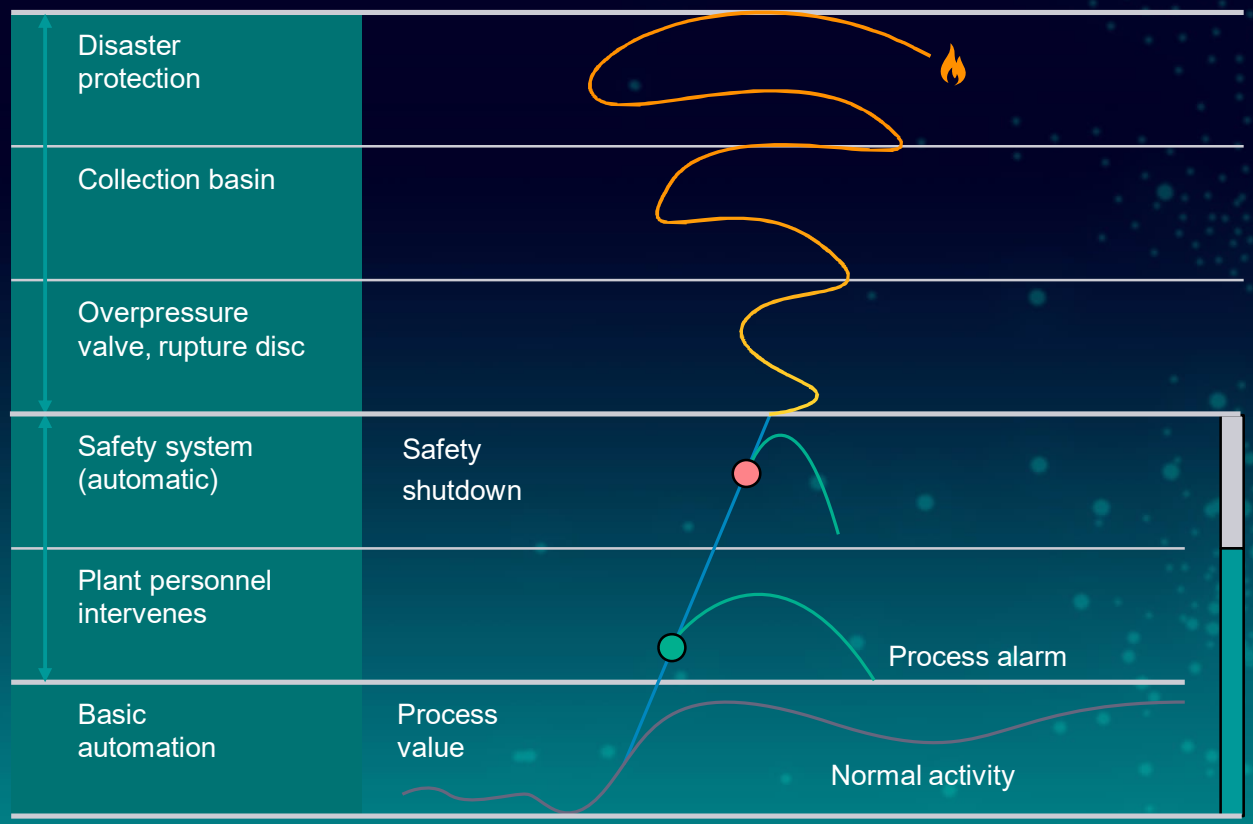
Safety Integrated for Process Automation

Safe and Secure | siemens.com/process-safety

Jussi Salomaa & Timo Laakso

SIEMENS

Safety concept



Disaster protection

Passive protection

Active protection

Safety Instrumented System (SIS)

Process control system

SIEMENS

Risk Reduction

The Approach of Safety

“Zero risk” is not feasible.

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, IEC 61513 for the nuclear industry or IEC 62061 for machinery. These sector standards are important for planners and operators of corresponding plants.

Safety Integrity Levels (SIL) (Low Demand mode)

Probability of failure on demand

1/PFD =
Risk Reduction Factor

Safety Integrity Level	Probability of failure on demand (PFD) per year (Demand mode of operation)	Risk Reduction Factor = 1/PFD
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$	100,000 to 10,000
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	10,000 to 1,000
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	1,000 to 100
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	100 to 10

SIL: A performance criteria of a SIF (Safety Instrumented Function) and the SIS (Safety Instrumented System), describes the probability of failure on demand.

International Standard
IEC 61508 – Certification bodies

IEC61508

Certification according IEC 61508/11

TÜVRheinland®

exida®

TÜV SÜD

ZERTIFIKAT ◆ CERTIFICATE ◆ 認証証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD 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

Factory(ies): 67801, 67802

Certification Mark:

Product: 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 compension by safety related output modules
S7 FH: 2oo2 configuration of 1oo1D S7 F
Fieldbus: 1on1 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. Peerasak Sopavattanaku)

Page 1 of 1

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

SIEMENS

Safety Integrated IN DCS system

Overview

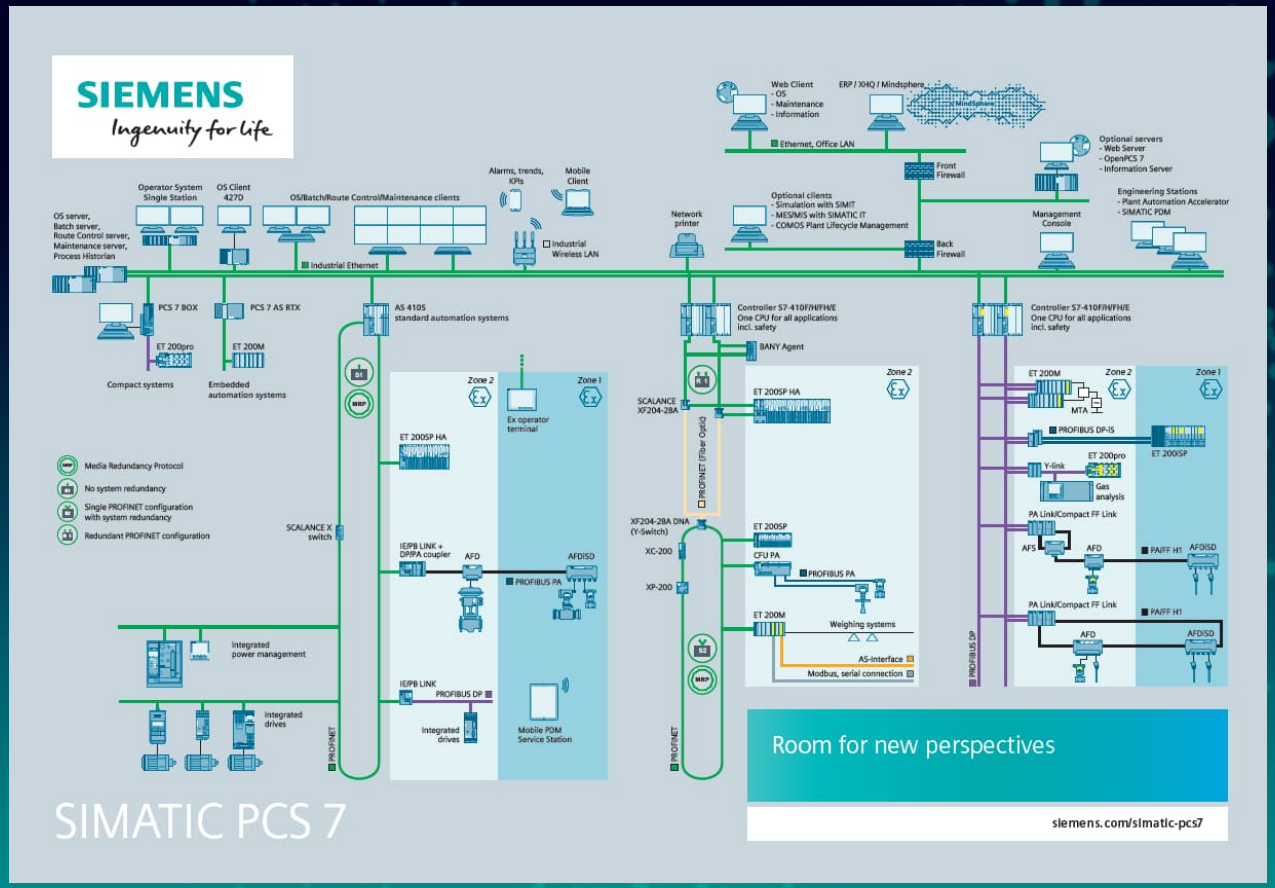
SIEMENS

Introduction
SIMATIC PCS 7 – System Overview and integrated safety

Plant Control
Process Management level
(SCADA, MES, IT/ERP)

Process Control
Automation level

Field level
(Sensors, I/O's, Actuator, Smart Devices)



SIEMENS

Siemens
Scalable Range of Safety Controllers and I/O

Certified for the use up to SIL 3

The CPU 410 is a powerful controller for system and failsafe solutions in the process automation

- Based on SIMATIC F Systems Library
- Physical separation of controllers possible
- Changes to the configuration during operation
- Failsafe and high availability versions
- Hot swapping
- Operation temperature 0…70° Celsius

SIMATIC ET 200SP HA
The high-performance I/O for process automation

Compact and modular I/O series

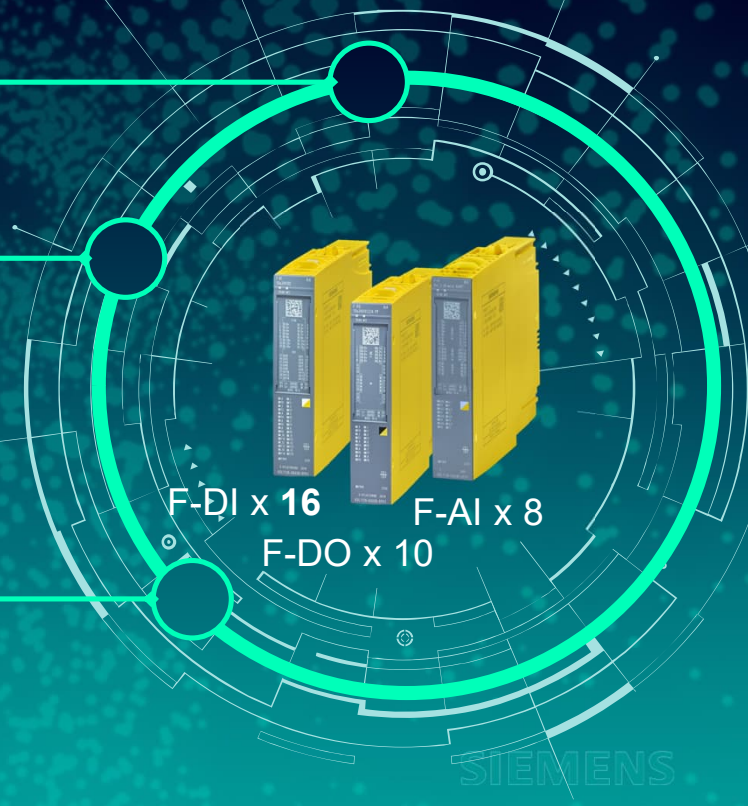
- Dimensions: 200 x 163 x 22,5 mm
- Up to 56 modules per rack

Designed for the process industries

- -40°…+70°C by horizontal mounting
- Conformal coating - protection against harsh environment
- NAMUR NE21, immunity to interference
- Operation up to 4,000 m above sea level

Highest availability

- Redundant power supply
- Redundant PROFINET
- Redundant I/O modules



Remote IO
Overview SIMATIC ET 200SP HA Failsafe Modules

Features

- Compact modular I/O-serie´s
- Designed for the process industries
- High availability due redundancy
- Fast and ease wiring

Scan QR code to learn more about ET200M

Modules	Features
F-DI 16 x 24V DC HA	16-channel input module, SIL 3/Cat. 4/Ple
F-DQ 10 x 24V DC/2 A HA	10-channel output module, SIL 3/Cat. 4/Ple, 24V DC/2 A
F-AI 8 x 0/4...20 mA HART HA	8-channel analogue input module, SIL3/Cat. 4/Ple, 4…20 mA HART

Benefits

- Up to 56 Modules per rack
- Environment temperature -40° …+70° C (installation), usable up to 4,000 m
- Integrated redundancy (power supply, PROFINET, I/O-Modules)

SIEMENS

Remote IO for the Hazardous Area
SIMATIC ET 200iSP

Failsafe modules for SIMATIC ET 200iSP

Features

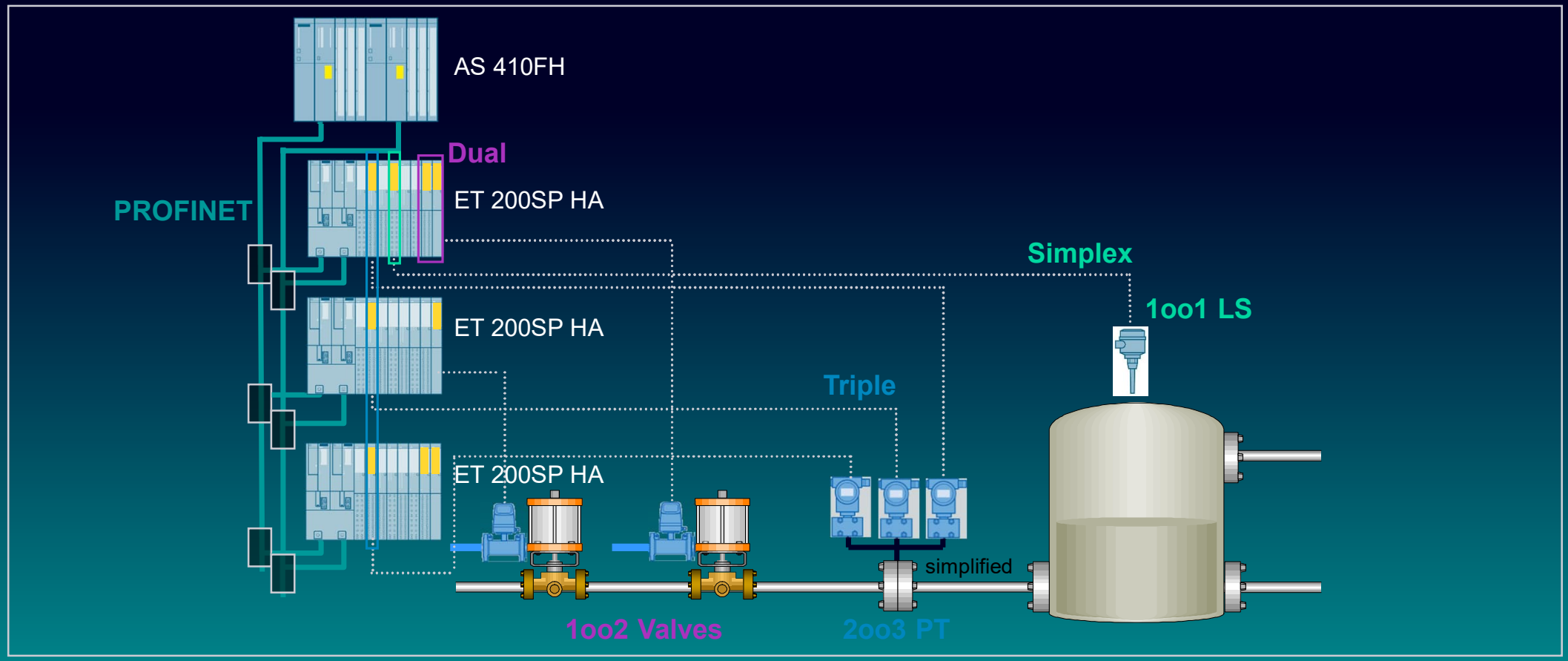
3 failsafe modules to install directly in Ex-zone 1/21; up to SIL 3, PLe

- Digital Input Module F-DI8 NAMUR
- Digital Output Module F DO4, 17.4 V DC 40 mA
- Analogue Input Module F-AI4 HART

Customer benefits

- Reduced installation effort by using ET 200iSP compared to traditional solutions (with Ex barriers)
- Diagnostics (e.g., line monitoring) to the field sensors and actuators
- SIL calculation advantages (no Ex barriers)
- Complete portfolio – failsafe protection in Ex-Zone 1 especially for applications like ESD (Emergency Shut Down), boiler protection (e.g., at biogas plants), fire-extinguishing system or gas/fire detection

Flexible Modular Redundancy – FMR
With PROFIBUS or PROFINET



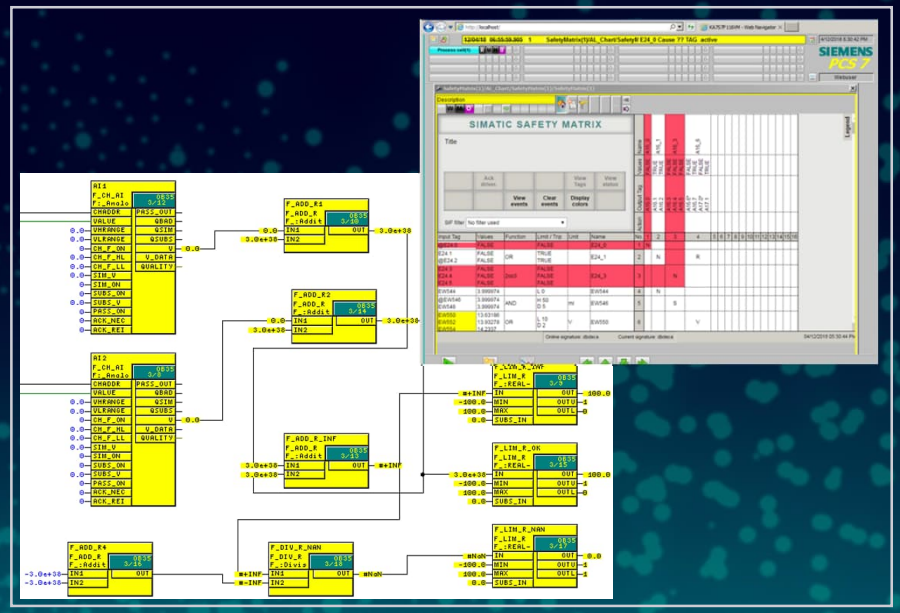
SIEMENS

Software
SIMATIC F-Systems und Safety Matrix

SIMATIC S7-400F/FH with S7 F Systems and SIMATIC S7 Safety Matrix

Is used for configuring the hardware and safety-related process applications acc. to IEC 61511

- STEP 7 option package or Safety Matrix with PCS 7 for configuring Safety Functions in S7-410 Controller (CPU410, CPU410E) as well as S7-400F and S7-400FH
- Simplifies the documentation of the safety programs, e.g., by administration of signatures



The configuration of the safety programs can be done on the one hand with function block language (CFC) or on the other hand with Cause & Effect tool SIMATIC S7 Safety Matrix.

SIEMENS

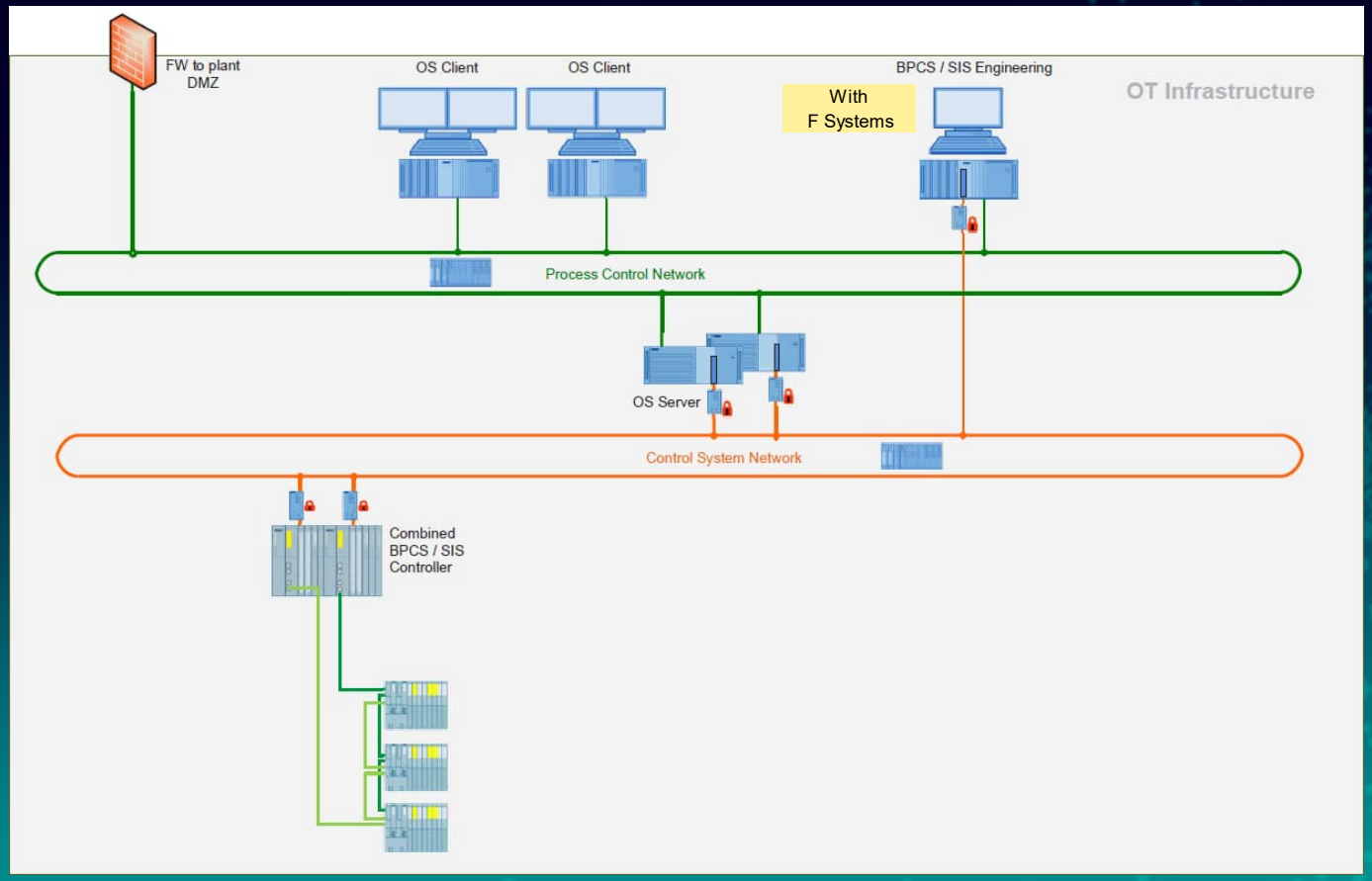
Security
Relationship between Functional Safety & Cybersecurity

Cyber security referenced in functional safety standards

IEC 62443

SIEMENS

PCS 7 SIS Architectures
Fully Integrated Architecture



PC environment

- DMZ / Firewall
- Whitelisting / Antivirus / VPN
- Access protection (Windows, BIOS)

Engineering-Tool

- Access protection project (SIMATIC LOGON)
- Access protection SIS Part (F-Password)

Communication

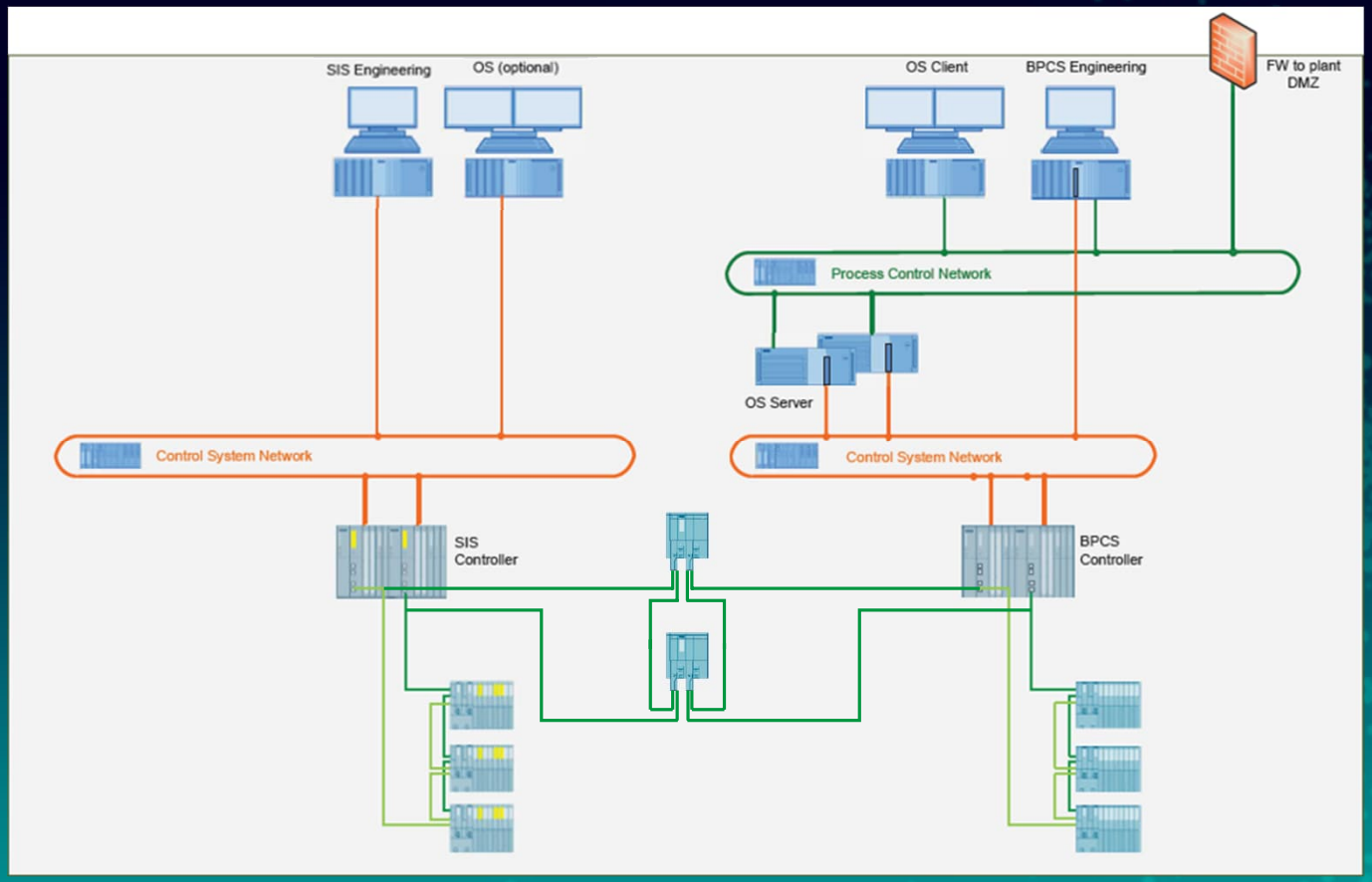
- Firewall / VPN

Control system

- Access protection CPU (CPU-Password)

SIEMENS

PCS 7 SIS Architectures
Interfaced Architecture with PN/PN Coupler



Major changes

- Physically separated SIS and BPCS
- Communication between SIS and BPCS via Fieldbus with PN/PN Coupler
- Avoidance of single point of failure with the usage of redundant PN/PN Coupler
- Operating and Monitoring of the SIS Controller via a separate OS in the SIS Structure

SIEMENS

Redundant Systems
SIMATIC S7-1500 R/HF

Technical Details / V19

SIEMENS

SIMATIC S7-1500 Redundant Systems
System Overview

Consistent concept –
Identical
Synchronization process

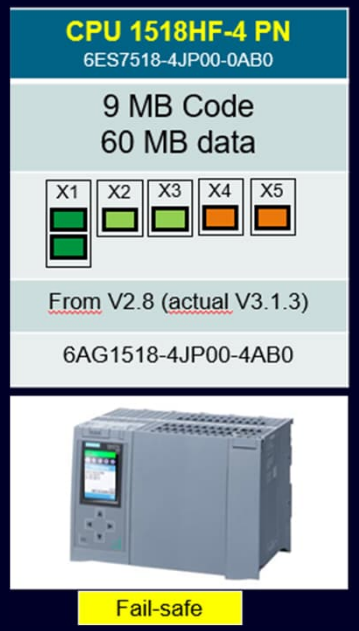
	Redundant S7-1500R	High Available S7-1500H
		
CPU Type	**CPU 1513R / CPU 1515R**	**CPU 1517H / CPU 1518HF**
Synchronization	via **PROFINET Ring** (MRP)	via **Sync-Module / FO**
Hot-Standby	**Yes** fail-over time ca. 300 ms	**Yes** fail-over time ca. 50 ms
Max distance between CPUs	**100 m,** with media converters a few km	**40 km**
PROFINET System Redundancy	**S2 and S1 switched**	**R1, S2 and switched S1**
Structure of the PROFINET network	**MRP Ring**	**Any**

SIEMENS

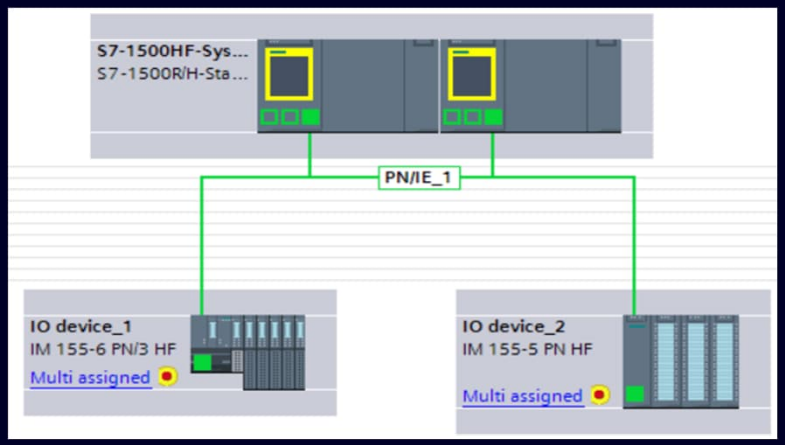
Safety for Redundant Systems
Realize Safety Applications with redundant Controller

High Availability + Failsafe = CPU 1518HF
- Engineering with STEP 7 Professional V17 and STEP 7 Safety
- Safety programming as with non-redundant fail-safe PLC
- Supported PROFIsafe Communication
- Supports flexible F-Link (safe controller/controller communication)
- Fail-over scenario without stop the safety program

Fast Commissioning Mode
- The Fast Commissioning Mode in deactiviated safety mode allows short turnaround times:
  - Faster compile time of the F program
  - In this mode, the F program can also be loaded in the System State RUN
  - To change back to the safety mode, a STOP-RUN transition is required



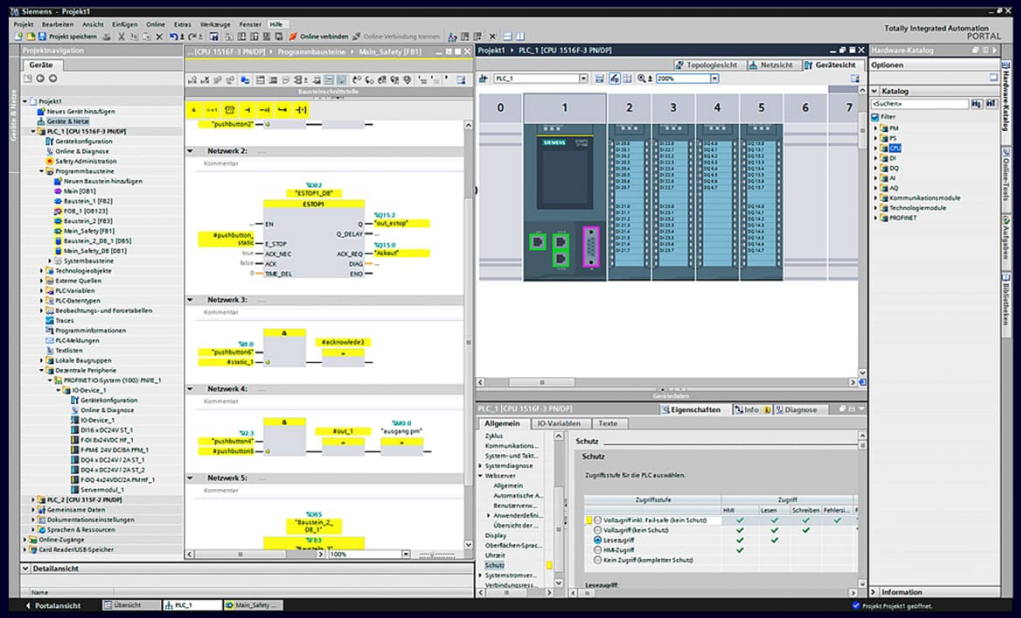
Certified for the use up to SIL 3



SIEMENS

Engineering made easy –
SIMATIC Safety in the TIA Portal V19

Fail-safe engineering



STEP 7 Safety Basic and Advanced

Fail-safe controller

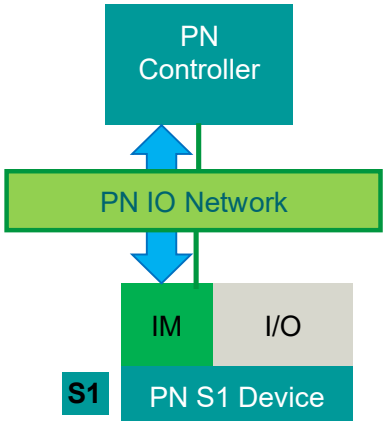
Fail-safe I/O

SIEMENS

PROFINET System Redundancy
Redundancy operating modes with PROFINET

Without System Redundancy

- **S**ingle Interface Module
- **1** connection to the controller

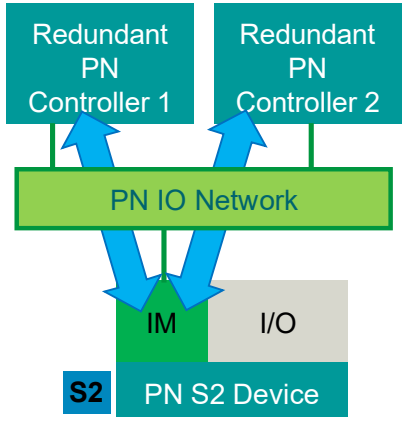


PN S1 devices can also be operated on redundant controllers S7-1500 R/H with the "Switched S1" function

No redundancy

System Redundancy S2

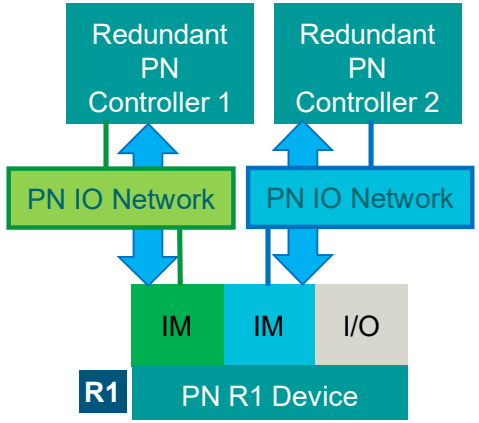
- **S**ingle Interface Module
- **2** connections to red. controllers



Controller Redundancy

System Redundancy R1

- **R**edundant Interface Module
- **2x1** connection to red. controller



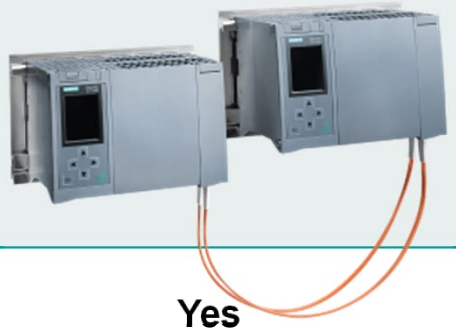
- Controller Redundancy
- Network Redundancy
- IM Redundancy

Availability

Details on PN System Redundancy operating modes: See https://support.industry.siemens.com/cs/ww/en/view/109756450

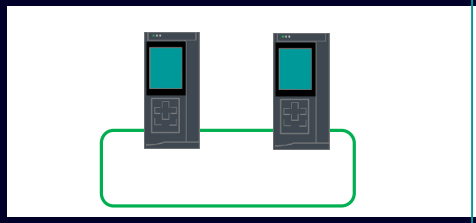
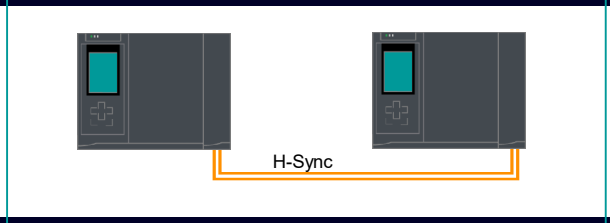
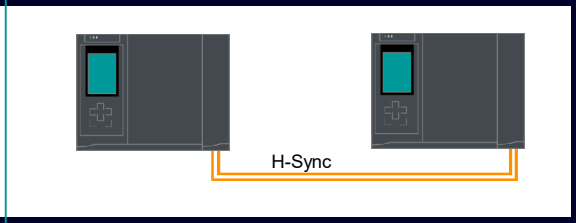
SIEMENS

PROFINET System Redundancy
Support of PN System Redundancy with SIMATIC S7-1500

		S7-1500 (Non-redundant)	S7-1500R	S7-1500HF
				
S1	Operation of PN devices **without System Redundancy**	**Yes**	**Yes** (Switched S1)	**Yes** (Switched S1)
S2	Operation of PN devices with **S2 System Redundancy**	**Yes** (S1 mode only)	**Yes**	**Yes**
R1	Operation of PN devices with **R1 System Redundancy**	**No**	**No**	**Yes** from firmware V3.0 and TIA Portal V18

SIEMENS

Network configuration with S7-1500R/H
Overview

	S7-1500R	S7-1500H/HF		S7-1500H/HF	
Controller					
PROFINET Topology	MRP Ring	MRP Ring	Line From FW V3.0	Redundant MRP Ring From FW V3.0	Redundant line From FW V3.0
Additional Topologies	MRP-Interconnection	MRP-Interconnection, combined topology		MRP-Interconnection, combined topology	
IO-Devices System Redundancy[1)]	S2 S1	S2 S1		R1 S2 S1 Via Y-Switch	

SIEMENS

PROFINET System Redundancy
Siemens I/O systems with PN S2 function (I)

S2

Product		Article
ET 200SP IM155-6 PN HF (FW>=4.2) IM 155-6MF (Multi Fieldbus)		6ES7155-6AU01-0CN0 6ES7155-6AU30-0CN0 6ES7155-6MU00-0CN0
ET 200MP IM155-5 PN HF (FW>=4.2) Also with active backplane bus for pulling/plugging in operation		6ES7155-5AA00-0AC0 6ES7590-0BL00-0AA0 The active backplane bus allows the pulling and plugging of ET 200MP modules while the CPU is in operation.
ET 200eco PN M12-L (from FW 1.1)		6ES7 14*-6**00-0BB0
PN/PN coupler		6ES7158-3AD10-0XA0

Overview in detail: https://support.industry.siemens.com/cs/ww/en/view/102325771

SIEMENS

System Redundancy R1

PROFINET System Redundancy

SIEMENS

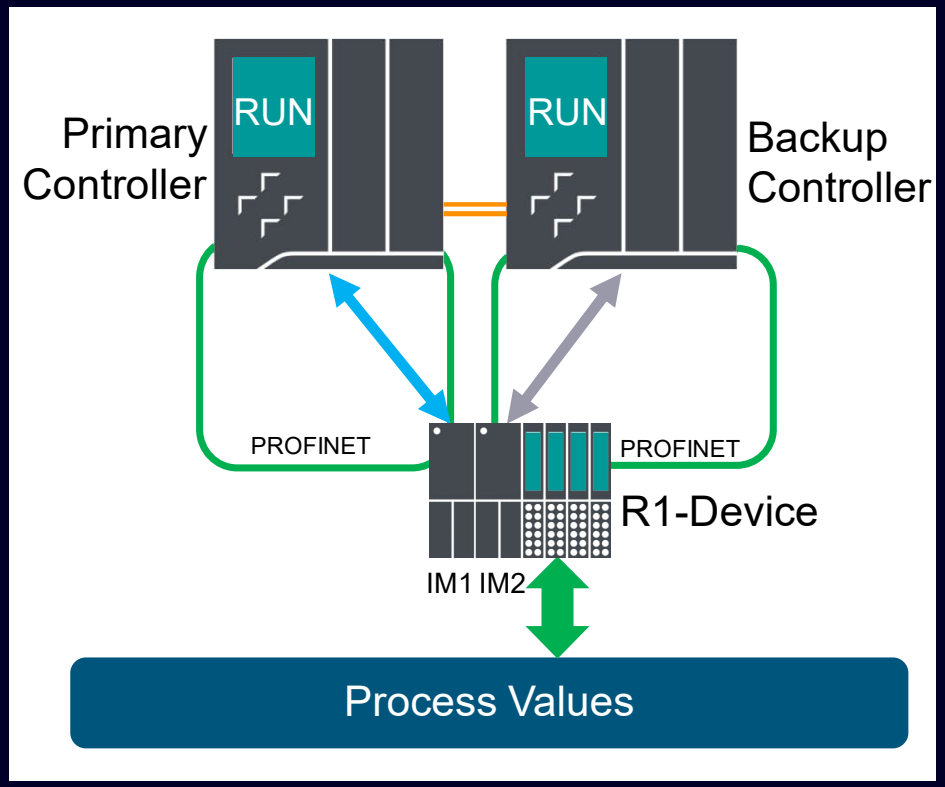
Switching behavior with PROFINET System Redundancy R1

Initial situation

R1

Primary Controller is connected to Interface Module 1 (IM1)
Backup Controller is connected to Interface Module 2 (IM2)

Process values are exchanged



Initial Situation | Switching behavior | Result

Primary AR

Backup AR

SIEMENS

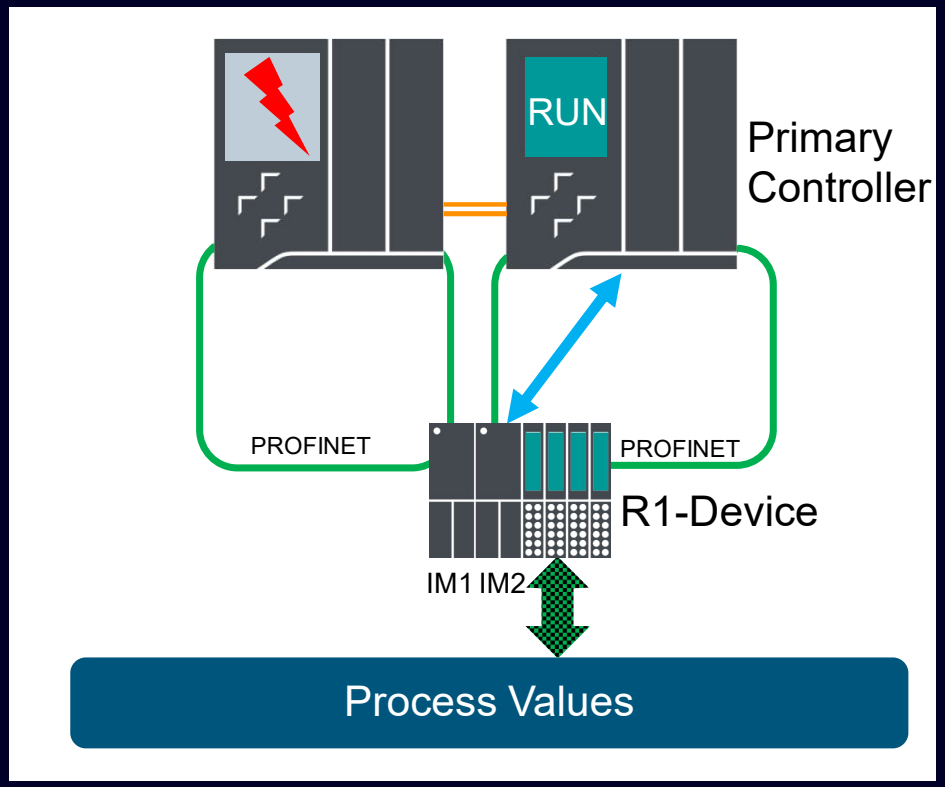
Switching behavior with PROFINET System Redundancy R1

Scenario: One controller fails – switching process begins

R1

Remaining controller takes over automatically.
The existing connection is activated

Process values are used for a very short time[1)] frozen:
I/O values remain at the last value



Initial Situation | Switching behavior | Result

Primary AR

Backup AR

[1)] Duration approx. 40ms

SIEMENS

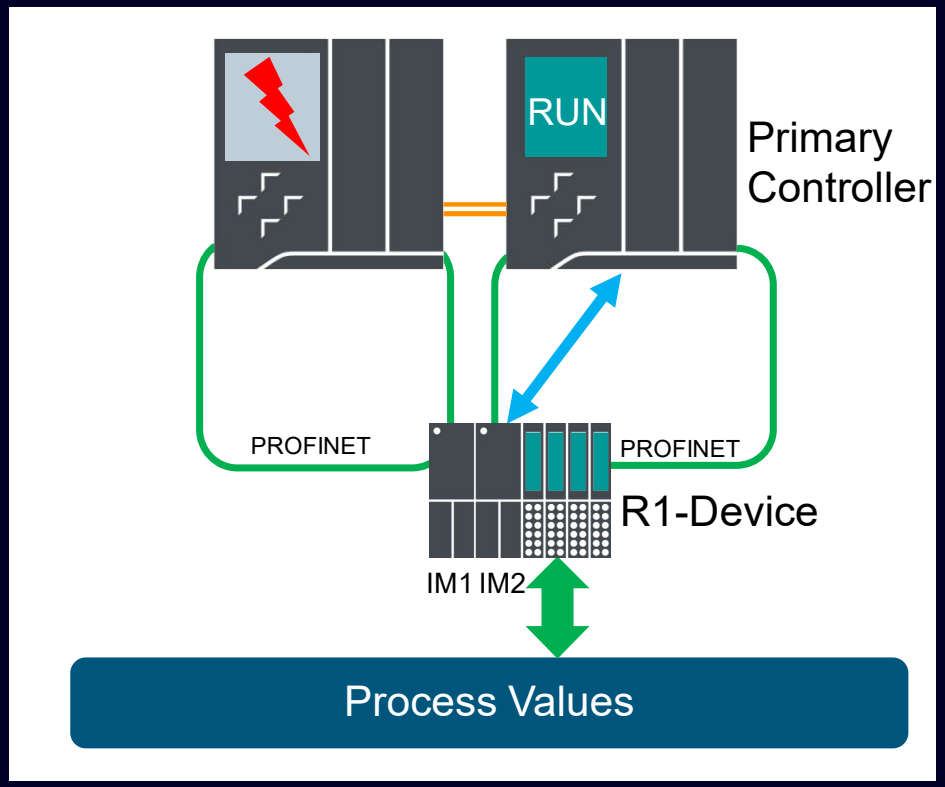
Switching behavior with PROFINET System Redundancy R1

Scenario: One controller fails - operation complete

R1

Remaining controller has a connection to interface module 2

Process values are exchanged



Initial Situation | Switching behavior | Result

Primary AR

Backup AR

SIEMENS

PROFINET System Redundancy
Siemens I/O systems with PN R1 function

R1

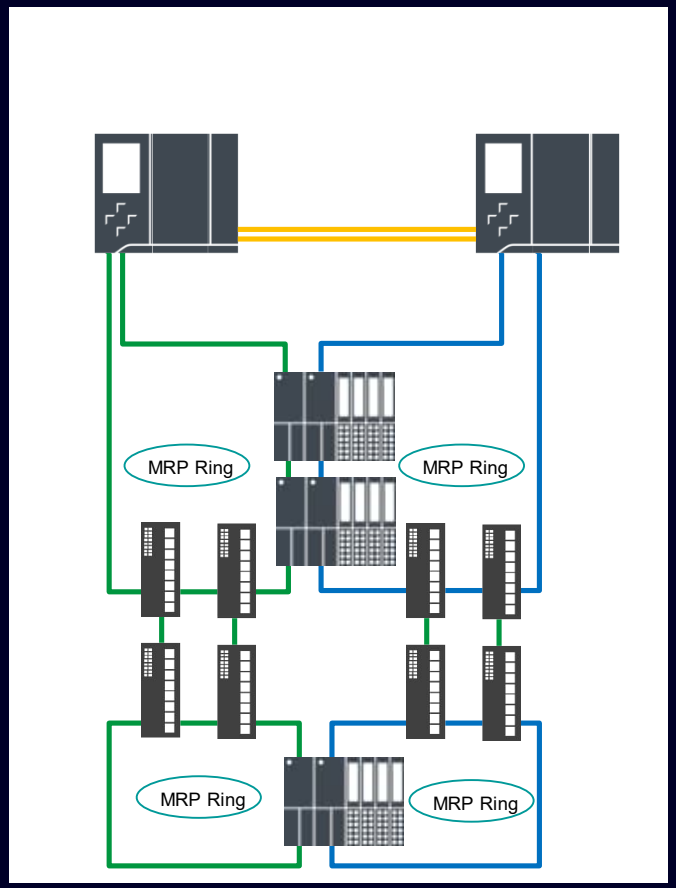
Product		Article
ET 200SP IM155-6 PN R1(with redundant IM) (with F-Modules)		6ES7155-6AU00-0HM0
ET 200SP HA IM155-6 PN HA (with redundant IM) (without F-Modules)		6DL1155-6AU00-0PM0
ET 200iSP IM155-6 PN HA (with redundant IM) (with F-Modules)		6ES7152-1BA00-0AB0

SIEMENS

Network Configuration Examples S7-1500HF

Ring topology for S7-1500HF – extended with MRP Interconnection

R1



Redundant ring coupling via MRP interconnection

- Redundant R1 rings can also be connected via MRP interconnection
- Thanks to redundant switch architecture, the coupled network remains functional even if one switch fails.
- Up to 50 devices can be connected per ring → The total number of participants of an H CPU can also be achieved without spur lines.
- Can be used with the following SCALANCE switches:
  XR500, XM400, XC200, XF204-2BA, XP200

SIEMENS

Network Configuration Examples S7-1500HF

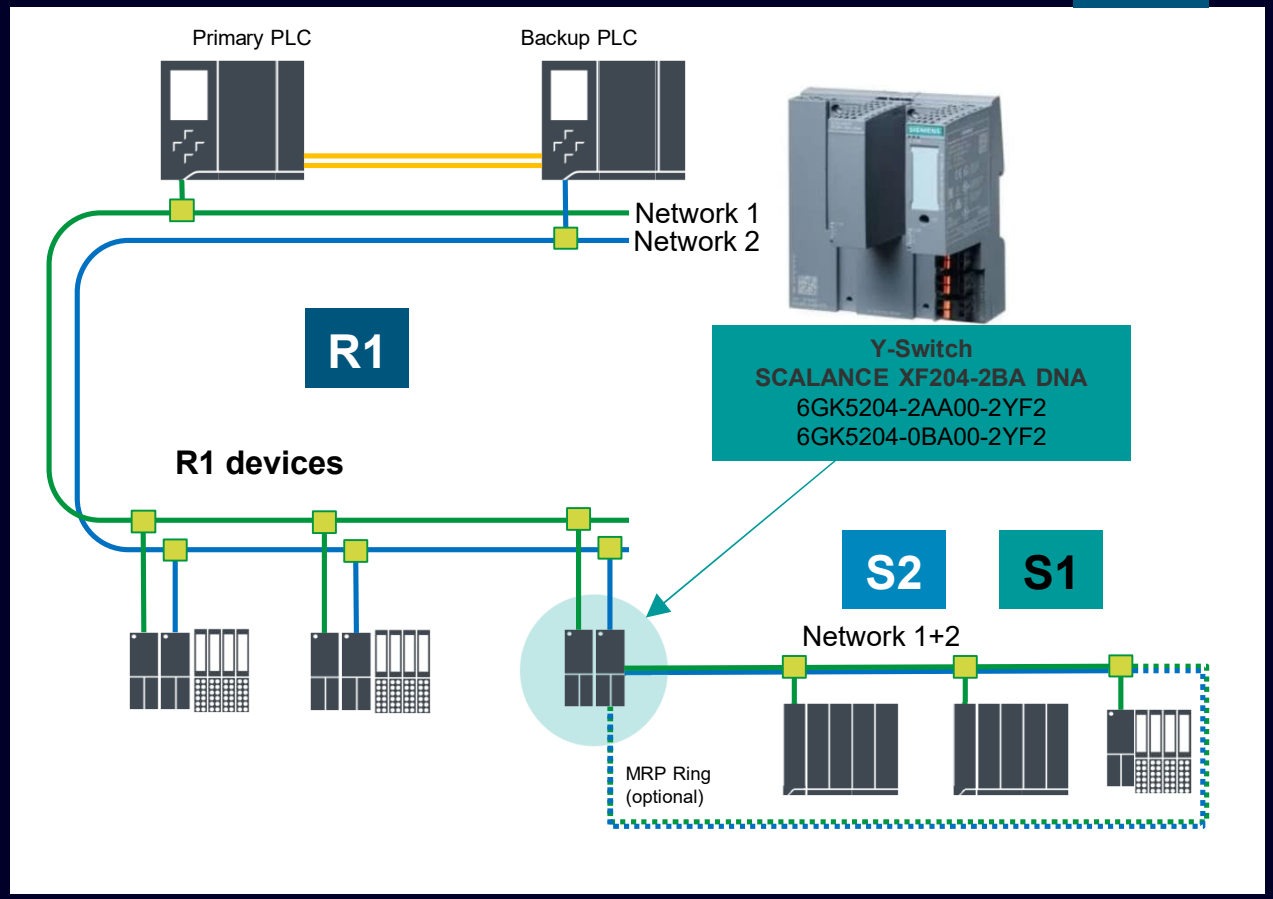
Combination of R1 and S1/S2 devices

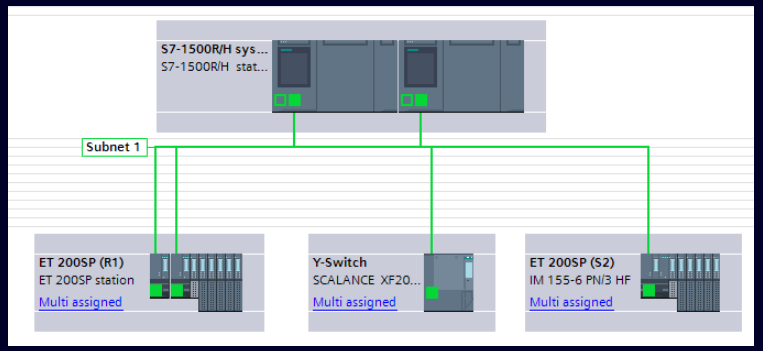
R1

R1 configurations can be extended with S2 or S1 devices using a Y-switch.

The prerequisite for this is the configuration in the TIA Portal on 1 subnet

Result: Unique IP addresses in Network 1+2 are required





Application examples with Y-Switch: See https://support.industry.siemens.com/cs/ww/en/view/109816704

SIEMENS

Network Configuration Examples S7-1500HF

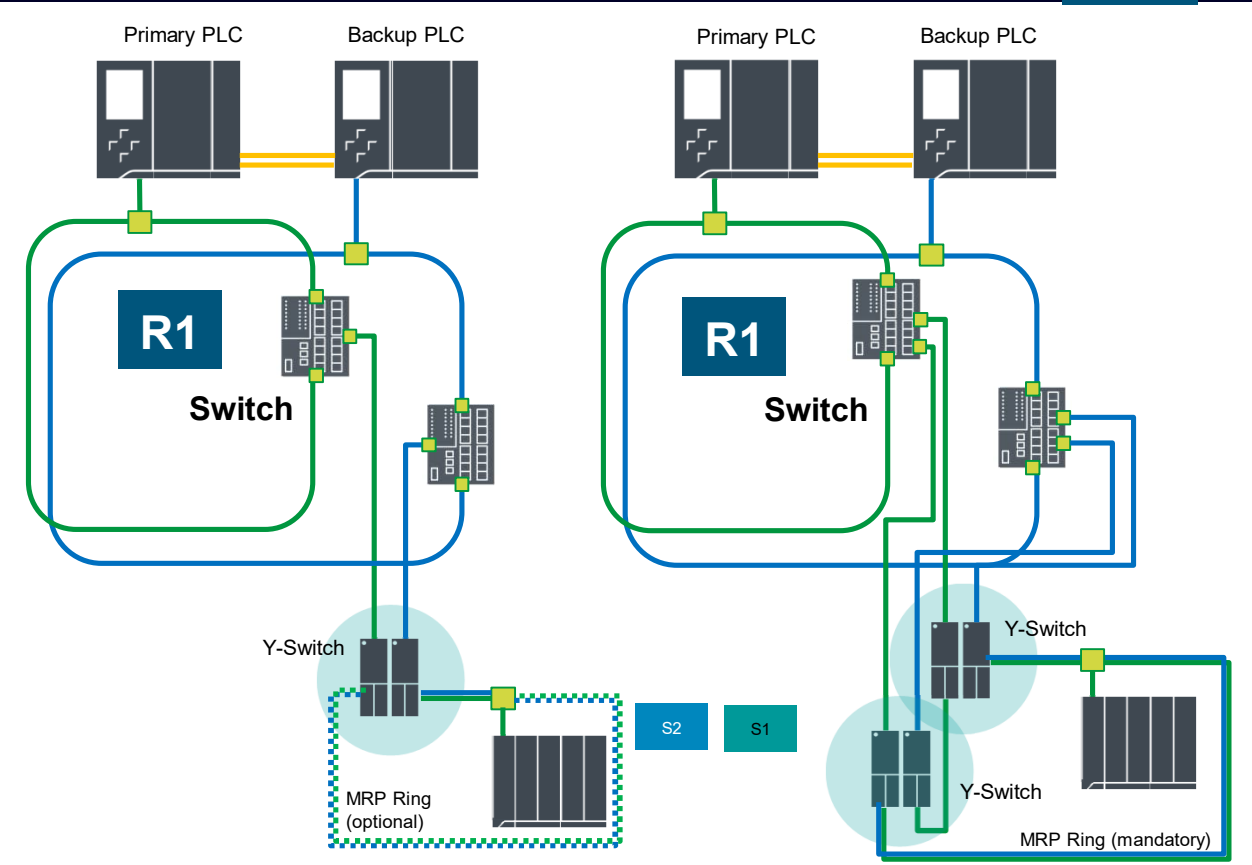
Combination of R1 and S1/S2 devices on ring structures

R1

In order to connect the Y-switch to MRP rings, additional switches are required.

To increase availability, the Y-Switch can also be designed redundantly "Redundant DNA".

In this case, an MRP ring must be used on the S1/S2 side.



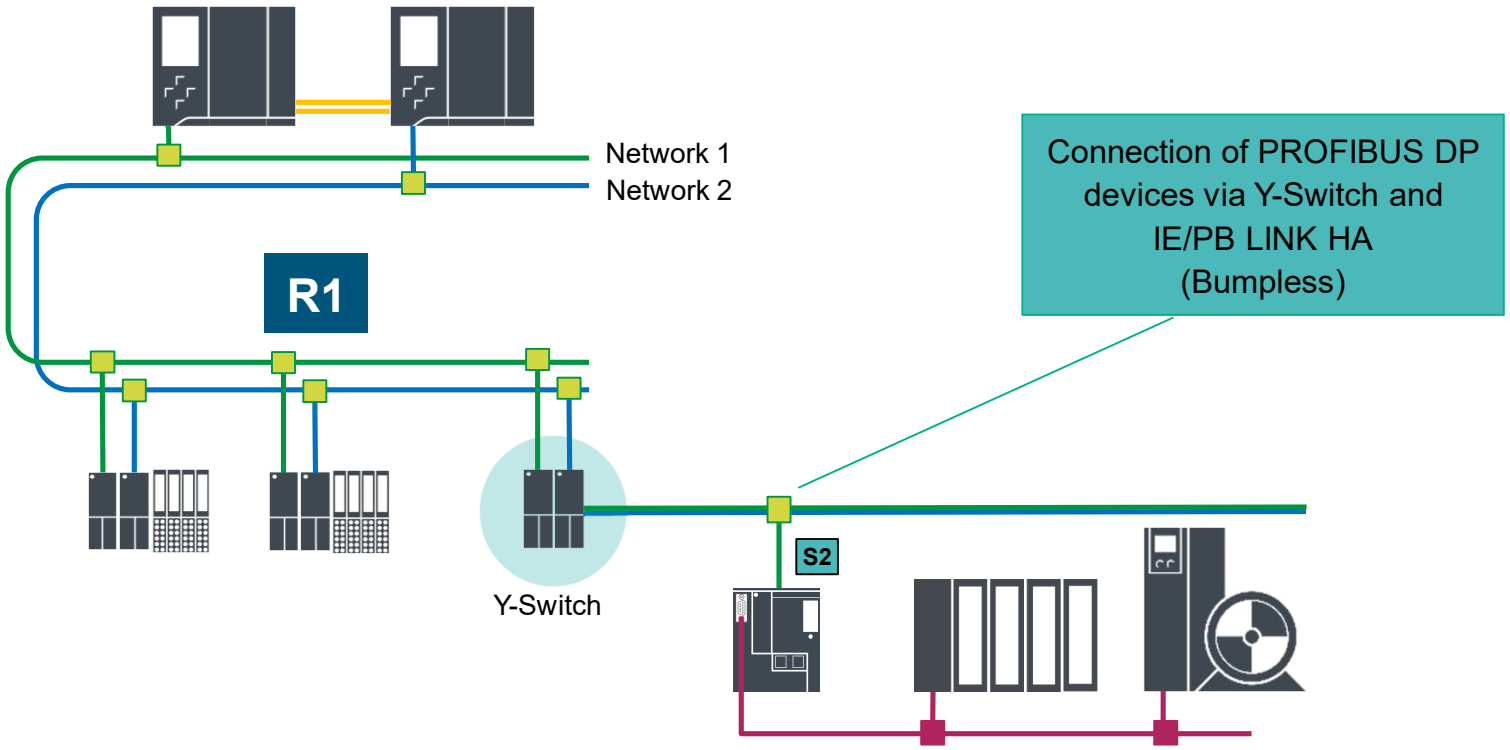
Single Y-Switch with MRP Ring

Redundant Y-Switch with MRP Ring

SIEMENS

R1 network configuration with S7-1500 HF
Connection of PROFIBUS DP devices

V19



SIEMENS

Thank you
for your attention!

Jussi Salomaa

Jussi.Salomaa@siemens.com

Timo Laakso

Timo.Laakso@siemens.com

siemens.com/process-safety