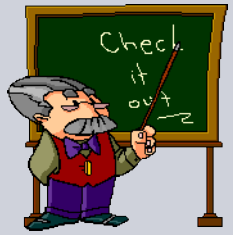
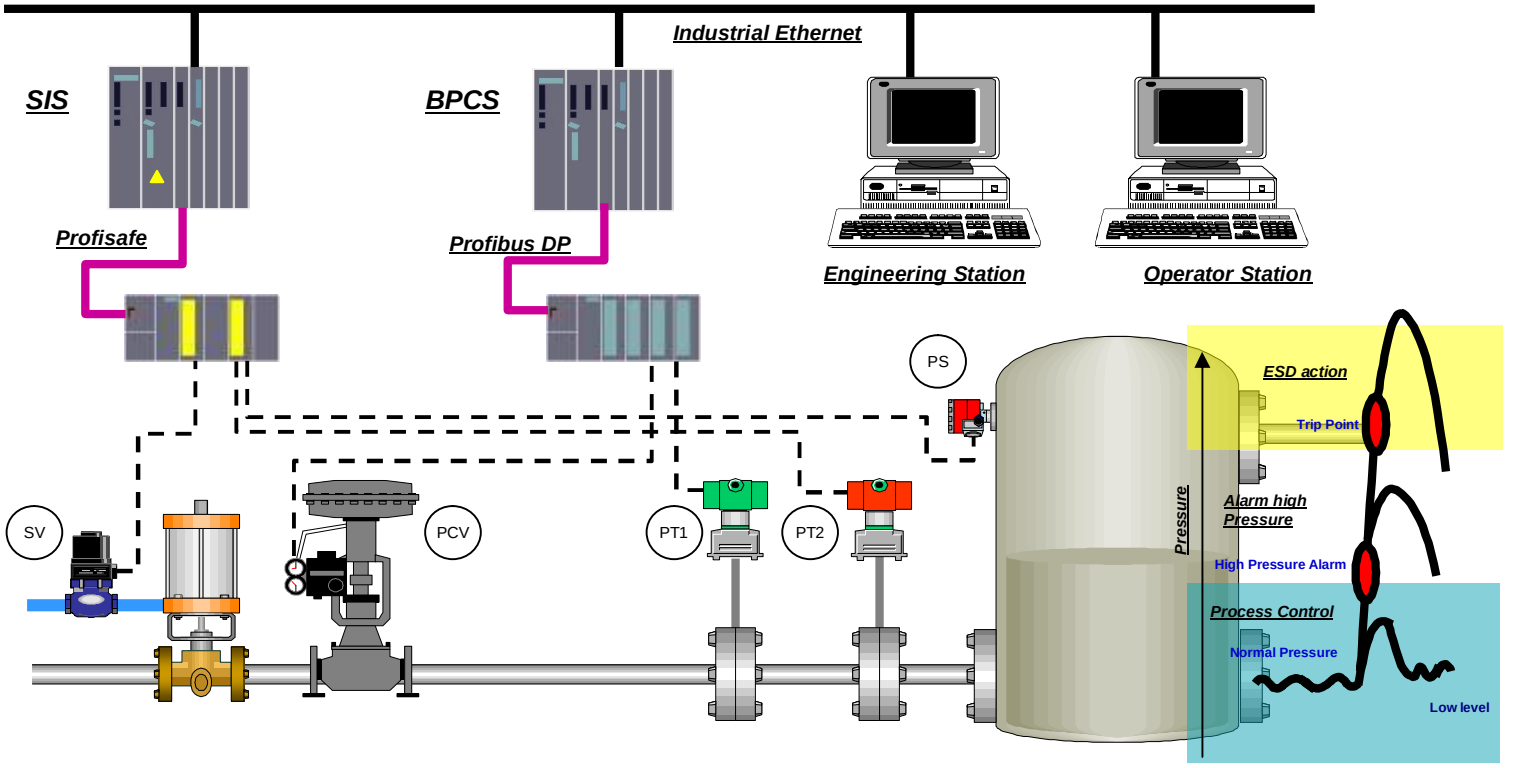

PI
South East Asia
PROFIBUS • PROFINET

Safety Instrumented System (SIS)



Independent system composed of sensors, logic solvers, and final control elements for the purpose of:

1) **Shutdown:** Automatically taking the process to a safe state when pre-determined conditions are violated
2) **Permissive:** Permit a process to move forward in a safe manner when specified conditions are met
3) **Mitigation:** Taking action to mitigate the consequences of an industrial hazard

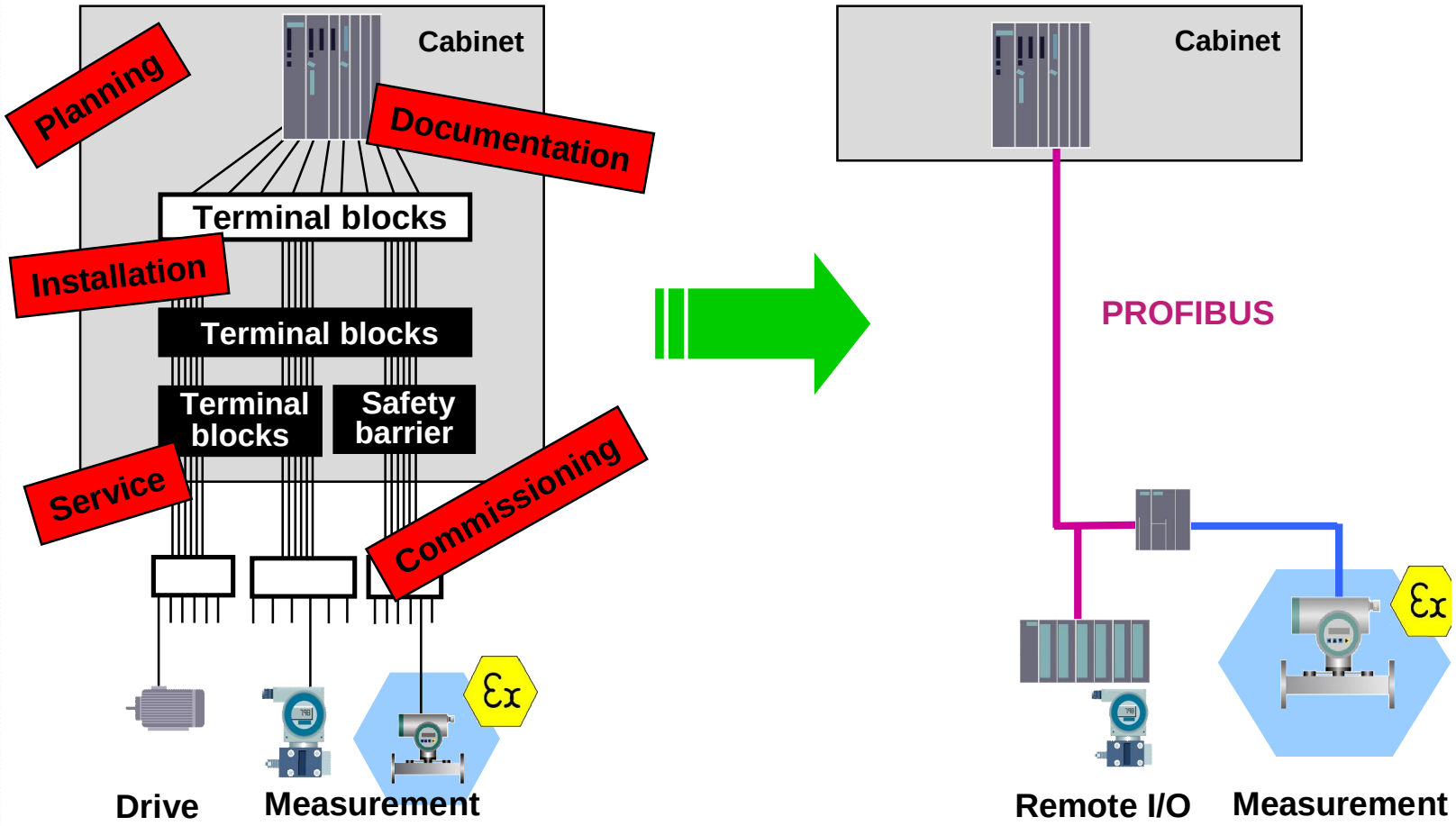


Traditional Safety Systems

- Traditional safety systems have implemented internal, proprietary implementations of safety communications for years
  - CPU to I/O communications
  - CPU to CPU communications
- Industry experts share differing opinions about the viability of today's buses for safety networking
  - Some say hard wire is the only safe way and requires a new standard
  - Some say what we have now will work fine in the process industry
- The whole industry is interested in a safety fieldbus because users have seen benefits of Fieldbus with their standard control systems and now want the same for their safety systems.

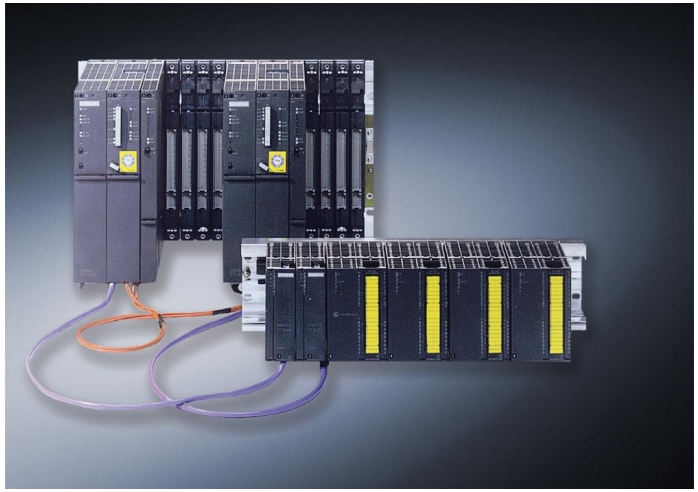
Automation & Instrumentation Fieldbus

Up to 70% space saving + 40% cost saving



Advantages

- Similar to those for conventional fieldbuses
  - Lower field wiring costs
  - Improved diagnostics
  - Increased uptime and plant utilization resulting from improved asset management
  - Improved maintenance and test data for reporting



End-User Requirements

- Reduced Total Cost of Ownership
  - **CAPEX (Hardware, Footprint, Commissioning, Power Consumption)**
  - **OPEX (Advanced diagnostics, Reduced test interval)**
  - **SIL 2 and 3 applications**
- Password protected access to field devices
- Support for discrete signals (e.g. switches, lights, PB's, etc.)
- System Approach to Asset Management – SIS and Non-SIS
  - **Diagnostics**
  - **Hybrid system architecture – SIS & traditional hardware**
  - **Proof test guidance (manual, auto, opportunity-based)**
  - **Logging/documentation of results**
  - **Failure rate tracking**

International Safety Standards

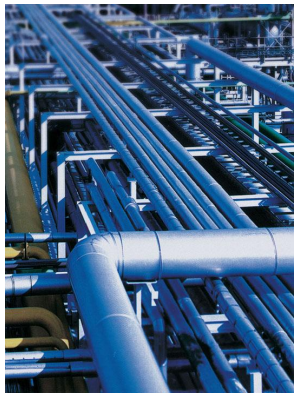
IEC Commission Electrotechnique Internationale International Electrotechnical Commission Международная Электротехническая Комиссия

IEC61508

The IEC 61508 is considered to be the basic standard and the basis for safety standardization.

It covers all applications in which safety-relevant protective functions are implemented with the help of electrical, electronic, or programmable (logic) control systems.

DIN 0801 and DIN V19250 become invalid from August 1, 2004.

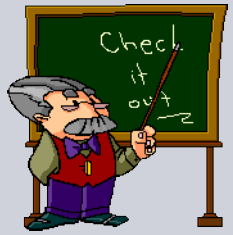


IEC Commission Electrotechnique Internationale International Electrotechnical Commission Международная Электротехническая Комиссия

IEC61511

Based on IEC 61508 there are sector-specific standards, such as IEC 61511 for the process industry or IEC 61513 for nuclear power generation.
These sector-specific standards are important for planers and operators of the corresponding plants.

Process Safety Standards



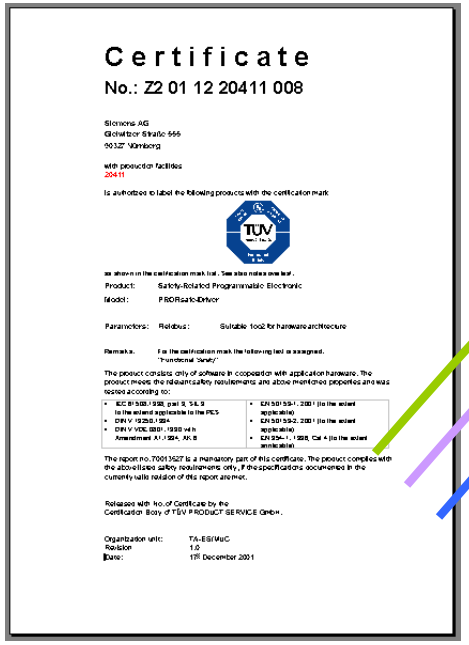
- **ISA S84-1996**
  - "Each individual field device shall have its own dedicated wiring to the system" – clause 7.4.1.3
  - Standard does not address technologies not currently in use (ie. Fieldbuses), but revisions will address technologies as they become available
- **IEC 61511-2003 / ISA S84.00.01 - 2004**
  - Allows "a digital bus communication with overall safety performance that meets the integrity of the SIF (Safety Instrumented Function) it services" - clause 11.6.3
- **ISA TR84.00.06 (Safety Fieldbus)**
  - Safety Fieldbus Technical Report

Key Requirements from ISA TR84.00.06

- **"Certified" safety fieldbus communication protocol to support the highest Safety Integrity Level (SIL) of the Safety Instrumented System (SIS)**
- **Interoperable and non-proprietary**
- **Safety-related and non-safety-related devices may coexist provided non-safety-related devices are "non-interfering"**
- **Diagnostics implemented in a manner "transparent" to the user and capable of reporting to asset management system**
- **Fault tolerance should be optional**
- **Sufficient security to prevent inadvertent changes**
- **Online replacement of devices possible**
- **System shall be "testable"**

PROFIsafe

- **PROFIsafe is a application layer (profile) that describes the communications between fail-safe devices**
- **Supports safe communication over open standard buses PROFIBUS (DP, PA) and PROFINET**
- **TUV Certified to IEC 61508 SIL 3 / EN 954-1 Cat 4**



Certificate

No.: Z2 01 12 20411 008

Siemens AG
Gleiwitzer Straße 555
90327 Nürnberg

with production facilities
20411

is authorized to label the following products with the certification mark:

as shown on the certification mark list. See also notes overleaf.

Product: Safety-Related Programmable Electronic

Model: PROFIsafe-Driver

Parameters: Fieldbus: Suitable tool for hardware architecture

Remarks: For the certification mark the following text is assigned:
"Functional Safety"

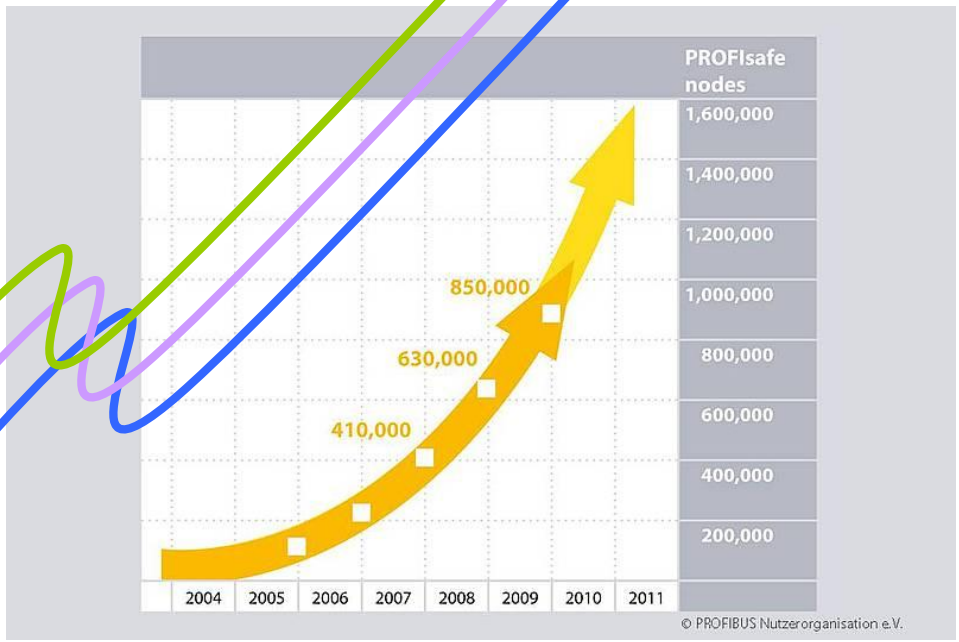
The product consists only of software in cooperation with application hardware. The product meets the relevant safety requirements and above mentioned properties and was tested according to:

• IEC 61508:1998, part 3, SIL 3 to the extent applicable to the PES	• EN 50155-1, 2001 (to the extent applicable)
• DIN V 19250:1994	• EN 50155-2, 2001 (to the extent applicable)
• DIN V VDE 0801:1990 with Amendment A1:1994, AK 8	• EN 954-1:1998, Cat 4 (to the extent applicable)

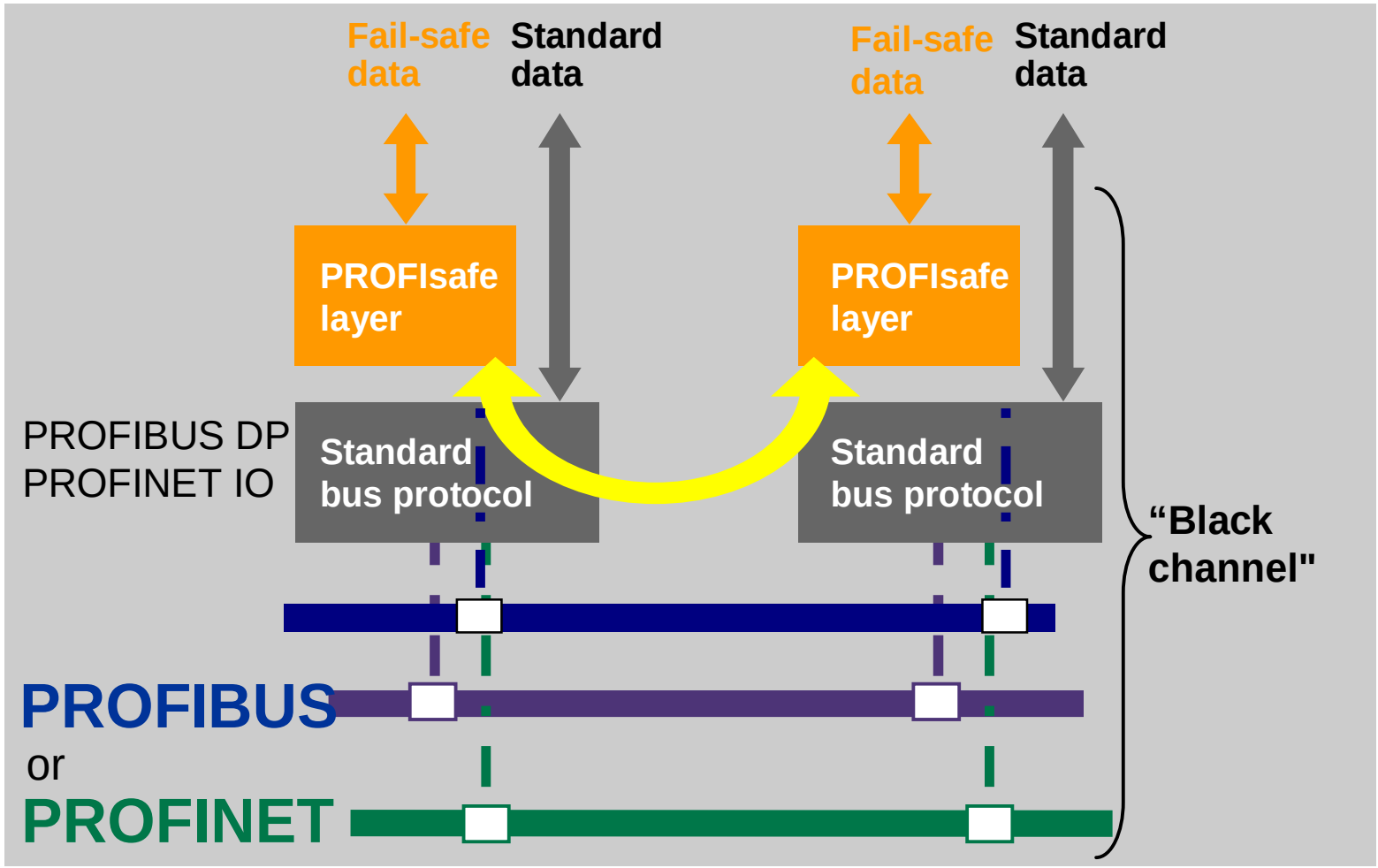
The report no. 70013627 is a mandatory part of this certificate. The product complies with the above-listed safety requirements only, if the specifications documented in the currently valid revision of this report are met.

Releases with No. of Certificate by the Certification Body of TÜV PRODUCT SERVICE GmbH.

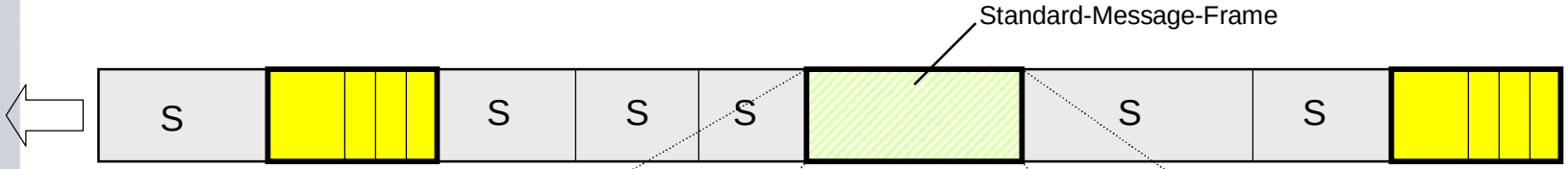
Organization unit: TA-EB/MuC
Revision 1.0
Date: 18th December 2001



Same Protocol Supports PROFIBUS (DP, PA) & Profinet



PROFIsafe Message Format



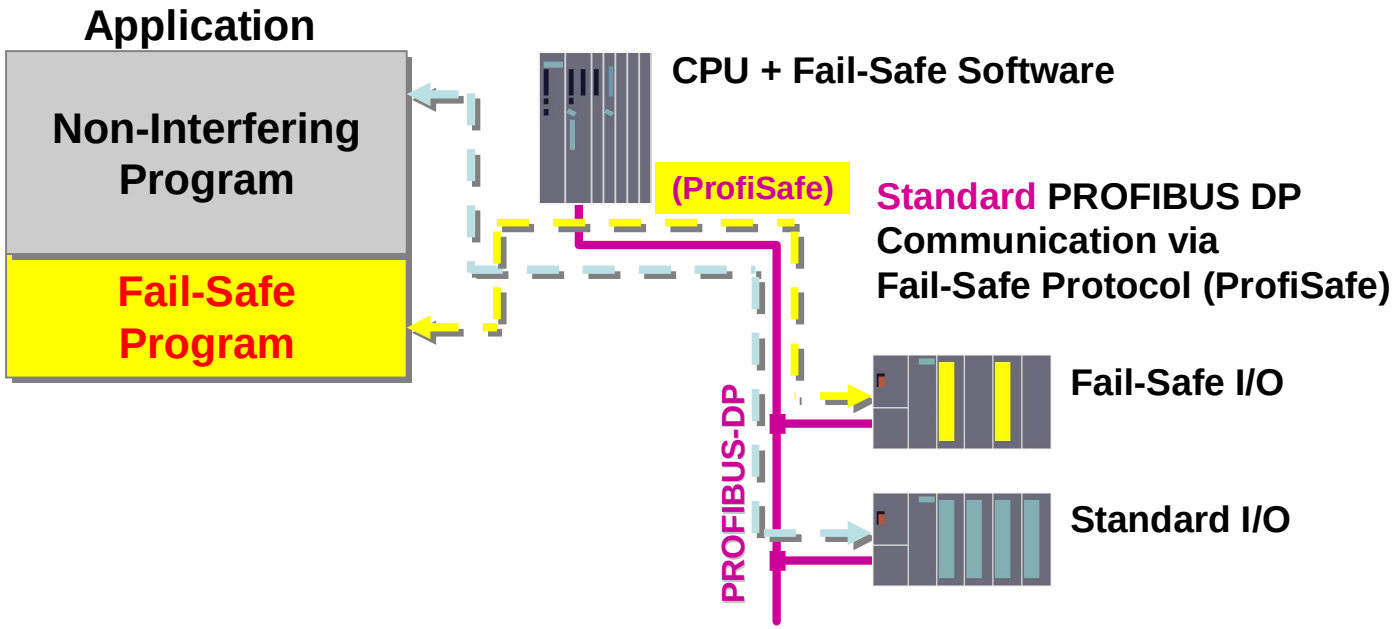
F-I/O-Data	Status / Controlbyte	Sequence Number	CRC	Standard-I/O-Data
		Sender based Counter	across F-Data and F-Parameter	
Max. 12 / 122 Bytes	1 Byte	1 Byte	2/4 Bytes *)	(240/238 - F-Data)

*) 2 Byte for a max. of 12 Byte F I/O data
4 Byte for a max. of 122 Byte F I/O data

Max. 244 Bytes DP-Data

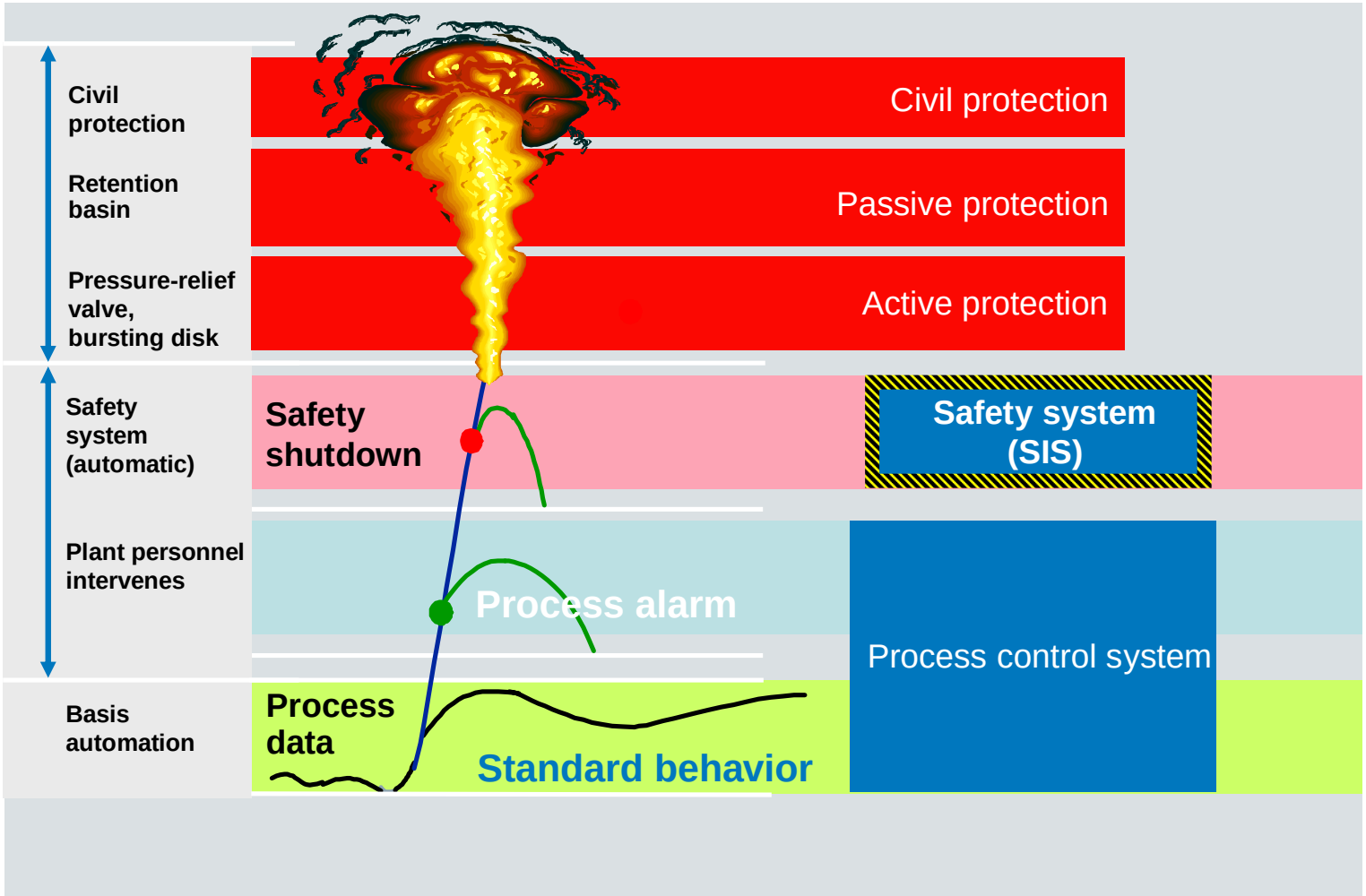
Fully Integrated Safety Communications

Standard Components are Non-Interfering with PROFIsafe Components

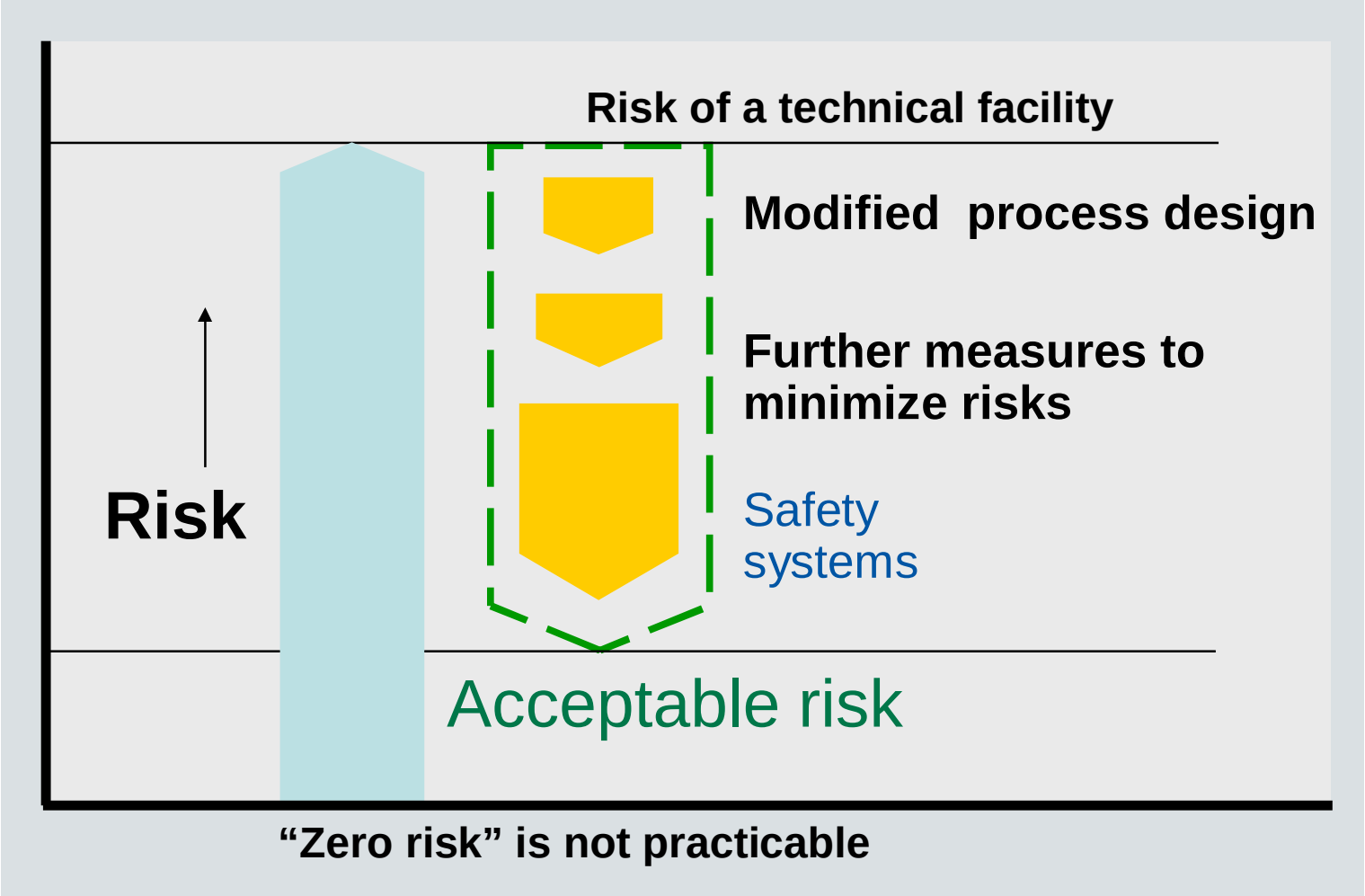


- **Fail-Safe I/O Modules for safety signals**
- **Standard I/O modules for non-safety signals**

Safety Concept of a Plant



Assessment of Risks → Minimizing Risks



International Safety Standards

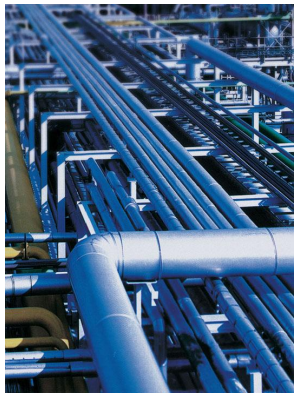
IEC Commission Electrotechnique Internationale International Electrotechnical Commission Международная Электротехническая Комиссия

IEC61508

The IEC 61508 is considered to be the basic standard and the basis for safety standardization.

It covers all applications in which safety-relevant protective functions are implemented with the help of electrical, electronic, or programmable (logic) control systems.

DIN 0801 and DIN V19250 become invalid from August 1, 2004.



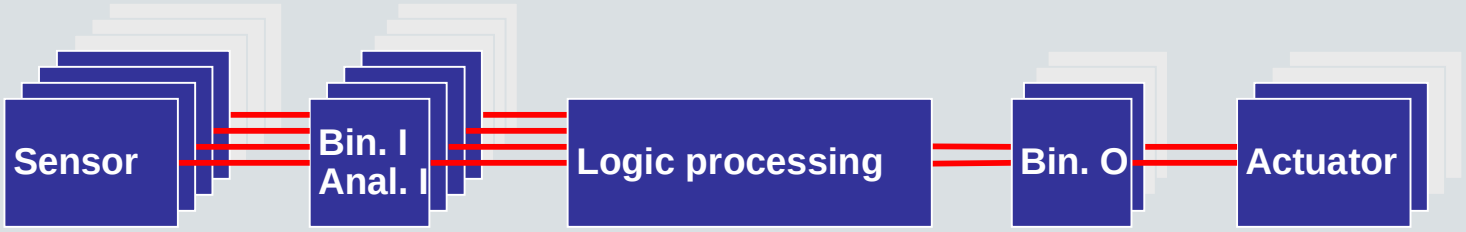
IEC Commission Electrotechnique Internationale International Electrotechnical Commission Международная Электротехническая Комиссия

IEC61511

Based on IEC 61508 there are sector-specific standards, such as IEC 61511 for the process industry or IEC 61513 for nuclear power generation.
These sector-specific standards are important for planers and operators of the corresponding plants.

Safety Functions
IEC 61508

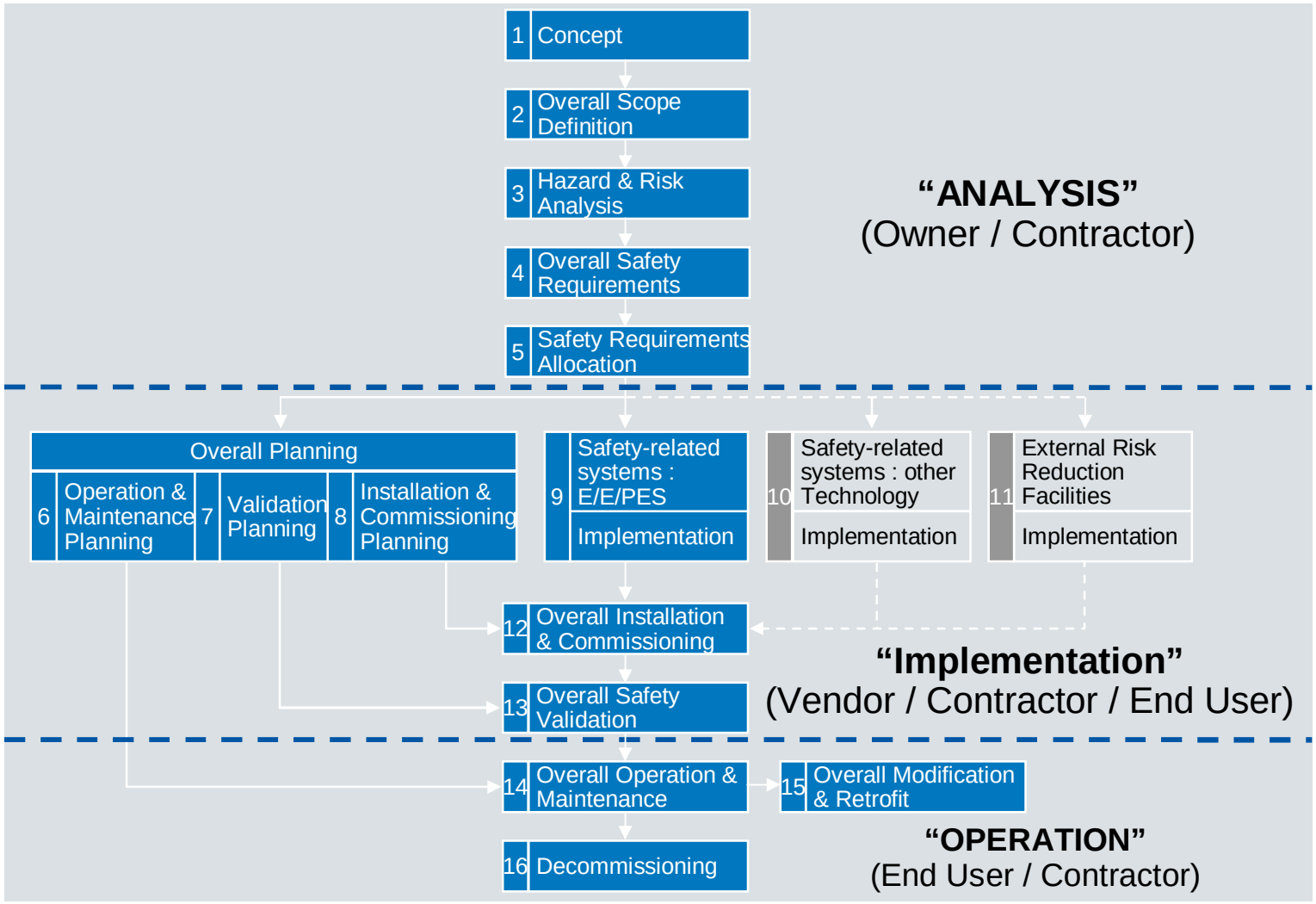
- **Considering the complete** safety functionality **of** loops **acc. to IEC 61508:**



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

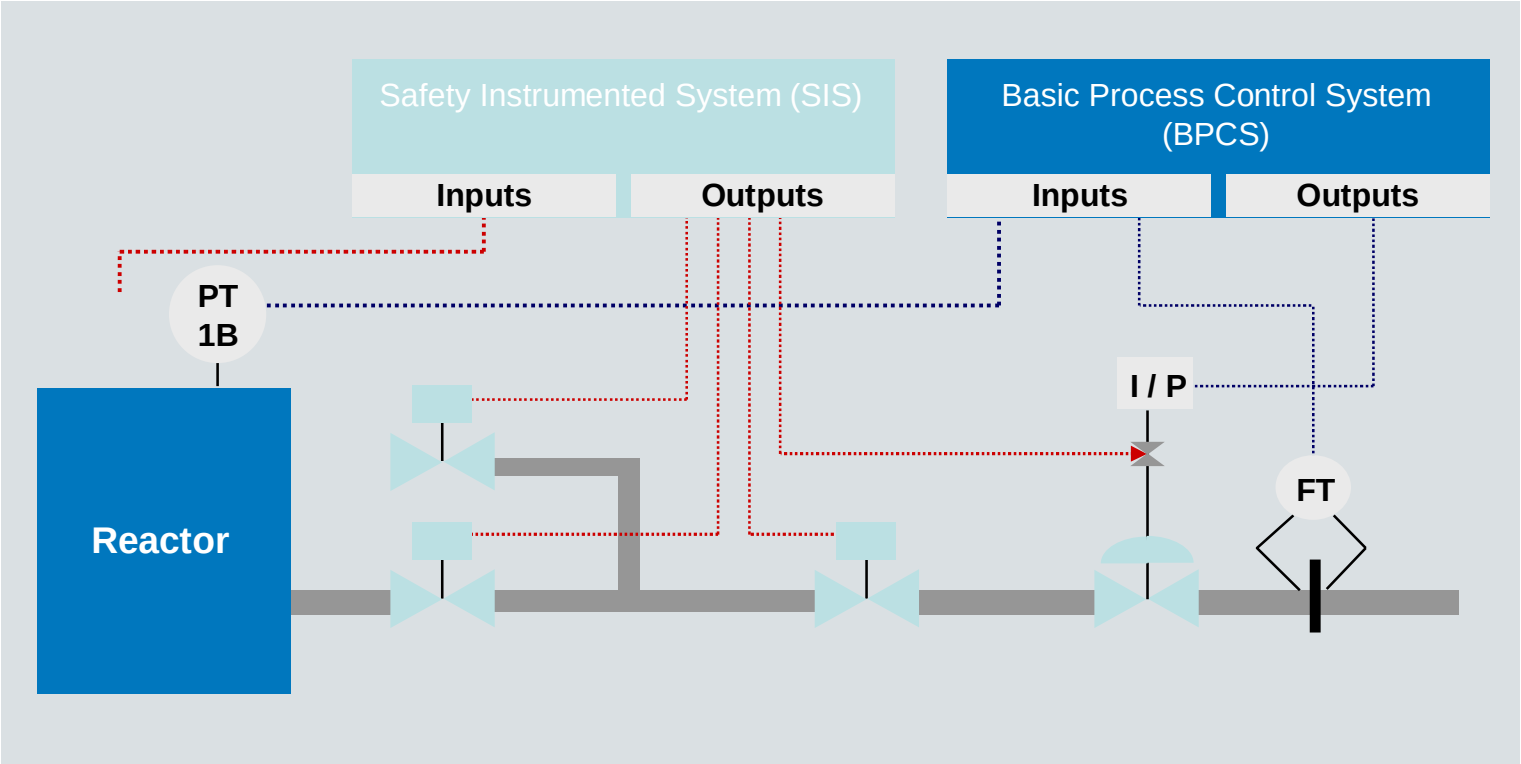
Acquire safe Information → **Combine Safe Information** → **Initiate Safe Response**

Safety Life Cycle
IEC 61508



Safety Instrumented System (SIS)

- **SIS: A combination of sensors, logic modules (e.g. controls) and actuators which detect abnormal operating conditions and return the plant AUTOMATICALLY to a safe state again.**



Safety Integrity Levels
IEC 61508

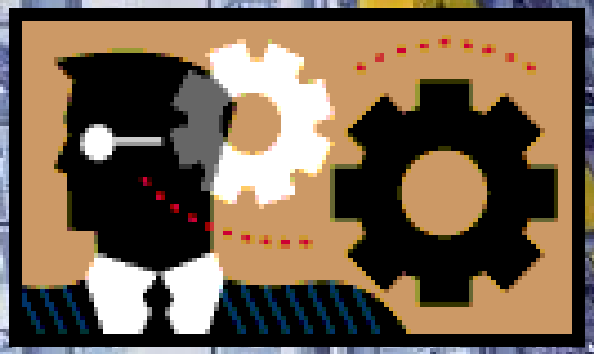
Safety Integrity Level	Probability of failure on demand (PFD) per year (Low Demand mode of operation)
SIL 4	>=10^{-5} to <10^{-4}
SIL 3	>=10^{-4} to <10^{-3}
SIL 2	>=10^{-3} to <10^{-2}
SIL 1	>=10^{-2} to <10^{-1}

SIL: A performance criterion of an SIS which describes, for example, the probability of the SIS failing in case of a disturbance.

Summary

- **Safety fieldbus is an emerging trend in process safety applications**
- **Technology to implement fieldbus in safety applications is available today**
- **Implementing safety fieldbus technology can provide distinct advantages over hardwired solutions:**
  - Improved diagnostics
  - Remote access to instrument data for asset management
  - Data to support reporting requirements (test and maintanance records)
  - Ability to design multiple fault tolerant Safety Instrumented System Architectures

Thank you - Questions?



THANK YOU.
QUESTIONS ?

PH: +65 6490 6370

stanley,joseph@siemens.com

Presenter: Stanley Joseph
Siemens Singapore