



DOE Standard for the Design of Safety Instrumented Systems at DOE Nuclear Facilities

Presentation at 2009 EFCOG Workshop

Pranab Guha
Office of Nuclear Safety Policy and Assistance





Presentation Overview



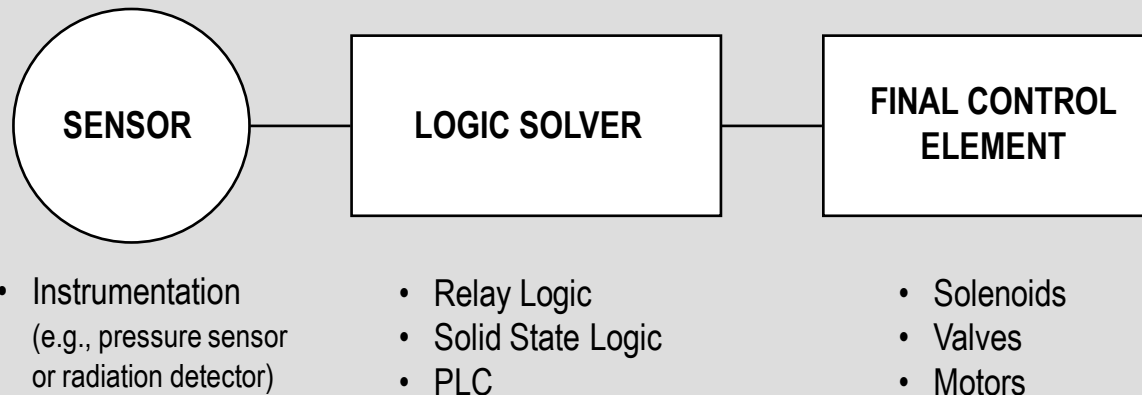
- Background
- New Approach for Design of Safety Instrumented Systems Used in Safety Significant Applications
- Examples of Use of New Guidance
- Summary



Background



Safety Instrumented System (SIS): Used to implement one or more safety functions. A SIS is composed of any combination of sensors, logic solvers, and final control elements.



DOE uses safety instrumented systems to prevent or mitigate the effects of potential accidents.



Background (cont.)



- SISs are used in nuclear facilities in both Safety Class and Safety Significant applications.
- DOE Order 420.1B, *Facility Safety*, provides requirements and DOE Guide 420.1-1 provides implementing guidance that points to application of industry standards.
- **Safety Class SIS:** Nuclear Power Industry Standards referenced and applied in practice.
- **Safety Significant SIS:** Several Industry Standards referenced in Guide 420.1-1, but their application is not well defined.

Note: Proposed Standard only addresses Safety Significant SISs



Applicability and Scope of the SIS Standard



- **Applicability:** Safety Significant SISs that include instrumentation and controls that are either analog or digital systems (including computer-based systems)
- **Scope:**
 - Guidance for use of Process Industry Standard – ANSI/ISA 84.00.01 – 2004 – Part 1 (IEC 61511-1 Mod), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements* (ISA 84)
 - Additional guidance on:
 - Commercial grade dedication
 - Software quality assurance
 - Human factors engineering
 - Installation and testing
 - Operation and maintenance



Design Approach



ISA 84 is a performance-based standard that covers the entire lifecycle of a safety instrumented system. The ISA 84 design approach can be broken down into five steps:

- Step 1:** Perform a hazard analysis and develop overall safety requirements.
- Step 2:** Allocate safety requirements to safety functions, including safety instrumented functions.
- Step 3:** Design safety instrumented systems and safety software.
- Step 4:** Testing, installation, commissioning, and safety validation of integrated safety instrumented systems.
- Step 5:** Operation and maintenance, modification and retrofit, decommissioning, or disposal phases.



Step 1: Perform Hazard Analysis



- Initial focus: “How much risk reduction will be required throughout the SIS life cycle?”
- DOE uses the criteria of DOE STD 3009, DOE Order 420.1B, and DOE STD 1189 to:
 - Perform the Hazard Analysis;
 - Determine the likelihood and consequence of event scenarios;
 - Establish the functional classifications; and
 - Design requirements for the safety systems.
- Design is built in layers of defense, called Independent Protection Layers (IPLs), to protect against the release of hazardous materials.
- One of the protection layers could be the SIS designated for preventing or mitigating the hazardous event.



Step 2: Allocate Safety Requirements



- Safety Requirements are “allocated” to different “safety layers” with the SIS being a potential safety layer.
- ISA 84 uses a graded approach by defining needed robustness, using a Safety Integrity Level (SIL) as a figure of merit.
- There are four SIL levels (SIL 1 to SIL 4) expressed in reliability terms.
 - Probability of failure on demand-average (PFDavg).
 - The numerically higher the SIL, the higher the reliability of the SIS.



Step 2: Allocate Safety Requirements (cont.)



SIL Level	Probability of Failure On Demand (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 $\leq 1,000$ RRF
SIL-3	$< 10^{-3}$ to $\geq 10^{-4}$ PFDavg	$> 1,000$ to $\leq 10,000$ RRF
SIL-4*	$< 10^{-4}$ to $\geq 10^{-5}$ PFDavg	$> 10,000$ to $\leq 100,000$ RRF

* Note: SIL-4 is not used in the Process Industry Sector



Step 2: Allocate Safety Requirements (cont.)



- ISA 84 (Part 3, Annex C) provides an example of a SIL determination method called the Safety Layer Matrix (SLM).
- SLM is used to determine the SIL of a SIS classified as safety significant.
- The SLM accounts for:
 - The likelihood/consequence of events; and
 - The number of Independent Protection Layers (IPLs) that are credited for a specific safety function as defined by hazard analysis and DOE STD 3009.



Step 2: Allocate Safety Requirements (cont.)



- The SLM is a qualitative SIL determination method.
- The proposed method to utilize the SLM is to:
 - Determine the hazard likelihood category;
 - Determine the number of “credited” IPLs; and
 - Identify SIL level from the grid intersection on SLM.

Safety Layer Matrix SIL Determination Methodology				
No. of IPLs (including SIS)	3	SIL-1	SIL-1	SIL-1*
	2	SIL-1	SIL-1	SIL-2*
	1	SIL-2*	SIL-2*	SIL-3*
Hazardous Event Likelihood		Extremely Unlikely	Unlikely	Anticipated

* Consider increasing the SIL level or credit an additional IPL for chemical events with potential of significant impact to the public or fatalities of immediate collocated workers.



Step 2: Allocate Safety Requirements (cont.)



- Rules on the use of the qualitative Safety Layer Matrix:
 - IPLs may include all credited passive safety features, a Specific Administrative Control (SAC), SC and SS mechanical and/or process systems, administrative control program for worker protection, and the SIS itself.
 - Regardless of the number of IPLs credited, a safety significant SIS will have a SIL of no less than SIL 1.
- The determined SIL is the required minimum performance level of the SIS as measured by the PFD_{avg} .
- The SIL is a design requirement and the objective for design decisions, component specifications, and procurements.



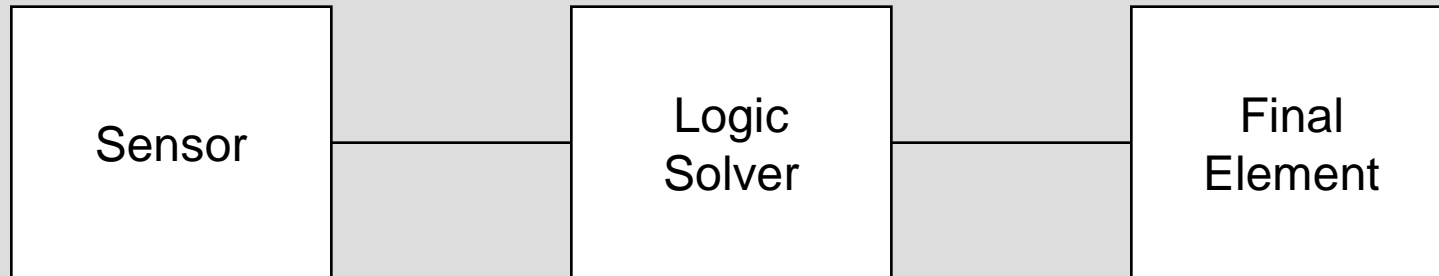
Step 3: Design SIS



- Factors that can affect the PFD_{avg} may be considered in the design process.
 - Component failure rate (λ^D)
 - Redundancy of structures, systems, and components
 - Voting (e.g., one out of two or two out of four)
 - Testing frequency (TI)
 - Diagnostic coverage (DC)
 - Common cause failure (β)
 - Human factors
 - Technology (i.e., digital vs. analog)
 - Software integrity (e.g., language complexity, failure detection)



Step 3: Design SIS (cont.)



Common Voting Architectures

1001
1002
2002
2003

1001
1002
2002
2003

1001
1002
2002

$$PFD_{SIS} = PFD_{PT} + PFD_{LS} + (PFD_{SOV} + PFD_{VALVE})$$



Step 3: Design SIS (cont.)



$$1001 \quad PFD_{avg} = \frac{\lambda^D * TI}{2}$$

$$1002 \quad PFD_{avg} = \left[\frac{\lambda^D * TI}{2} \right]^2 + [\beta * \lambda^D * TI/2]$$

$$2002 \quad PFD_{avg} = 2 * \left[\frac{\lambda^D * TI}{2} \right] + [\beta * \lambda^D * TI/2]$$

$$2003 \quad PFD_{avg} = 3 * \left[\frac{\lambda^D * TI}{2} \right]^2 + [\beta * \lambda^D * TI/2]$$



Step 3: Design SIS (cont.)



- **Software Quality Assurance (SQA):** SIS must meet safety software quality assurance requirements of DOE Order 414.1C and Guide 4141.1-4.
 - Clarification relative to SIS terminology (e.g. application and embedded software)
 - Crosswalk between ISA 84 and G 414.1-4 software quality assurance requirements
- **Human Factors Engineering (HFE):** The standard provides additional details for HFE considerations that are implemented during the SIS design process thereby ensuring that actions necessary for safety are performed correctly and in a timely manner (e.g., task analysis, human reliability analysis, testing, etc.).



Step 3: Design SIS (cont.)



- **Procurement and Commercial Grade Dedication (CGD):**
The DOE Standard endorses the use of CGD in addition to the methods provided in ISA 84 for qualifying components for use in a SIS. The Standard provides additional details for CGD providing reasonable assurance that an item will perform its intended safety function and can be deemed equivalent to an item designed and manufactured using appropriate national or international consensus standards.



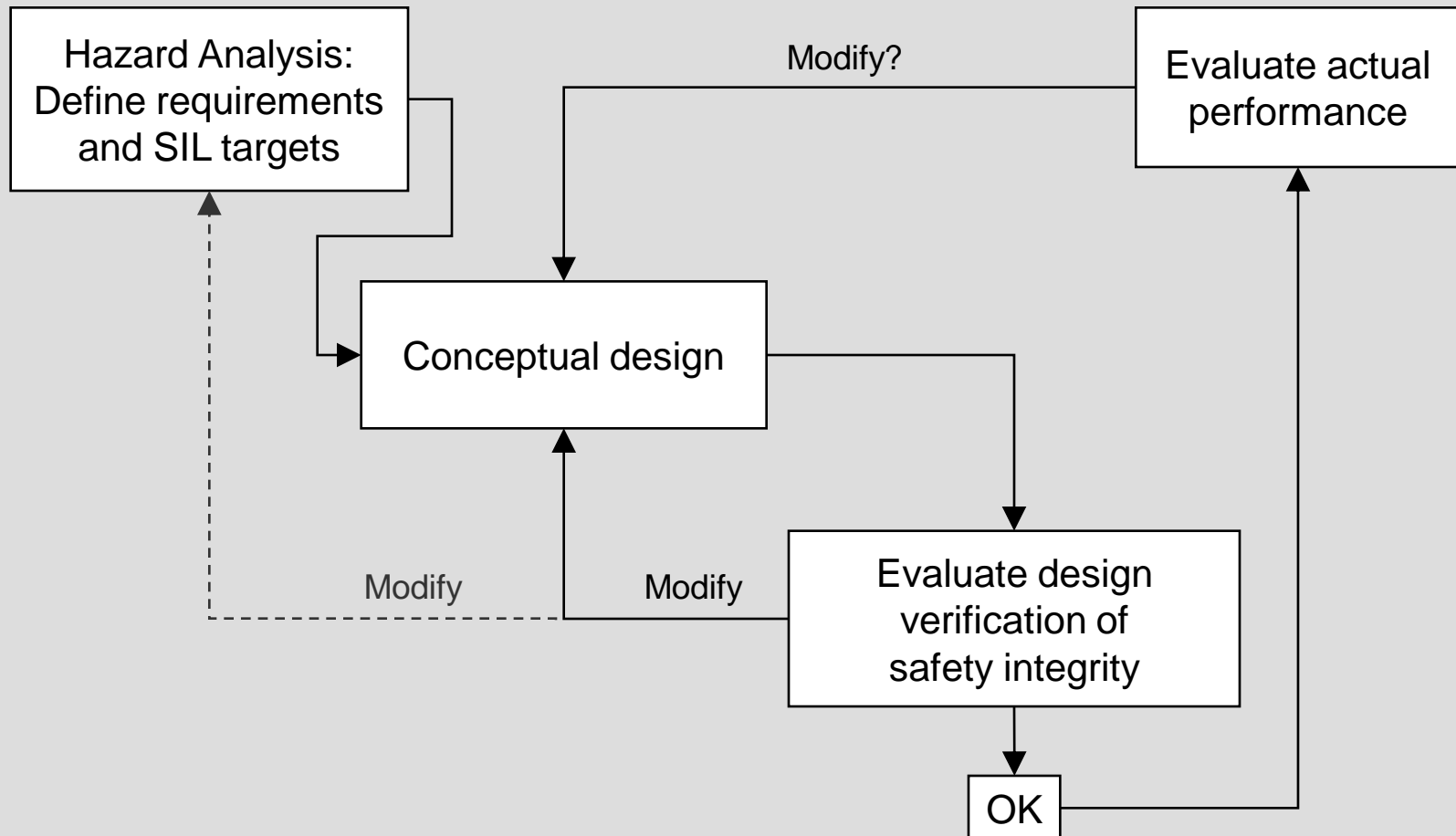
Steps 4 & 5: Testing, Installation, Verification, Operation, and Maintenance



- The SIL should be verified at the end of the detailed design to ensure that the design can achieve the assigned PFD_{avg} .
- The final SIL verification is performed after installation and/or modification.
- The Standard requires verification that the design as installed and maintained complies with the assigned SIL.
- The verification calculation requires a level of understanding and expertise about the factors that affect the PFD_{avg} for a device and system and the ability of the device or system to perform the safety function.

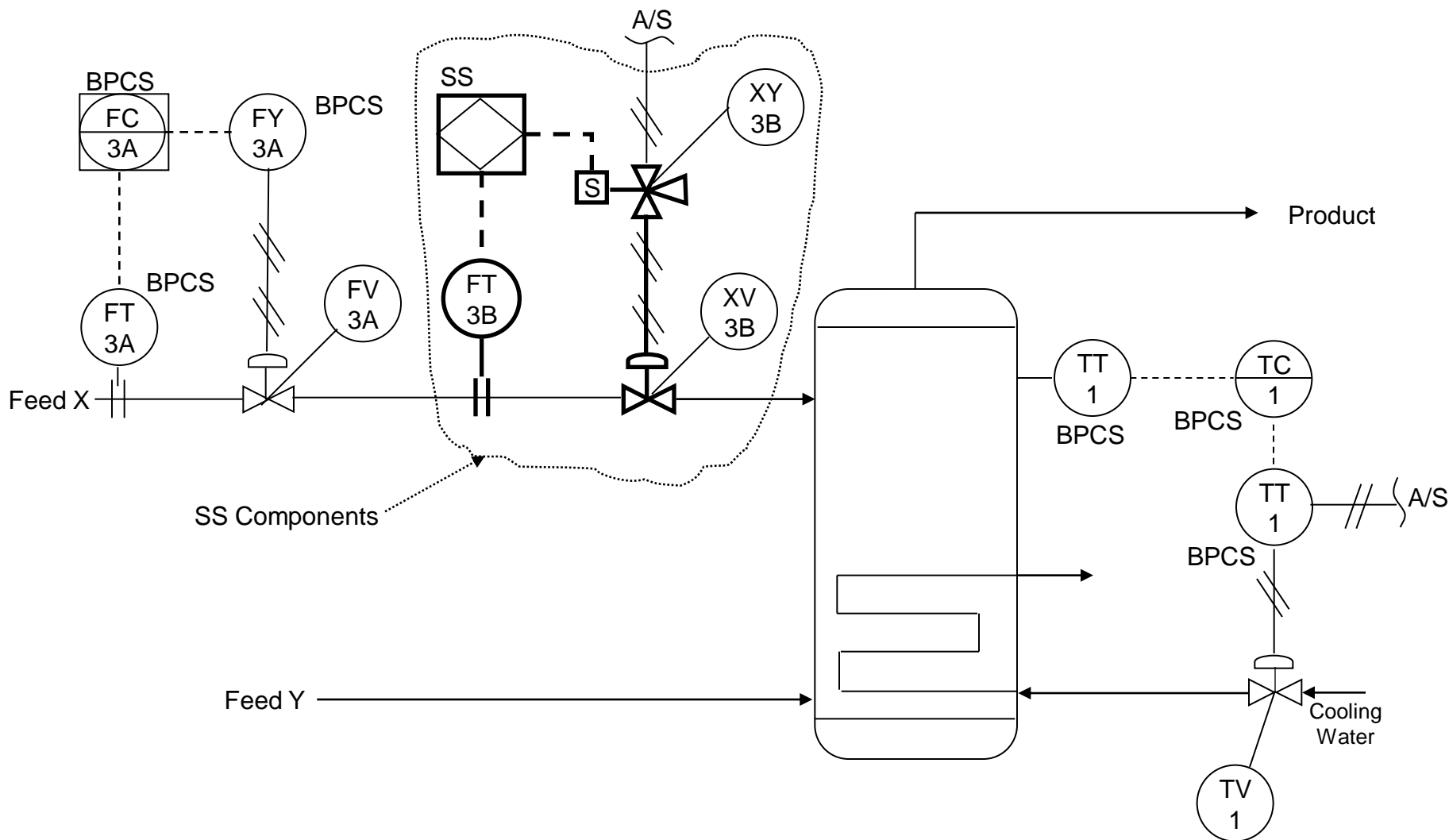


SIS Life Cycle



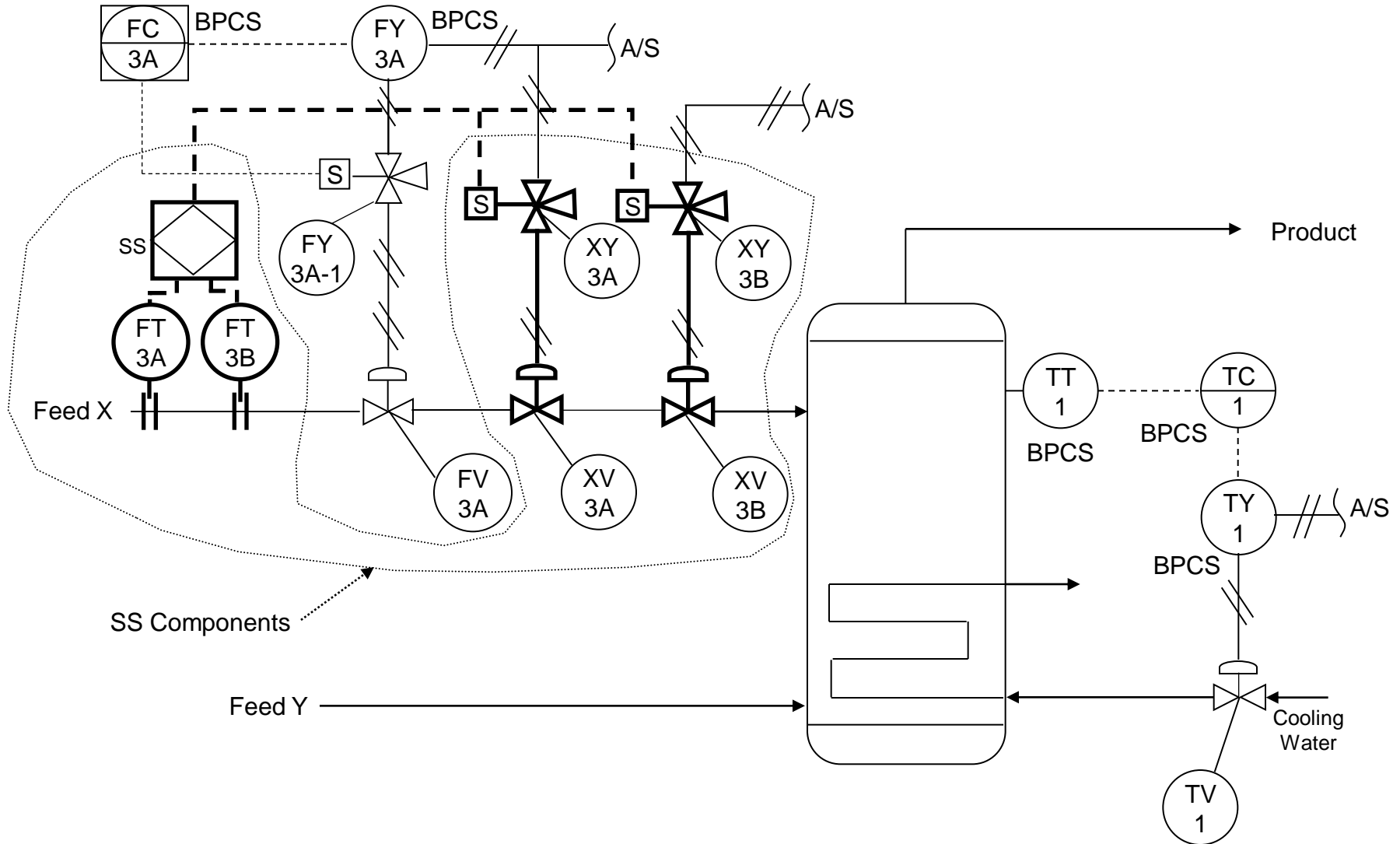


SIL-1 Design Example



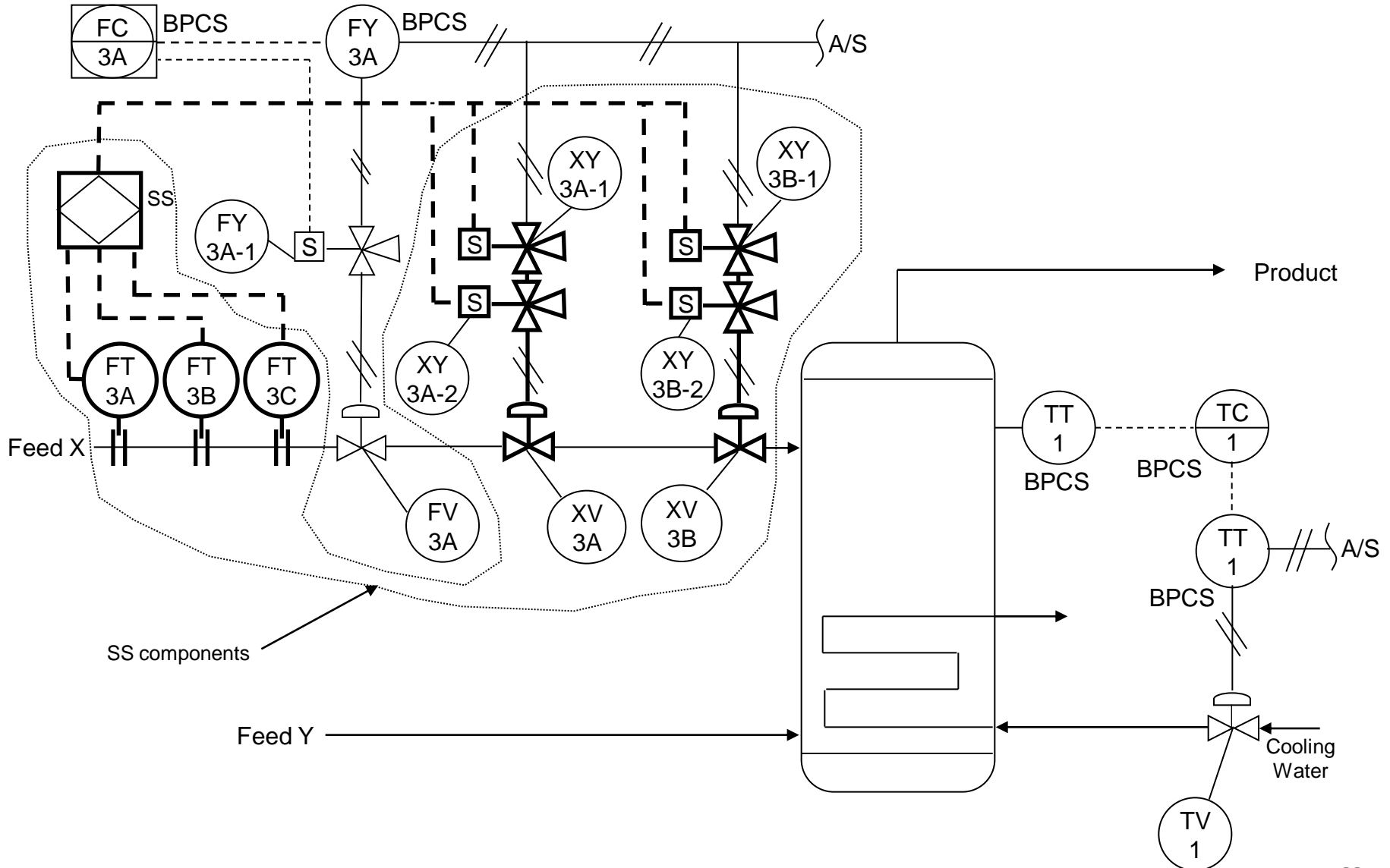


SIL-2 Design Example





SIL-3 Design Example





Summary



- DOE will benefit from more specific guidance for SISs used in safety significant applications which also address digital instrumentation and controls.
- Use of ISA 84 will provide appropriate design, safety, and operation criteria to ensure reliable design of safety significant SISs.
- DOE Standard is under development that provides an approach for use of ISA 84 within DOE's Safety Analysis and Facility Design requirements and practices.



Contact Information



Pranab Guha

Office of Nuclear Safety Policy and Assistance
Office of Nuclear Safety, Quality Assurance and Environment
Office of Health, Safety and Security

Tel: 301-903-7089

Fax: 301-903-6172

pranab.guha@hq.doe.gov