SIEMENS
Ingenuity for life

Reducing the human error impact on Safety Instrumented system (SIS)

Purdue Process Safety & Assurance Center
December 5, 2019

Your presenter

Charles M. Fialkowski, CFSE

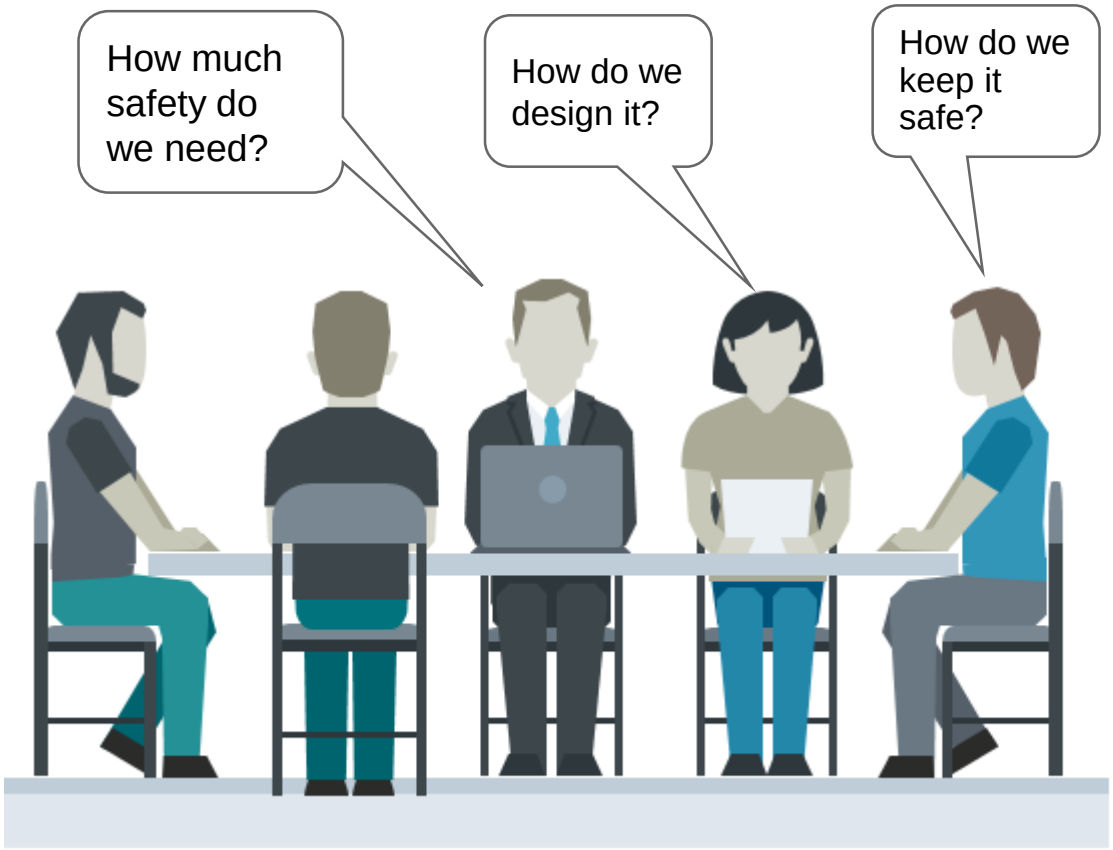
Charles.Fialkowski@siemens.com

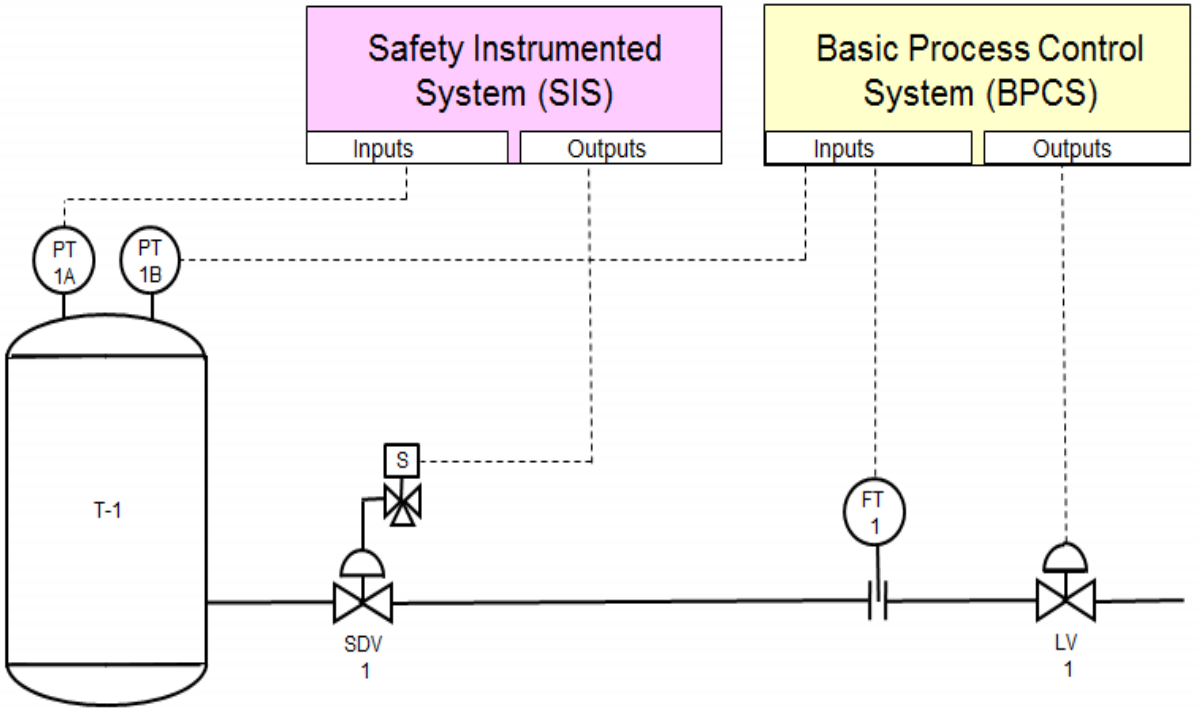
- Siemens Director for Process Safety (I&C)
- ISA 84 voting member
- 25 years of Process Industry experience
- ISA course developer/instructor (BMS and SIS)
- Electrical Engineering (OSU)
- Descendent of Cyrus McCormick

Safety Instrumented System (SIS)

SIEMENS
Ingenuity for life

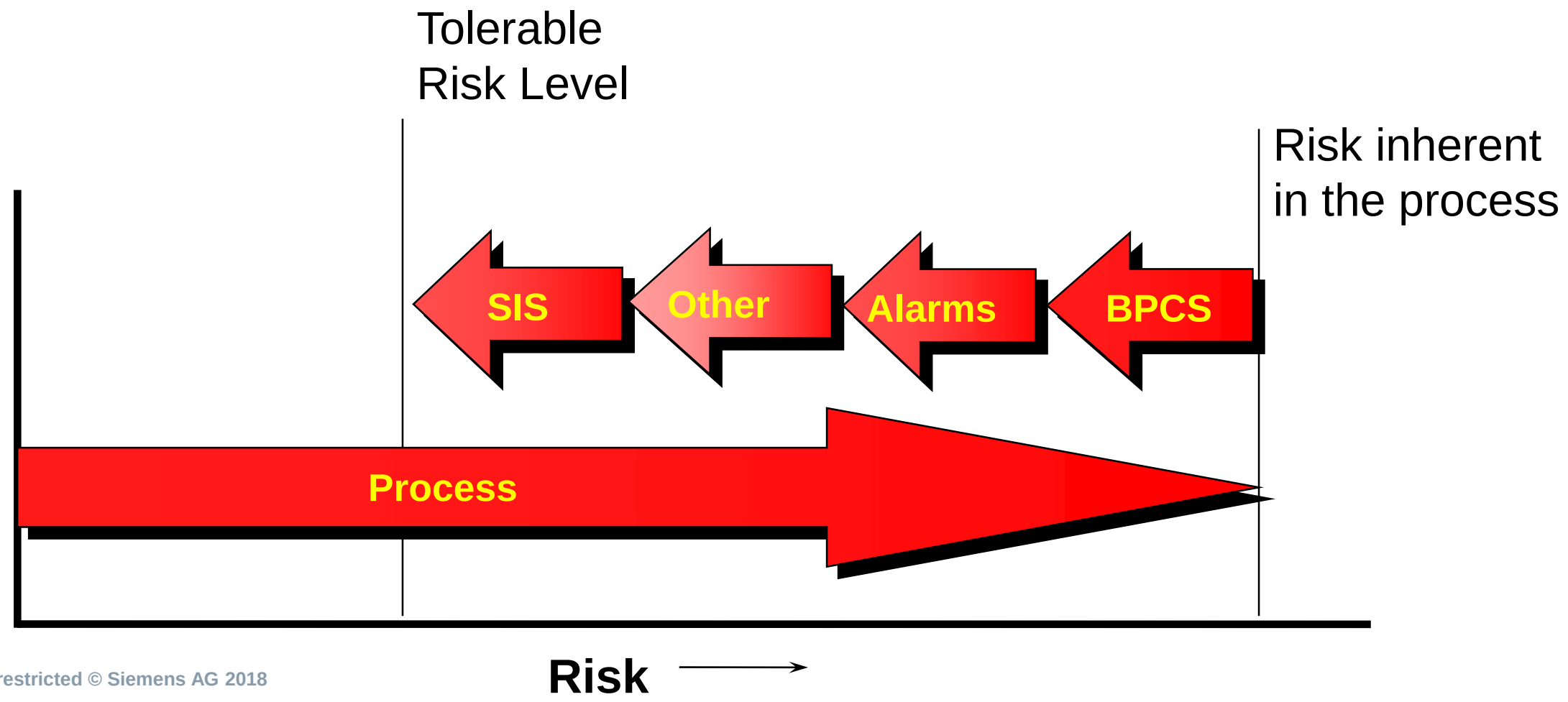
A system composed of sensors, logic solvers, and final control elements for the purpose of taking the process to a safe state when pre-determined conditions are violated.





How much safety do we need? (Risk Reduction)

SIEMENS
Ingenuity for life



SIS Design Documents

ANSI/ISA 61511: Functional Safety:

Safety Instrumented Systems for the process industry sector, 2018

- 1996 - 1st edition of ISA 84
- 2004 - ISA 84 (IEC 61511 Mod)
- 2016 – 2nd edition of IEC 61511

Applied to ensure the functional safety requirements are met.

Addresses 2 concepts:

SIS safety life-cycle

Safety integrity levels (SILs).

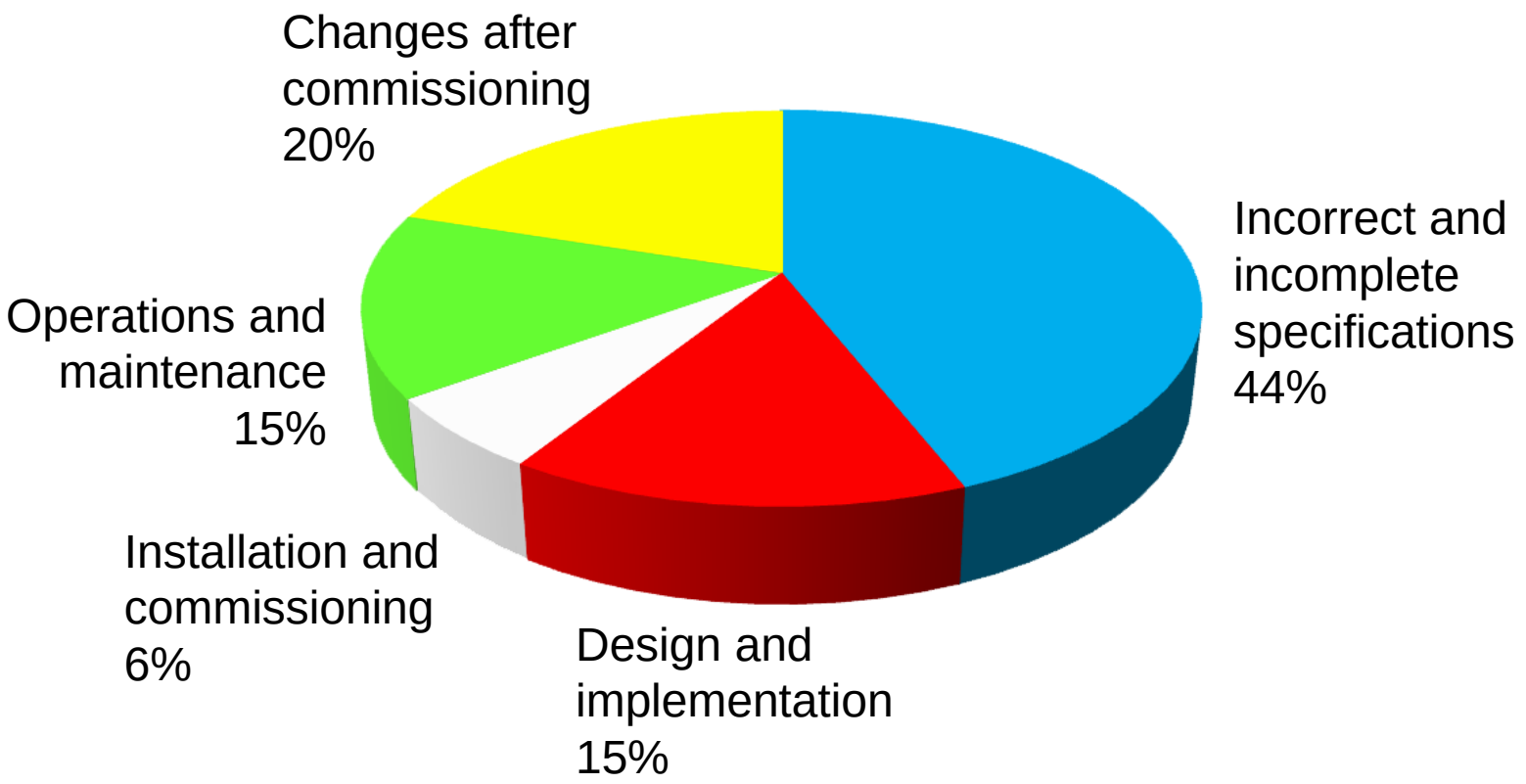
Safety Instrumented System Performance

SIEMENS
Ingenuity for life

Safety Integrity Level (SIL)	Probability of Failure on Demand (PFD)	Risk Reduction Factor (1/PFD)	Safety Availability (1-PFD)
4	≥ .00001 to < .0001	> 10,000 to ≤ 100,000	> 99.99 to ≤ 99.999
3	≥ .0001 to < .001	> 1,000 to ≤ 10,000	> 99.9 to ≤ 99.99
2	≥ .001 to < .01	> 100 to ≤ 1,000	> 99 to ≤ 99.9
1	≥ .01 to < .1	> 10 to ≤ 100	> 90 to ≤ 99

Decide how much safety performance you need, and design to meet it

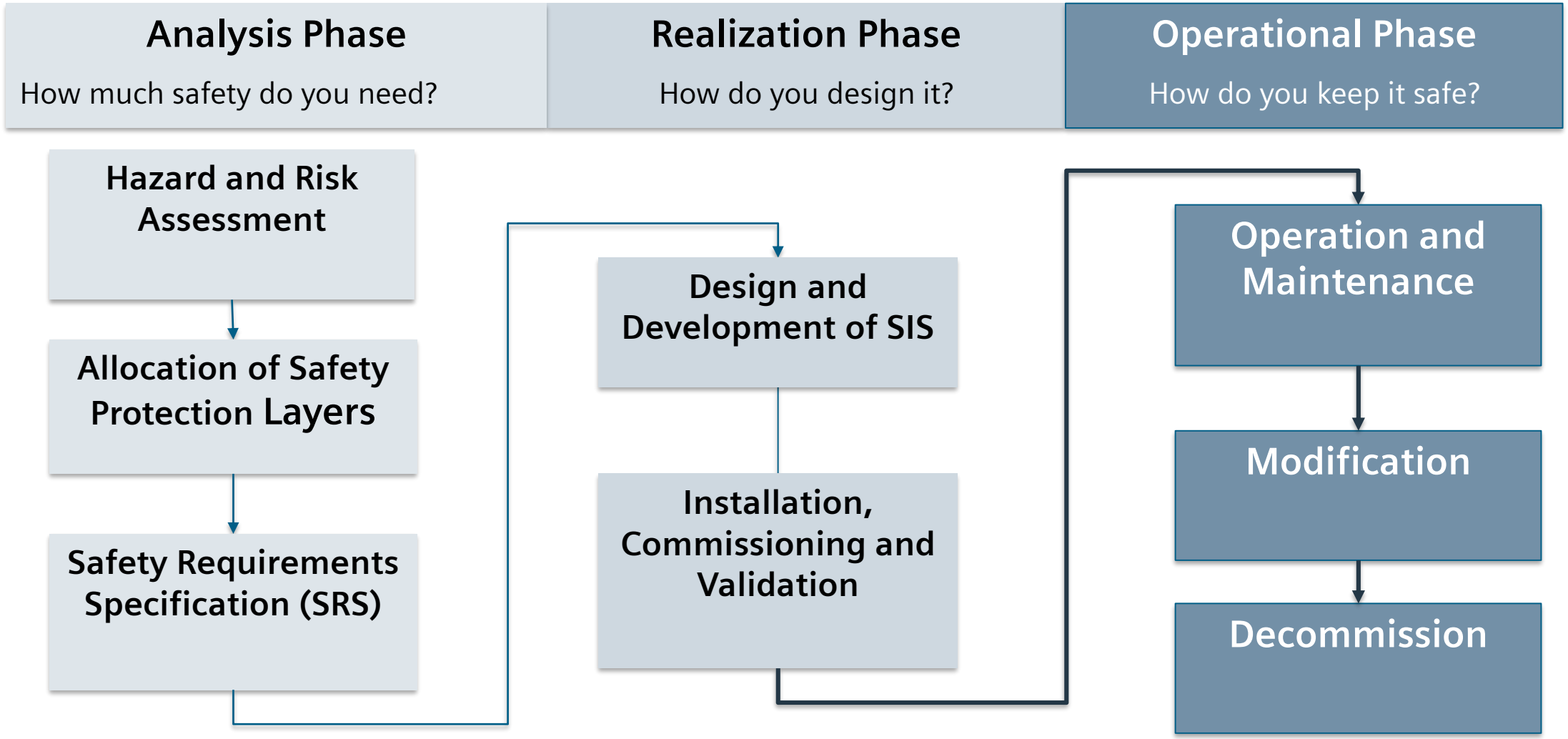
Control system failure – Root Causes



From 'Out Of Control'
(A compilation of incidents involving control systems) by the United Kingdom Health and Safety Executive (UK HSE)

Safety Design Lifecycle (ANSI/ISA 61511, Clause 6)

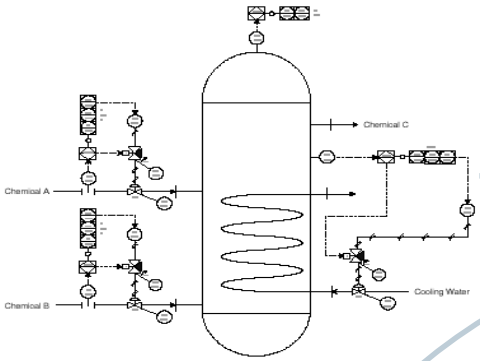
SIEMENS
Ingenuity for life



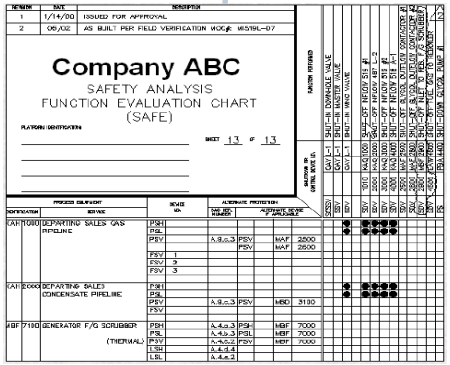
Analysis Phase

How much safety do you need?

SIEMENS
Ingenuity for life



P&ID



Cause & Effect Diagram

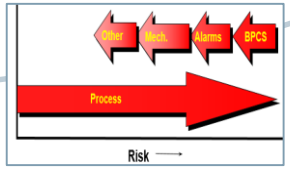
Hazard and Risk Assessment

Allocation of Safety Protection Layers

Safety Requirements Specification (SRS)

HAZOP

LOPA



SIF List

SRS

Hazards

IPLs

SIFs

SIL

C&E Matrix

Realization Phase

How do you design it?

SIEMENS
Ingenuity for life

Conceptual Design of SIS

(Select Architecture, SIL Verification)

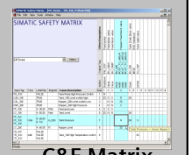
SRS

Hazards

IPLs

SIFs

SIL

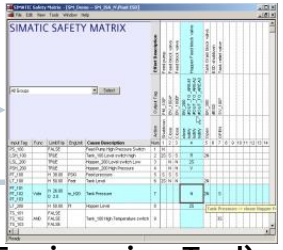


C&E Matrix

SIL Verification Report

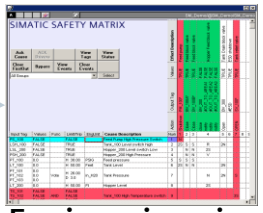
Design and Development of Safety Instrumented System

Cause and Effect



(Engineering Tool)

Installation, Commissioning and Validation



(Online Engineering viewer)

Operational Phase

How do you keep it safe?

Operation and Maintenance

SIS HMI Viewer

- Operator Log
- First Out
- Sequence of Events

Modification

SIS Engineering Tool

- Compare Reporting
- Change Documentation

Decommission

SIS Engineering Tool

- Configuration Report

Integrated safety lifecycle tool

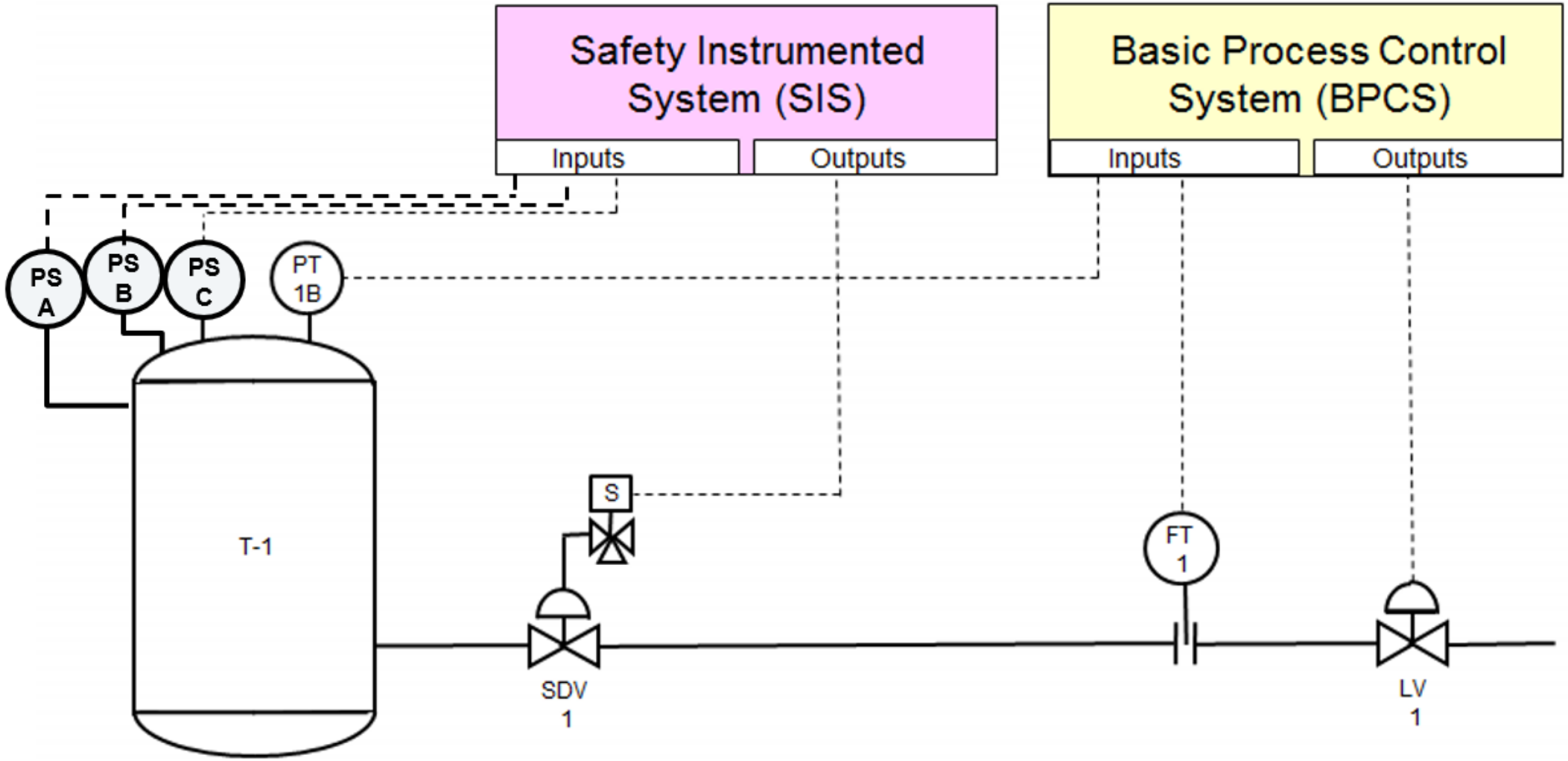
SIEMENS
Ingenuity for life

- ✓ **Documentation**
- ✓ **System Validation**
- ✓ **Design and Engineering**
- ✓ **Installation and Commissioning**
- ✓ **Operation** and **maintenance**
- ✓ **Modifications (MOC)**

$$\text{Output} = \overline{A}BC + A\overline{B}C + AB\overline{C} + ABC$$

Minimiz

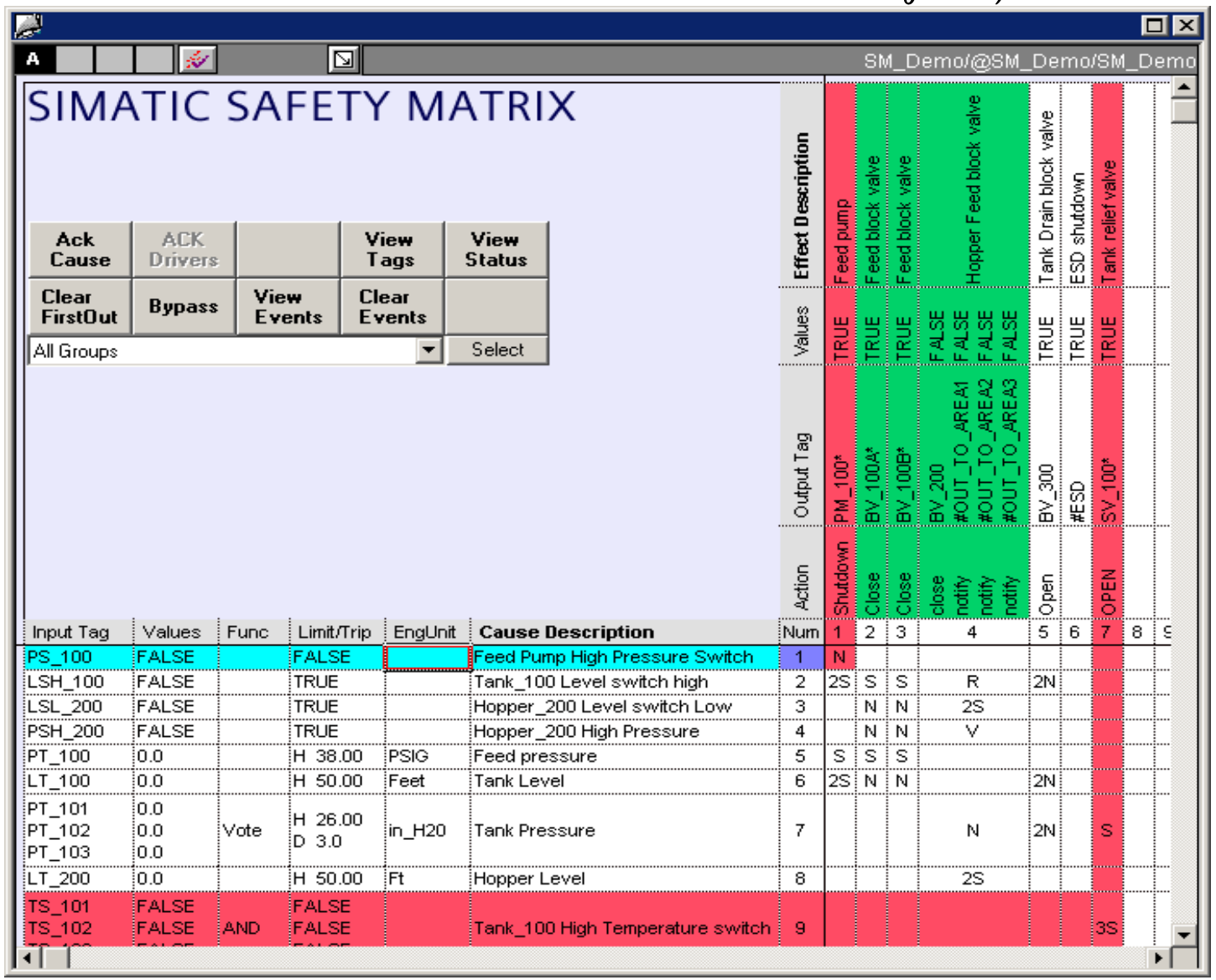
- ✓Intuitive (
- ✓Automate
- ✓Common
- ✓Easy trou



SIEMENS
Ingenuity for life

Integrated Documentation

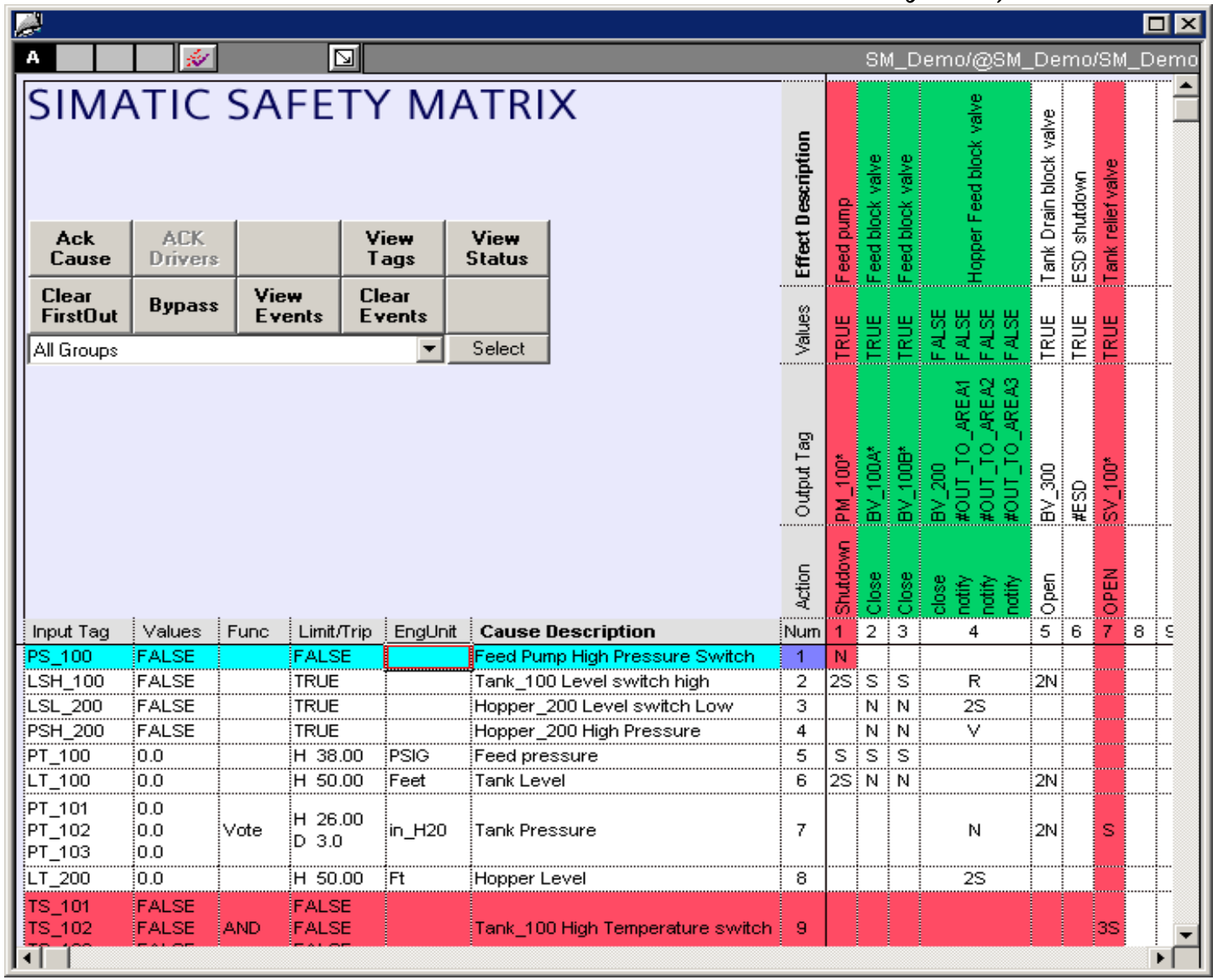
- ✓Validation Reports
- ✓On-Line Changes
- ✓Bypass Management
- ✓First out identification



SIEMENS
Ingenuity for life

HMI Visualization

- System diagnostics
- Alarm management
- MOC documentation
- Sequence of Events (SOE) reporting
- Maintenance overide



Questions and Answers

SIEMENS
Ingenuity for life