DOE-STD-1195-2011
Design of Safety Significant Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities

Pranab Guha
Office of Nuclear Safety Policy and Assistance

Presentation Overview

I. Scope & Applicability

II. Safety Instrumented System

III. Performance based design of safety significant instrumented systems

- Two Design Approaches
- Definitions
- SIL Table and Determination Process

IV. Design Examples

V. Summary

Scope

DOE-STD-1195-2011, *Design of Safety Significant Safety Instrumented Systems Used at DOE Nonreactor Nuclear Facilities provides guidance on:*

- the design, procurement, installation, testing, maintenance, operation, and quality assurance of safety instrumented systems (SIS) for safety significant (SS) functions; and
- how ISA 84.00.01-2004, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector,* can be utilized to support the design of a reliable SIS for SS functions.

Applicability

Applicability:

- New nonreactor nuclear facilities
- Major Modifications (as defined in 10 CFR 830 and DOE STD-1189)
- Facilities other than hazard category 1, 2, and 3 nonreactor nuclear facilities

Safety Instrumented System

Safety Instrumented System (SIS): An 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 control element(s).

- DOE uses SISs to prevent or mitigate the effect of potential accidents

- Instrumentation (e.g., pressure sensor or radiation detector)

- Relay Logic
- Solid State Logic
- PLC

- Solenoids
- Valves
- Motors

Two Design Approaches

DOE-STD-1195-2011:

Allows two approaches for the design of SS SIS:

1. Use of Commercial Nuclear Standards (used for both Safety Class and Safety Significant SISs)
   - DOE Guide 420.1-1
2. Use of Process Industry Standard (used for safety significant SISs)
   - ANSI/ISA 84.00.01-2004

ISA 84.00.01

ISA 84.00.01:

- Performance-based design to achieve an acceptable risk/reliability
- Two fundamental principles
  - Safety Integrity Levels (SILs)
  - Safety life cycle
- Graded approach based on required reliability
- Setpoint determination and uncertainty analysis (ISA 67.04.01)

Definition

Safety Integrity Level (SIL):

A discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to safety instrumented systems.

Independent Protection Layer (IPL):

A structure, system, component, or administrative control that prevents or mitigates a safety significant hazardous event to an acceptable condition.

Definition (cont.)

Probability of Failure on Demand average (PFDavg):

The average probability that an IPL, when demanded, will not 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.

SIL Table

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 ≤ 1,000 RRF
SIL-3	$< 10^{-3}$ to $\geq 10^{-4}$ PFDavg	> 1,000 to ≤ 10,000 RRF
SIL-4*	$< 10^{-4}$ to $\geq 10^{-5}$ PFDavg	> 10,000 to ≤ 100,000 RRF

* Note: SIL-4 is not used by DOE, also not used in the Process Industry Sector

SIL Determination Process

- It begins with hazards identification and risk analysis
- Safety Analysis per DOE STD 1189 and STD 3009
- Outcome of analysis is identification of SC and SS SSCs, including selection of controls
- Identify credited Independent Protection Layers (IPLs)
- One of the protection layers could be the SIS designated for preventing or mitigating the hazardous event
- DOE-STD-1195-2011 recommends the use of a SIL Table to determine the required SIL for the SIS

SIL Determination Table

DOE's approach is a
deterministic SIL determination method.

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

SIL Determination Notes

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 App B and C of DOE-STD-1189), the design authority may consider decreasing the SIL number of the SIS to SIL-1.

Permitted IPL Types

IPL Types:

- Credited passive safety design features
- Safety Class Systems
- Safety Significant Systems
- Specific Administrative Control (SAC)
- Administrative Control programs (ACs)
- An SIS whose SIL is being determined

Design Guidance

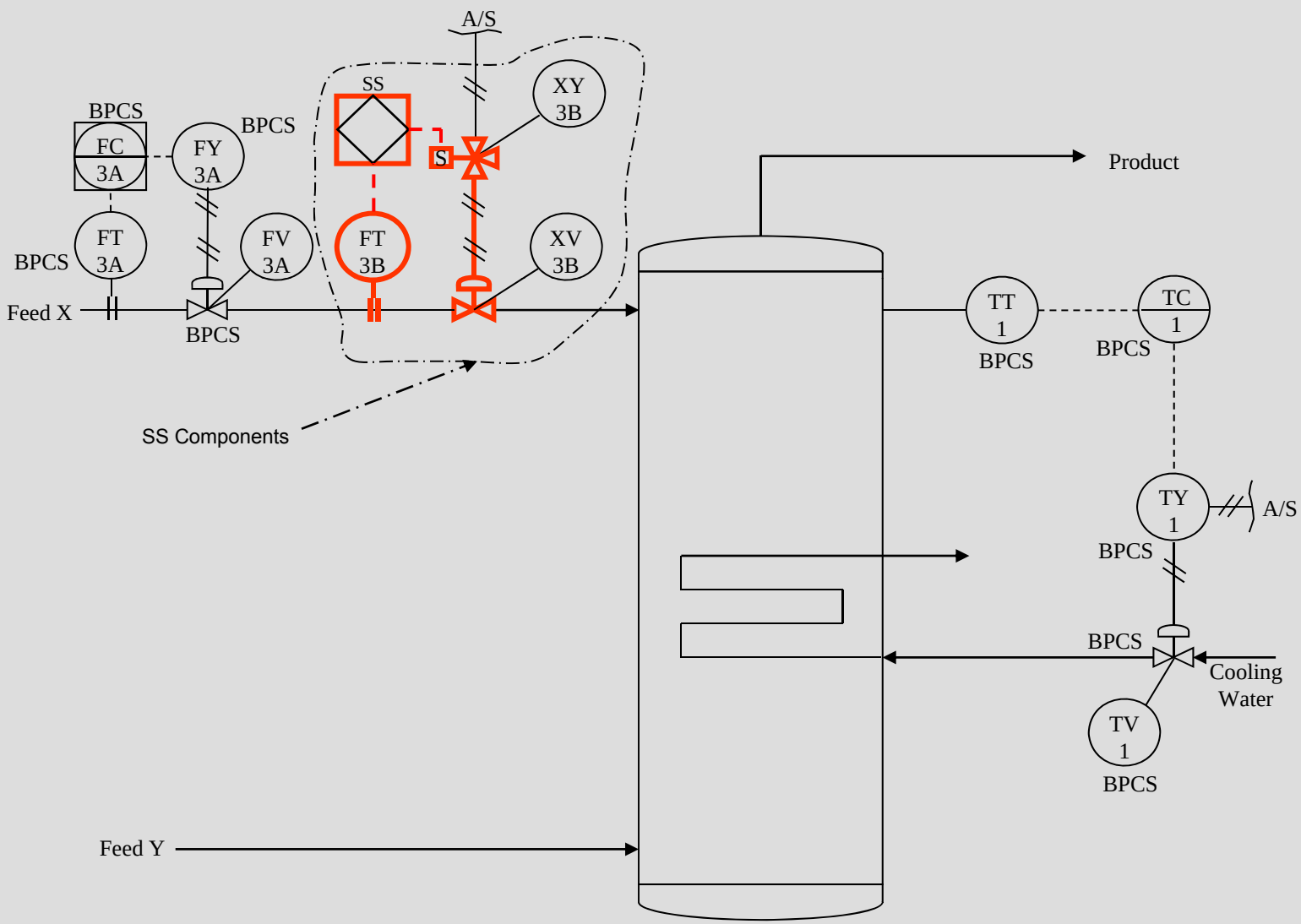
$$PFDavg_{(SIS)} = PFDavg_{(S)} + PFDavg_{(LS)} + PFDavg_{(FE)}$$

Design Guidance (cont.)

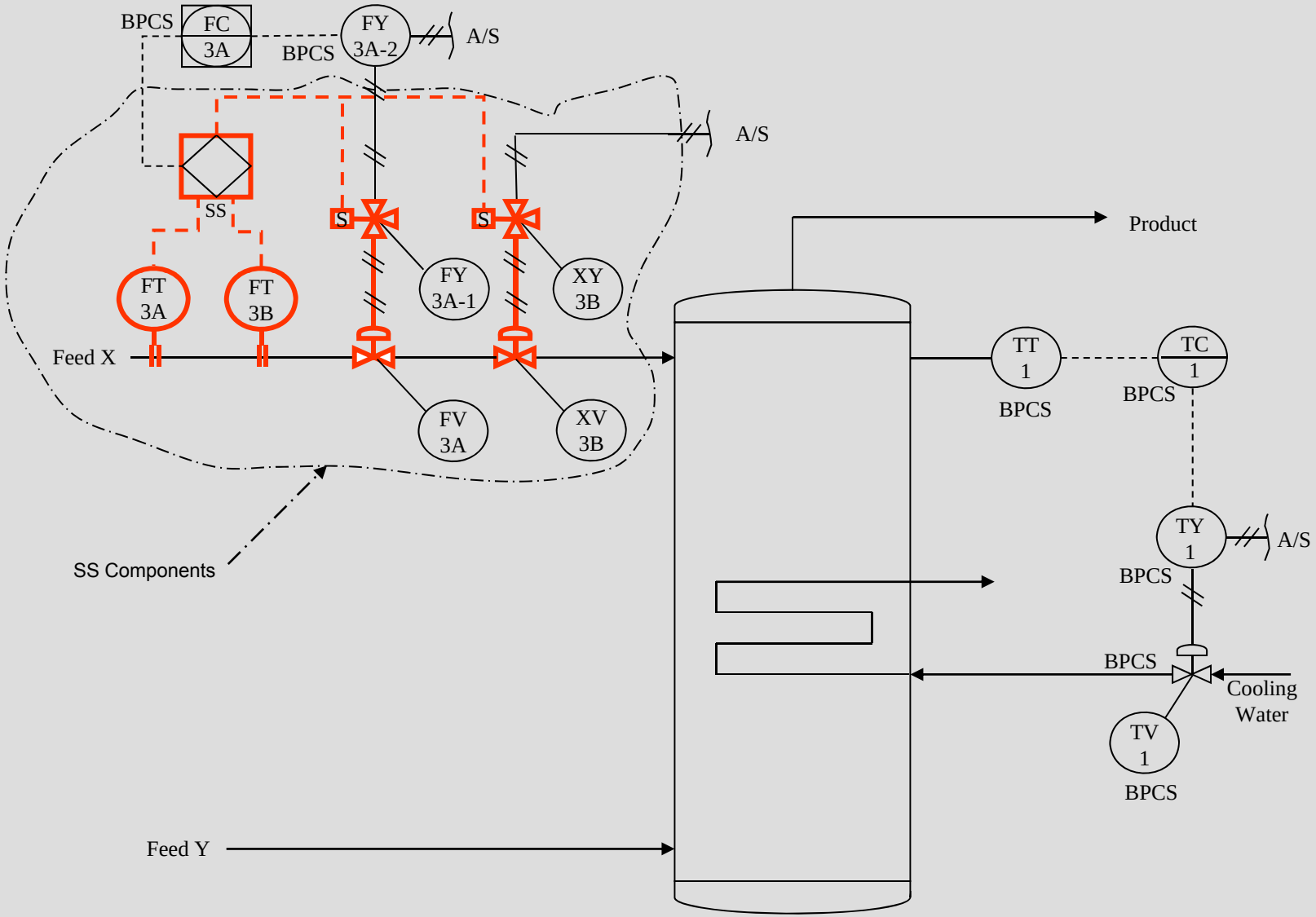
Factors affecting the PFDavg:

- Component failure rates
- Periodic test frequency
- Diagnostic coverage
- Common cause failure
- System configuration
- Technology
- Fault tolerance
- Diversity
- Human reliability
- Other SIS design issues

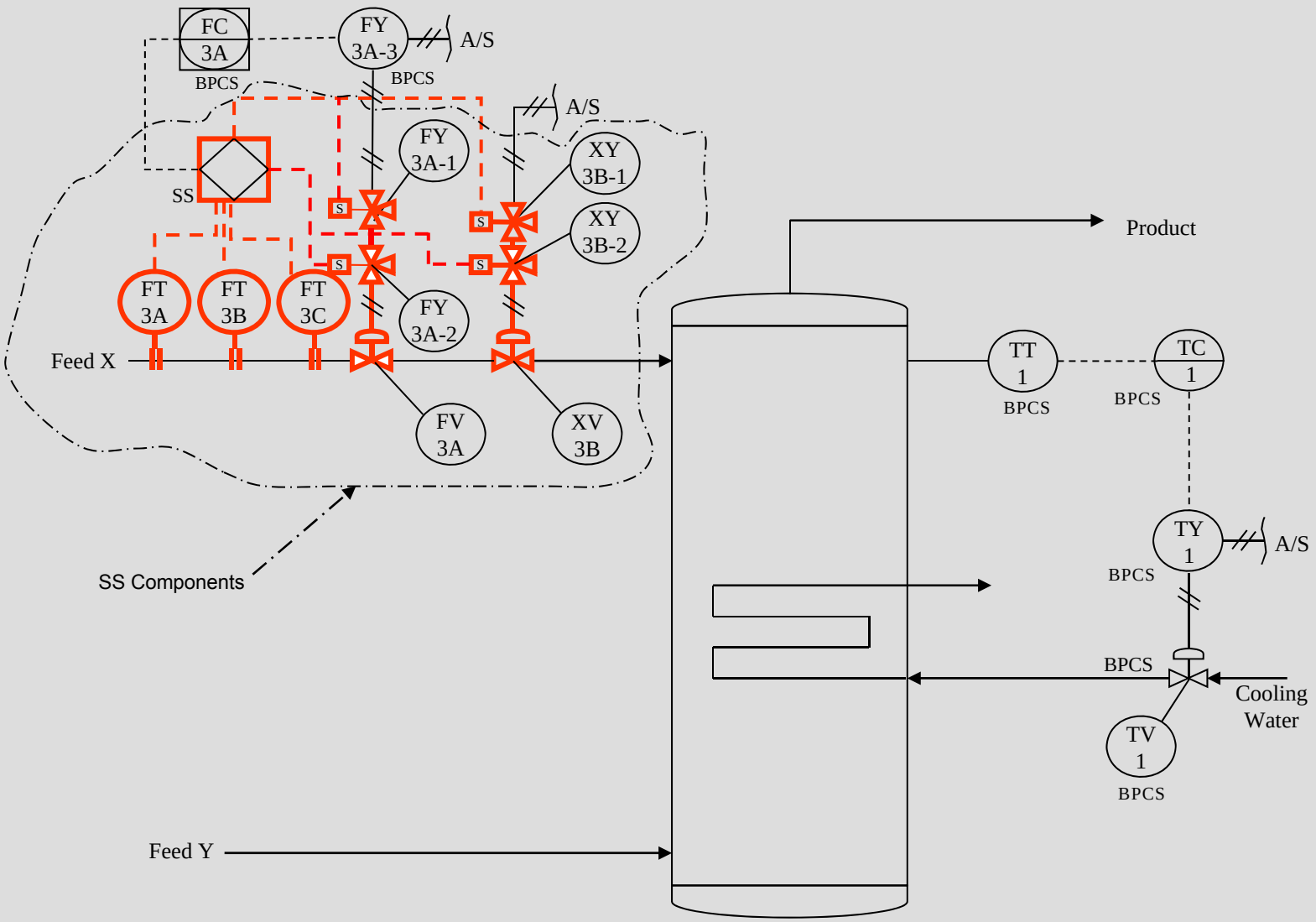
SIL-1 Design Example



SIL-2 Design Example



SIL-3 Design Example



Summary

- DOE will benefit from specific guidance for SISs used in safety significant applications which also address digital instrumentation and controls.
- Use of ISA 84.00.01 will provide appropriate design, safety, and operational criteria to ensure reliable design of SS SISs.
- DOE SIS Standard provides a deterministic approach for the use of ISA 84.00.01 within DOE's safety analysis and facility design requirements and practices.

Contact Information

Pranab Guha

Office of Nuclear Safety Policy and Assistance

Tel No. 301-903-7089

Pranab.Guha@hq.doe.gov