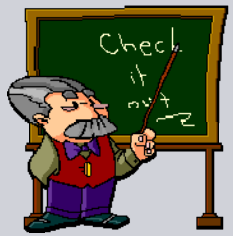
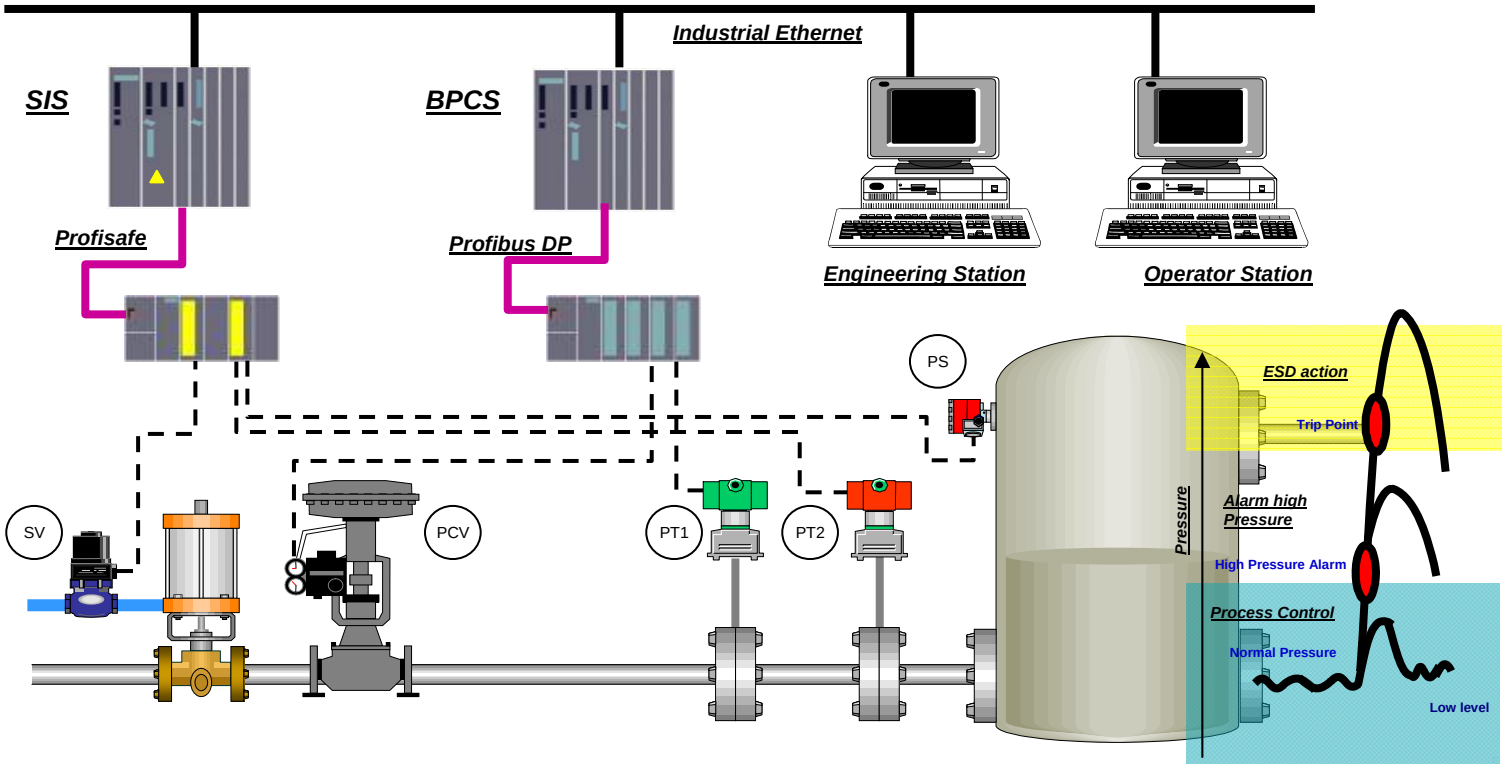

PI
South East Asia
PROFIBUS • PROFINET

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

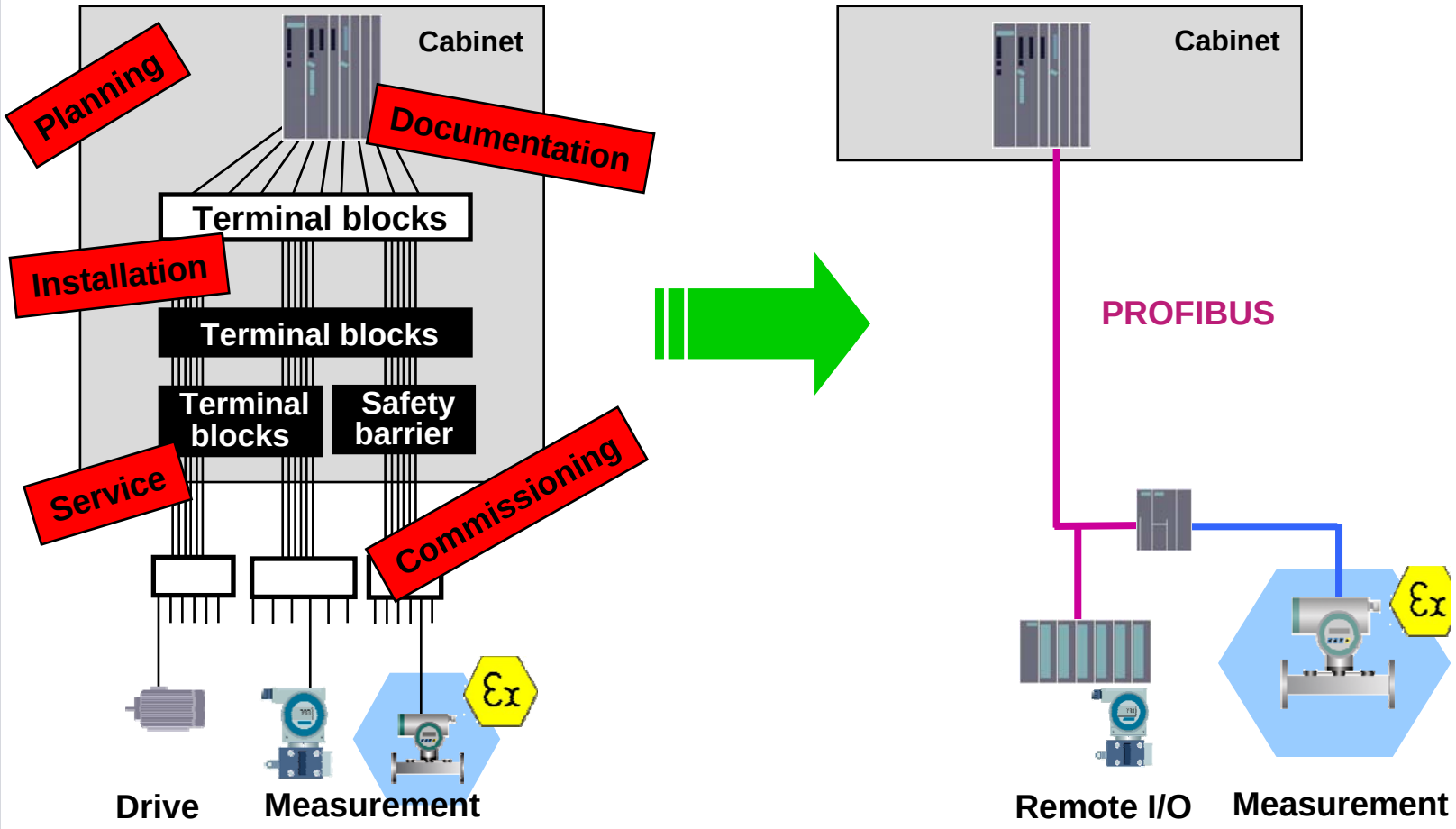
- Traditional safety systems have implemented internal, proprietary implementations of safety communications for years
  - CPU to I/O communications
  - CPU to CPU communications
- Industry experts share differing opinions about the viability of today's buses for safety networking
  - Some say hard wire 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

PROFIsafe

- Why Safety Fieldbus
- Safety Standards
- PROFIsafe Comms
- Flexible Architectures
- Benefits
- Application Example
- Summary

Up to 70% space saving + 40% cost saving



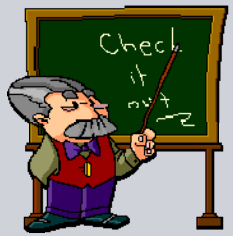
Advantages

- 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**

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

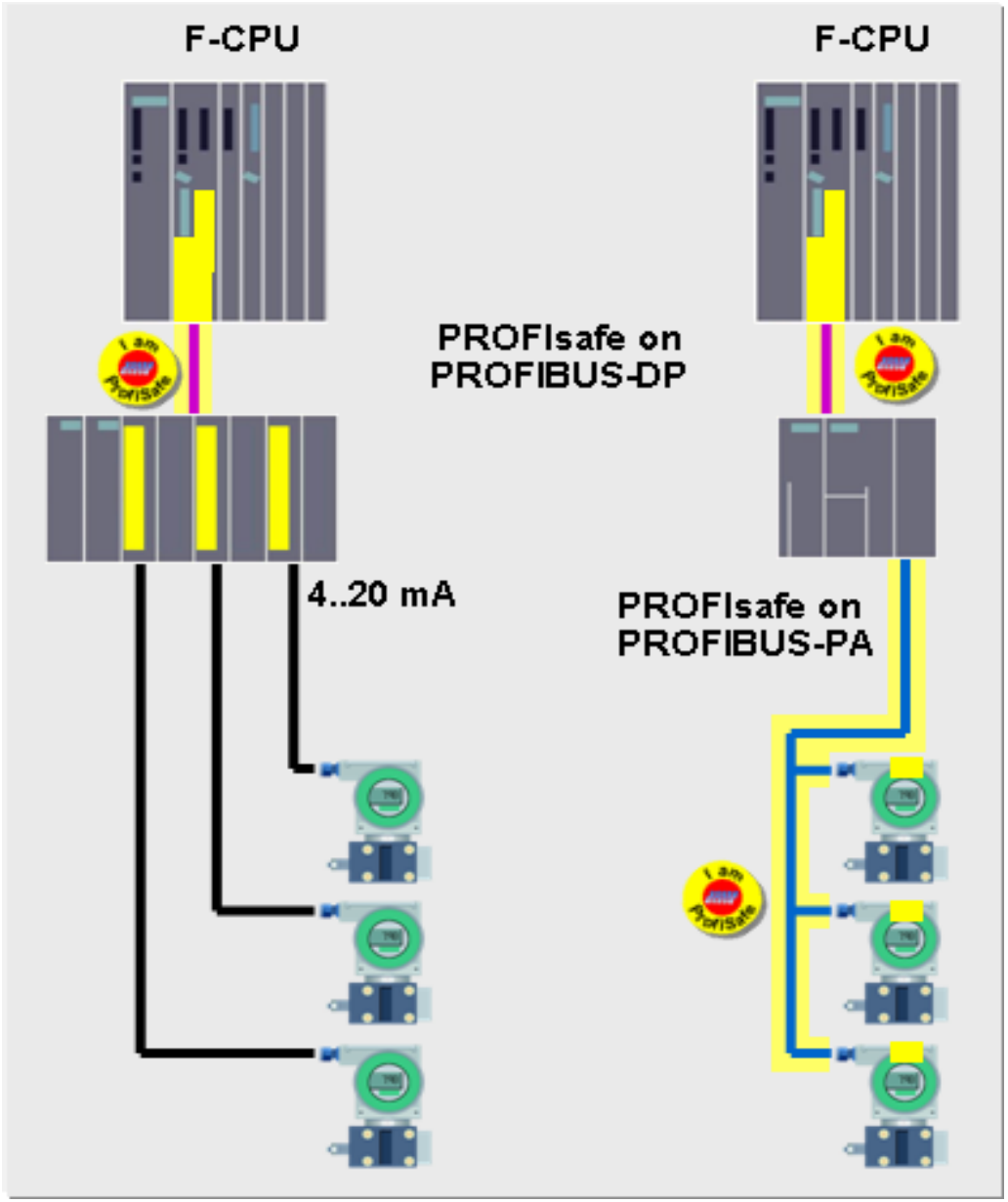
Key Requirements from ISA TR84.00.06

- **"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"**
- **Sufficiently fast response time**

Available Safety Fieldbus Technology

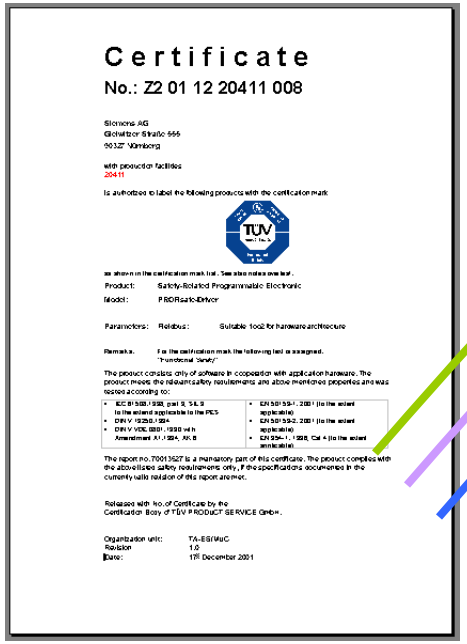
- Machine
  - **PROFIsafe**
  - **AS-i Safe**
  - **Interbus-S**
  - **DeviceNet Safety**
  - **Pilz SafetyBUS p**
  - **ABB AC31 Safety Fieldbus**
- Process
  - **PROFIsafe**
  - **FF-SIS**

Process Safety Fieldbus



PROFIsafe

- **PROFIsafe is a application layer (profile) that describes the communications between fail-safe devices**
- **Version 1.0 was published for review in 1999**
- **Current version (V1.30) published in June 2004**
- **Supports safe communication over open standard buses PROFIBUS (DP, PA) and PROFINET**
- **TUV Certified to IEC 61508 SIL 3 / EN 954-1 Cat 4**
- **850,000+ nodes installed**



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:

Product: Safety-Related Programmable Electronic

Model: PROFIsafe-Driver

Parameters: Fieldbus: Suitable 1oo2 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 2, 3 & 3 (to the extent applicable to the PES	• EN 50156-1: 2001 (to the extent applicable)
• DIN V 19250:1994	• EN 50156-2: 2001 (to the extent applicable)
• DIN V VDE 0801:1990 +A1 Amendment A1:1994, AK 6	• EN 954-1:1996, Cat 4 (to the extent applicable)

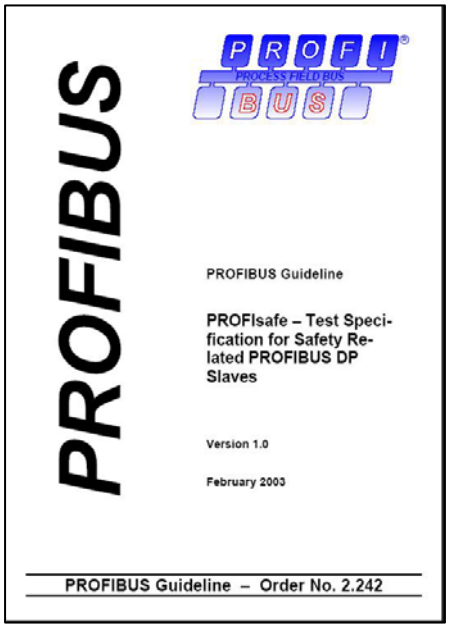
The report no. 70013627 is a mandatory part of this certificate. The product complies with the above listed safety requirements only, if the specifications documented in the currently valid revision of this report are met.

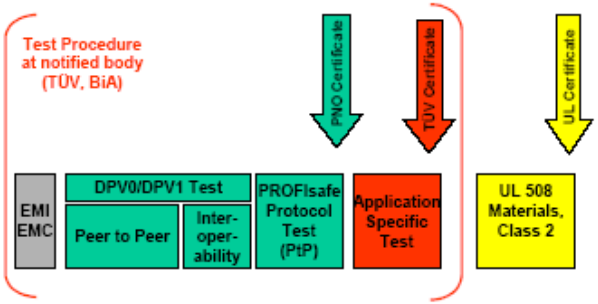
Released with the Certificate by the Certification Body of TÜV PRODUCT SERVICE GmbH.

Organization unit: TA-EB/MuC
Revision 1.0
Date: 17th December 2001

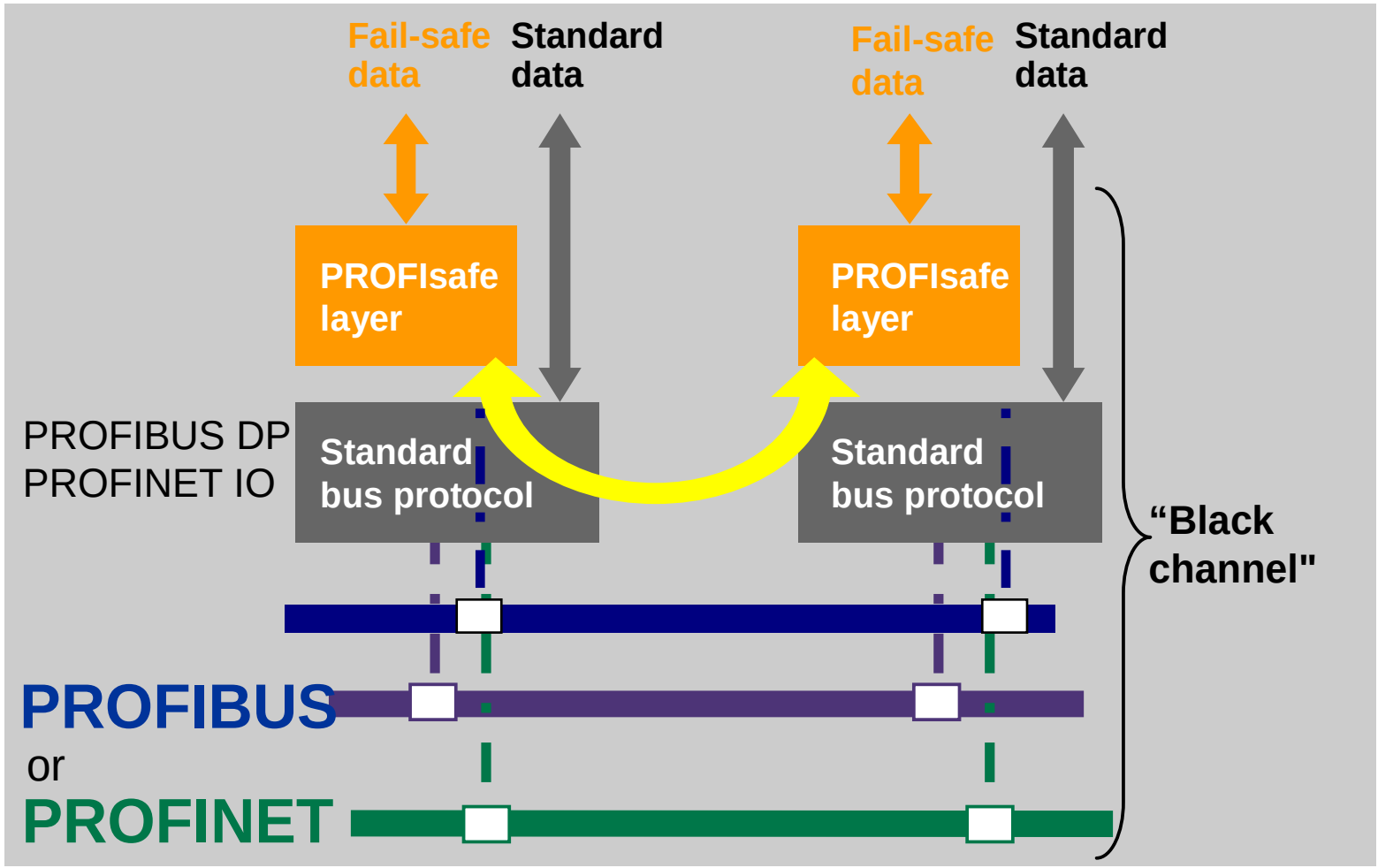
Interoperability

- PROFIsafe slave software development is supported by a generic PROFIsafe driver
  - Distributed as ANSI C source code as part of a PROFIsafe starter kit
- Use of this driver saves development resources and time and ensures interoperability
- TÜV approved this driver for SIL 3 requirements
- Test Specification
- Proven device certification process (7 independent test labs)

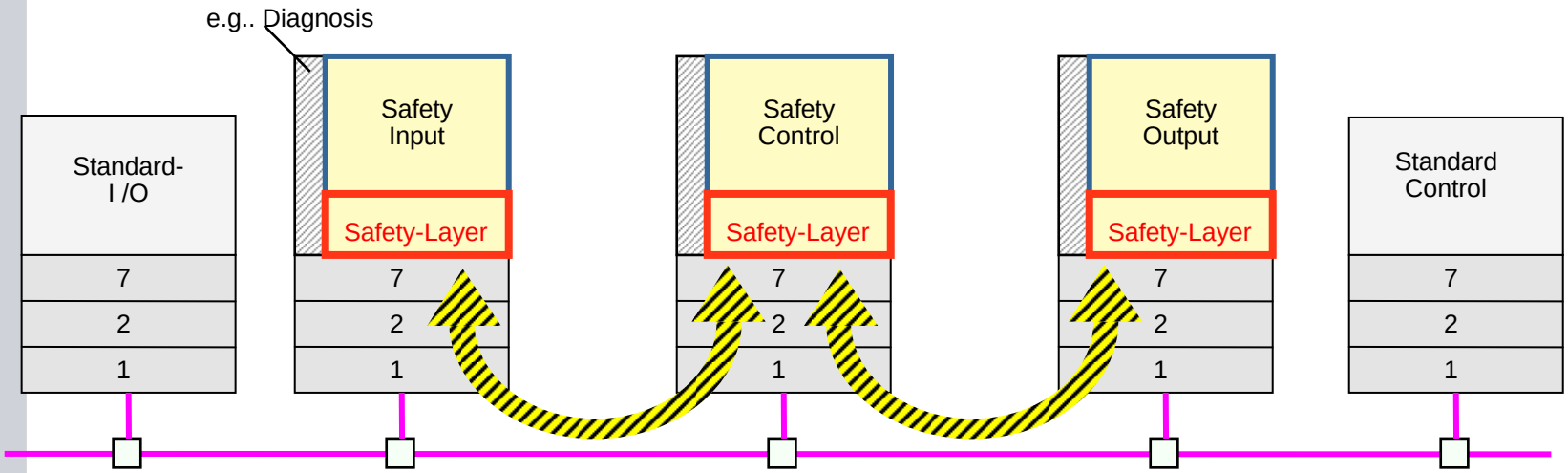




Same Protocol Supports PROFIBUS (DP, PA) & Profinet



PROFIsafe Communications Layer



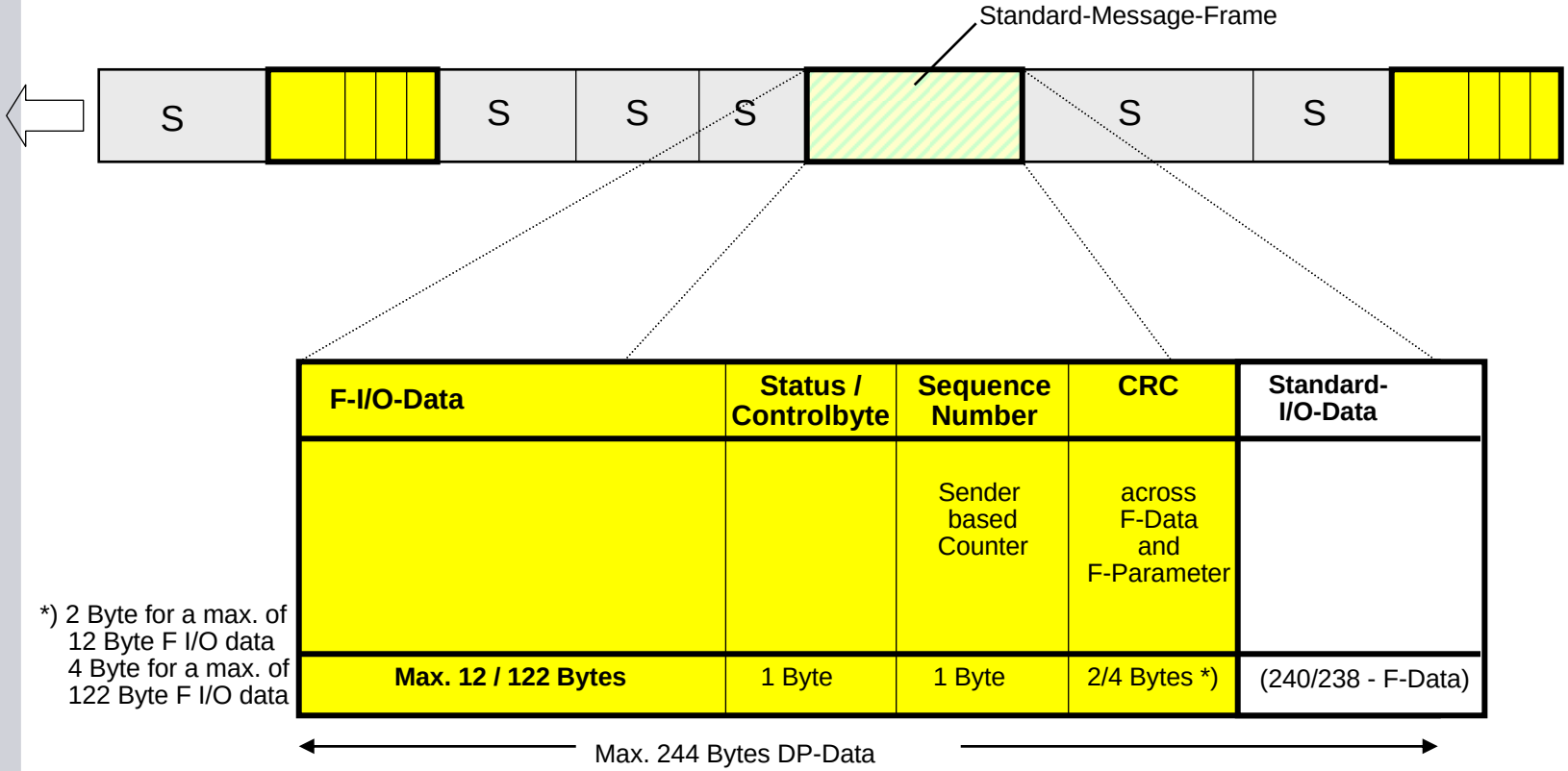
"Black Channel": ASICs, Links, Cables, etc. are not safety relevant

Non safety critical functions, like e.g. diagnosis

"**PROFIsafe**": Parts of the safety critical communications systems: Adressing, Watch Dog Timers, Sequencing, Signature, etc.

Safety relevant, but not part of the PROFIsafe-Profils: Safety I/O and the Safety Control Systems

PROFIsafe Message Format



Comm Failures and PROFIsafe Remedial Measures

Remedy: / Failure type:	Consecutive Number	Time Out with Receipt	Codename for Sender and Receiver	Data Consistency Check (CRC)
Repetition	X			
Deletion	X	X		
Insertion	X	X	X	
Resequencing	X			
Data Corruption				X
Delay		X		
Masquerade (standard message mimics failsafe)		X	X	X
FIFO failure within Router		X		

From: Position paper DKE-AK 226.03

EVALUATION REPORT

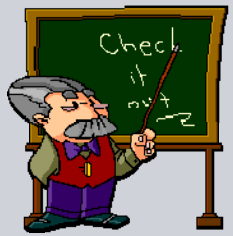
PROFIBUS Specifications
PROFIsafe - Profiles for Failsafe Technology

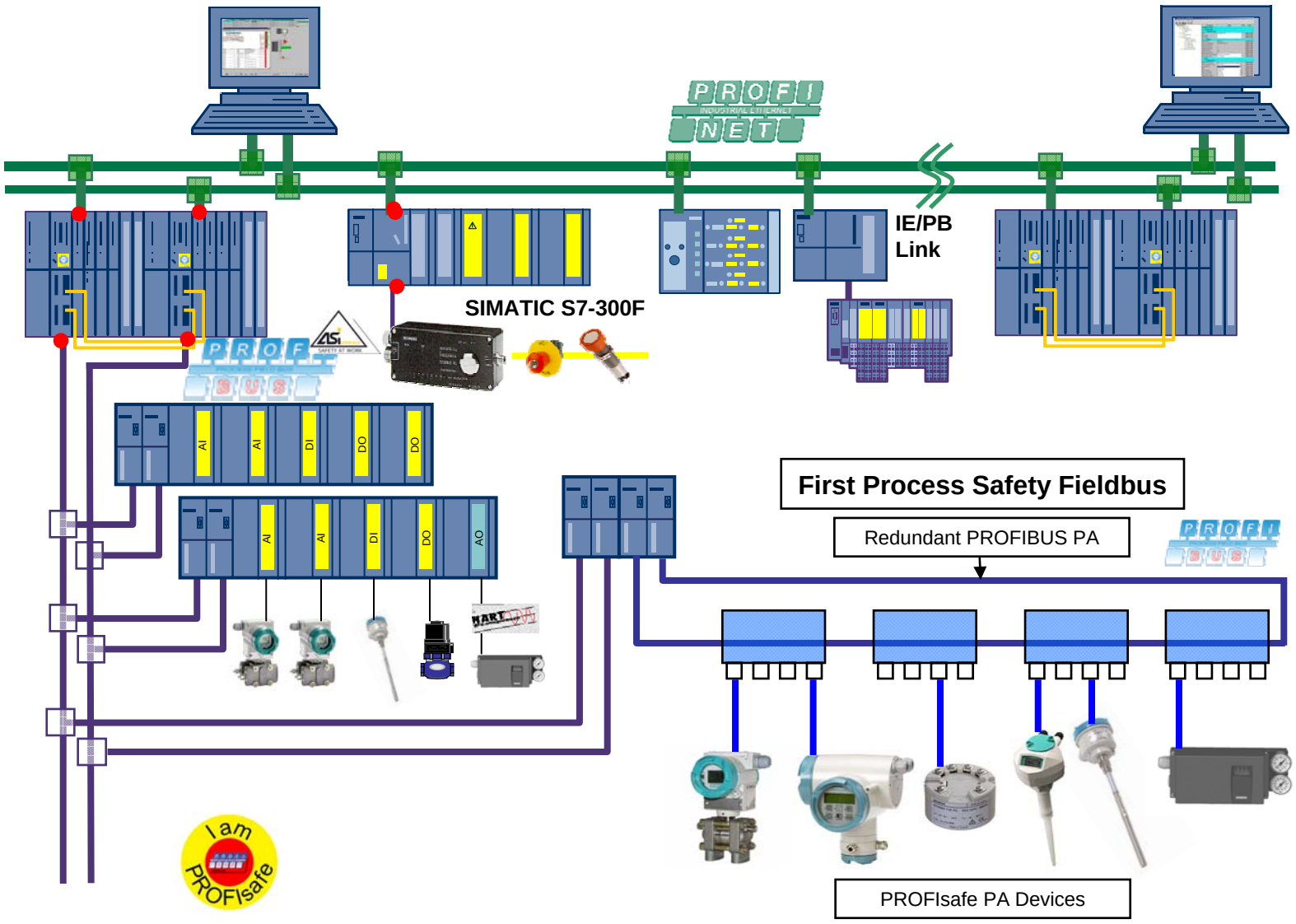
The measures shall be executed and monitored inside **one** fail-safe unit

Fully Integrated Safety Communications

PROFIsafe

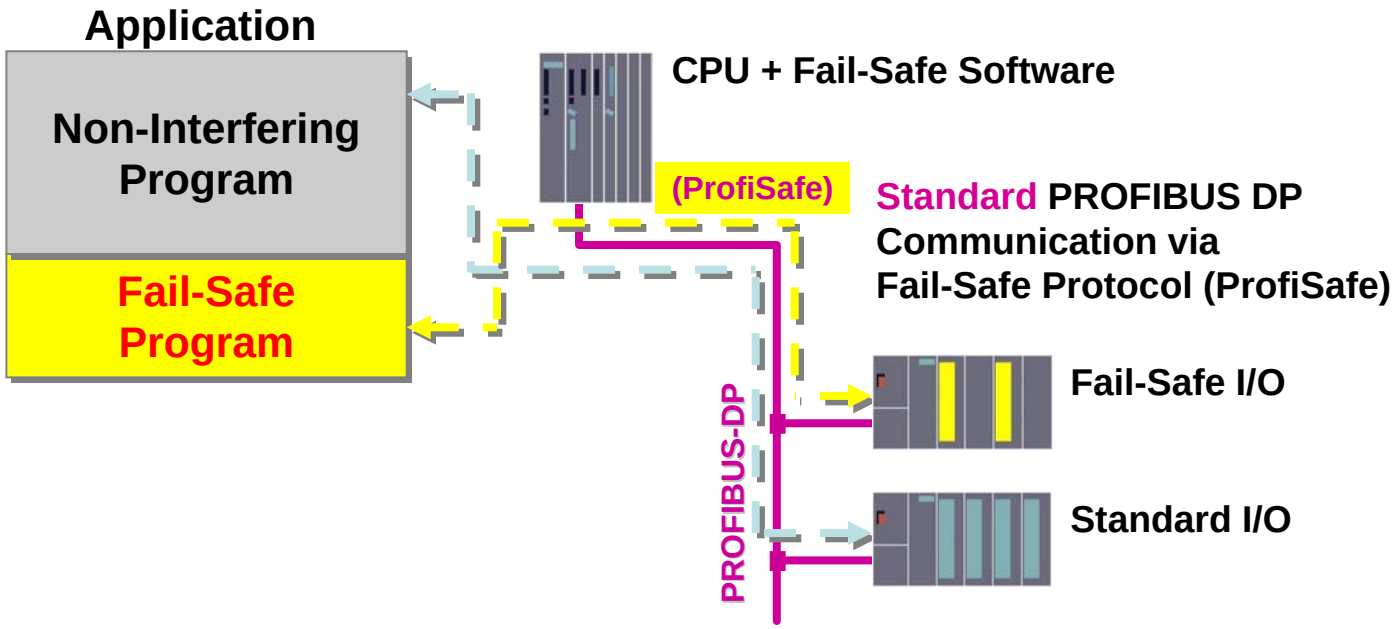
- Why Safety Fieldbus
- Safety Standards
- PROFIsafe Comms
- Flexible Architectures
- Benefits
- Application Example
- Summary





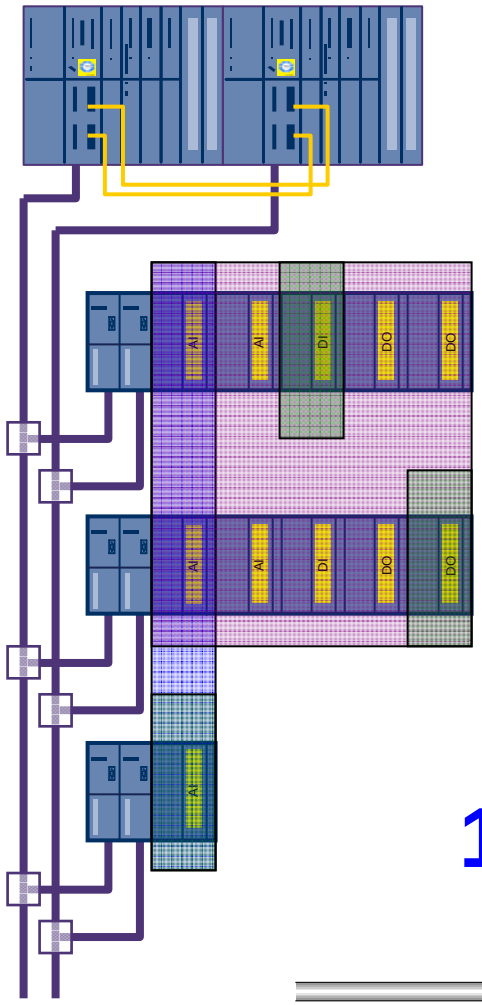
Fully Integrated Safety Communications

Standard Components are Non-Interfering with PROFIsafe Components



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

Flexible Architectures with Profisafe



- **Flexibility to choose the redundancy levels to fit each Safety Instrumented Function (SIF)**
- **Mix and Match to meet the goals of the application**

2oo2D (Dual 1oo1D)

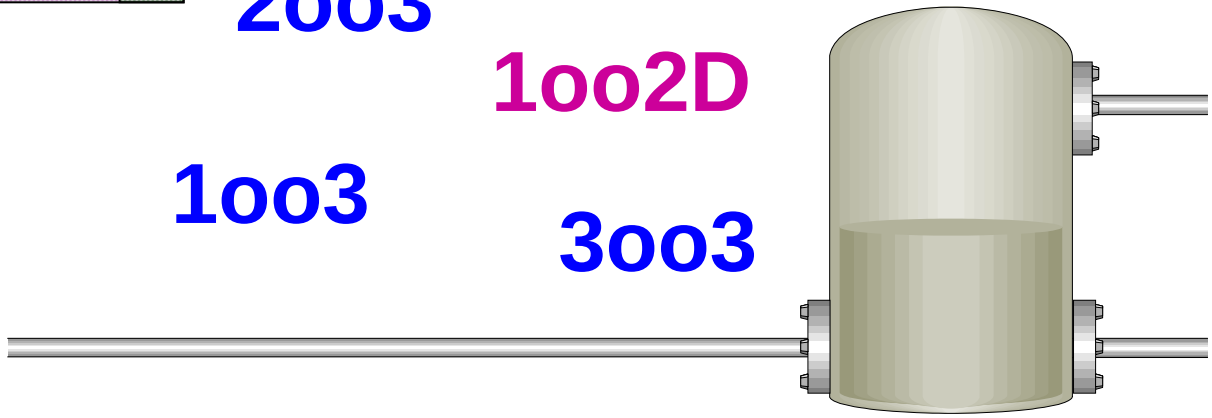
1oo1D

2oo3

1oo2D

1oo3

3oo3



Flexible Architectures with Profisafe

PROFIsafe

Why Safety Fieldbus

Safety Standards

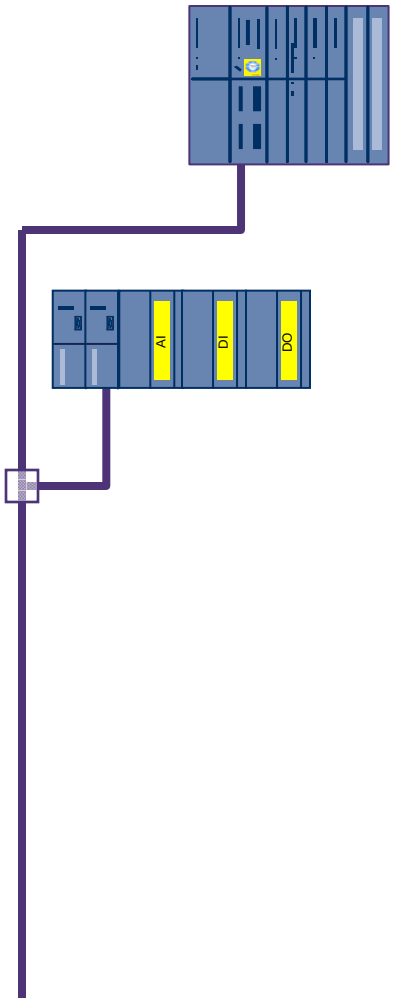
PROFIsafe Comms

Flexible Architectures

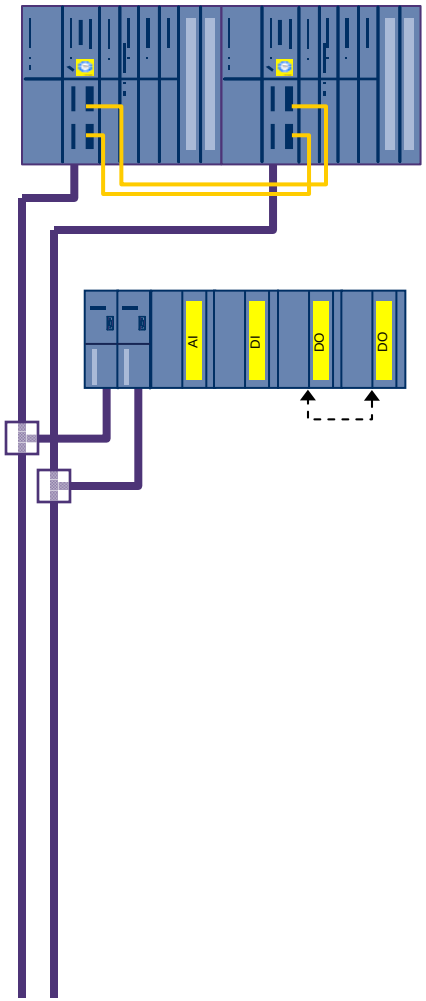
Benefits

Application Example

Summary

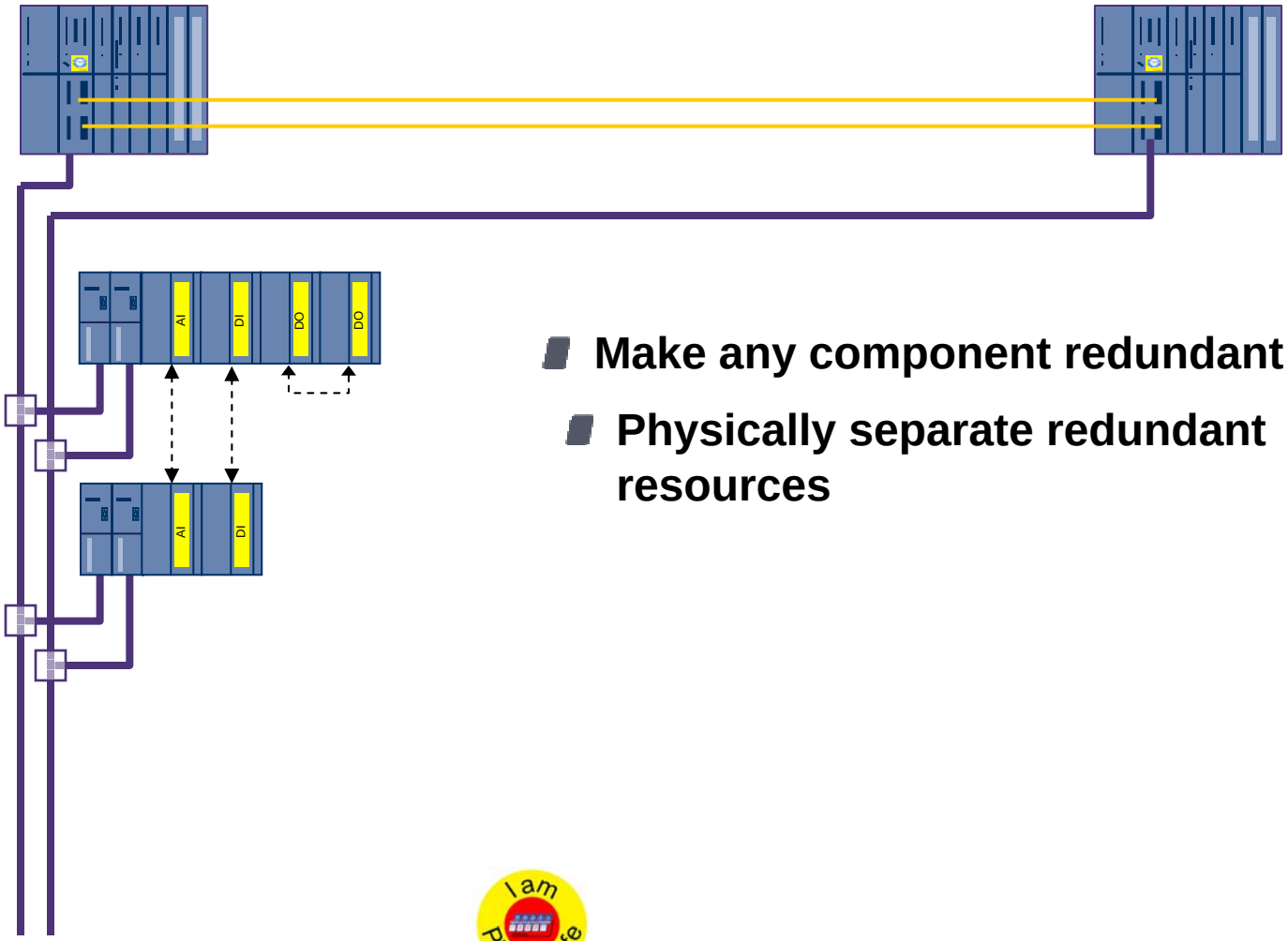


Flexible Architectures with Profisafe



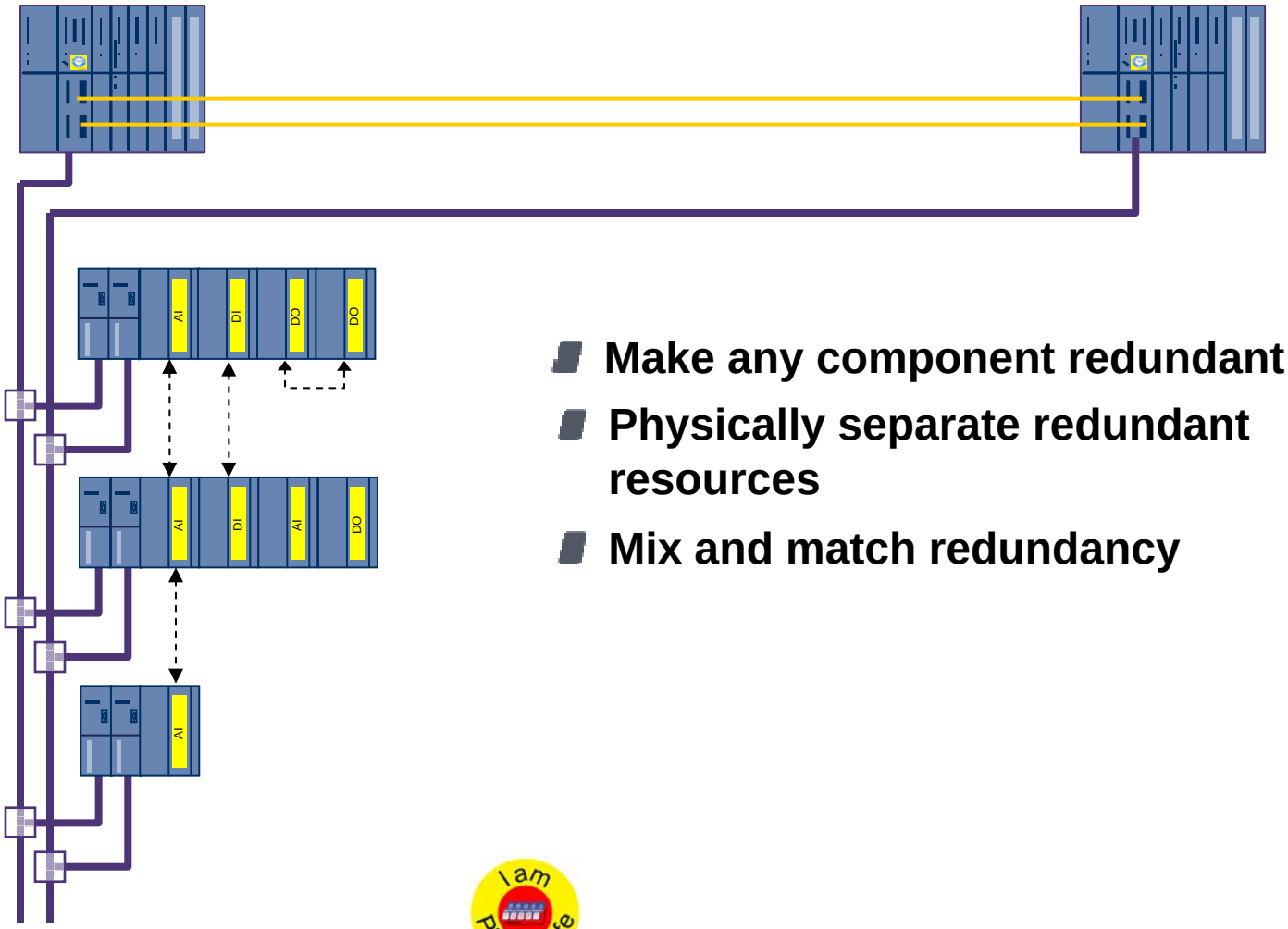
- **Make any component redundant**

Flexible Architectures with Profisafe



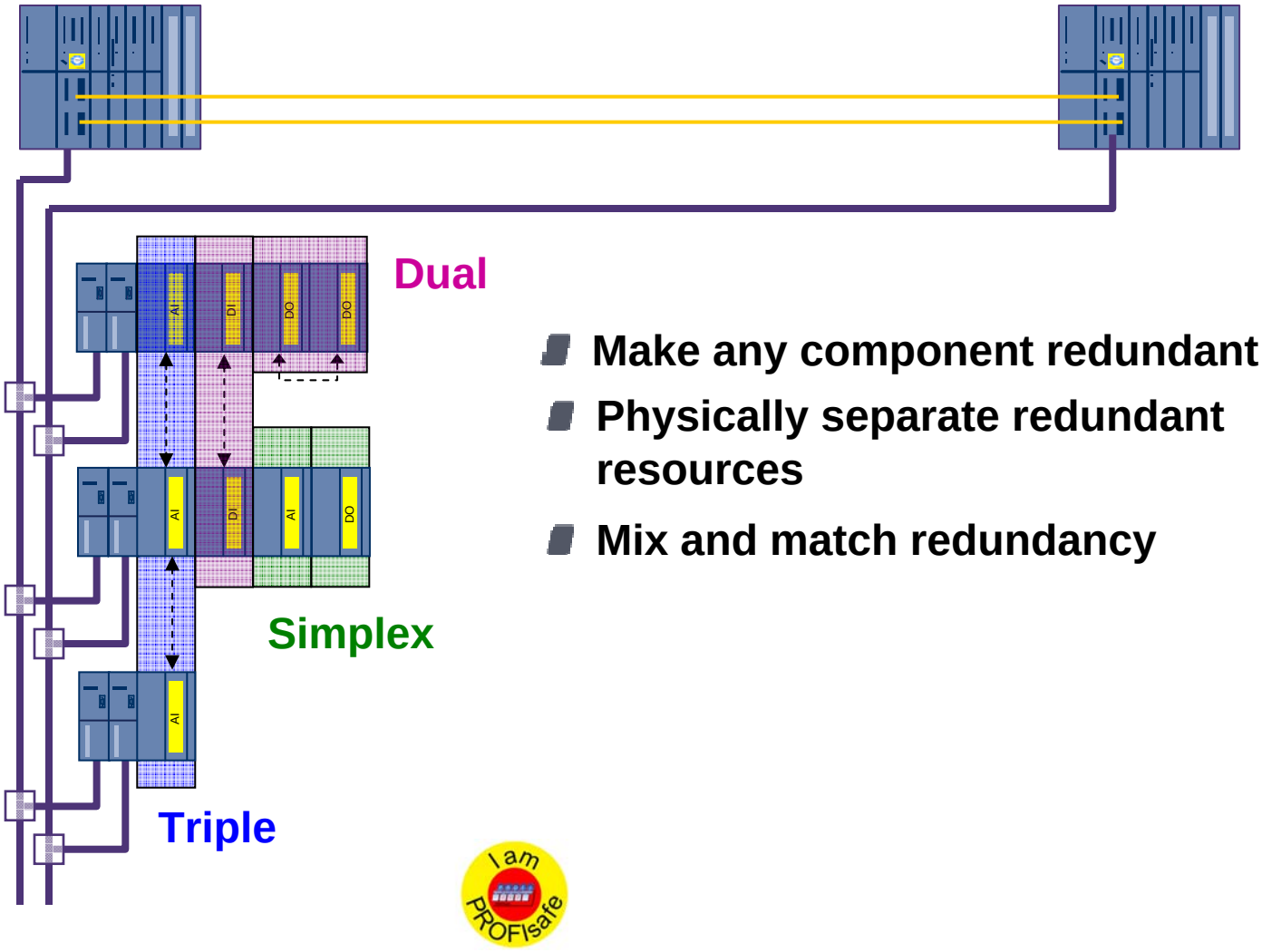
- **Make any component redundant**
- **Physically separate redundant resources**

Flexible Architectures with Profisafe



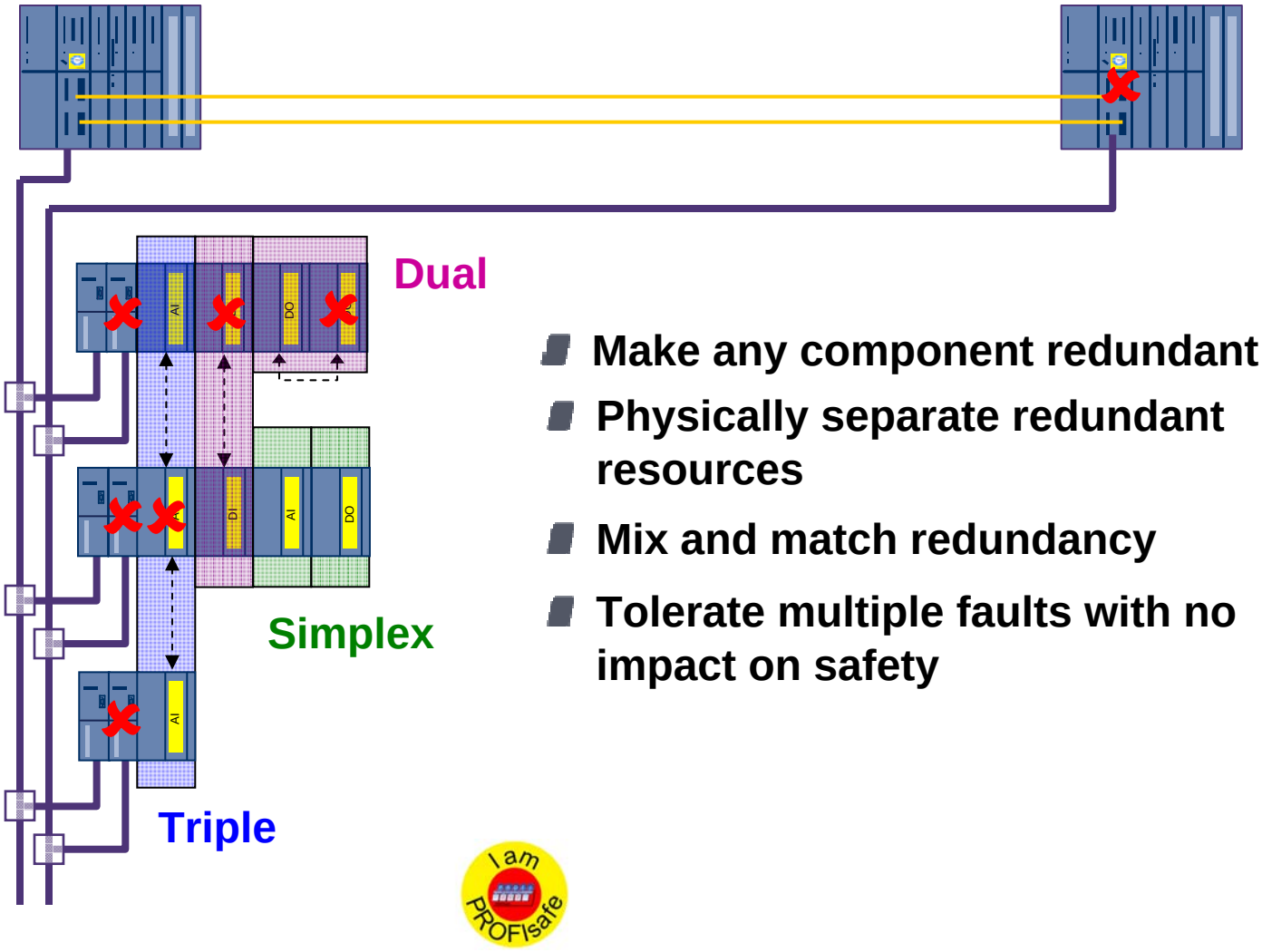
- **Make any component redundant**
- **Physically separate redundant resources**
- **Mix and match redundancy**

Flexible Architectures with Profisafe



- **Make any component redundant**
- **Physically separate redundant resources**
- **Mix and match redundancy**

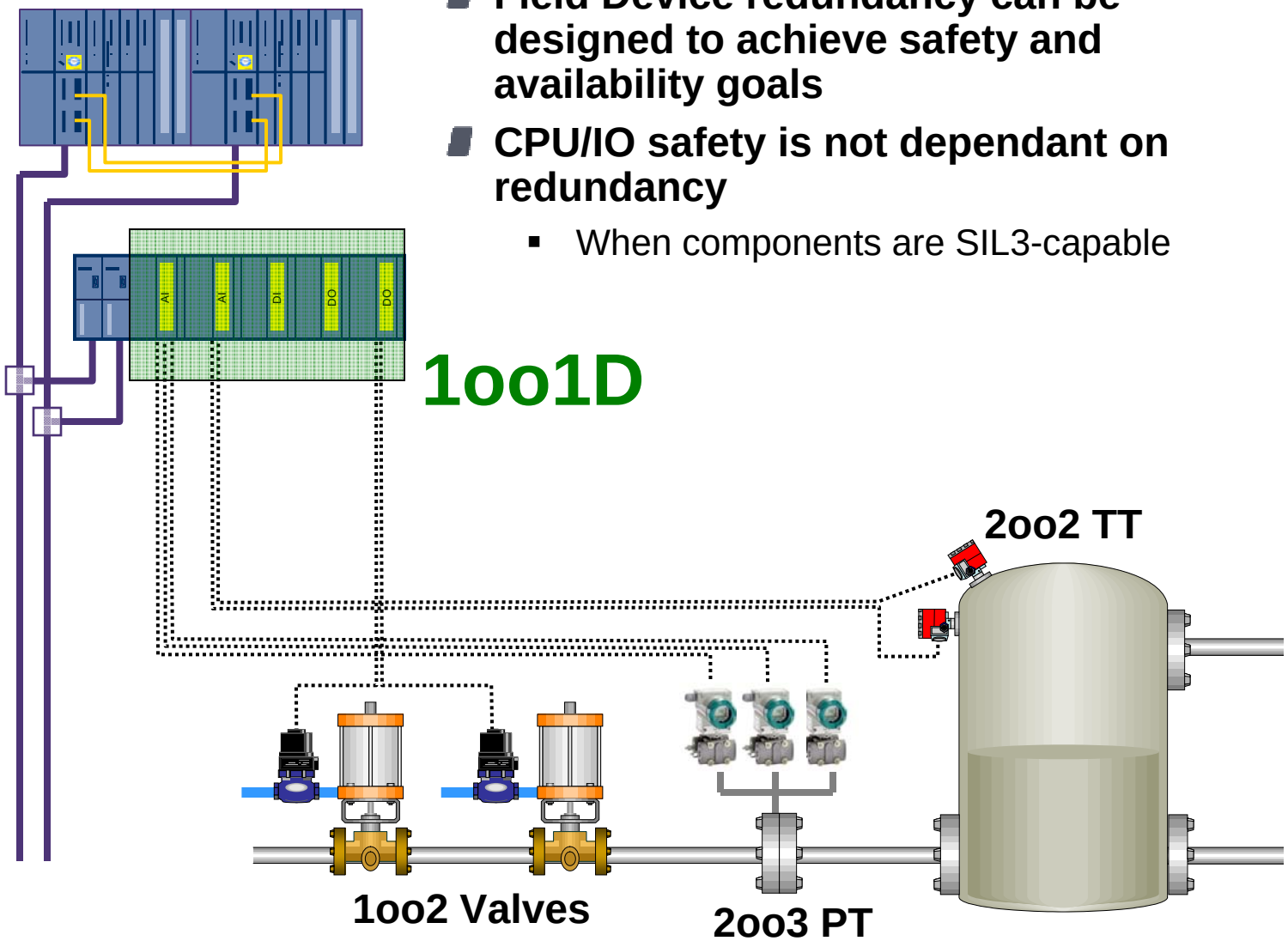
Flexible Architectures with Profisafe



- **Make any component redundant**
- **Physically separate redundant resources**
- **Mix and match redundancy**
- **Tolerate multiple faults with no impact on safety**

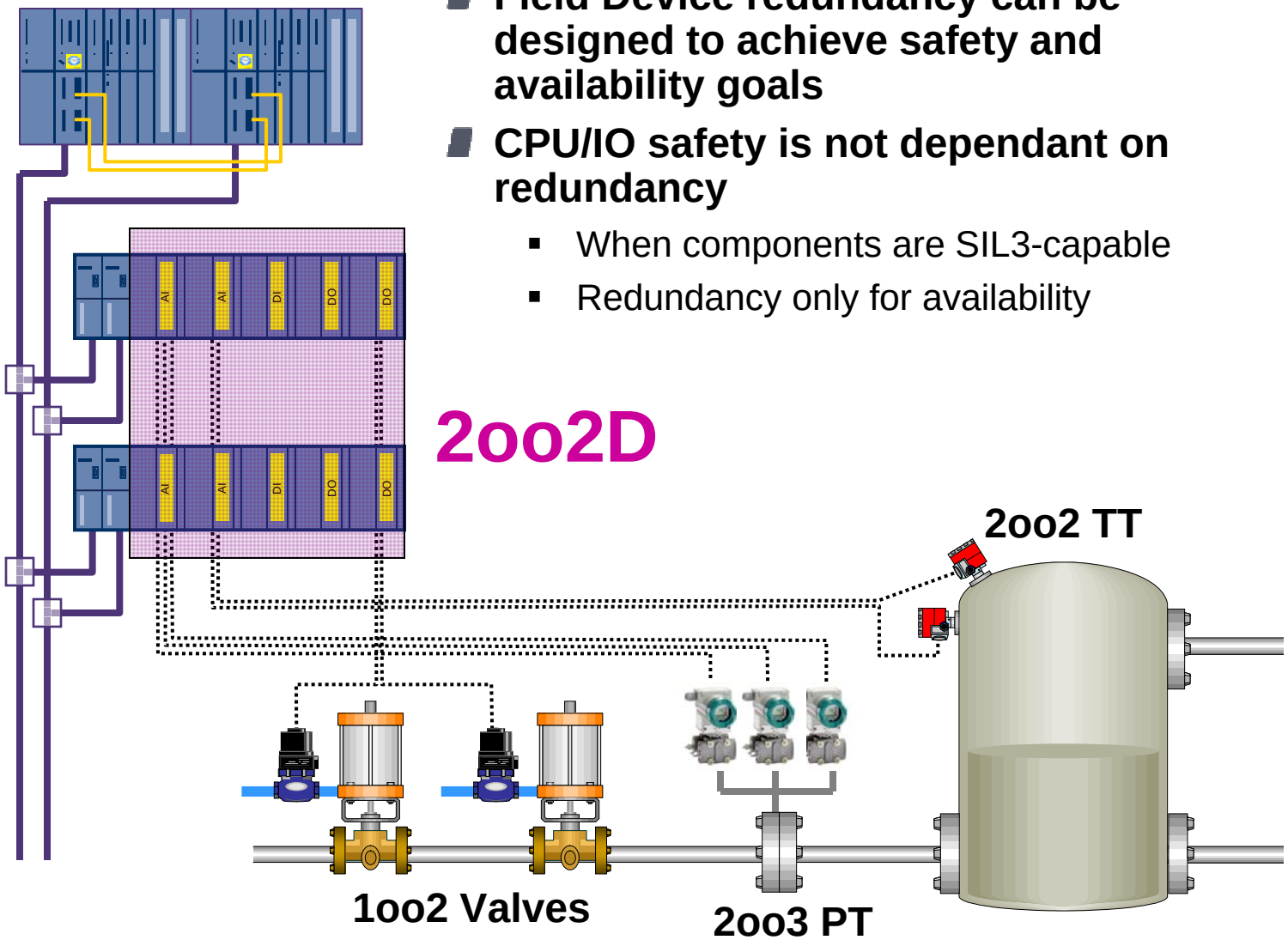
Flexible Architectures with Profisafe

- **Field Device redundancy can be designed to achieve safety and availability goals**
- **CPU/IO safety is not dependant on redundancy**
  - When components are SIL3-capable



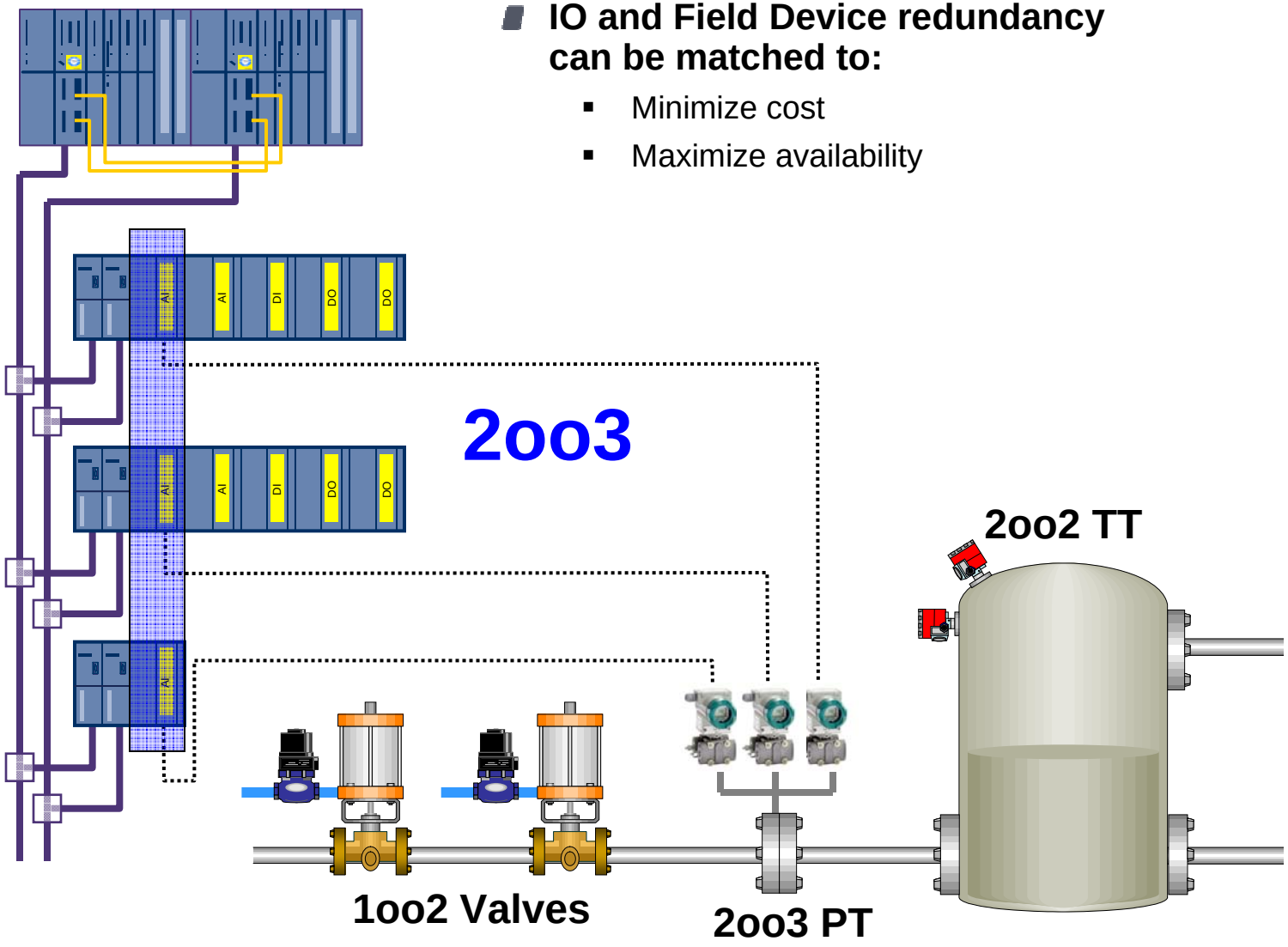
Flexible Architectures with Profisafe

- **Field Device redundancy can be designed to achieve safety and availability goals**
- **CPU/IO safety is not dependant on redundancy**
  - When components are SIL3-capable
  - Redundancy only for availability



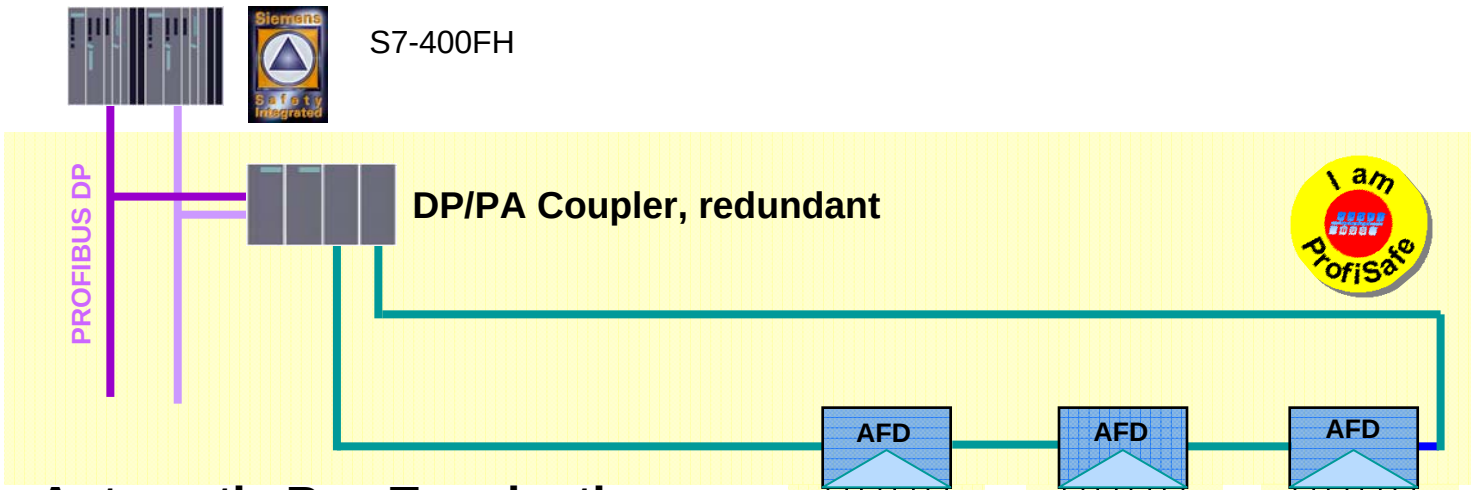
Flexible Architectures with Profisafe

- **IO and Field Device redundancy can be matched to:**
  - Minimize cost
  - Maximize availability

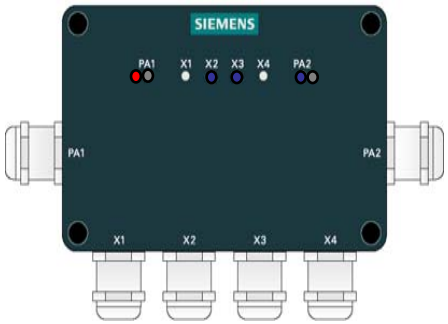


And Now with PROFIBUS PA Redundancy

- **Ring Architecture with Active Field Distributor**

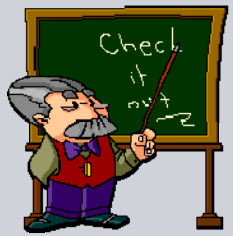


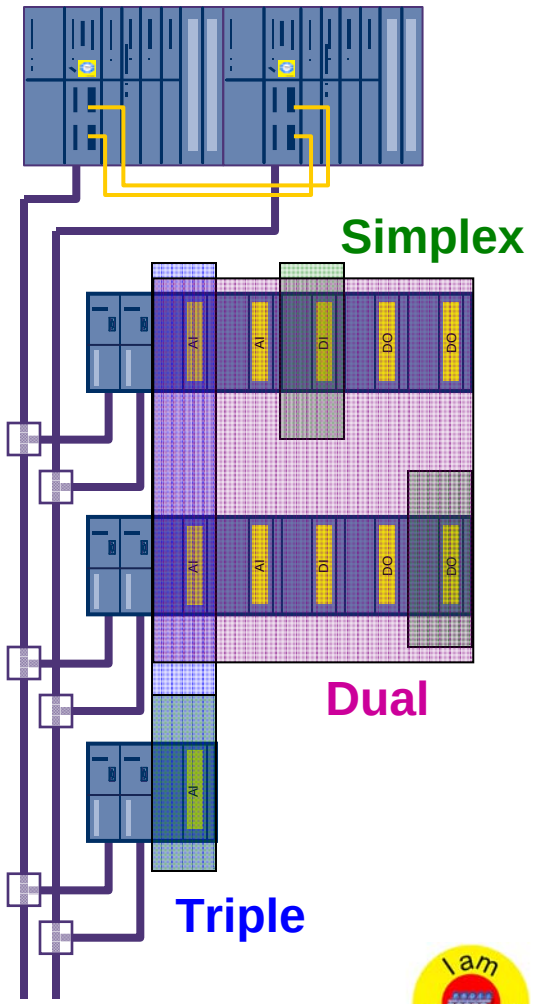
- **Automatic Bus Termination**



- **Safe communication down to the field device**
- **Safety and high availability on one segment**

Flexible Architectures with Profisafe





- **Ultimate flexibility to choose the redundancy levels to fit the Safety Instrumented Function (SIF)**
- **Mix and Match to meet the goals of the application**
- **CPU/IO safety is not dependant on redundancy**
  - When components are SIL3-capable
  - Redundancy only for availability
- **IO and Field Device redundancy can be matched to:**
  - Meet Target Safety Performance
  - Maximize availability
  - Minimize cost

Example Application for Profibus with PROFIsafe

- **PROFIsafe**
- Why Safety Fieldbus
- Safety Standards
- PROFIsafe Comms
- Flexible Architectures
- Benefits
- Application Example
- Summary

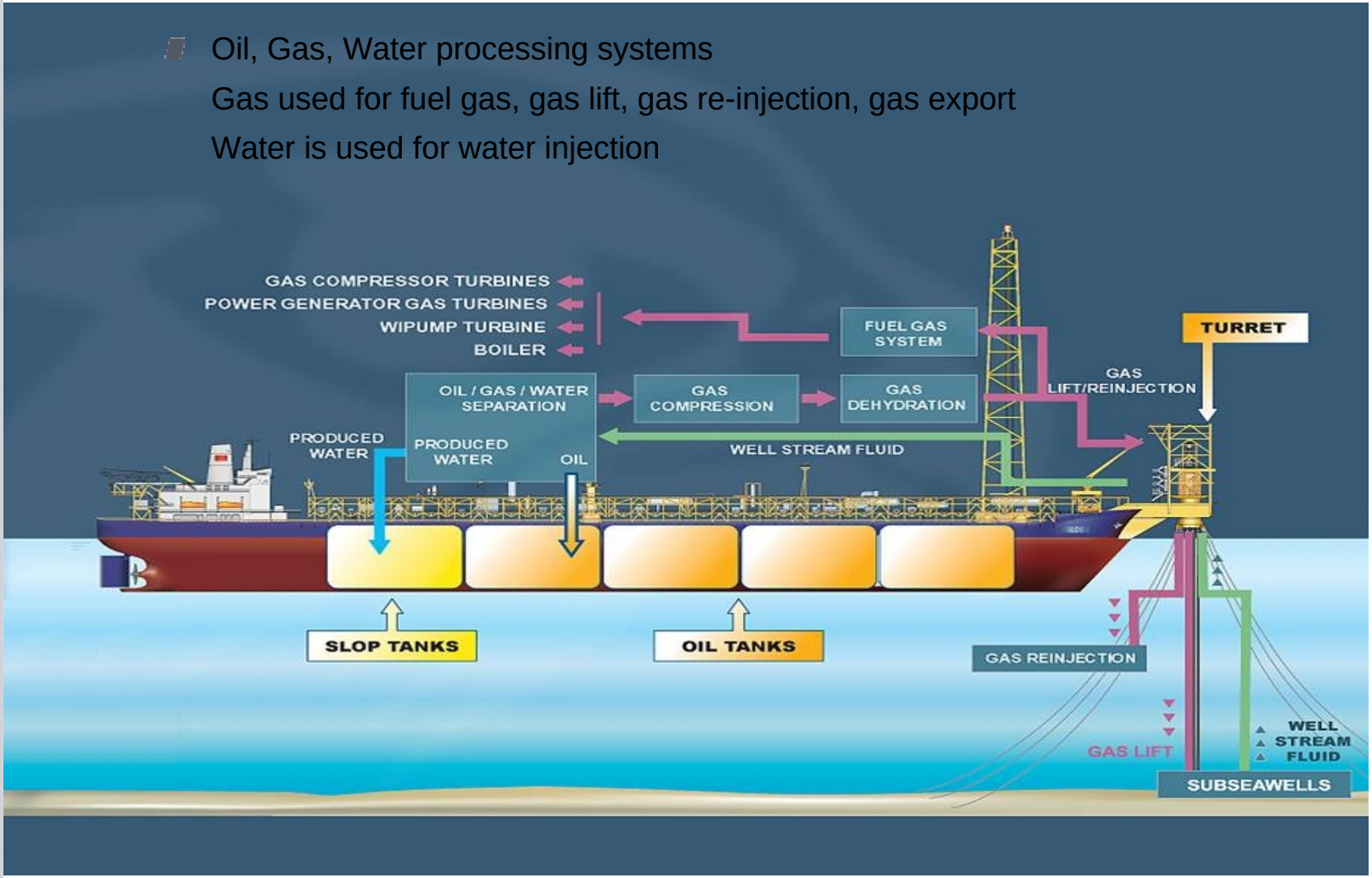
What is an FPSO ?

Floating Production Storage and Offloading

- Oil, Gas, Water processing systems

  Gas used for fuel gas, gas lift, gas re-injection, gas export

  Water is used for water injection



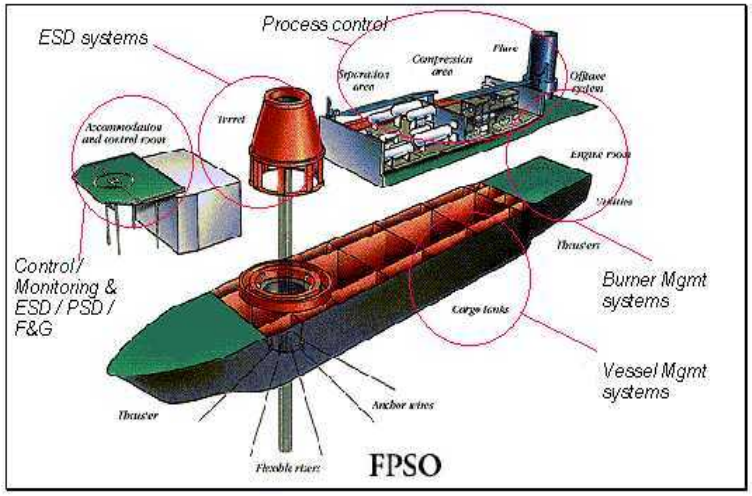
FPSO Control Systems

Process control (PCS)

- Production inlet
- Fiscal metering
- Heating and cooling
- Oil & Gas separation
- Gas compression
- Water injection
- Gas dehydration
- Power generation
- Water treatment
- Gas re-injection

Safety systems

- Process shutdown (PSD) - SIL1 or SIL2
- Emergency shutdown (ESD) SIL3 system
- Fire and Gas (F&G)



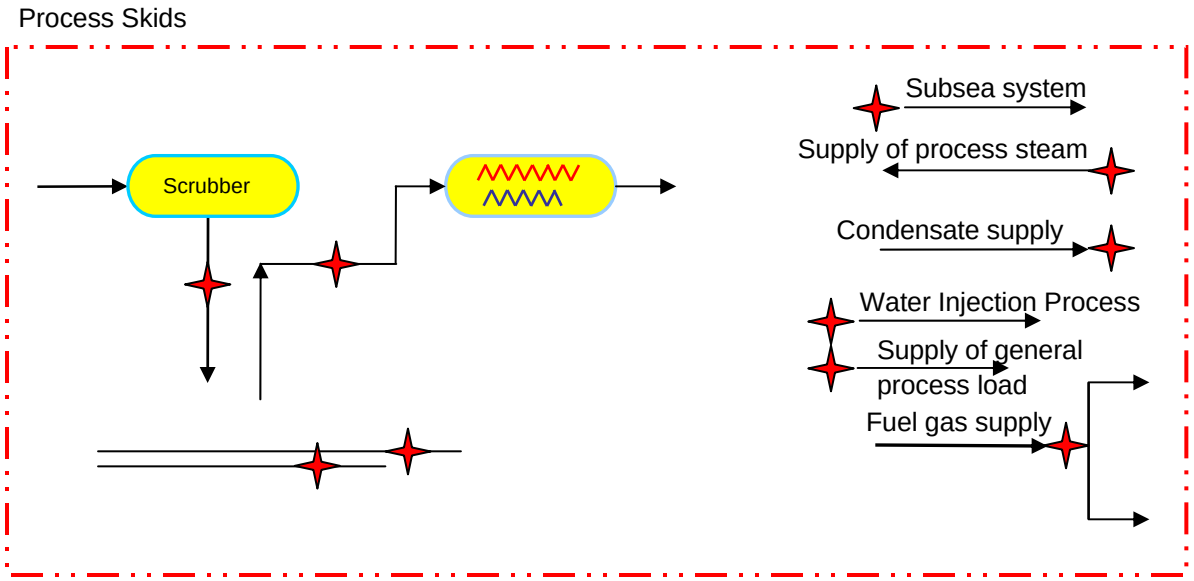
Vessel utilities

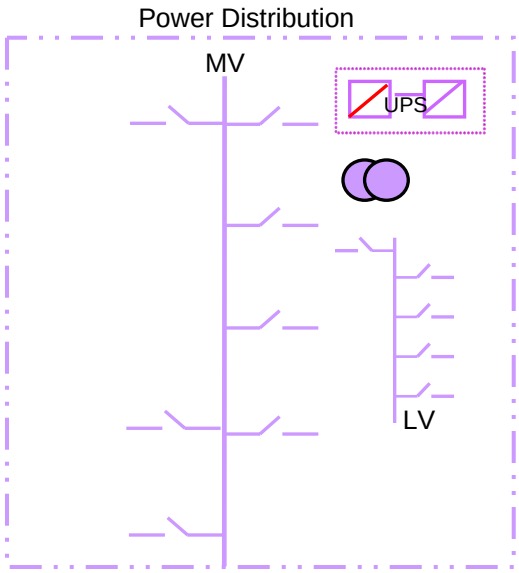
- Monitoring and alarm system
- Ballast monitoring and control
- Cargo offloading
- Standby motor control
- Power management
- Load, stress and stability calculations
- Bilge control

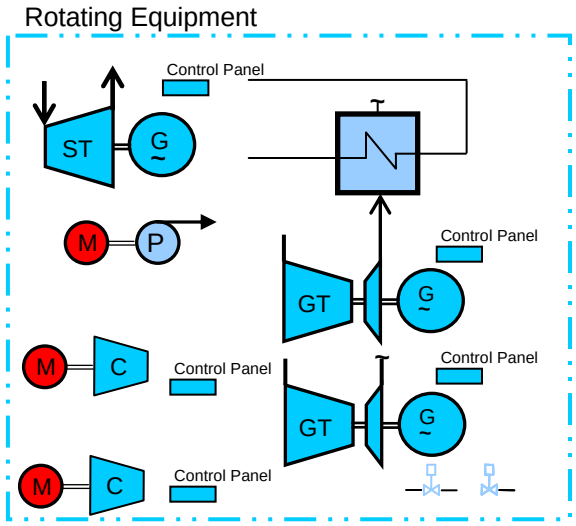
Engine room

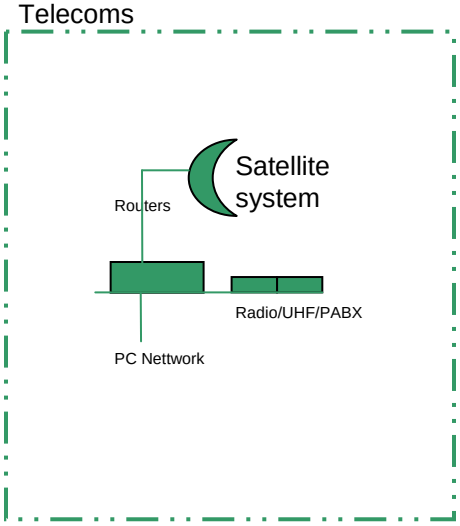
- Boiler regulatory control
- Boiler safety / burner management

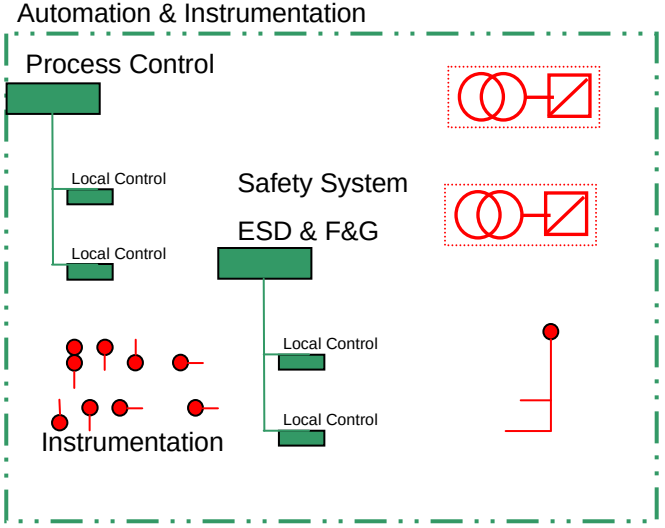
Traditional Automation and Electrical



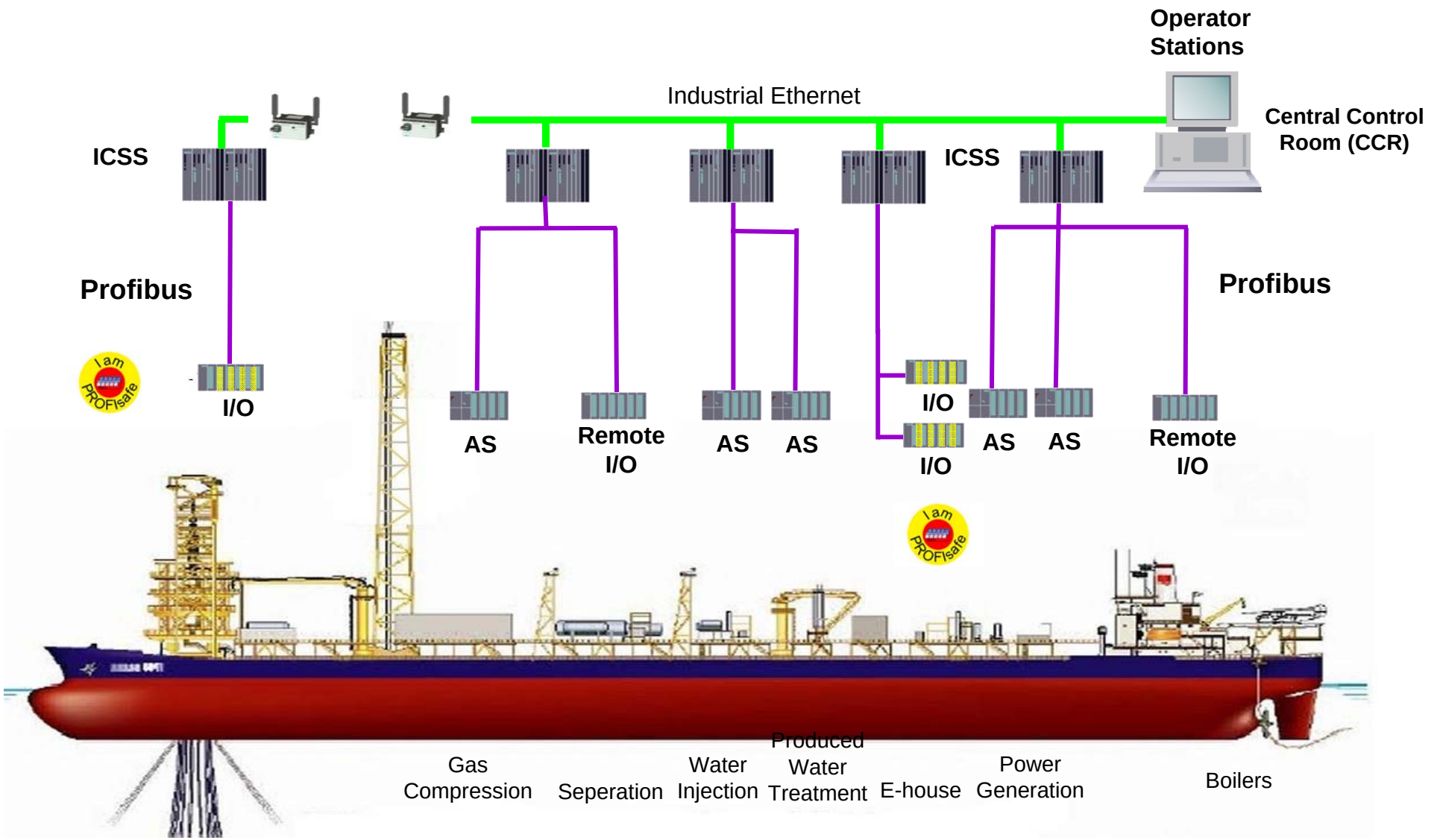




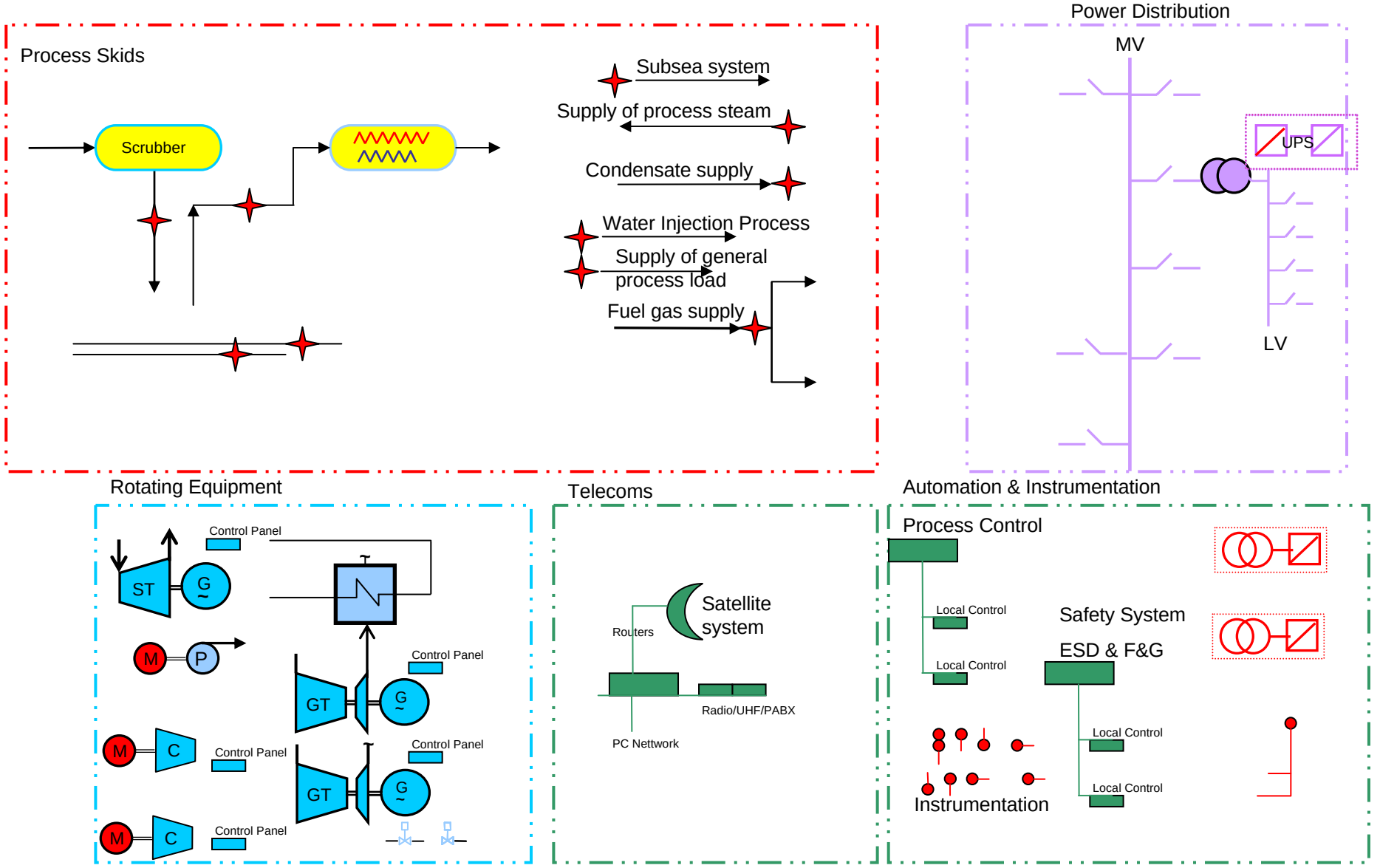


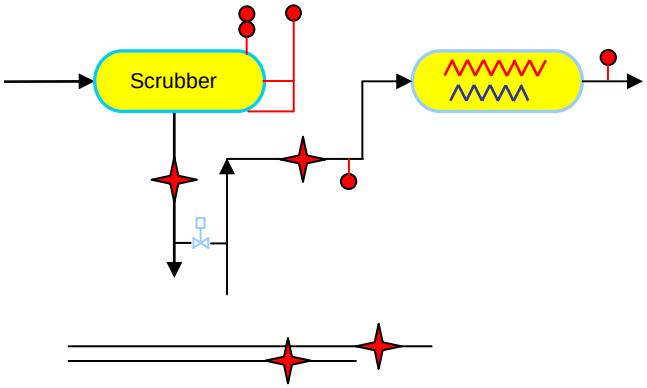


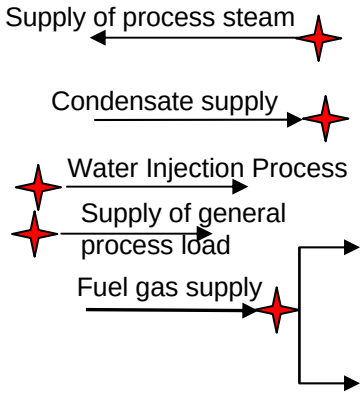
Networks for Integration of FPSO Packages

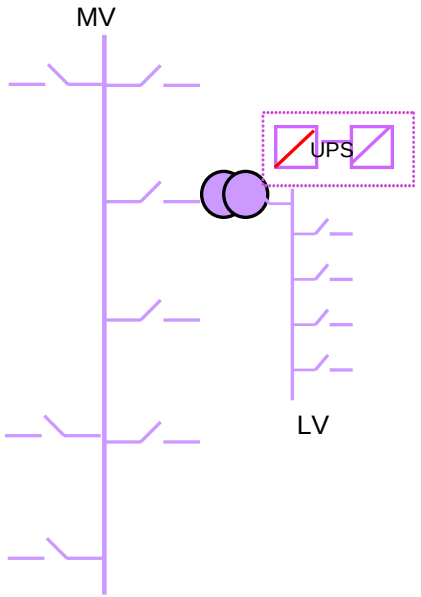


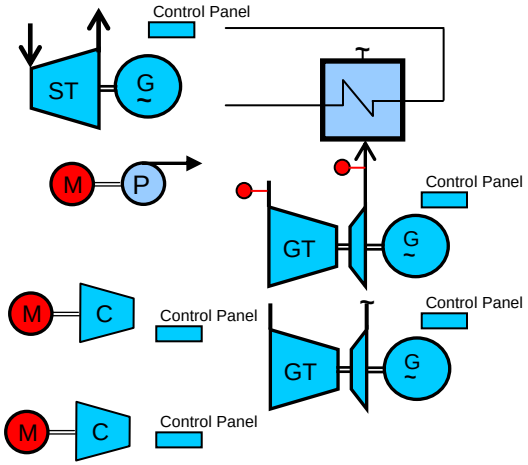
Traditional Separation

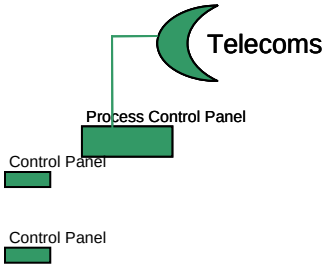


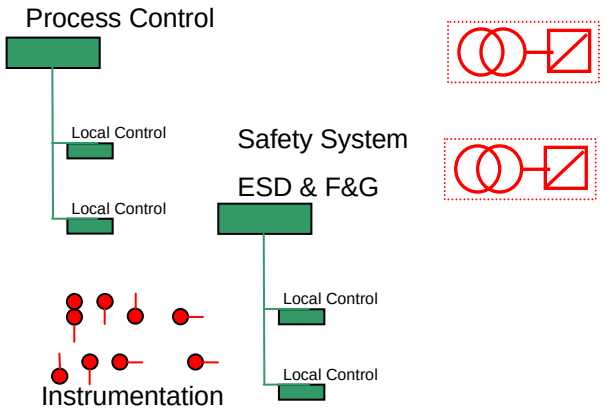

Scrubber


Supply of process steam
Condensate supply
Water Injection Process
Supply of general process load
Fuel gas supply

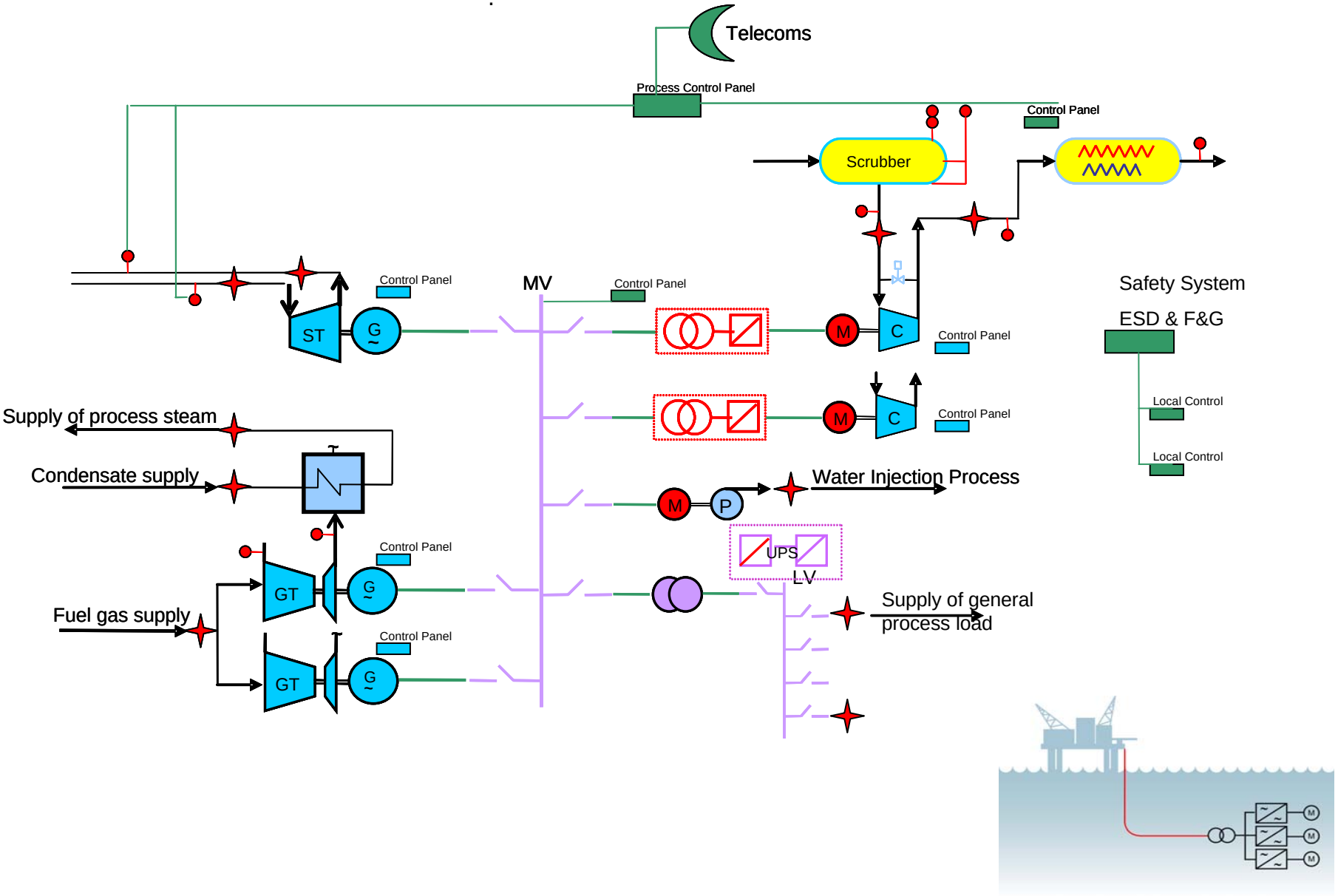

MV
UPS
LV


Control Panel
ST
G
M
P
GT
Control Panel
M
C
Control Panel
Control Panel
GT
G
M
C
Control Panel

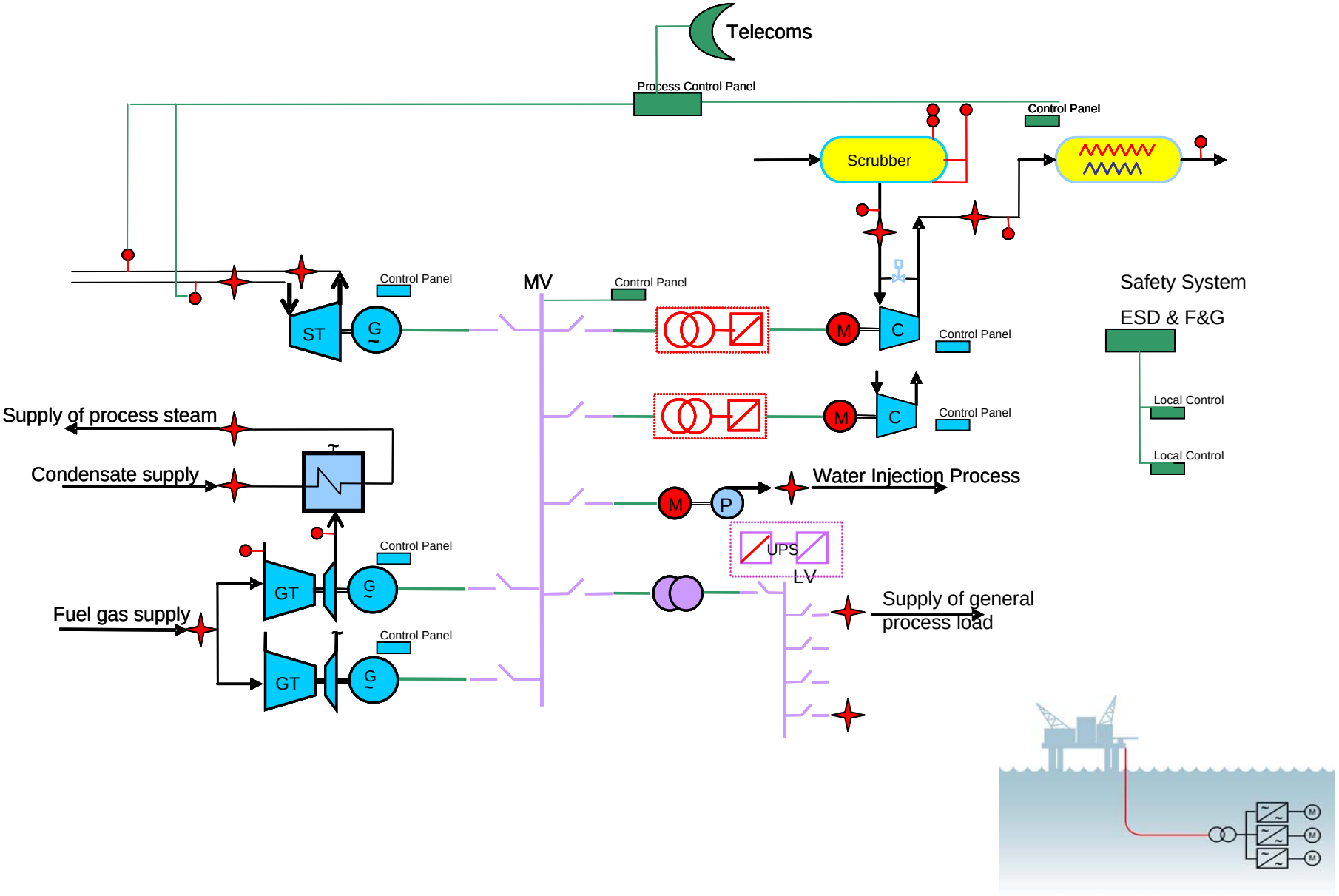

Telecoms
Process Control Panel
Control Panel
Control Panel


Process Control
Local Control
Local Control
Safety System
ESD & F&G
Local Control
Local Control
Instrumentation

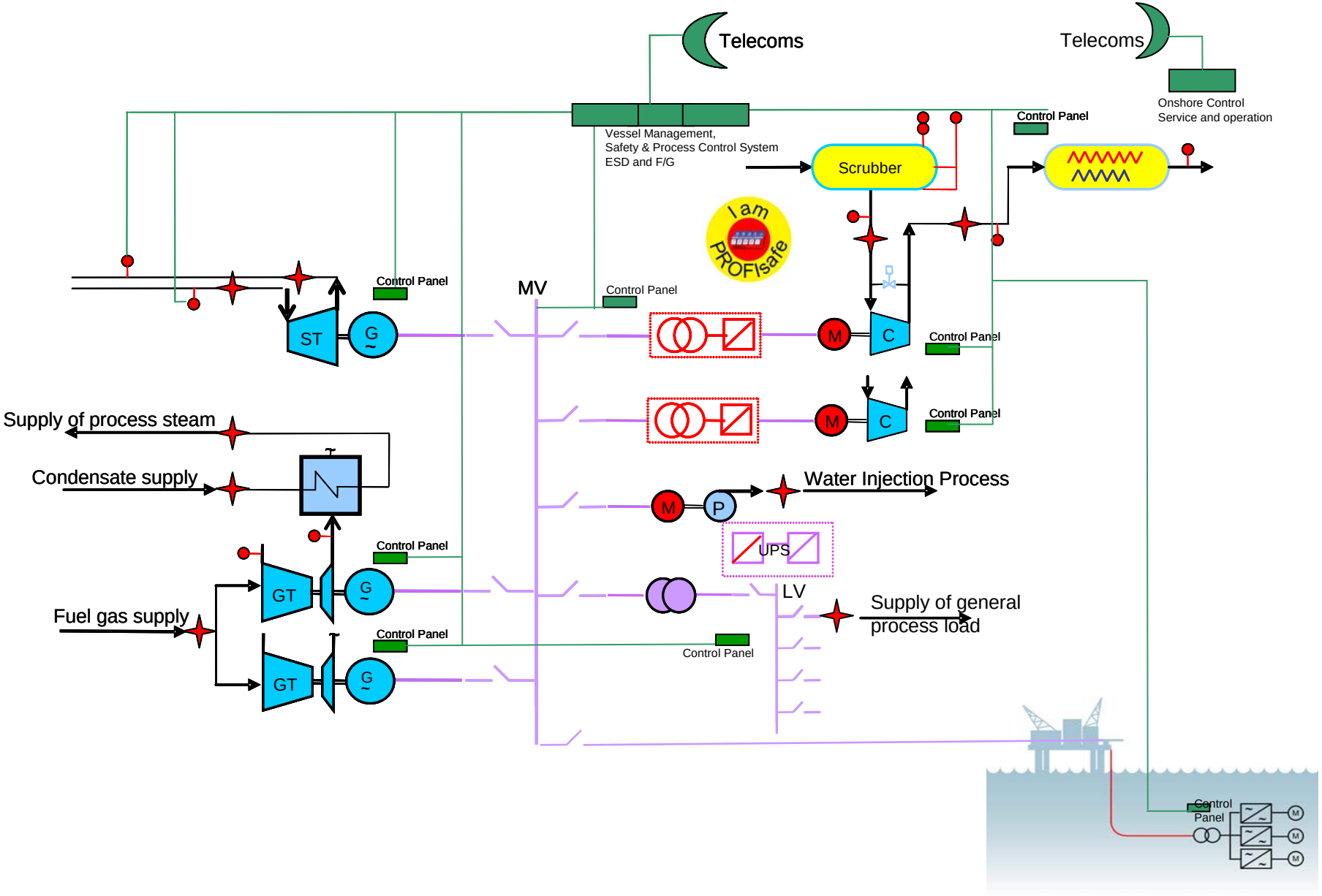
Partially Integrated



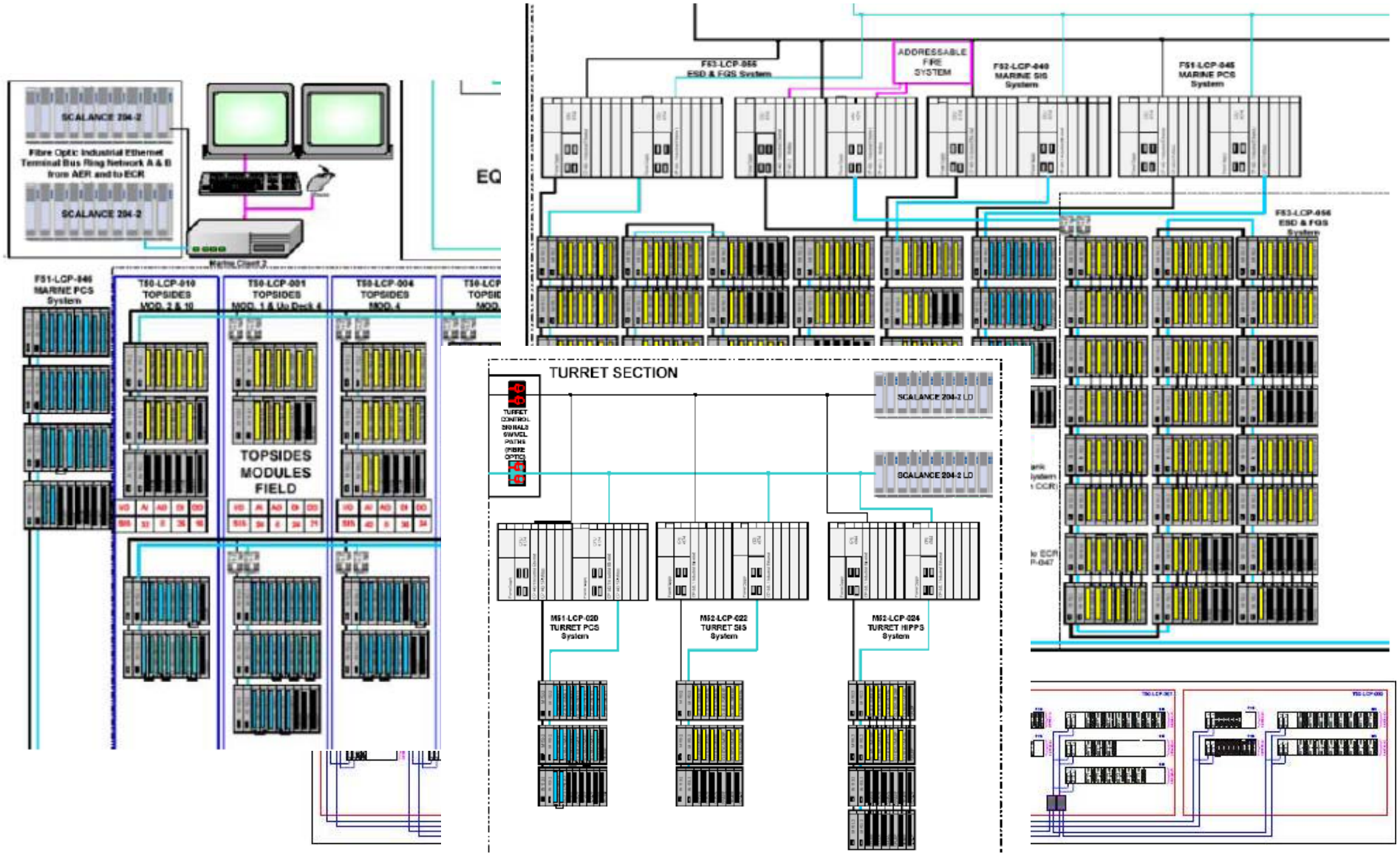
Integrated Automation



The Totally Integrated Solution.



Typical FPSO ICSS Architecture



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?

HP: +65 8121 8700

stephen_burke@siemens.com

Presenter: Stephen Burke
Siemens Singapore