (DCS) or other non-safety system, is limited to 10 by requirement 9.4.2.”

The provision allowing Criticality Engineering to designate a higher or lower reliability requirement recognizes that the application of ANSI/ISA 84.00.01-2004¹ will yield a safety function whose reliability is well quantified; adjustment of the reliability target may be appropriate in light of this reduced uncertainty.

The discussion of non-SS criticality protections, in the last paragraph, emphasizes that ISA 84.00.01¹ sets a maximum allowable credit for protections implemented in the BPCS, which is non-safety. If protections, which were previously implemented as independent, distinct hardware elements, are migrated to DCS system, the risk reduction provided by those functions must be determined in light of this standard.

DESIGN INPUT

Merely defining that the design must meet the requirements of ISA 84.00.01-2004¹ is insufficient. The implementation of the ISA standards requires a team approach. At a minimum, the team should include nuclear criticality engineering, design engineering and design authority engineering. At least one member of the team should be an expert on the application of the ISA standard. A safety requirements specification for the SIF must be developed that includes items listed below:

- Identification of the safety function. Define the safe state of the process. The complete description of the safety function should be provided including requirements such as the maximum allowed shutoff valve leakage. If the safe state involves sequencing, then the required sequencing should be identified.
- Required modes of operation
- The target SIL of the SIF
- The required operating range and analytical safety limit of the system should be specified.
- The response time required of the system, including time for operator action, from the detection of a hazardous event to the completion of the final control element action should be specified.
- Environmental/seismic/fire/NPH design requirements
- Desired system functional test interval
- Maximum acceptable nuisance/spurious trip rate
- Need for bypasses, manual trip or reset action by operator should be identified.

FACTORS THAT AFFECT SIL VERIFICATION

The following factors affect the verification of the PFDavg achieved by a design and its operation:

- Fail-safe design
- Equipment reliability
- Component/system redundancy
- Common cause failure fraction for redundant components
- Fault tolerance
- Diagnostic coverage of component/system failures
- Functional test interval
- Reliability of support systems
- Operator reliability
- Technology used (i.e. switch, analog sensor, or smart sensor)

DESIGN APPLICATION

The target SIL assigned to the SIF is the major driver for the architecture of the SIS. A SIL-1 system can be implemented with a simplex design. That is, for an automatic SIL-1 SIF it will normally require only one sensor, a logic device (i.e. relays, certified PLC), and a final element (i.e. valve, breaker). Figures 1 through 3 provide comparative examples of SIL designs that achieve the same function to shutdown a feed into a tank. The SIL-3 SIS design provides 100 times the RRF of a SIL-1 SIS design. The examples assume the same failure rate for common components and the same periodic test frequencies.

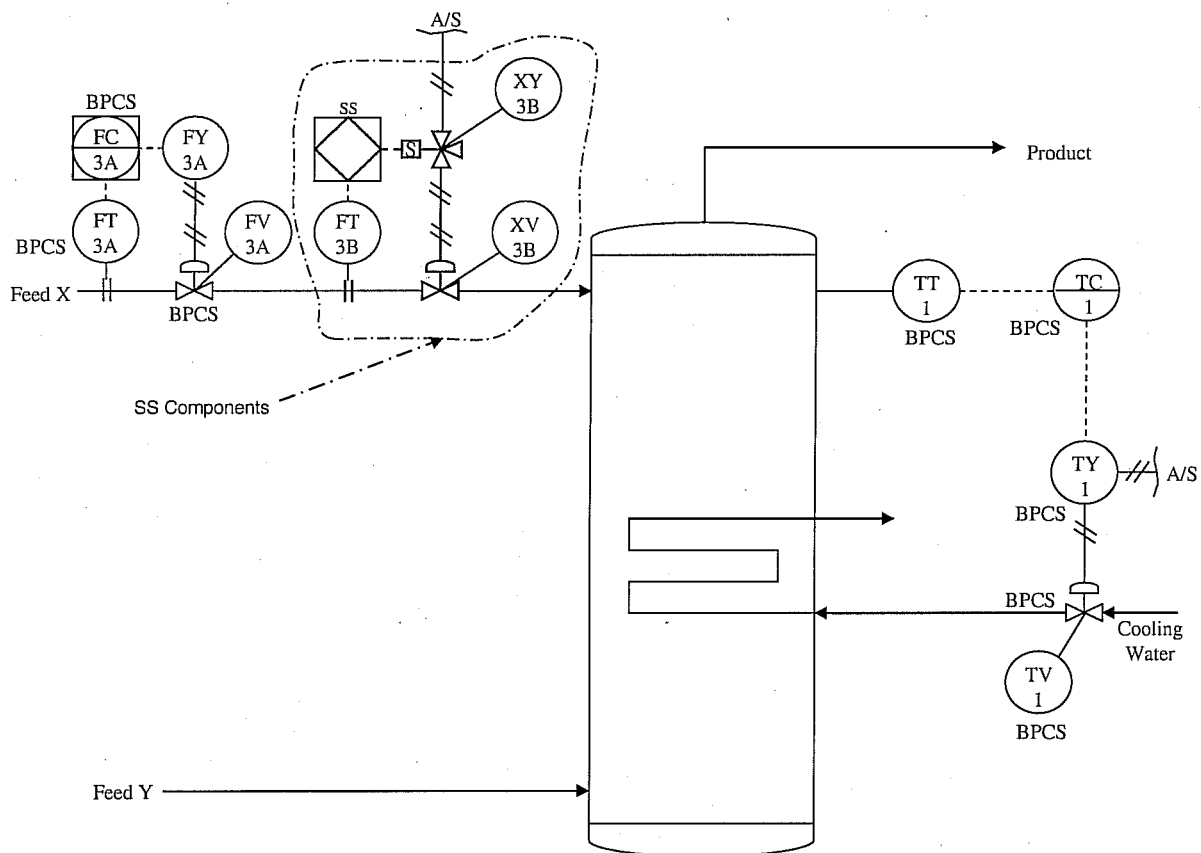


Figure 1 – SIL-1 Feed Blending.

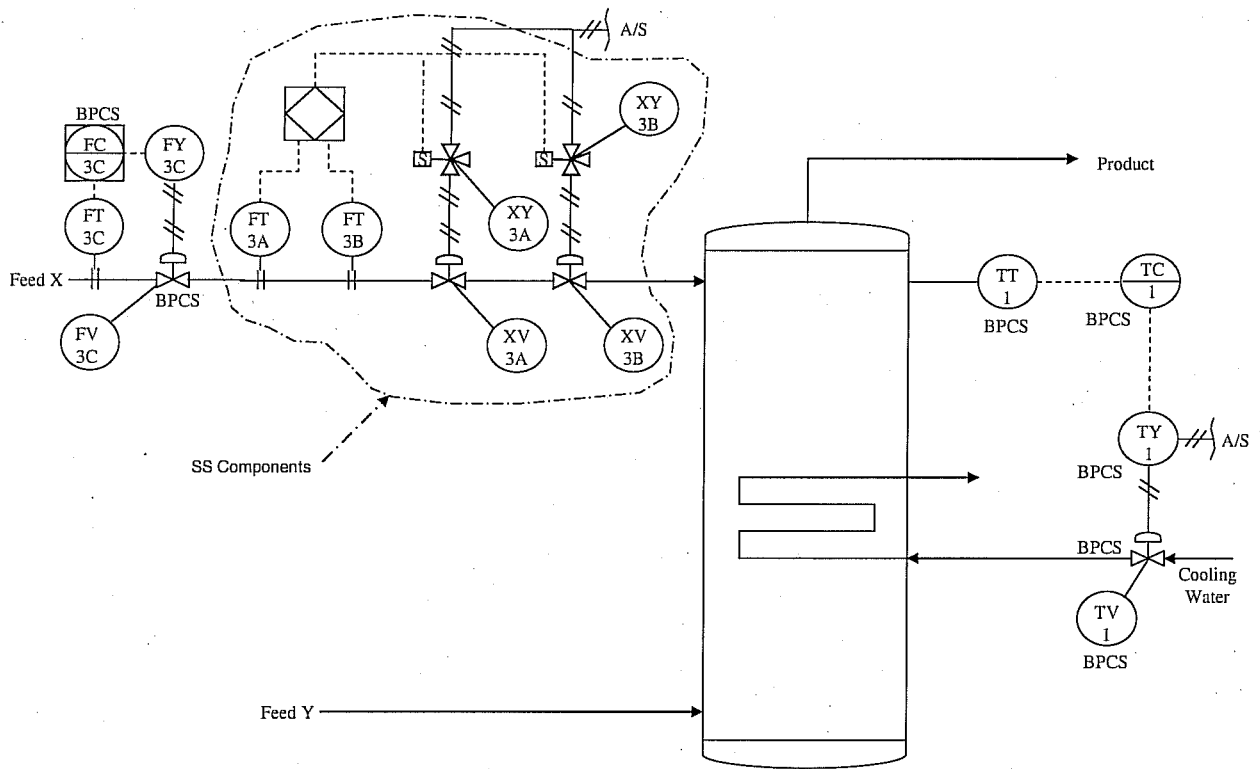


Figure 2 – SIL-2 Feed Blending.

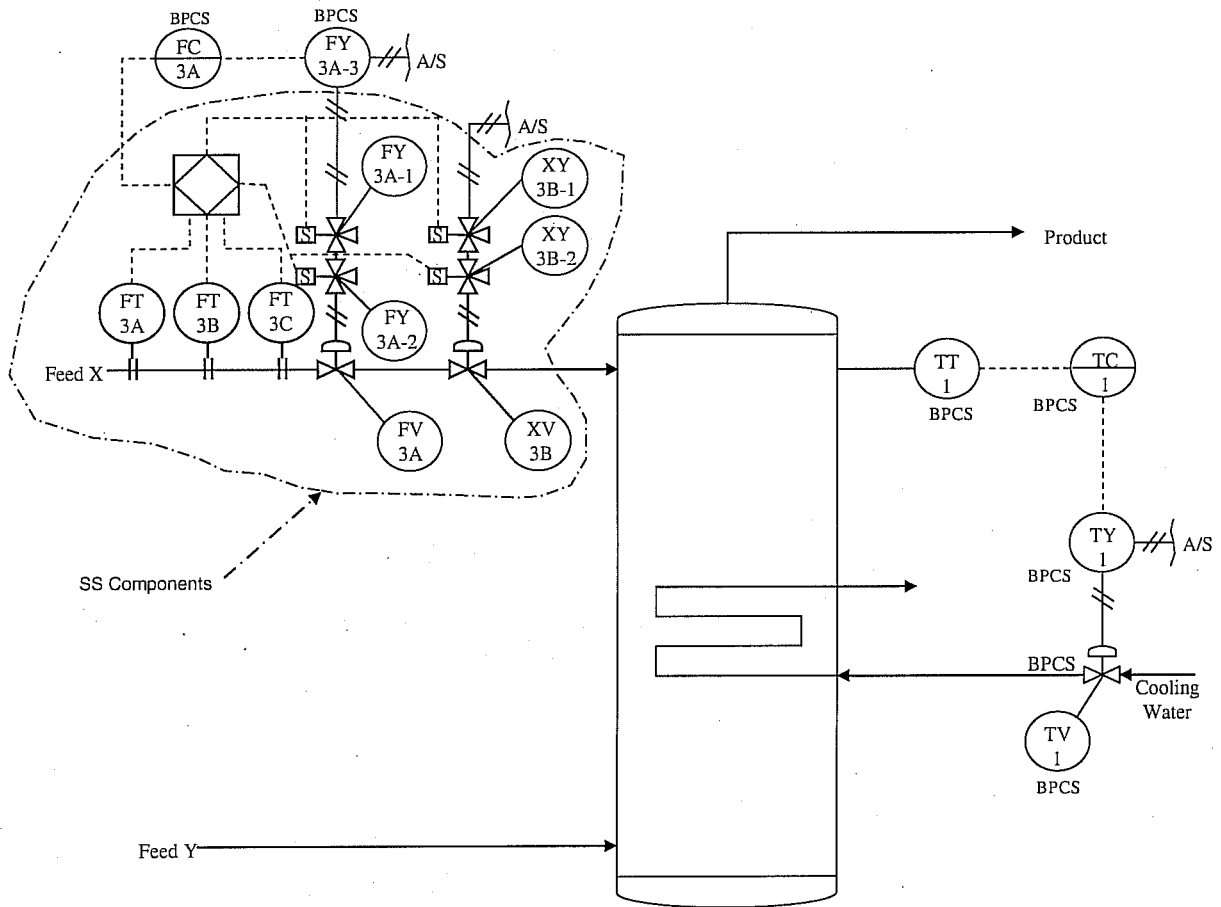


Figure 3 – SIL-3 Feed Blending.

CONCLUSION

ISA 84.00.01¹ provides a structured verifiable approach to design and maintain the probability of failure on demand limits established by DOE for nuclear criticality systems. The ISA Standard's methodology for providing a graded approach to the life cycle design of safety instrumented systems is recognized by the process industries both nationally and internationally. It provides a methodology to design a SIF to meet safety unavailability goals and the reliability of the SIF design over the life of the facility. Correct implementation the methodology requires a team approach between DSA preparers, the design authority, and the design agency. The team must include expertise in the ISA Standard.

The benefits of the ISA 84.00.01¹ process are clear understandable design requirements, and operation and maintenance requirements that provide the required risk reduction to meet ANS and DOE standards. The final SIF design is defensible; the reliability and effectiveness of the SIF is well quantified. Recognizing this increased assurance about the active-engineered criticality barrier, the Criticality Engineer has a new opportunity to optimize the set of barriers selected to prevent inadvertent criticality.

REFERENCES

1. ANSI/ISA 84.00.01-2004, Functional Safety: Safety Instrumented Systems for the Process Industry Sector
2. DOE G 421.1-1, Criticality Safety Good Practices Program Guide for DOE Nonreactor Nuclear Facilities
3. ANSI/ISA S84.01-1996, Application of Safety Instrumented Systems for the Process Industries
4. ANSI/ANS 8.1-1998, Nuclear Criticality Safety in Operations with Fissionable Material Outside Reactors
5. ANSI/ANS 8.3-1997, Criticality Accident Alarm System
6. SRS Engineering Standard 01703, Application of ISA 84.00.01-Part 1 for SRS Non-Reactor Nuclear Facilities