Integrated
Safety Systems for Tankfarms

with SIMATIC Safety Integrated

Koen Druyts
Account Manager

Siemens n.v./s.a.
Industry Solutions
IS ST

Nateus Business Park
Nieuwe weg,1
B - 2070 Zwijndrecht
Belgium

Tel.: +32 2 536 98 95
Mobile: +32 495 59 92 90
Fax: +32 2 536 72 05
mailto: koen.druyts@siemens.com

http://www.siemens.com/tankterminals

SIEMENS

Objective of safety engineering

To avoid accidents and damage when a fault occurs and to ensure maximum safety for

People

Process

Environment/ nature

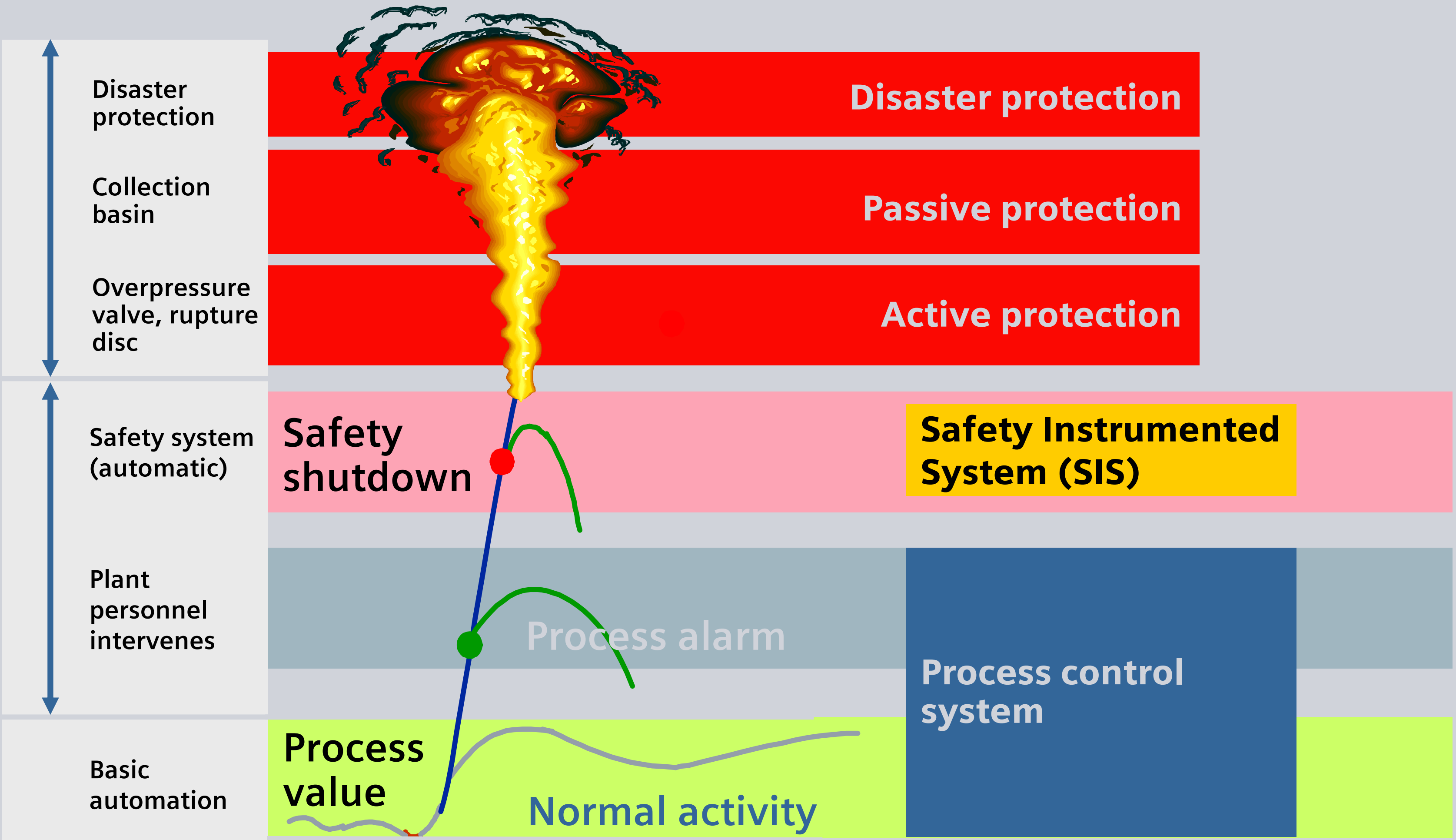
Negligence blamed for Buncefield explosion

A 2006 report by an independent investigation board did not apportion blame, but found **<u>that human error and faulty safety equipment</u>** were responsible.

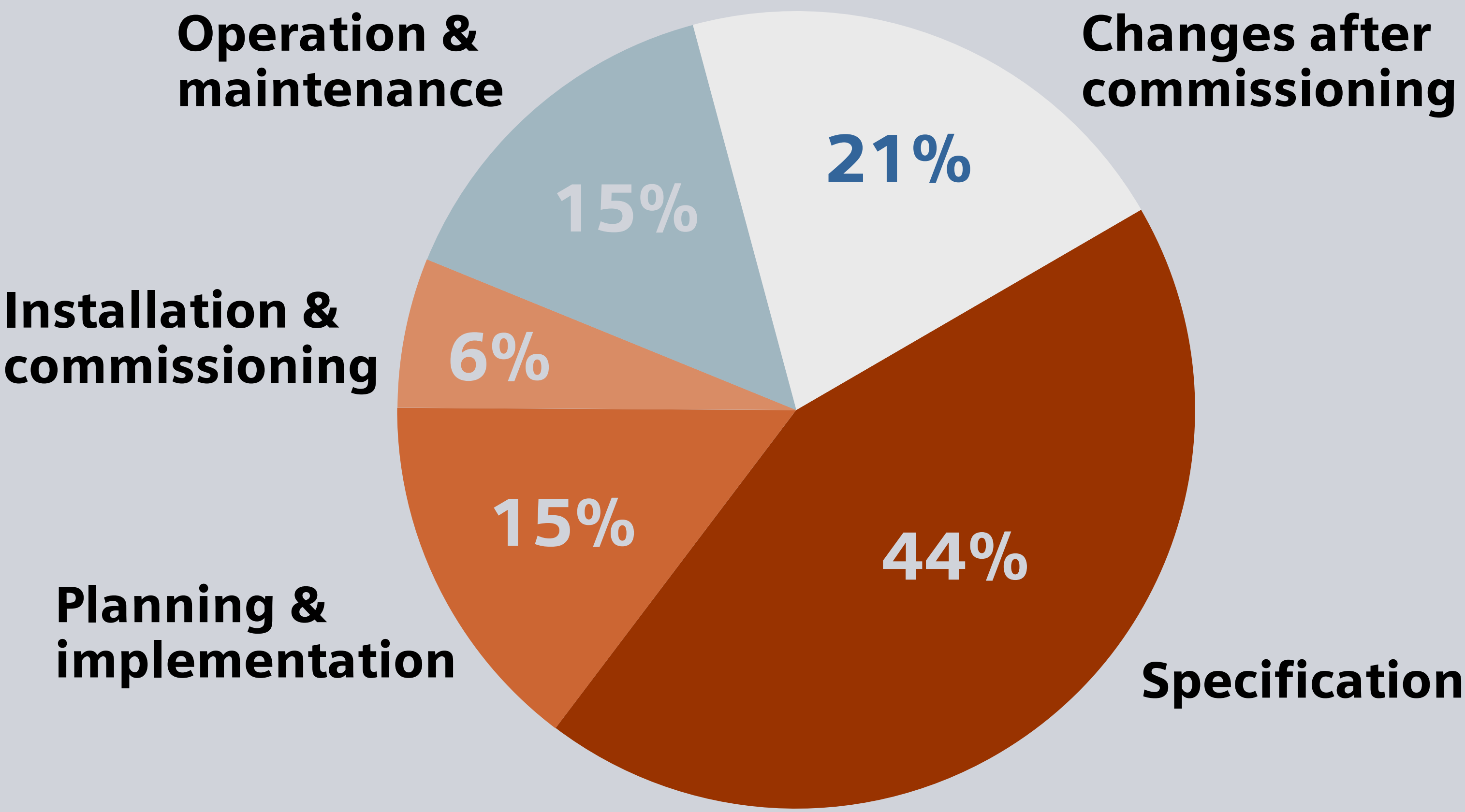
Total UK admitted that 300 tonnes of fuel was spilled after a gauge failed to register that a storage tank was full. But the company argues that it was not liable for damages because it could not reasonably have predicted the spillage would have such devastating consequences.

The blaze engulfed more than 20 fuel storage tanks

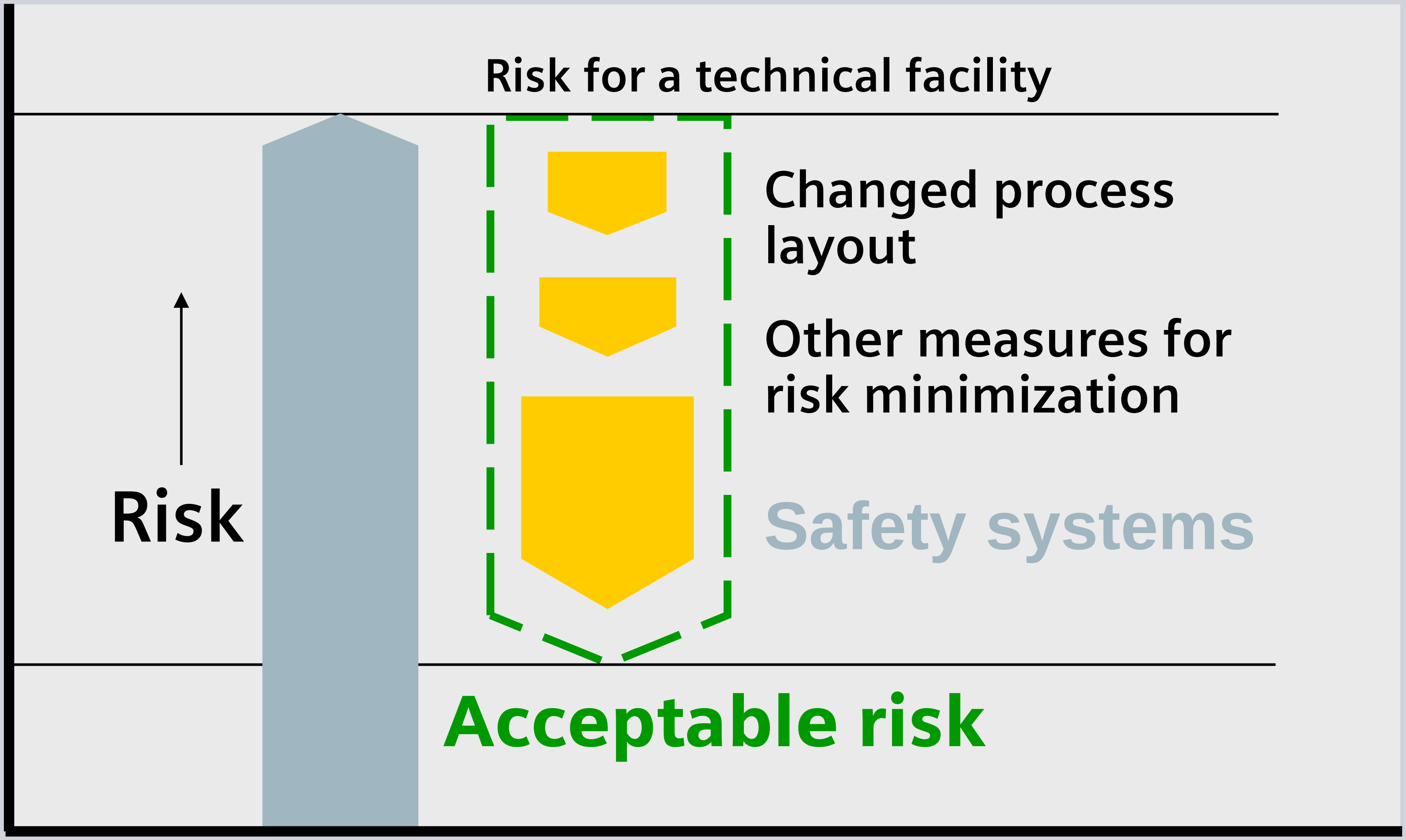
Safety concept for a plant



Cause of faults in automation systems



Risk analysis → risk minimization



"Zero risk" is not feasible

Risk Analysis -> HAZOP

Hazard and Operability Analysis (HAZOP)

The Hazard and Operability (HAZOP) study is a widely used formal technique for examining potential safety and operational problems associated with a system.

A HAZOP study is usually carried out by a team, headed by a chairman and a secretary, who have experience both in the use of the HAZOP technique and the system under investigation.

SIEMENS

International safety standards

IEC61508

IEC 61508 serves as the basic standard and basis for safety standardization.

It covers all areas where electrical, electronic or PLC systems are used to realize safety-related protection functions.

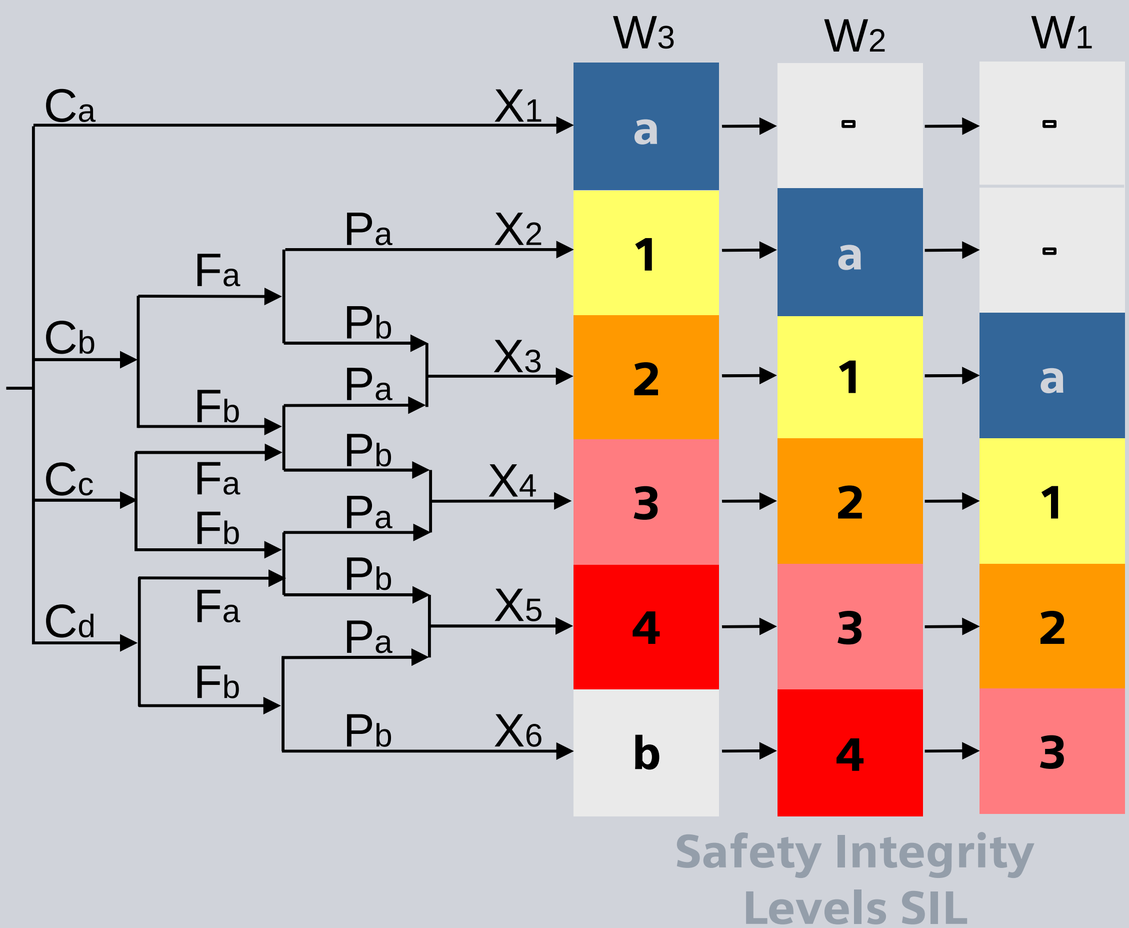
IEC61511

There are sector-specific standards based on IEC 61508, such as IEC 61511 for the process industry or IEC 61513 for the nuclear industry

These sector standards are important for planners and operators of corresponding plants.

Evaluation of risk to define the SIL risk chart
Safety Integrity Level

SIEMENS



a = no special safety requirements
b = individual safety system insufficient

Effect

Ca Minor injury
Cb Major, irreversible injury or death of one person
Cc Death of several persons
Cd Death of very many persons

Frequency and duration

Fa Seldom to often
Fb Frequent to constant

Danger prevention

Pa Possible under cert. circum.
Pb Nearly impossible

Probability of occurrence

W1 Very low
W2 Low
W3 Relatively high

SIEMENS

Target Safety Integrity Levels

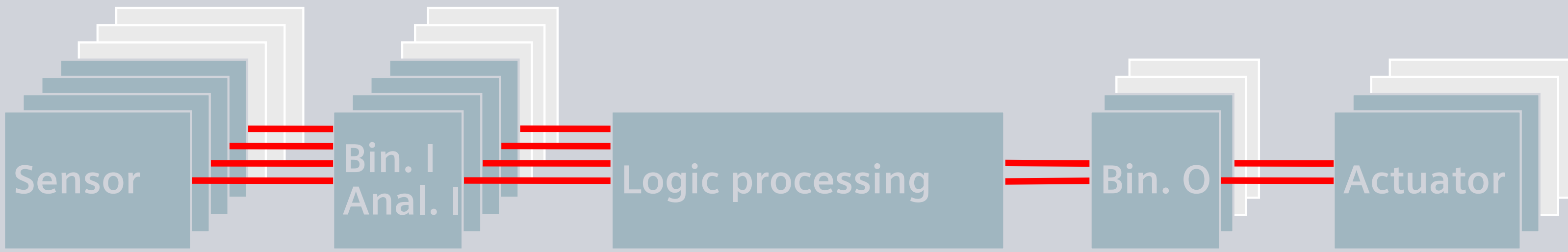
Safety Integrity Level	Probability of failure on demand (PFD) per year (Demand mode of operation)	Risk Reduction Factor = 1/PFD
SIL 4	>= 10^{-5} to < 10^{-4}	100000 to 10000
SIL 3	>= 10^{-4} to < 10^{-3}	10000 to 1000
SIL 2	>= 10^{-3} to < 10^{-2}	1000 to 100
SIL 1	>= 10^{-2} to < 10^{-1}	100 to 10

SIL: A performance criteria of a SIS, among other things, describes the probability of failure on demand.

Safety Functions
IEC 61508

SIEMENS

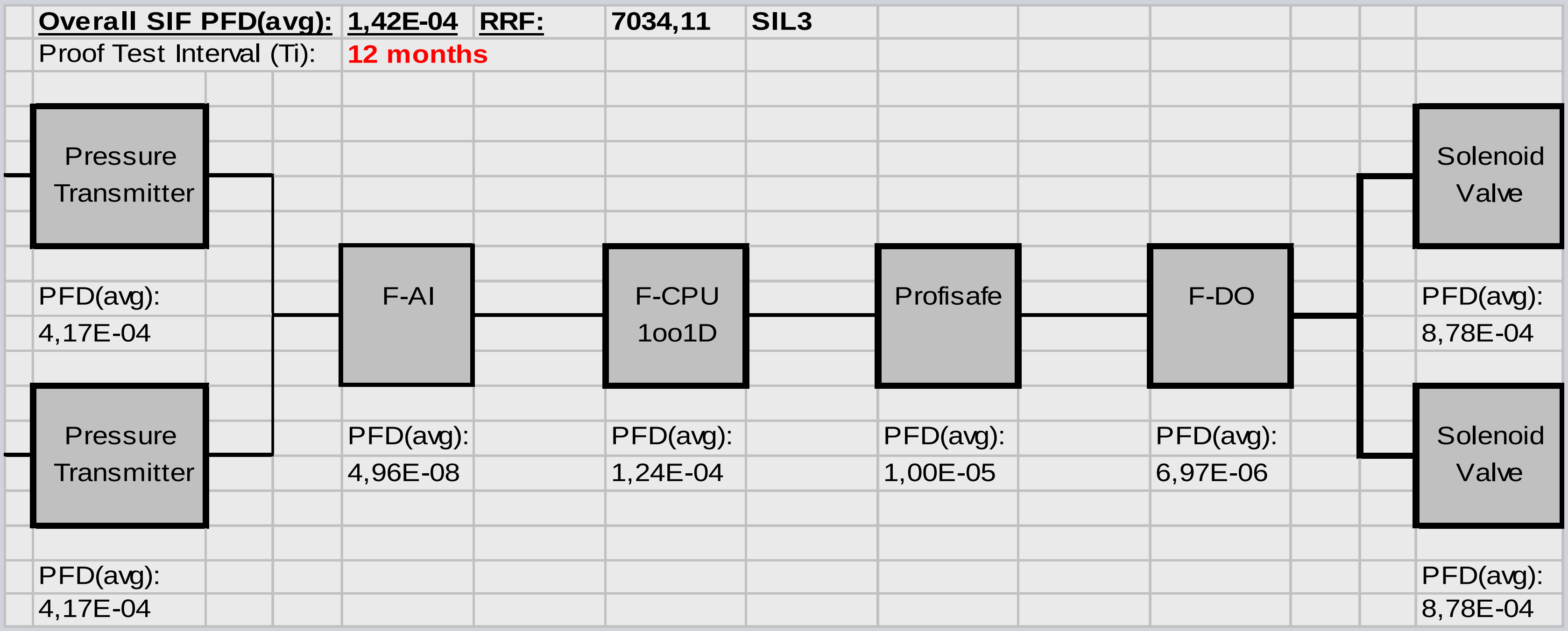
Considering the complete safety functionality of loops acc. to IEC 61508:



Each safety function always comprises the entire chain, from the collection and processing of information to the intended action

Simplified SIL Calculation
SIL of a Safety Instrumented Function (SIF)

SIEMENS



Overall SIF PFDavg = (PFDPT * PFDPT) + PFDAI + PFDCPU + PFDCom + PFDDO + (PFDValve * PFDValve)

For Sensors and actors evaluation:

Pressure transmitter: MTTF = 600 years

Failure rate (λ) = 1 / MTTF (mean time to failure)

For SIF

IEC61508 specifies: $\lambda_d = (\lambda_{du} + \lambda_{dd}) = \lambda/2$

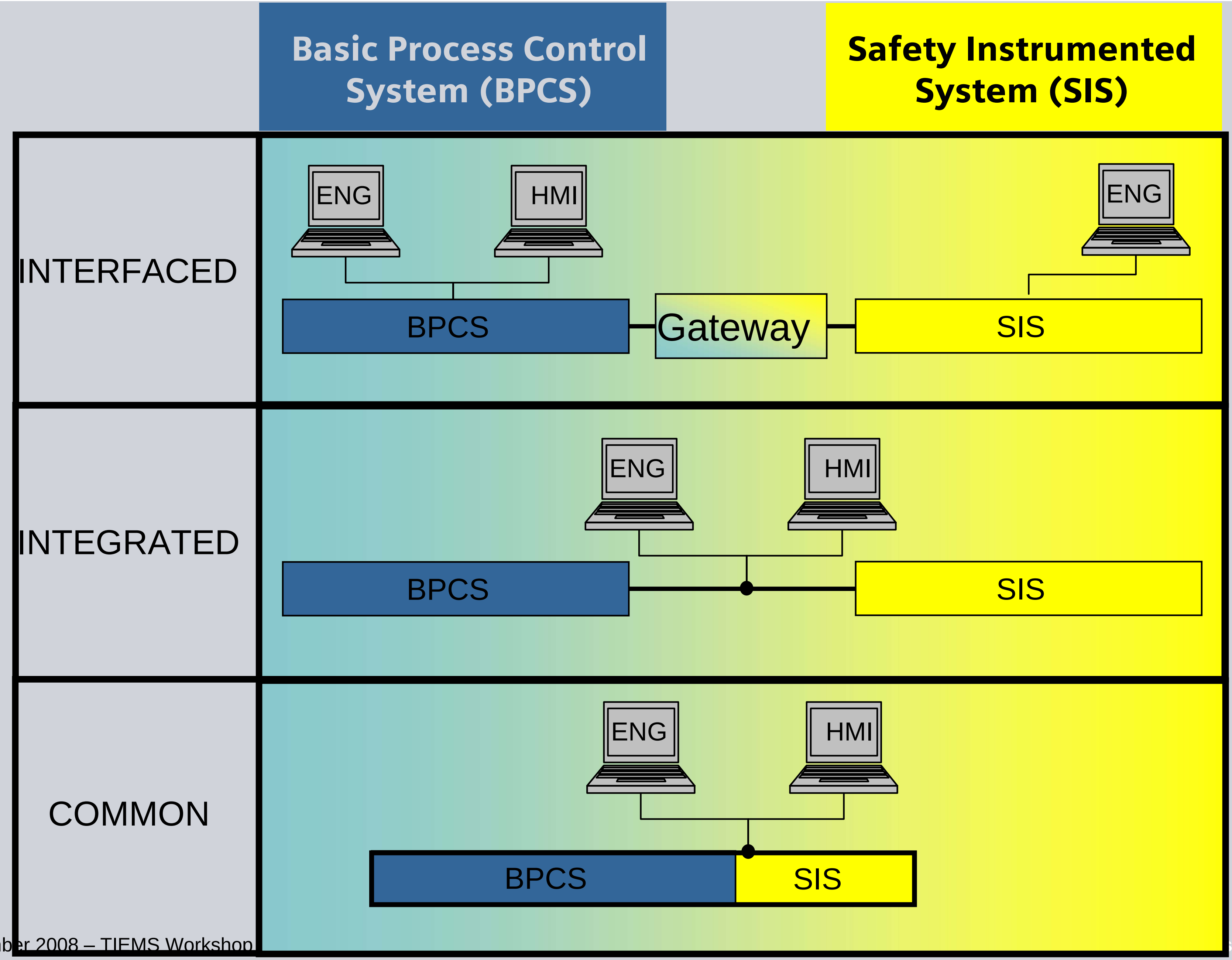
Dangerous failure rate λ_d **= half of the total failure rate (λ)**

PFDavg = $l^{D}t/2$

RRF (Risk Reduction Factor) = 1/PFDavg

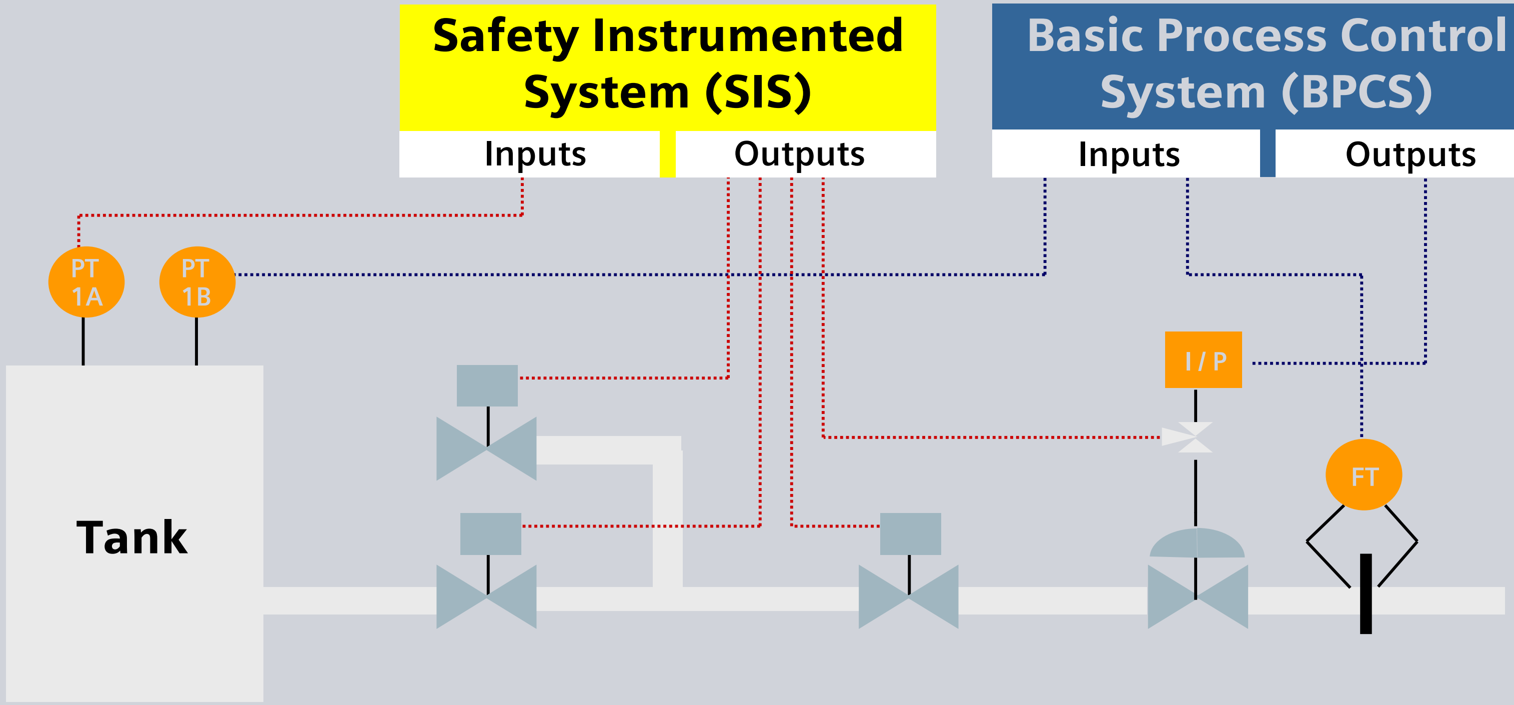
Integrated Control & Safety

The “Right” Level of Integration



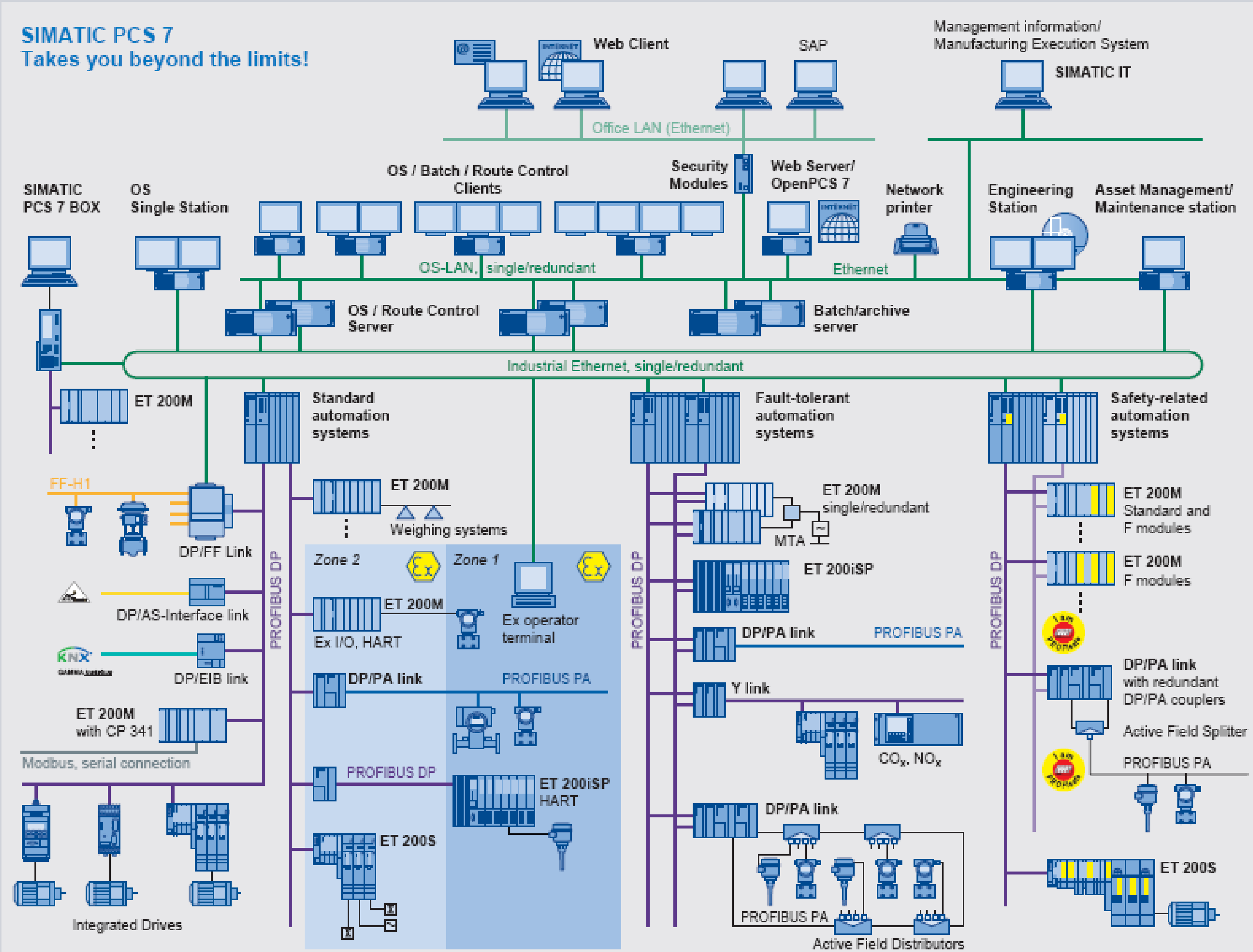
Safety Instrumented System (SIS)

SIS: A combination of sensors, logic units (e.g. controllers) and actuators which detect abnormal operating conditions and AUTOMATICALLY switch the plant to a safe state.



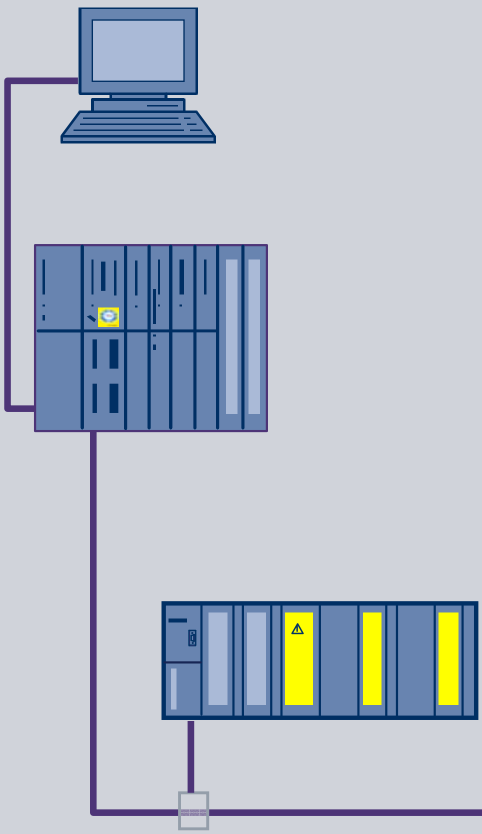
SIEMENS

Overview totally integrated solution with PCS7



SIMATIC Safety Integrated
The Concept

SIEMENS



Standard programming software STEP 7 + Fail-safe programming tool Distributed Safety

Standard CPU
F-HW
+ Fail-safe application program

Standard Remote I/O + Fail-safe I/O module

Standard PROFIBUS DP + PROFIsafe

Safety Integrated for Process Automation

SIEMENS

Common controller platform for process control and process safety

- One hardware for all

One engineering system for process control and process safety application

- Reduces training and uses the available knowledge

User-friendly display of process safety information in PCS 7

Automatic integration of process safety diagnostics into the operator interface

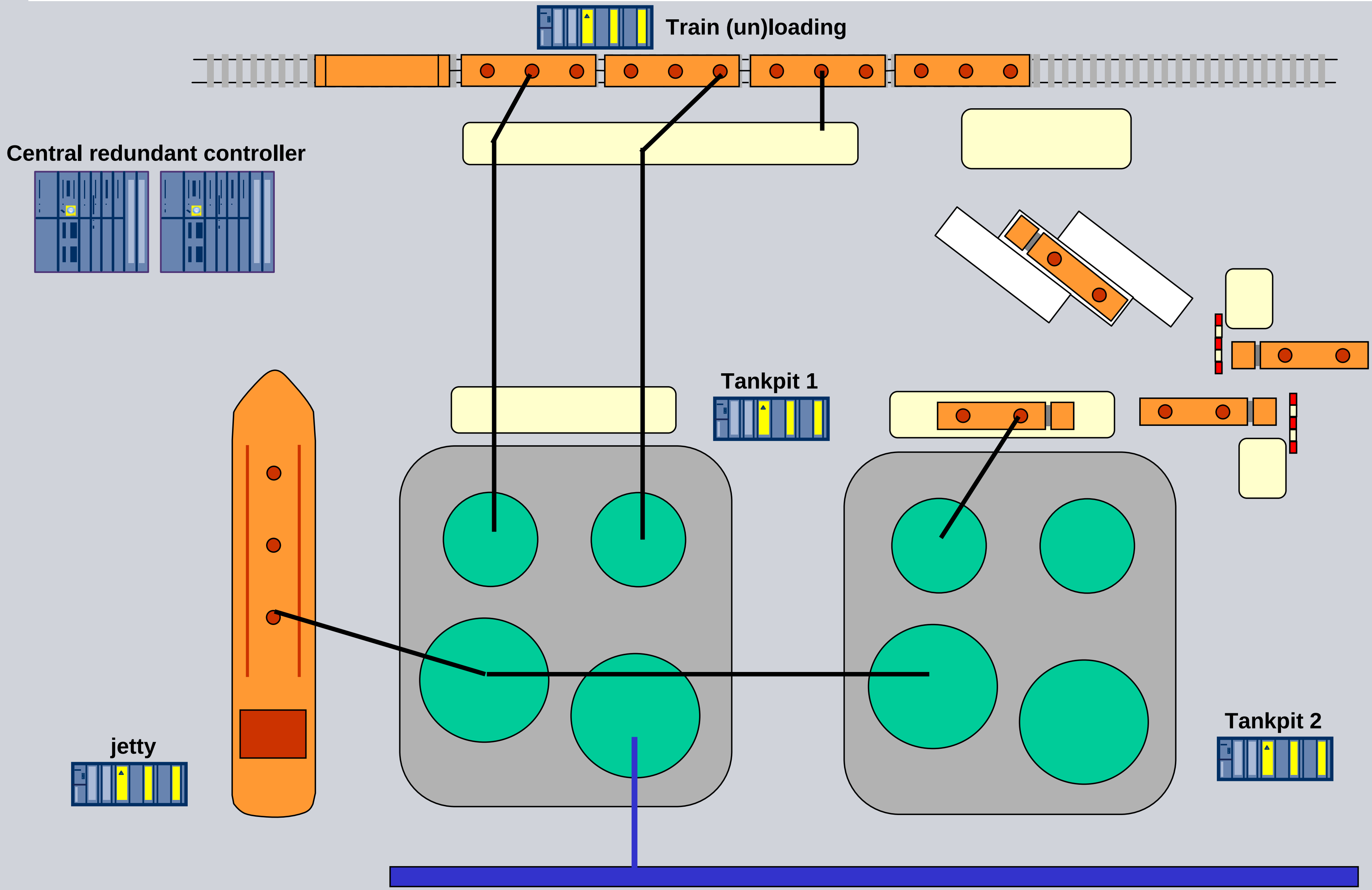
Direct communication between DCS and SIS

- Less engineering work

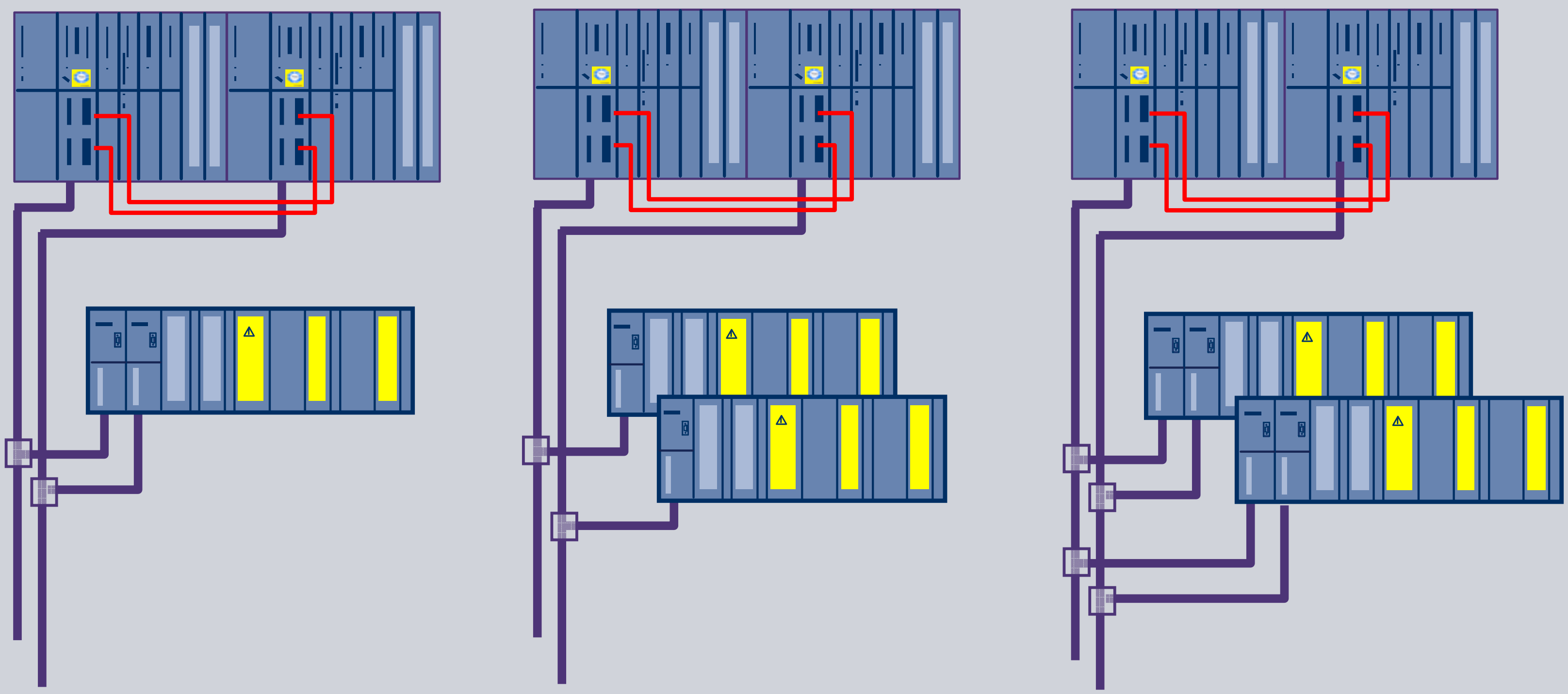
SIEMENS

Flexible Modular Redundancy

Typical Tank Farm Lay-out
Simplified concept distributed I/O



Flexible Modular Redundancy (FMR)



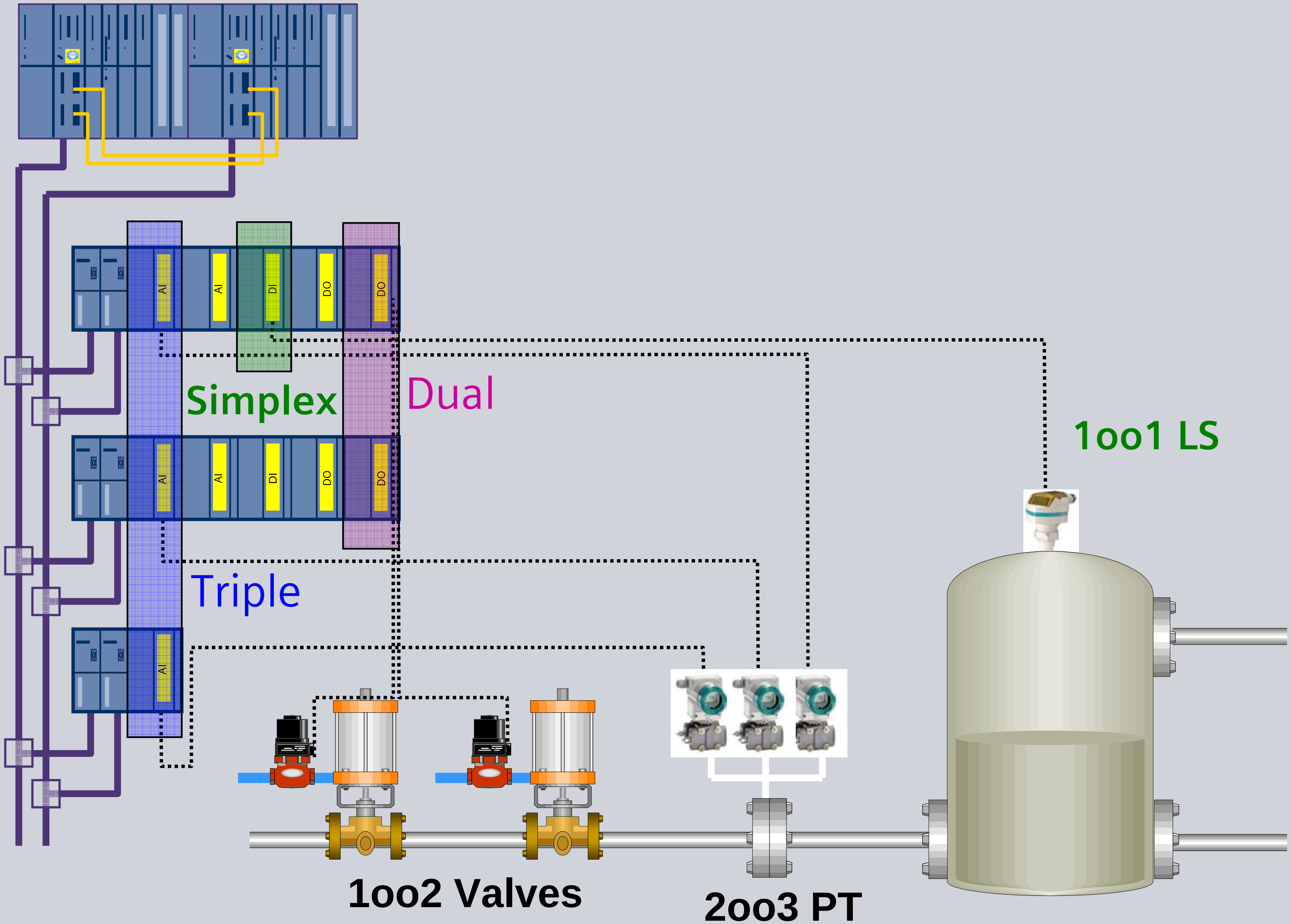
- Redundant S7-400FH
- Redundant PROFIBUS DP
- Switched I/O – ET 200M

- Redundant S7-400FH
- Redundant PROFIBUS DP
- Redundant I/O – ET 200M

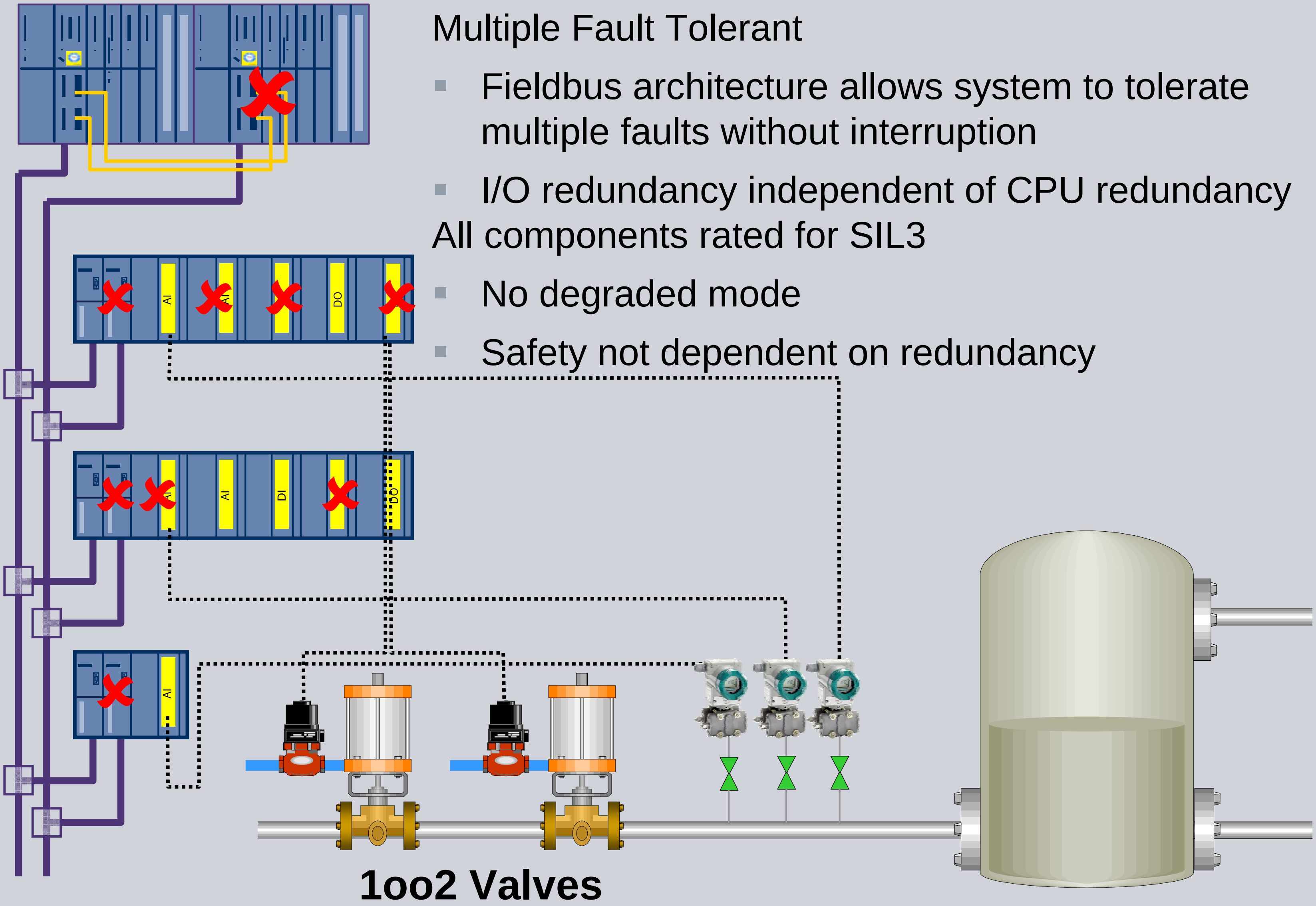
- Redundant S7-400FH
- Redundant PROFIBUS DP
- Redundant, switched I/O – ET 200M

SIEMENS

Flexible Modular Redundancy (FMR)



Flexible Modular Redundancy (FMR)



Multiple Fault Tolerant

- Fieldbus architecture allows system to tolerate multiple faults without interruption
- I/O redundancy independent of CPU redundancy

All components rated for SIL3

- No degraded mode
- Safety not dependent on redundancy

SIEMENS

Flexible Modular Redundancy (FMR)

Safety Integrity Level **up to SIL 3** with one controller

- Highest Safety Integrity Level

Highest Flexibility

- Separate or combine safety and standard application in one CPU
- Use redundancy for safety only where it is needed
- Parallel use of PROFIsafe on PROFIBUS

Highest Availability through Multiple Fault Tolerance

- Architecture allows system to tolerate multiple faults
- IO redundancy independent of CPU redundancy
- IO and device redundancy can be matched to maximize availability

Cost reducing

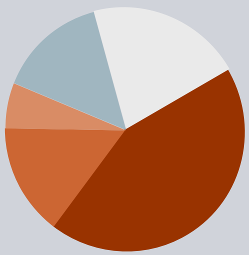
- Use redundancy only where you need it for safety or availability
- Parallel use of PROFIsafe on PROFIBUS

Safety Lifecycle Engineering

The IEC 61511(ISA S84) Safety Lifecycle

The different phases of the safety Lifecycle

- **Analysis Phase**
  - Identification of Hazards and Risks
  - Development of the Safety Requirement Specification for the Safety Instrumented System
  - Allocation of Safety Function to Protective Layers
- **Realization Phase**
  - Design and Engineering of Safety Instrumented System
  - Design and Development of other Means of Risk Reduction
  - Installation, Commissioning & Validation
- **Operation Phase**
  - Operation & Maintenance
  - Modification
  - Decommissioning



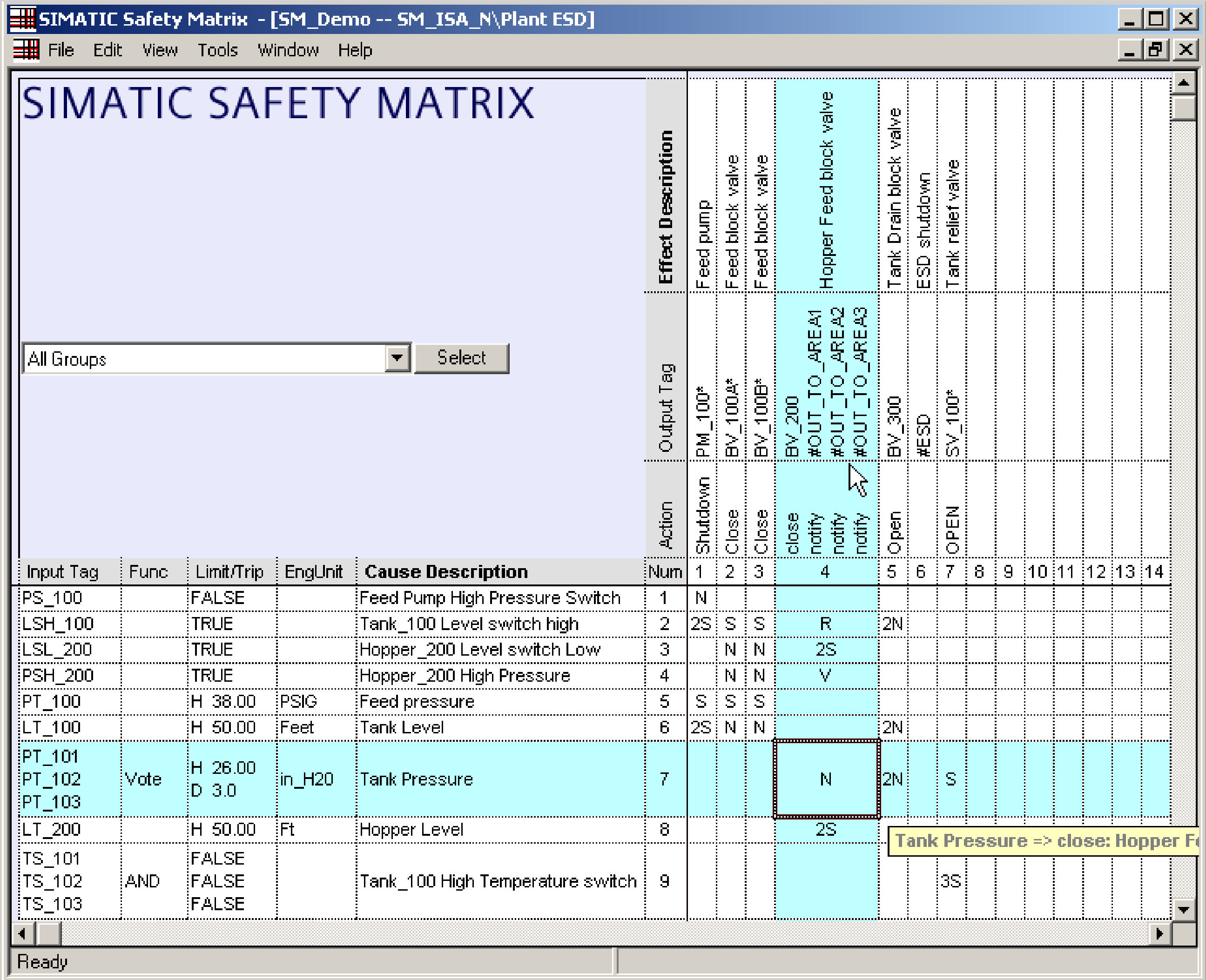
The Realization Phase with the Safety Matrix

SIEMENS

Configuration of the Safety Functions with the Cause & Effects Method

Automatic TÜV-certified Creation of the Safety Logic from the Cause & Effect matrix

Easy Configuration without special Programming Knowledge



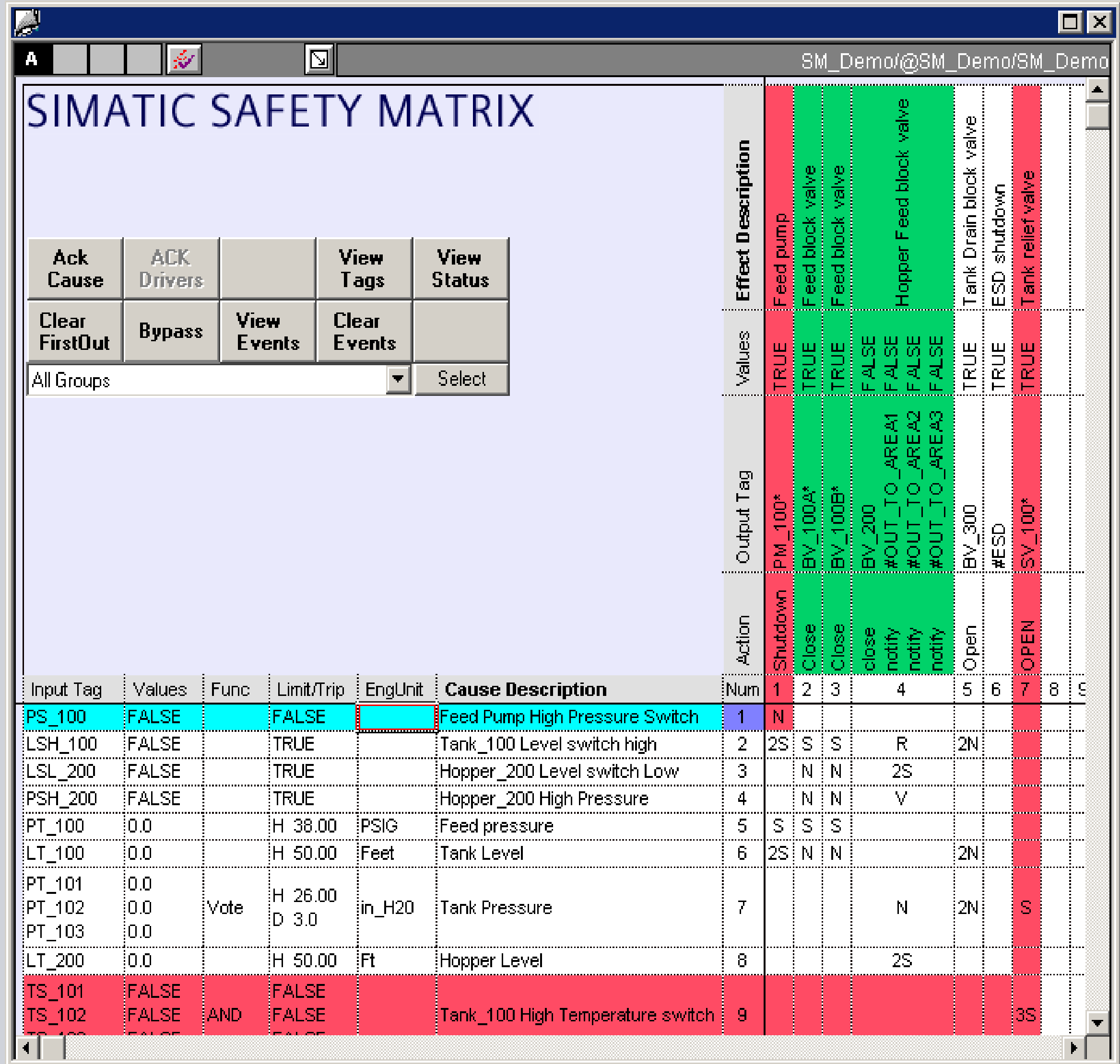
The Operation Phase with Safety Matrix

Operation and Maintenance

- Online View
- Support Operation functions like Bypass, Reset and Override
- Sequence of Event Recording
- First Alarm Display

Safety Lifecycle Management Tool

- Integrated Version Tracking
- Integrated Documentation of Operator Manipulations
- Integrated Documentation of Changes



Summary

Process Safety and Totally Integrated Automation

Integrated Control & Safety

- Best Integration into the distributed control system PCS 7
- Less training and easy handling due using same tools
- Less hardware due using same CPU for standard and safety

Flexible Modular Redundancy

- Save money by mix and match to meet the goals of the application
- Highest availability due the multiple fault tolerance

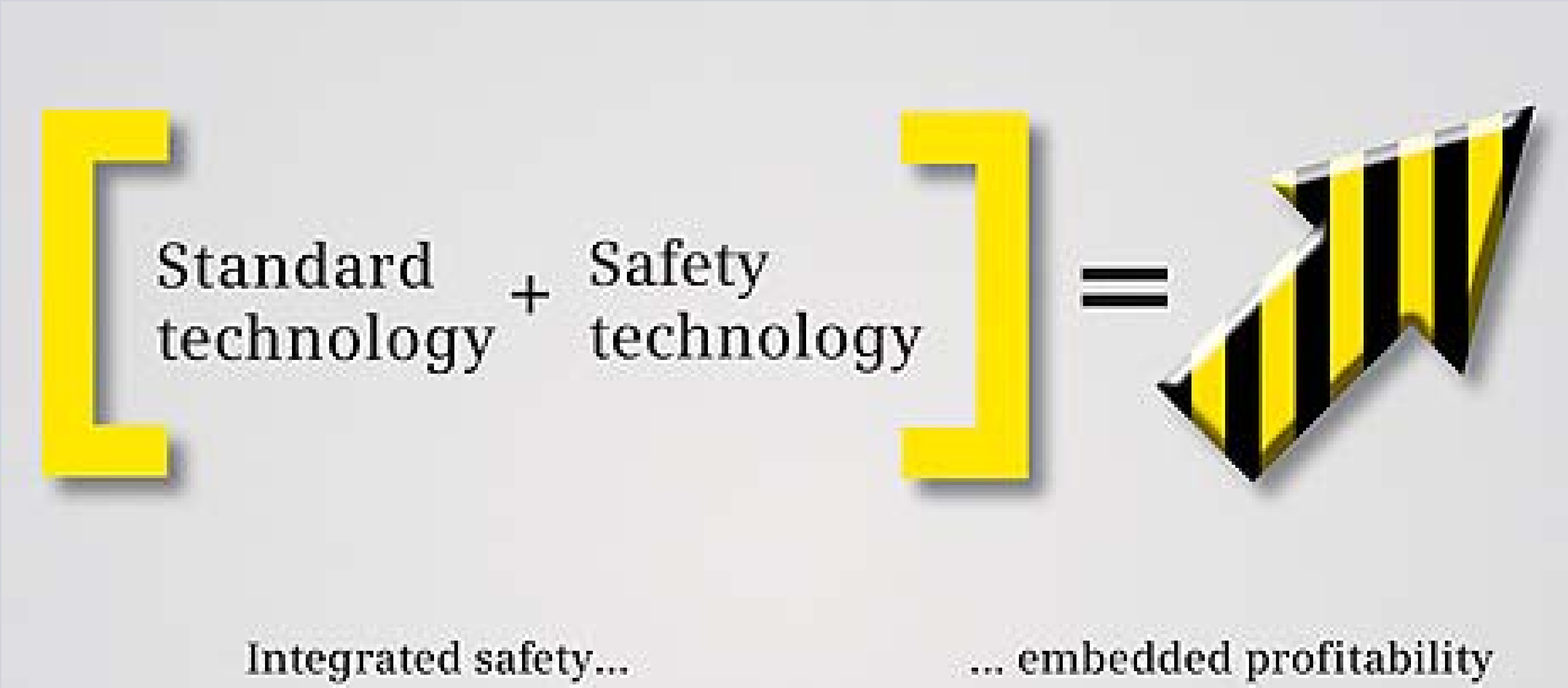
Integrated Safety Fieldbus

- Less wiring due PROFIsafe on PROFIBUS, one cable for the communication safe and non-safe
- Prepared for safety fieldbus instruments

Safety Lifecycle Engineering

- Safety Matrix supports the phases of the Safety Lifecyle

Process Safety and Totally Integrated Automation



Totally Integrated Automation