ISA Delhi Section

Setting the Standard for Automation™

FERTILIZER MEET 2017
16TH DECEMBER 2017

Topic-
The safe way to a reliable plant

Standards

Certification

Education & Training

Publishing

Conferences & Exhibits

The International Society of Automation Delhi Section

Functional Safety for Process Industry – Basics

- **Safety Instrumented System (SIS)**

- Processes are very often NOT inherently safe

- Often we need to protect them with additional
  Safety Systems

- In the process industry these safety systems are called **Safety Instrumented Systems (SIS)**

SIEMENS

Functional Safety for Process Industry – Standards

International safety standards

IEC61508

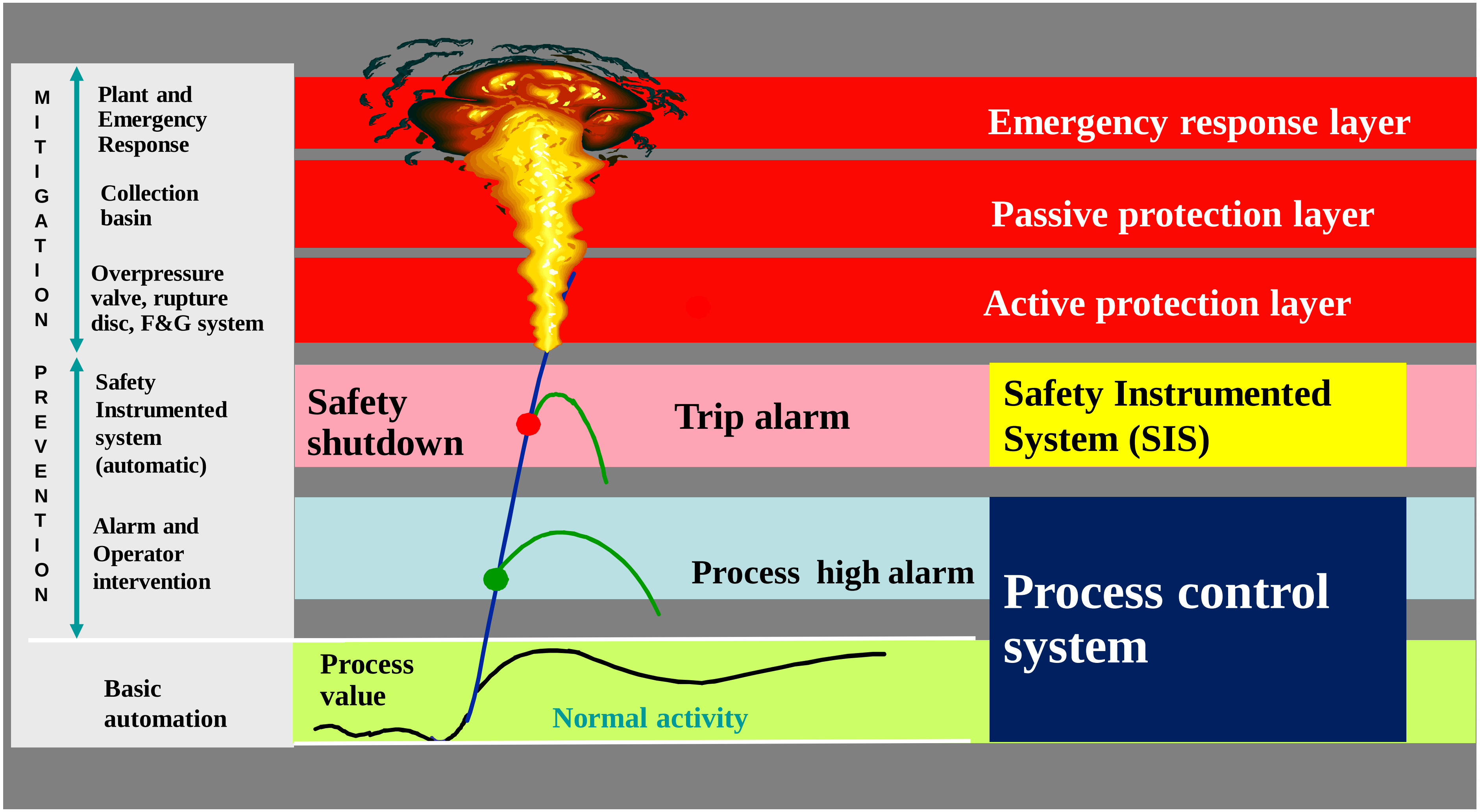
IEC 61508 serves as basic standard and basis for safety standardization . It covers all areas where electrical, electronic or PLC systems are used to realize safety-related protection functions.

IEC61511

There are sector-specific standards based on IEC 61508, such as
IEC 61511 for the process industry
(IEC 61513 for nuclear industry, IEC 62061 for machinery safety).
These sector standards are important for planners and operators of corresponding plants.

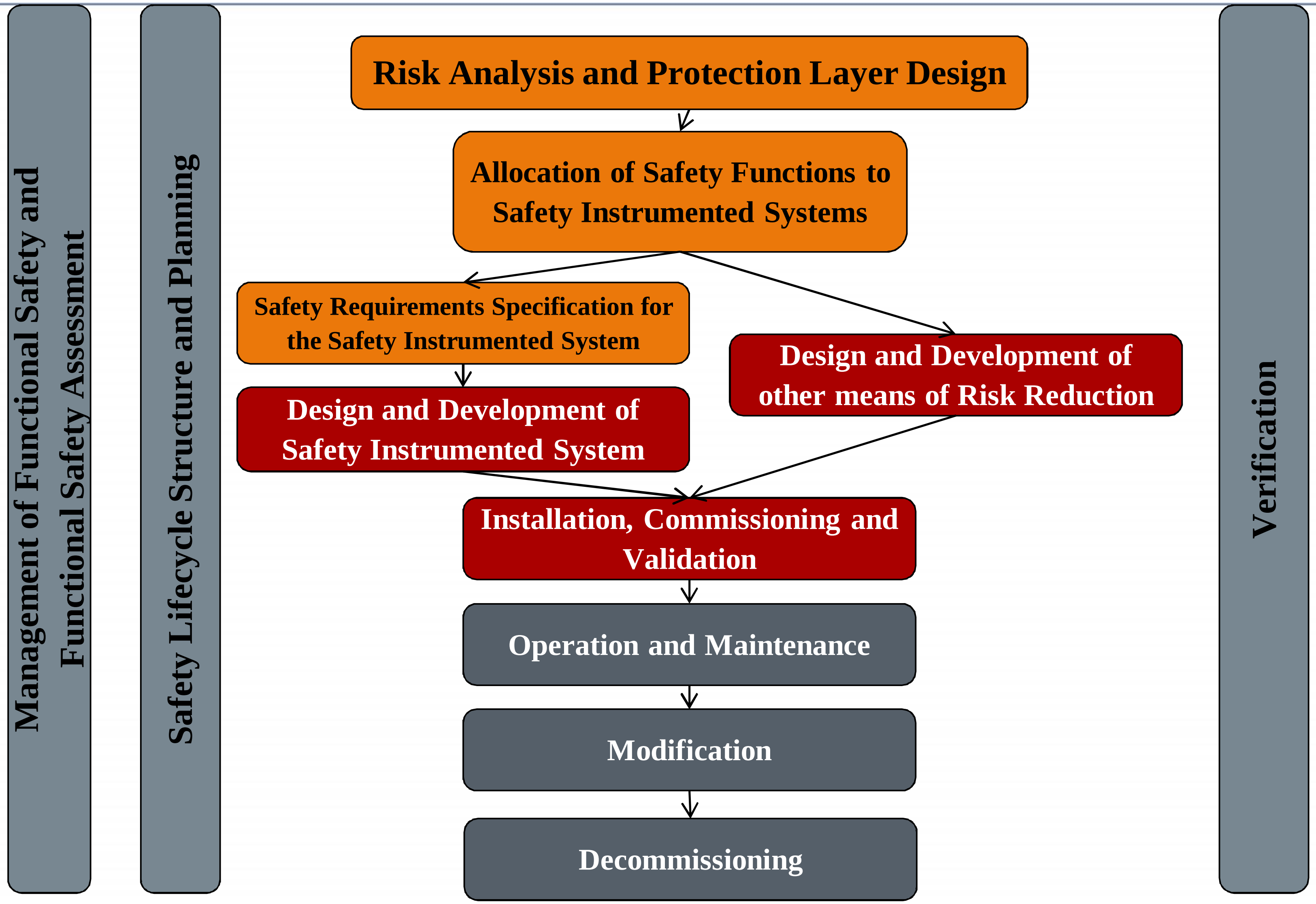
SIEMENS

The safety concept for a plant



SIEMENS

IEC 61511
Safety Lifecycle



Management of Functional Safety and Functional Safety Assessment
Safety Lifecycle Structure and Planning
Risk Analysis and Protection Layer Design
Allocation of Safety Functions to Safety Instrumented Systems
Safety Requirements Specification for the Safety Instrumented System
Design and Development of other means of Risk Reduction
Design and Development of Safety Instrumented System
Installation, Commissioning and Validation
Operation and Maintenance
Modification
Decommissioning
Verification

SIEMENS

As per IEC 61511-1

Safety Integrity Level

The safety Integrity Level (SIL) specifies the necessary risk reduction of Safety Instrumented Functions (SIFs)

Safety Integrity Level	Probability of failure on demand (PFD) (Low 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

Safety Requirement Specification (SRS)

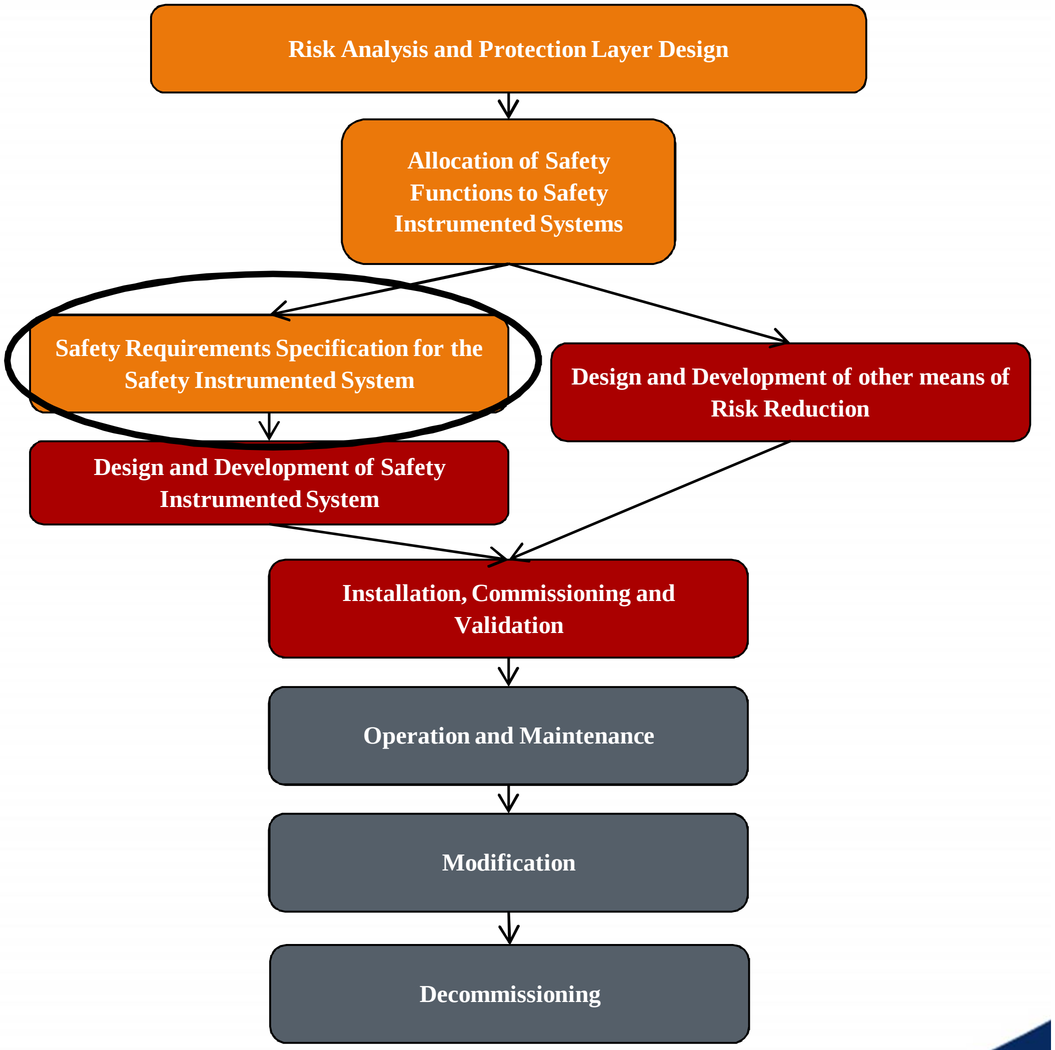
Aim:

- Avoidance of **systematical failures** during design, installation commissioning, operation and decommissioning of safety related functions

Realization:

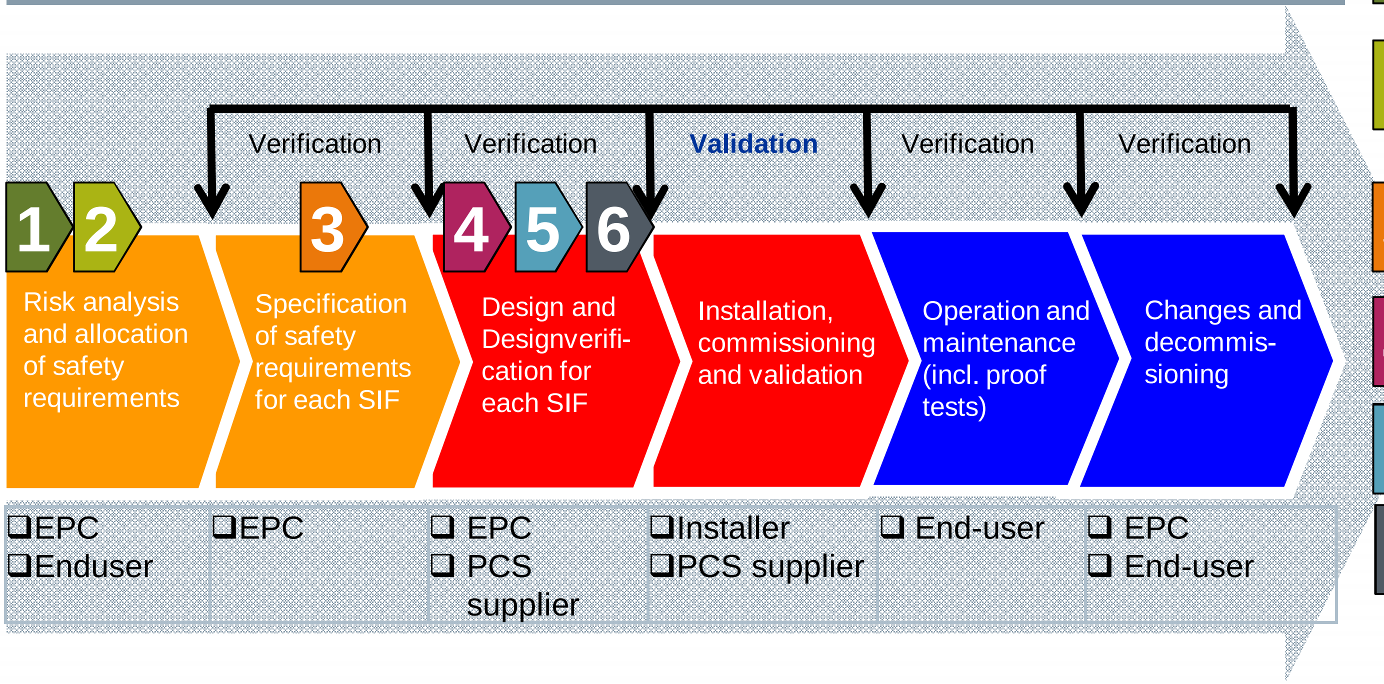
- Structured safety process according

The SRS is the "Interface" of the process environment in the world of automation


Risk Analysis and Protection Layer Design
Allocation of Safety Functions to Safety Instrumented Systems
Safety Requirements Specification for the Safety Instrumented System
Design and Development of other means of Risk Reduction
Design and Development of Safety Instrumented System
Installation, Commissioning and Validation
Operation and Maintenance
Modification
Decommissioning

Project Stages and Responsibilities according to IEC 61511

Each phase in the safety lifecycle must be verified



Verification | Verification | Validation | Verification | Verification

1 2	3	4 5 6			
Risk analysis and allocation of safety requirements	Specification of safety requirements for each SIF	Design and Designverification for each SIF	Installation, commissioning and validation	Operation and maintenance (incl. proof tests)	Changes and decommissioning
❑EPC ❑Enduser	❑EPC	❑ EPC ❑ PCS supplier	❑Installer ❑PCS supplier	❑ End-user	❑ EPC ❑ End-user

1 Project safety plan

2 Verification and validation plan, Functional Safety Assessment Plan

3 Safety requirement specification

4 Engineering guideline

5 Functional design specification

6 Test plan

- The whole responsibility lies according in each project phase with the EPC and end-user
- Interdependence of purchaser, contractor, sub-contractor etc. particularly in international business
- Scope of supply, limit of supply and responsibilities have to be clearly defined

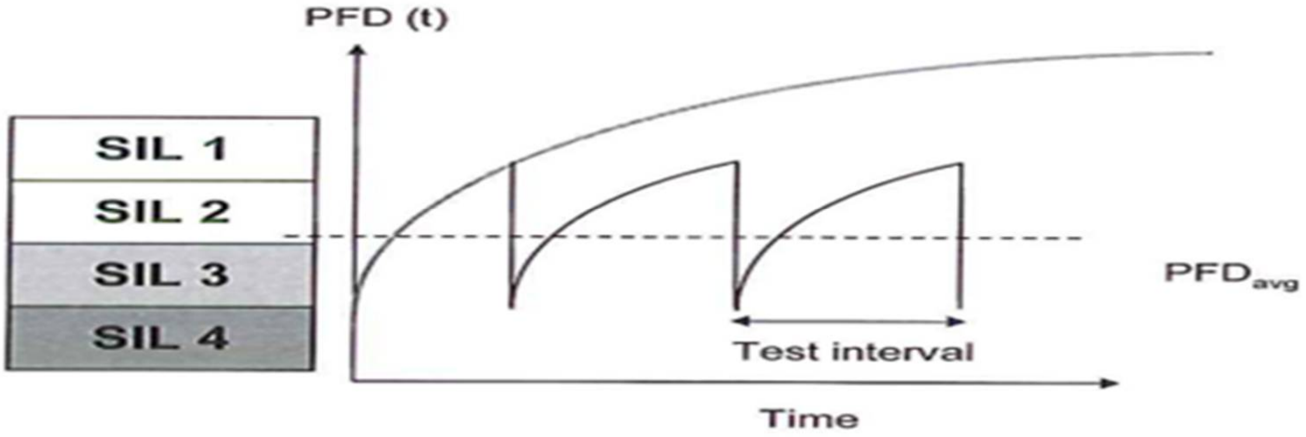
SIEMENS

Proof Test Interval

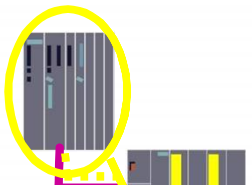
Proof Test Interval (TI):

The proof test interval is the time after which a subsystem must be either “totally checked” or “replaced” to ensure that it is in an “as new” condition.

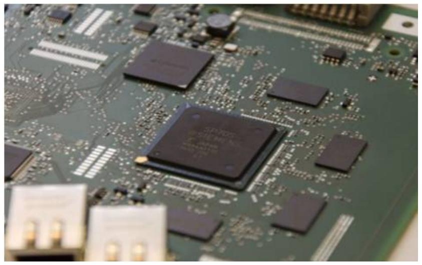
- Must detect 100% of all dangerous failures
- Separate channels must be tested separately
- Proof tests are usually performed manually and off line.

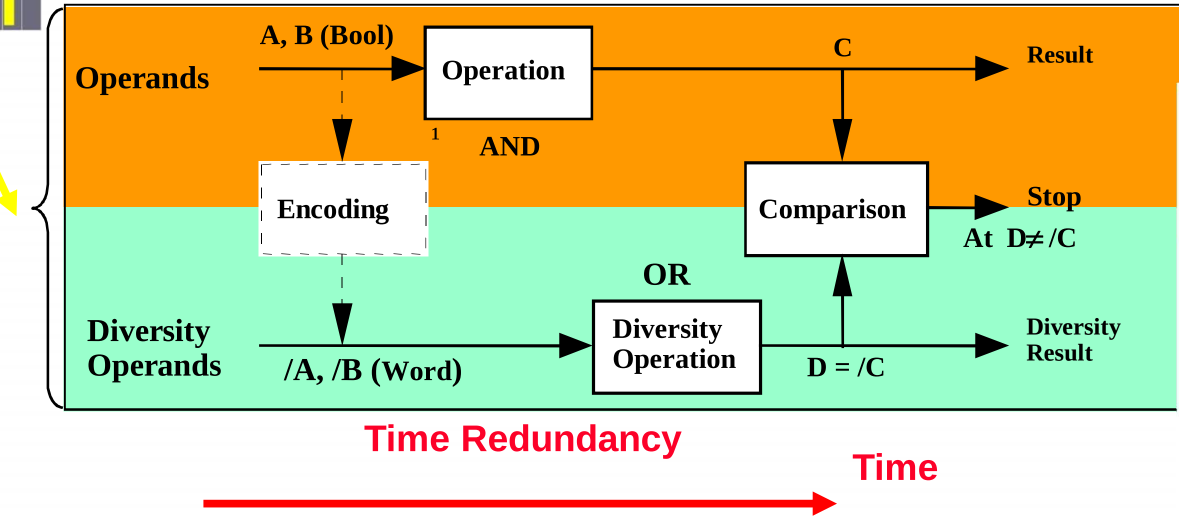


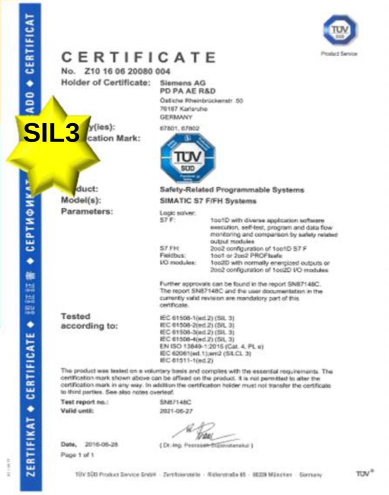
Safety mechanisms in the CPU



Time Redundancy and Software Diversity
instead of using two µPs (hardware redundancy)






SIL3
ZERTIFIKAT ◆ CERTIFICATE ◆ 認証証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT
Product Service

CERTIFICATE

No. Z10 16 06 20080 004

Holder of Certificate:	Siemens AG PD PA AE R&D Östliche Rheinbrückenstr. 50 76187 Karlsruhe GERMANY
y(ies):	67801, 67802
cation Mark:	
duct:	Safety-Related Programmable Systems
Model(s):	SIMATIC S7 F/FH Systems
Parameters:	Logic solver:
	S7 F: 1oo1D with diverse application software execution, self-test, program and data flow monitoring and comparison by safety related output modules
	S7 FH: 2oo2 configuration of 1oo1D S7 F
	Fieldbus: 1oo1 or 2oo2 PROFIsafe
	I/O modules: 1oo2D with normally energized outputs or 2oo2 configuration of 1oo2D I/O modules
	Further approvals can be found in the report SN87148C. The report SN87148C and the user documentation in the currently valid revision are mandatory part of this certificate.
Tested according to:	IEC 61508-1(ed.2) (SIL 3) IEC 61508-2(ed.2) (SIL 3) IEC 61508-3(ed.2) (SIL 3) IEC 61508-4(ed.2) (SIL 3) EN ISO 13849-1:2015 (Cat. 4, PL e) IEC 62061(ed.1);am2 (SILCL 3) IEC 61511-1(ed.2)

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: SN87148C
Valid until: 2021-06-27

Date, 2016-06-28

(Dr.-Ing. Poorasan Bijpovatanakul)

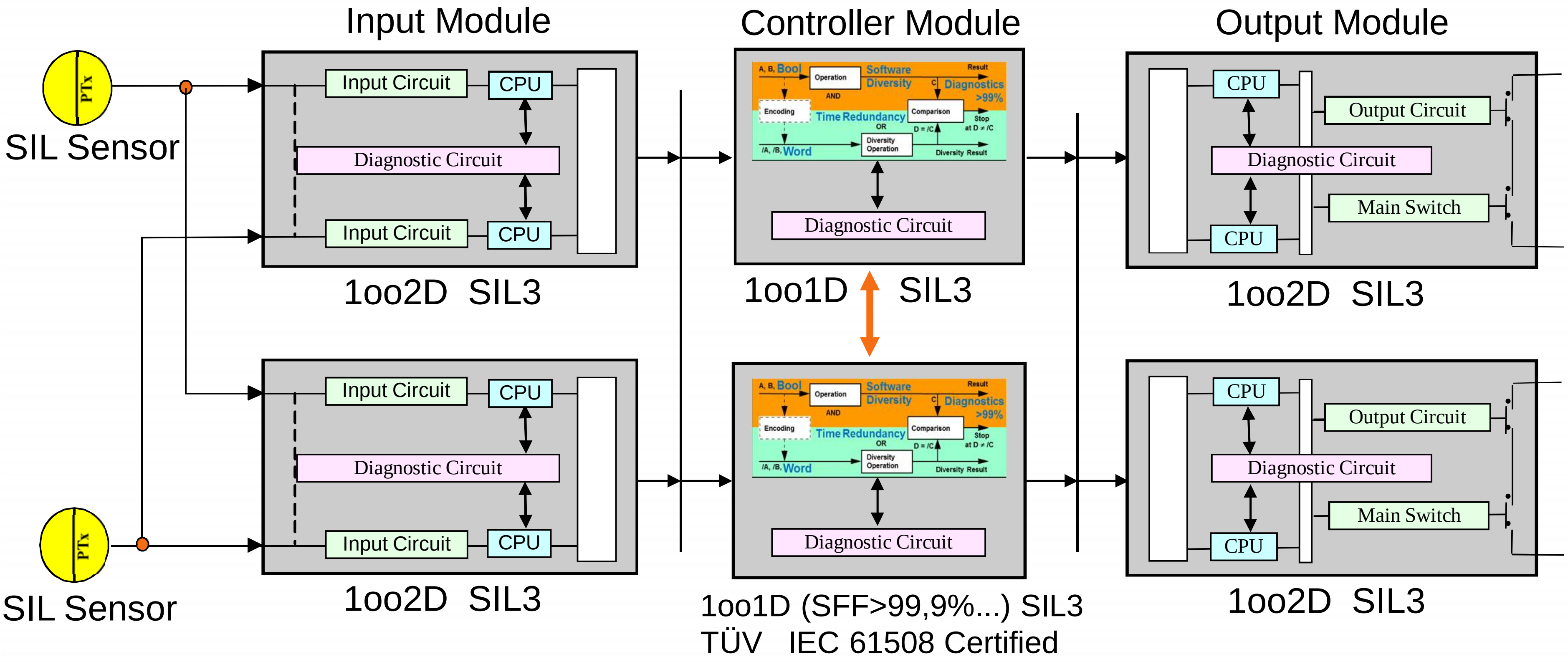
Page 1 of 1

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany

TÜV®

- Time redundancy and instruction diverse processing
- Logical program execution and data flow monitoring, **Diagnostics SFF > 99,9%**
- Bool and Word operations processed in different “Processing Units” PU of the ASIC
- 2 independent hardware timer

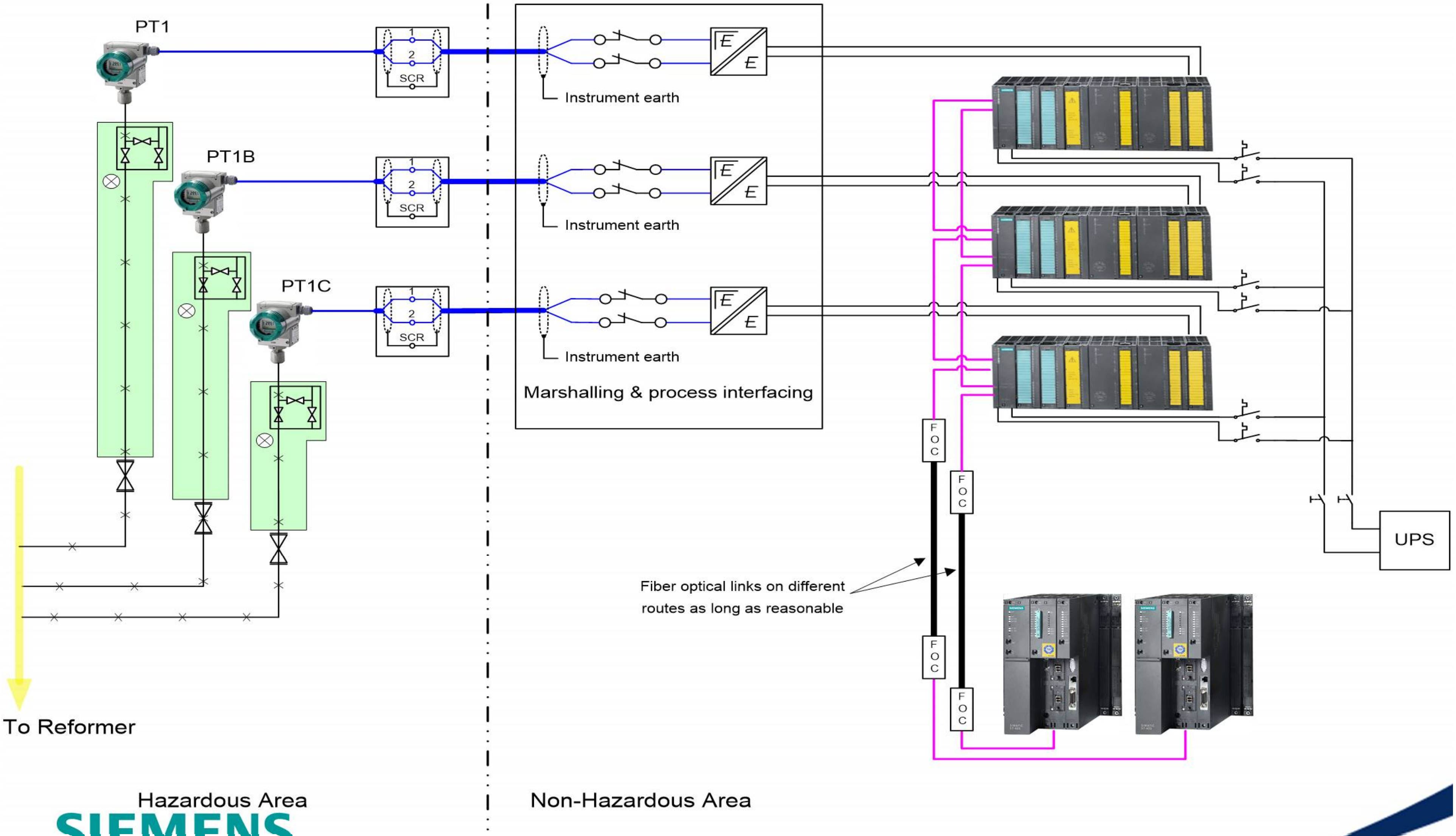
Safety and high availability



2x 1oo1D of SIL 3 controller

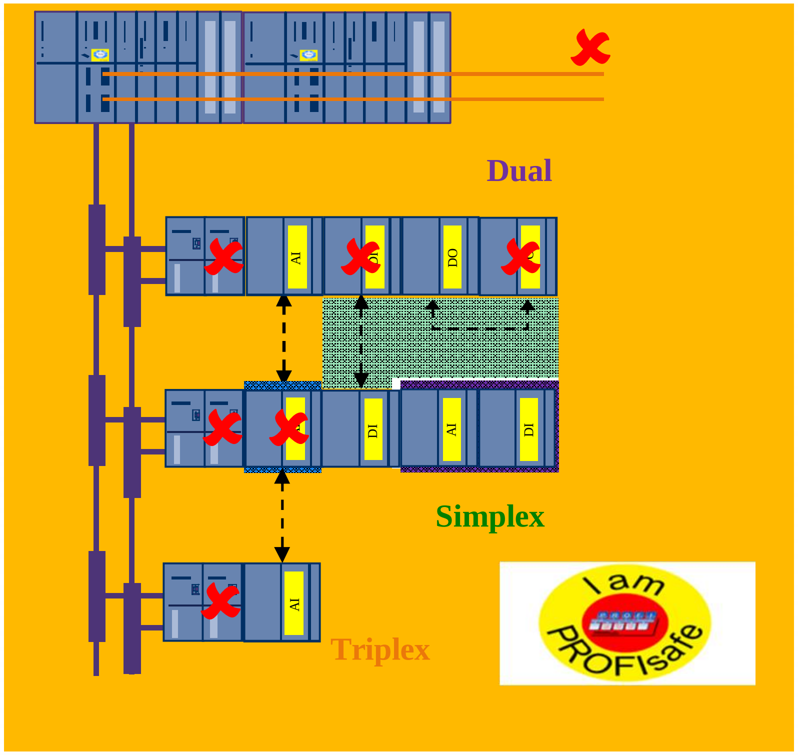
Emergency Shutdown System (ESD)

2oo3 Logic for Process Gas (CH4) pressure to Primary Reformer


PT1
PT1B
PT1C
1
2
SCR
Instrument earth
E
Marshalling & process interfacing
F O C
UPS
Fiber optical links on different routes as long as reasonable
To Reformer
Hazardous Area
Non-Hazardous Area

SIEMENS

Flexible Modular Redundancy

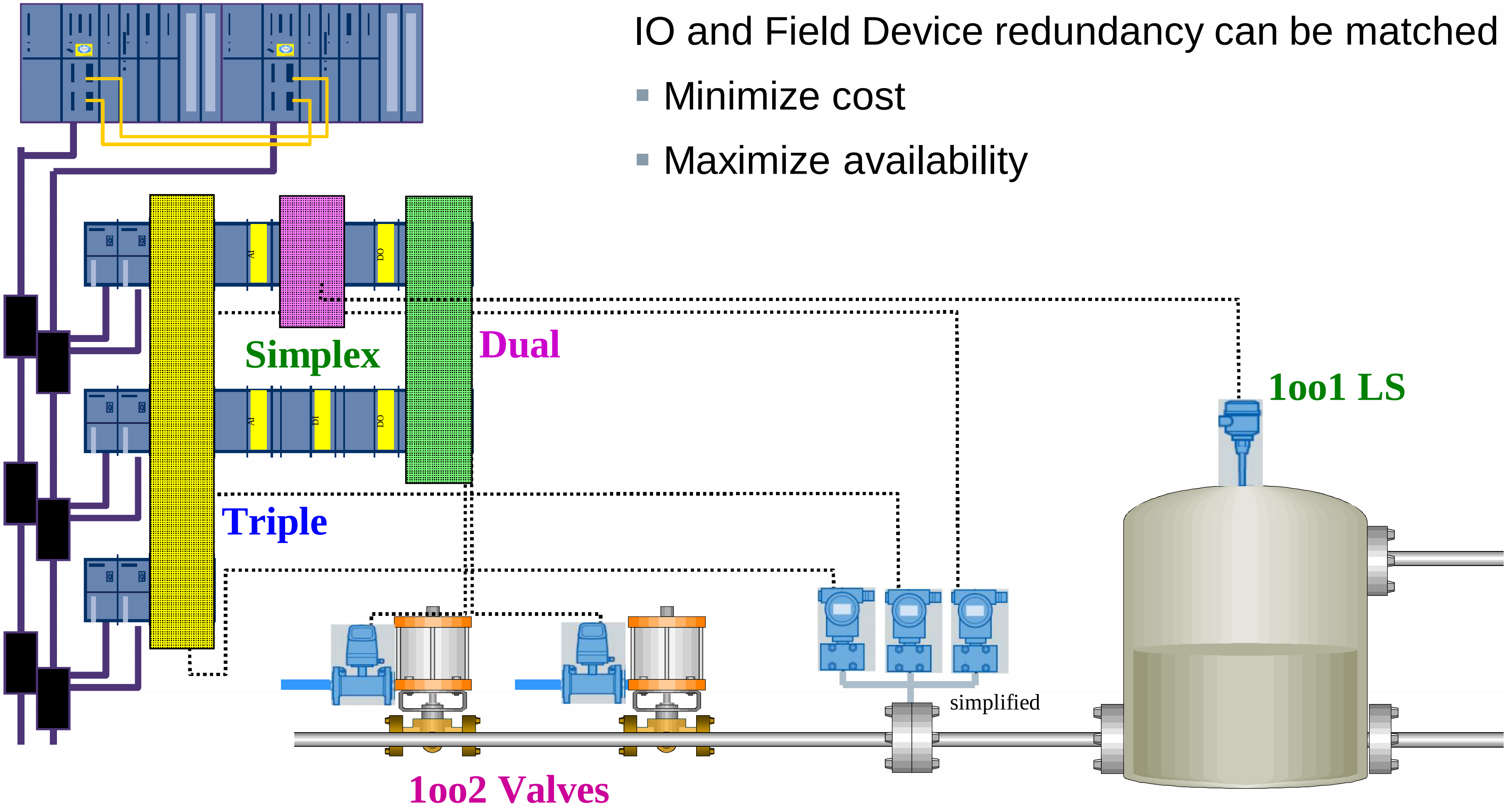


- Make any component redundant
- Physically separate redundant resources
- Mix and match redundancy
- Tolerate multiple faults with no impact on safety

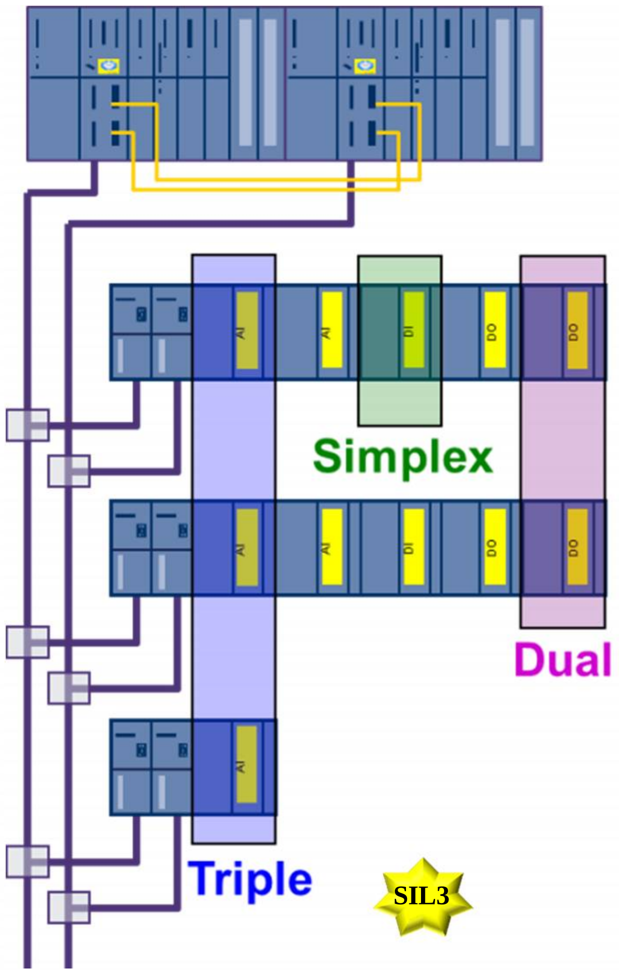
Flexible Modular Redundancy

IO and Field Device redundancy can be matched to:

- Minimize cost
- Maximize availability



Summary- differences in Architectures



- **Safety integrity via diagnostics rather than voting**
- **All architectures provide SIL 3 safety AND availability**
- **Fault tolerance is scalable rather than fixed - mix & match I/O structures**
- **Process availability not always impacted by SIS availability**
- **Siemens architecture gives you the choice to *pay for the availability you need***
- ***Please ask the right requirement …according the IEC 61511 and your plant***

Thank you very much for your attention

SIEMENS