



Savannah River Site

EFCOG-SAWG

Safety Instrumented Functions
as Criticality Defenses



William H. Hearn

Lawrence T. Suttinger

Washington Savannah River Company

Outline

- Criticality Background
 - Double Contingency Principle
 - DOE Guide G 421.1-1
- SIS Background
 - Safety Instrumented System
 - Purpose of the 84.00.01 Standard
- Merging the methodologies
- Benefits

Criticality Background

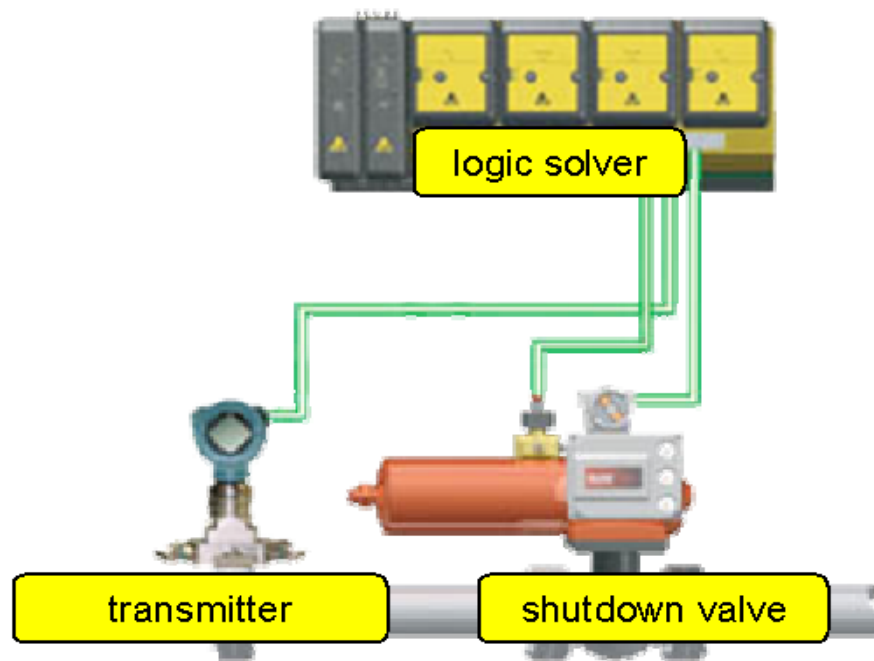
- **ANS 8.1 Double Contingency Principle**
 - “Process designs should incorporate sufficient factors of safety to require at least two unlikely, independent, and concurrent changes in process conditions before a criticality accident is possible.”
 - Prefer diverse parameters & methods

Background

- Criticality – Double Contingency Principle
 - Engineering judgment on reliability
 - No equipment reliability calculation
 - Independent barriers
- DOE Criticality Guide 421.1-1:
 - Reliability expectation
 - “the barrier will fail ... no greater than 1 in 100 demands”

Safety Instrumented System

- A **SIS** is typically **passive** and takes action when a dangerous condition is detected

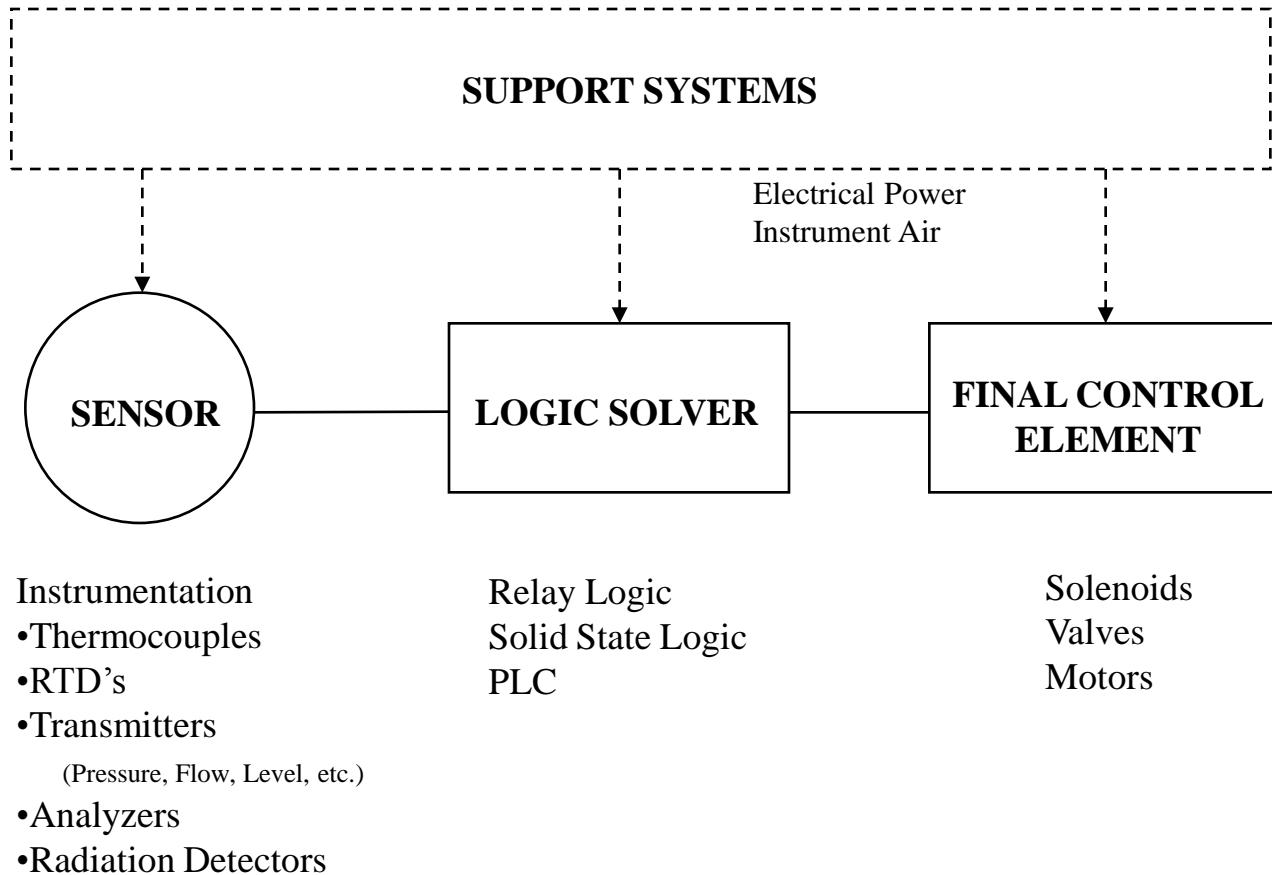


Evolution of SIS Loop
Emerson Confidential, Jan-05, Slide 18

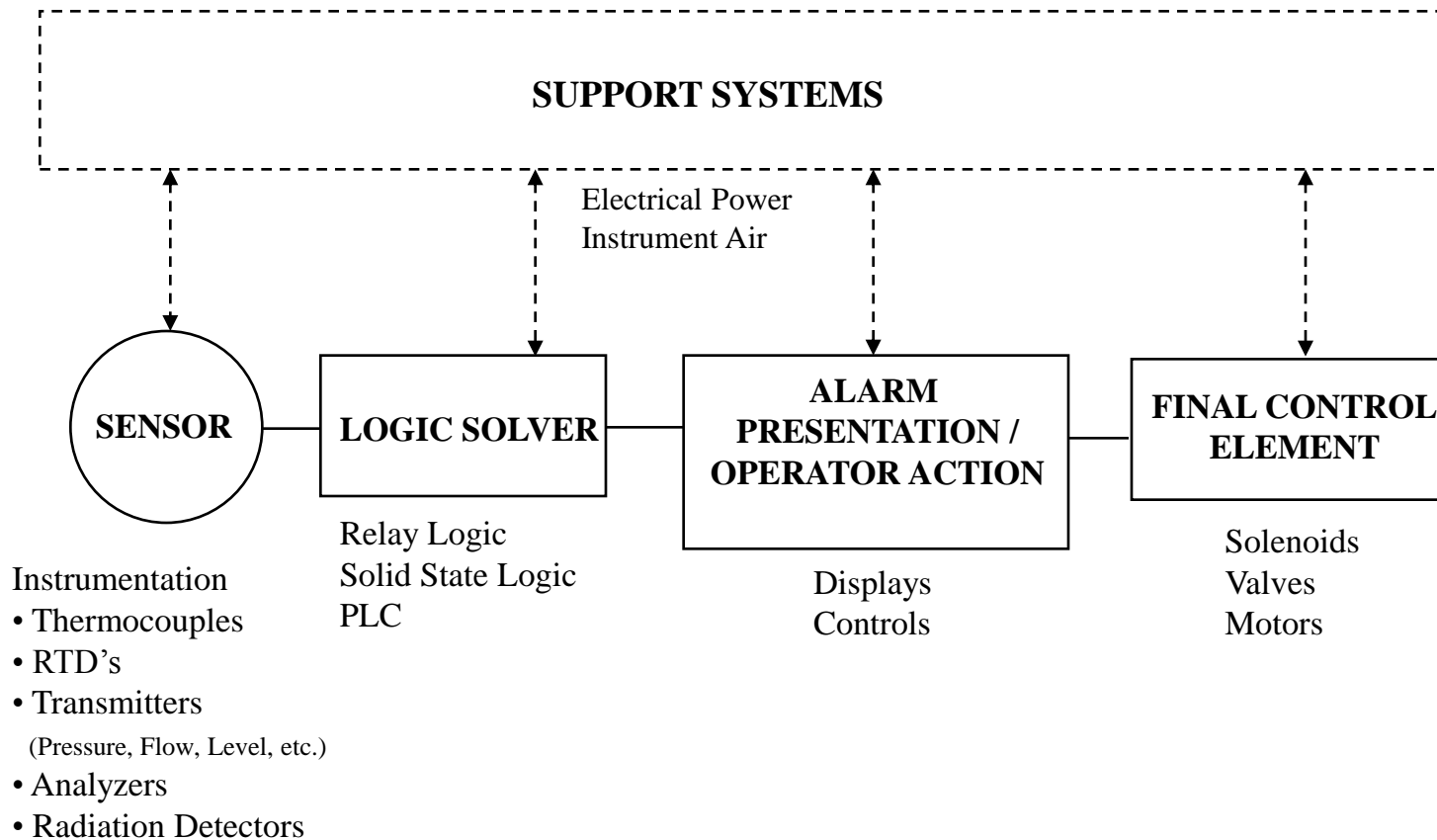

EMERSON
Process Management

SIS Block Diagram

Automatic Action

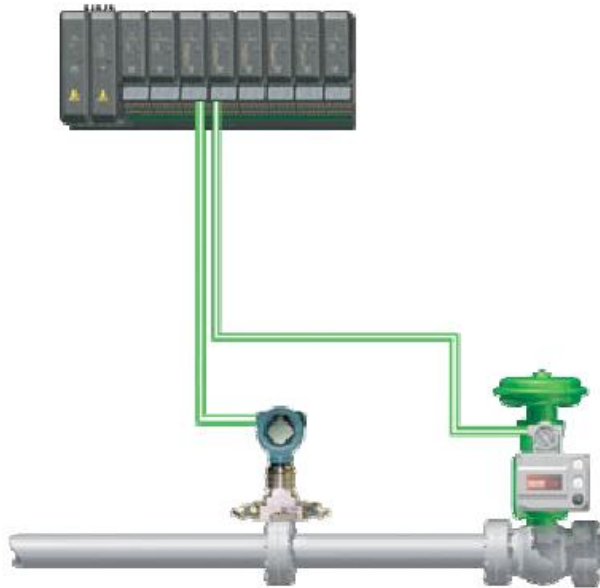


SIS Block Diagram Operator Actuation

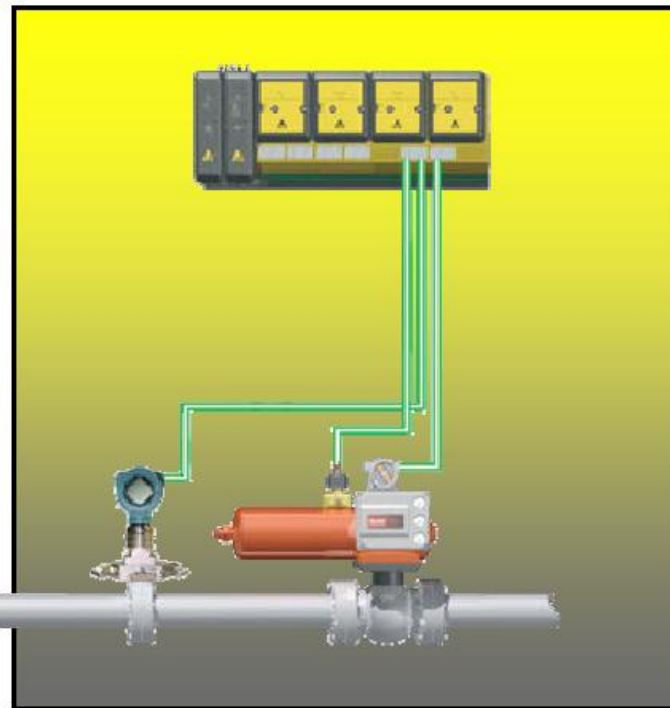


Independence of SIS

Basic Process Control System



Safety Instrumented System



Purpose of SIS & Standard

- The purpose of the safety instrumented system, in combination with other safety features, is to reduce the likelihood or consequences of a hazardous event to an acceptable level.
- The Standard gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system, so that it can be confidently entrusted to place and/or maintain the process in a safe state.

ANSI/ISA 84.00.01-2004

- Provides a graded approach to safety
(4 levels of safety)
- Requires verification of installed system reliability
- Requires fault tolerance for high reliability
 - Redundant field instruments and actuators
- Limits credit for non-safety control system
- Owner selects safety unavailability targets

SRS Standard 01703, Rev. 3

- Applies 84.00.01 methodology at SRS
 - Safety Significant SIFs
 - Includes SS Criticality SIFs
 - Requires performance monitoring
- Provides methodology to select reliability targets
- Points to DOE and ANS guidance for reliability targets

Risk and Reliability

- Basic Premise:
 - where safety instrumented systems are used, they have the ability to place and/or maintain the process in a safe state
- Graded approach to risk reduction
 - Safety Integrity Level – SIL
 - Reliability of your Safety Function
- Terms

Essential Jargon - PFD

- Probability of Failure on Demand

$$\text{PFD} = 1 - e^{-\lambda t}$$

This equation is for the probability of failure on demand at a given time of t between functional tests of a system or component

λ - Failure rate of the system/component*

*these rates are typically better than 1 per 100,000 hours

$$e^{-x} = 1 - x + \frac{x^2}{2!} - \frac{x^3}{3!} + \dots$$

$$\text{So PFD} = 1 - (1 - \lambda t + \frac{\lambda^2 t^2}{2!} - \frac{\lambda^3 t^3}{3!} + \dots)$$

... PFD = λt – very small factors

Essential Jargon

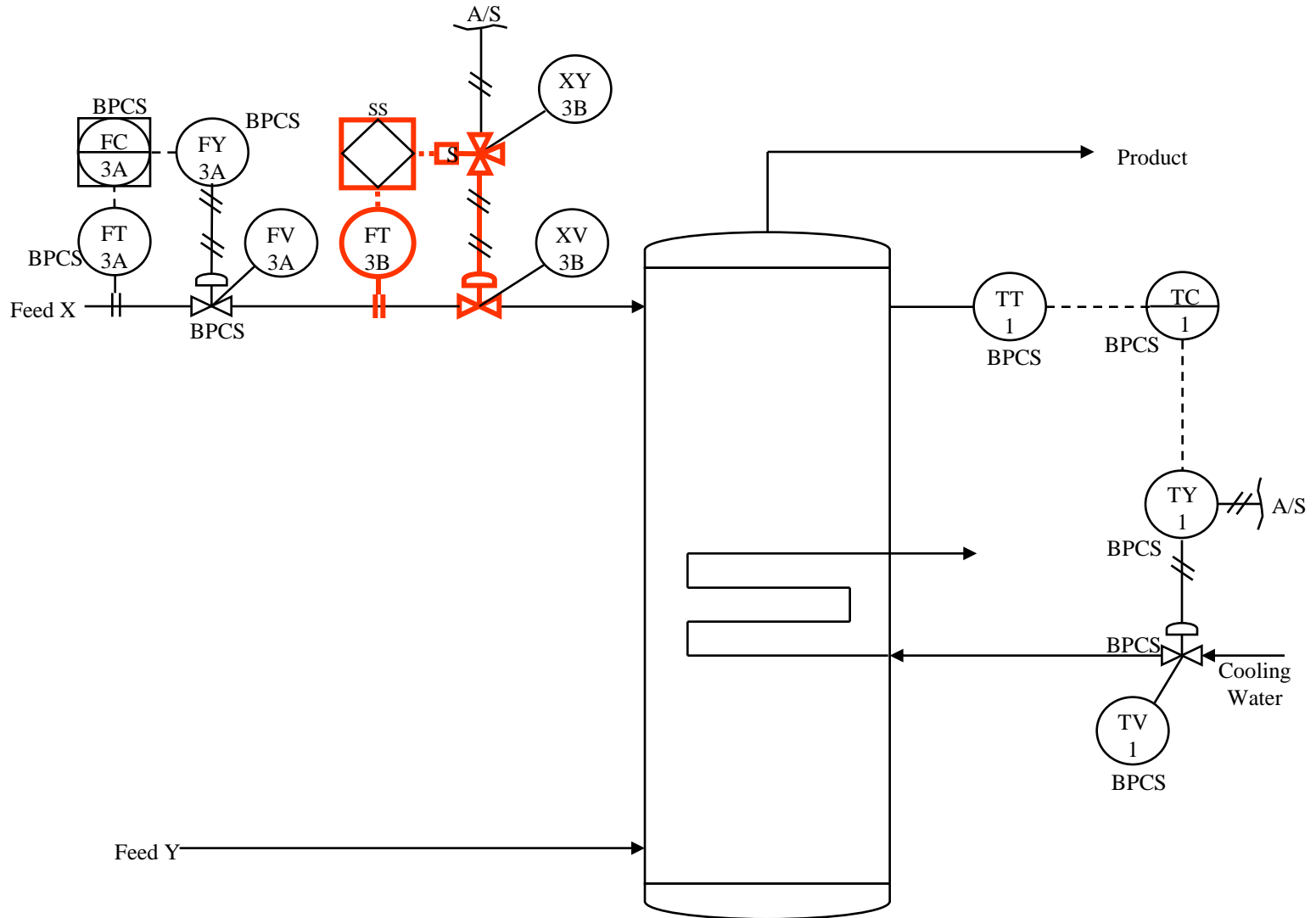
- Average Probability of Failure on Demand (PFD_{avg})
 - The average probability of a safety function or device failing to respond to a demand in a specified test interval.
 - $PFD_{avg} = \lambda * TI / 2$
 - Example: $PFD_{avg} = 2 \times 10^{-3}$
- Risk Reduction Factor (RRF)
 - RRF equals $1 / PFD$
 - Example: $PFD_{avg} = 2 \times 10^{-3} \Rightarrow RRF = 500$

Safety Integrity Level (SIL)

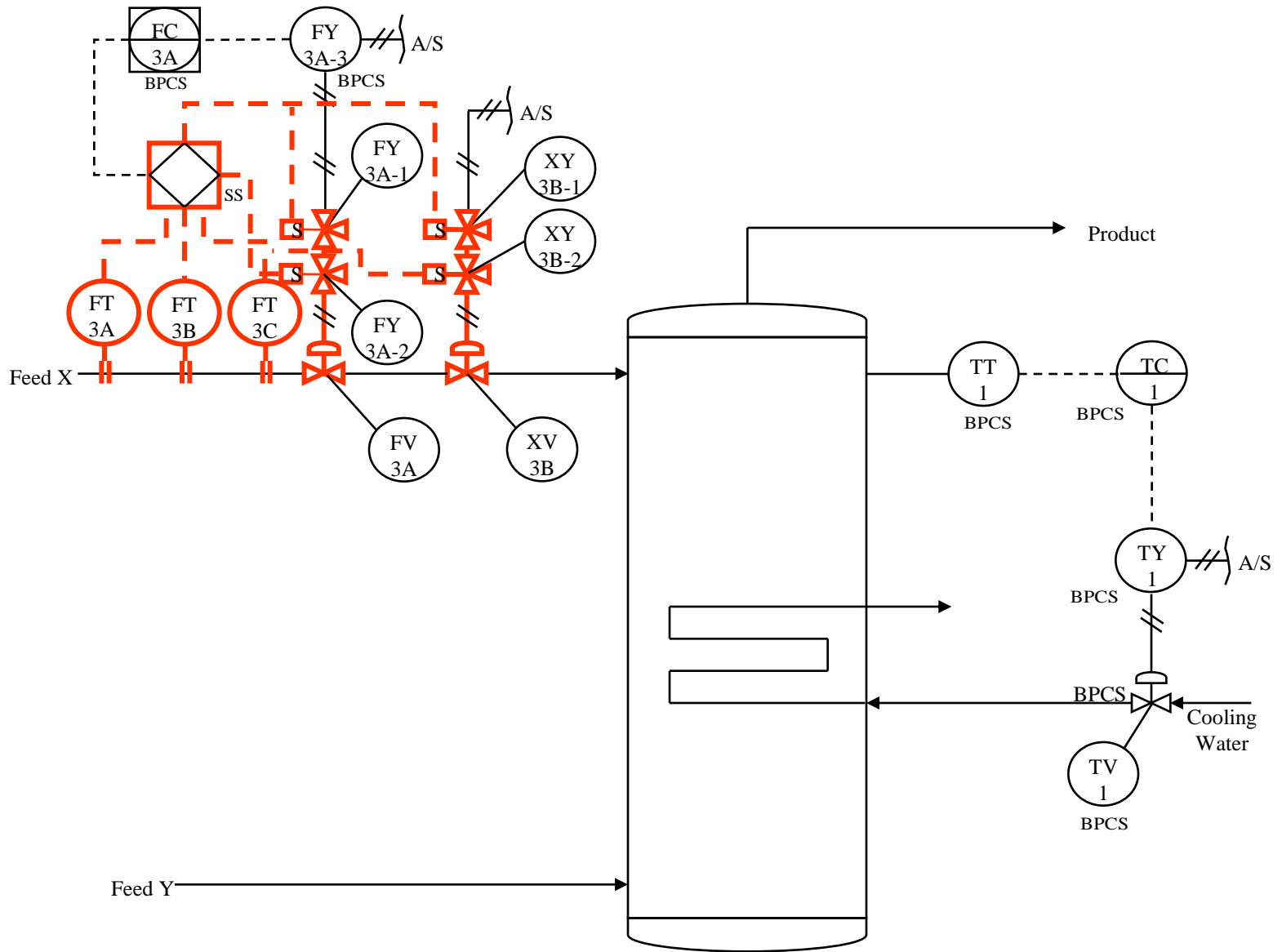
- SILs are Safety Integrity Levels.
- Ranges cover PFD_{avg} of the function.
 - SIL-1 10^{-1} to 10^{-2} PFD_{avg} ; RRF 10 to 100
 - SIL-2 10^{-2} to 10^{-3} PFD_{avg} ; RRF 100 to 1000
 - SIL-3 10^{-3} to 10^{-4} PFD_{avg} ; RRF 1,000 to 10,000
 - SIL-4 is not used at SRS.
- Fault Tolerance Requirements:
 - SIL-1 No Fault Tolerance
 - SIL-2 must tolerate 1 Fault
 - SIL-3 must tolerate 2 Faults

Factors Affecting Achieved SIL (PFDavg)

- Component failure rates
 - Safe failure fraction
- Periodic test frequencies
- Technology used (smart transmitters vs. analog devices)
- Diagnostic coverage
- System configuration
 - Redundancy
 - Common cause failure



EXAMPLE - SIL-1



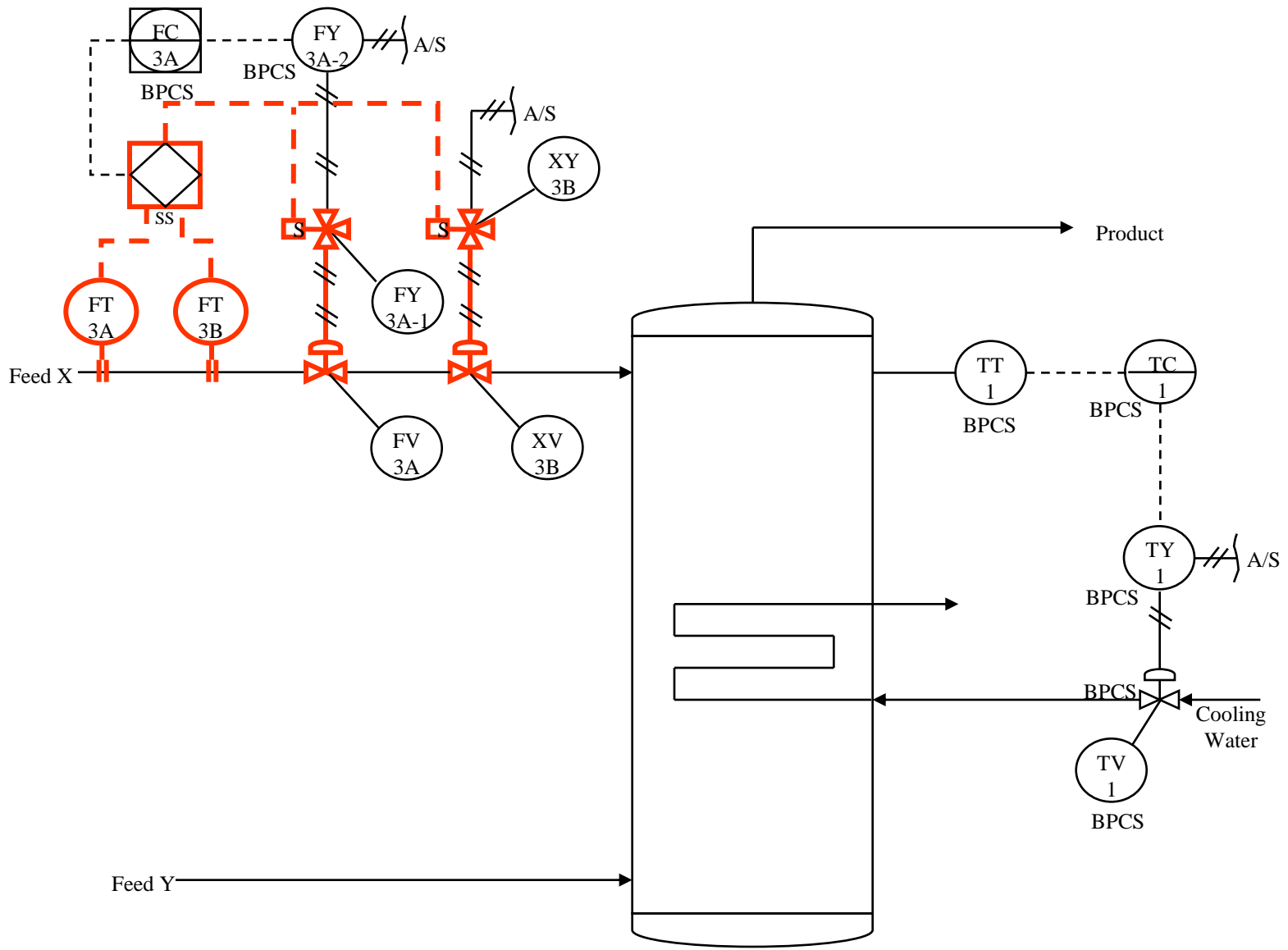
EXAMPLE - FEED BLENDING SIL-3

Criticality Engineering Role

- Set reliability targets
- Guidance from:
 - Current Safety Basis
 - Criticality - DOE Guide 421.1-1
- Design inputs:
 - Functional Safety Requirements
 - Process Safety Time
 - Trip Level
 - Test and Maintenance Frequencies
 - Operating Parameters

Application to Criticality

- ISA 84.00.01
 - Equipment reliability calculations
 - DOE Guide reliability target $\leq 1/100$ failures
 - SIL-2 in ISA 84.00.01
 - Only 1/10 in Basic Control System
- SIL-2 requirements
 - Fault tolerant design
 - RRF of 100 to 1000



EXAMPLE - SIL-2
EFCOG-SAWG 2007

Merging Methodologies

- From DOE G 421.1-1 :
 - While failure mode independence can be established, likelihood of failure cannot be well quantified.
 - Relies on independence of barriers
- ISA 84.00.01
 - Relies on equipment reliability calculations
 - Requires fault tolerance of SIL-2&3 designs

SIFs as Criticality Defenses

- Meet performance requirements
 - Goes beyond expectation of DOE Guide
 - Assured quantitative analysis
- Opportunity for reducing requirements
 - Layers
 - Administrative Backups

Benefits of Using ANSI/ISA 84.00.01

- Internationally accepted methodology
- Defined reliability of instrumented criticality system in terms of PFD_{avg}
- Provides proof of system reliability through verification calculation of achieved PFD_{avg}

Questions?