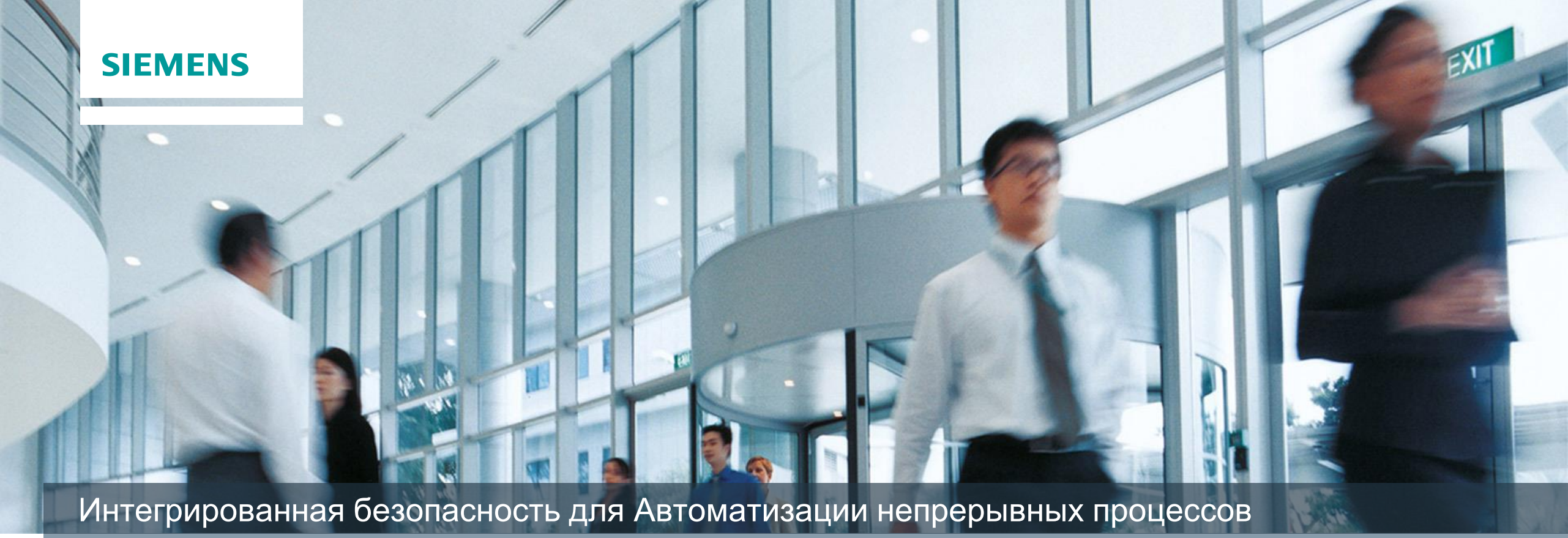


SIEMENS

Интегрированная безопасность для Автоматизации непрерывных процессов

Интегрированная безопасность для Автоматизации непрерывных процессов

SIEMENS

Введение

Интегрированная безопасность для Автоматизации непрерывных процессов

Интегрированная безопасность для Автоматизации непрерывных процессов
Полностью интегрированное решения безопасности

SIEMENS

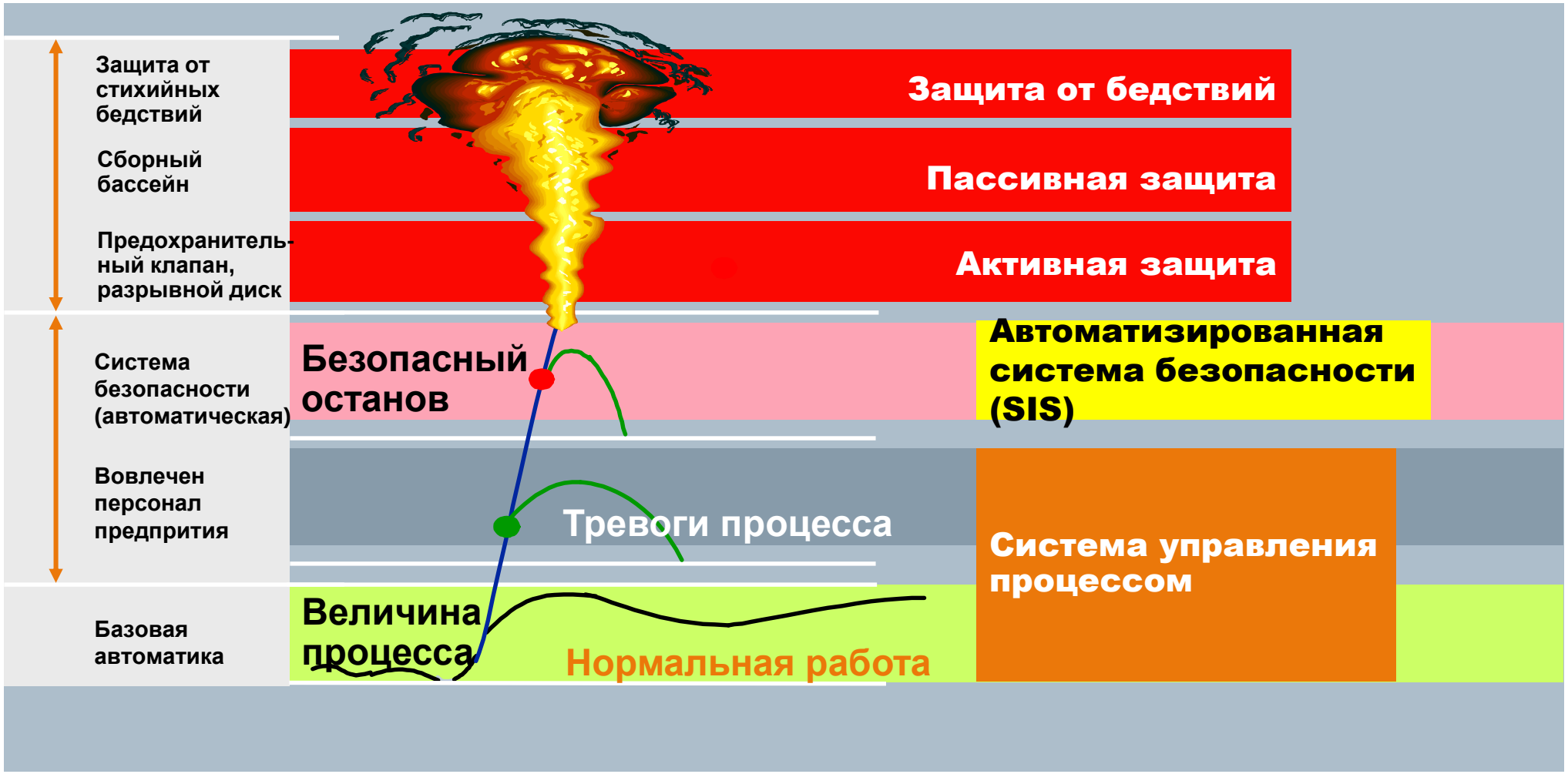
Управление функциональной безопасностью снижает риски инцидентов процесса и обеспечивает максимальную безопасность для:

Людей

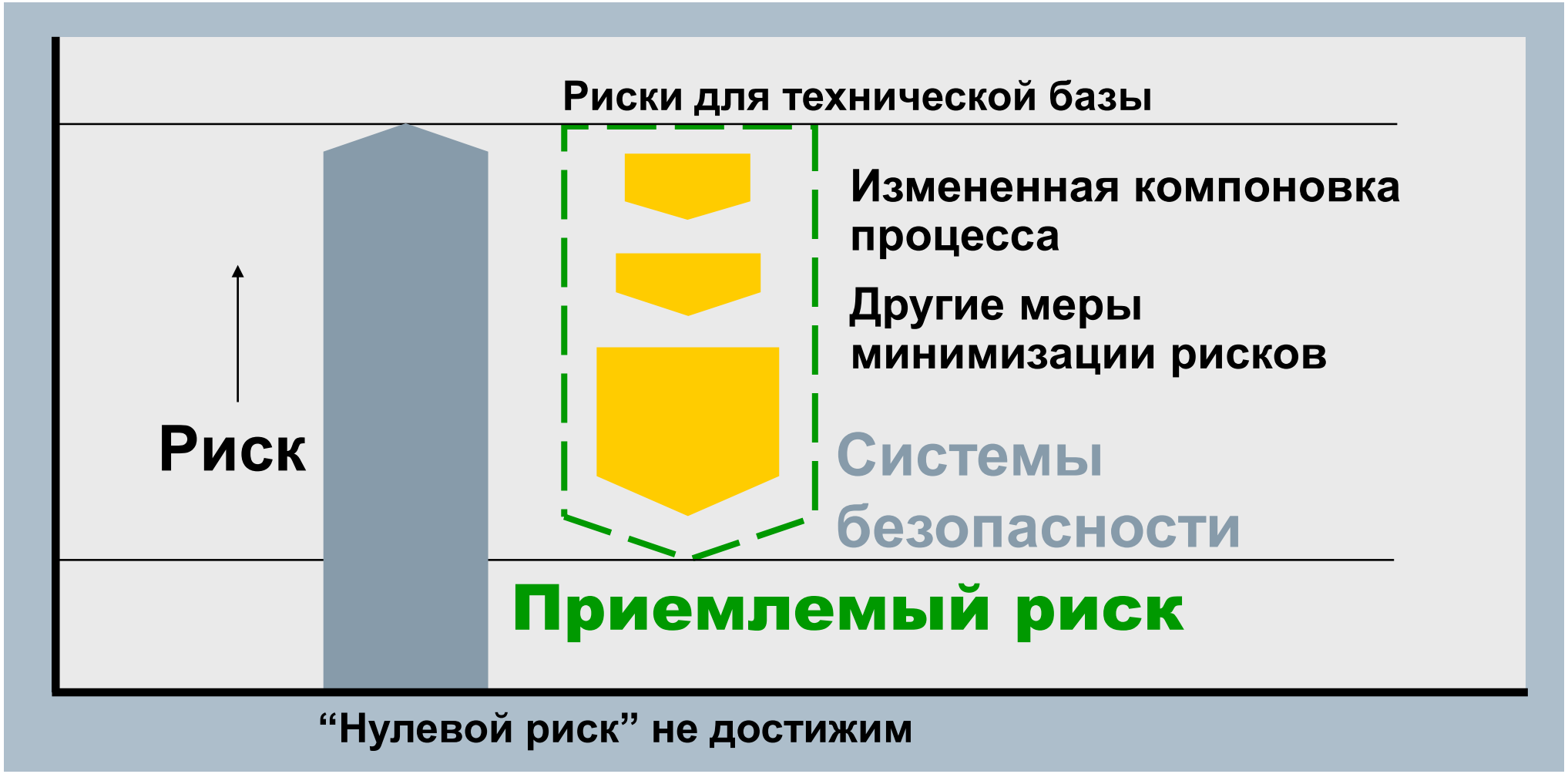
Процесса

Природы

Концепция безопасности для предприятия



Анализ рисков → минимизация рисков



Международные стандарты безопасности

IEC Commission Electrotechnique Internationale International Electrotechnical Commission Международная Электротехническая Комиссия

IEC61508

IEC 61508 служит как базовый стандарт и основа для стандартизации безопасности.

Покрывает все зоны, где для реализации функций защиты, связанных с безопасностью используются электрические, электронные или ПЛК системы.

IEC Commission Electrotechnique Internationale International Electrotechnical Commission Международная Электротехническая Комиссия

IEC61511

Отраслевые стандарты на базе IEC 61508, такие как IEC 61511 для перерабатывающей промышленности или IEC 61513 для атомной промышленности

Отраслевые стандарты важны для планирования и эксплуатации соответствующих предприятий.

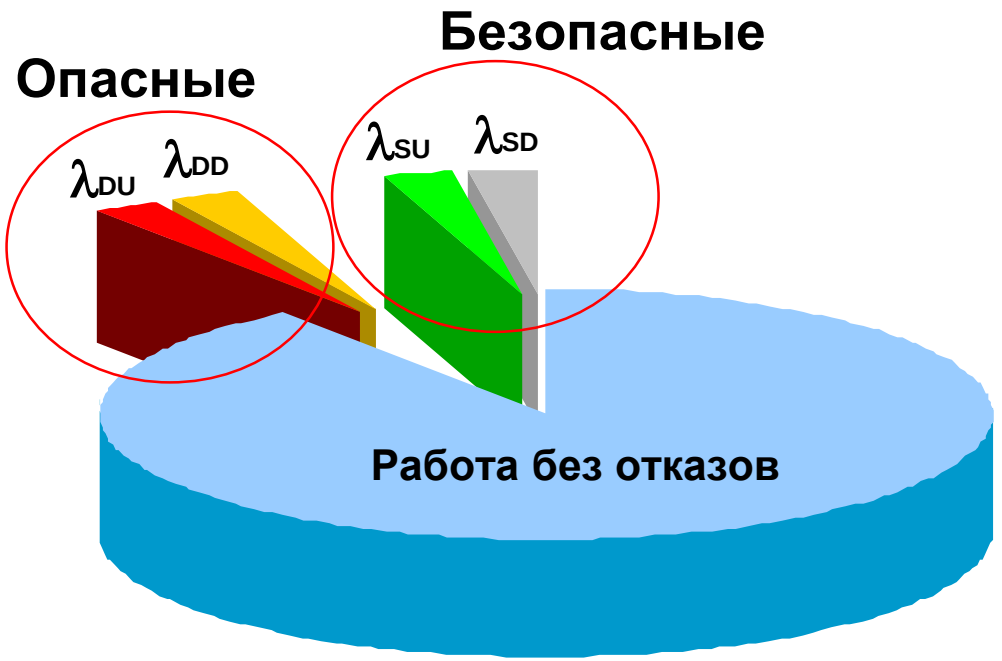
SIEMENS

Частота отказов

- λ_S **(частота всех "safe" безопасных отказов)**
  - λ_{SD} (частота всех "safe detected" безопасных обнаруживаемых отказов)
  - λ_{SU} (частота всех "safe undetected" безопасных не обнаруживаемых отказов)
- λ_D **(частота всех "dangerous" опасных отказов)**
  - λ_{DD} (частота всех "dangerous detected" опасных обнаруживаемых отказов)
  - λ_{DU} (частота всех "dangerous undetected" опасных не обнаруживаемых отказов)

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}}$$

SFF = Safe Failure Fraction - доля безопасных отказов



SIEMENS

Аппаратная отказоустойчивость - отказоустойчивость аппаратных средств – возможность аппаратуры продолжать выполнять требуемые функции даже в состоянии сбоя

В этом контексте:

Аппаратная отказоустойчивость N = N + 1 аппаратный отказ может привести к потере важной функции безопасности.

Пример:

Резервные каналы блока управления с взаимным контролем имеют Аппаратная отказоустойчивость - N = 1.

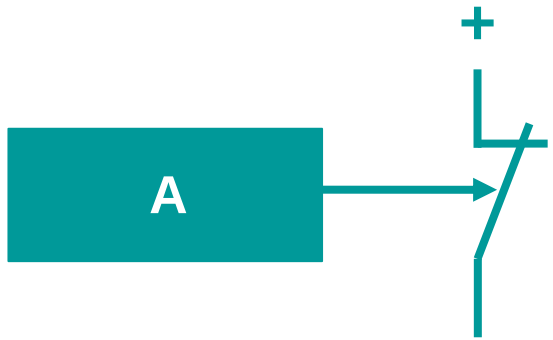
SIEMENS

Система с 1-каналом (Один канал) :

Эта архитектура состоит из одного канала, что значит – один опасный отказ достаточен что бы функция безопасности стала не эффективной.

Безопасный отказ: контакт реле размыкается и прерывает подачу питания

Опасный отказ: напр. контакт приварился, прерывание подачи питания не возможно



HFT = 0

здесь: “безопасно” значит обесточено

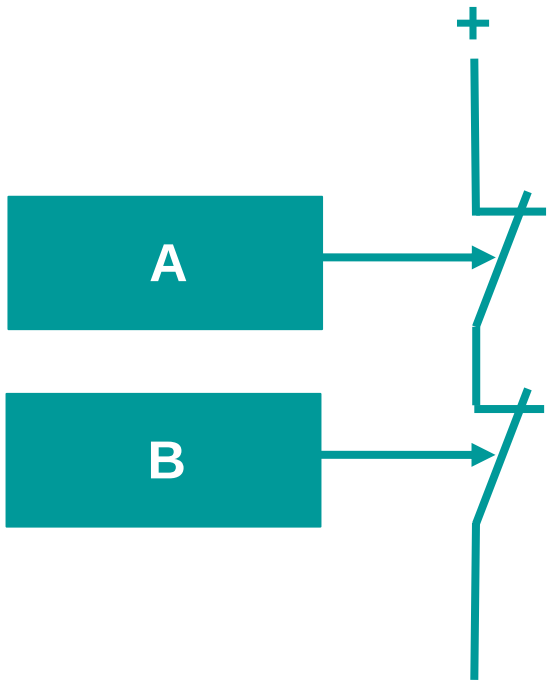
Hardware Fault Tolerance (HFT) – отказоустойчивость аппаратных средств

SIEMENS

Система с 2-каналами (Двойной канал):

Выходы подключены **последовательно**.

1 из 2 (1oo2):
Система требует только один канал для выполнения автоматической функции безопасности.
→ Выше доступность безопасности



HFT = 1

здесь: “безопасно” значит обесточено

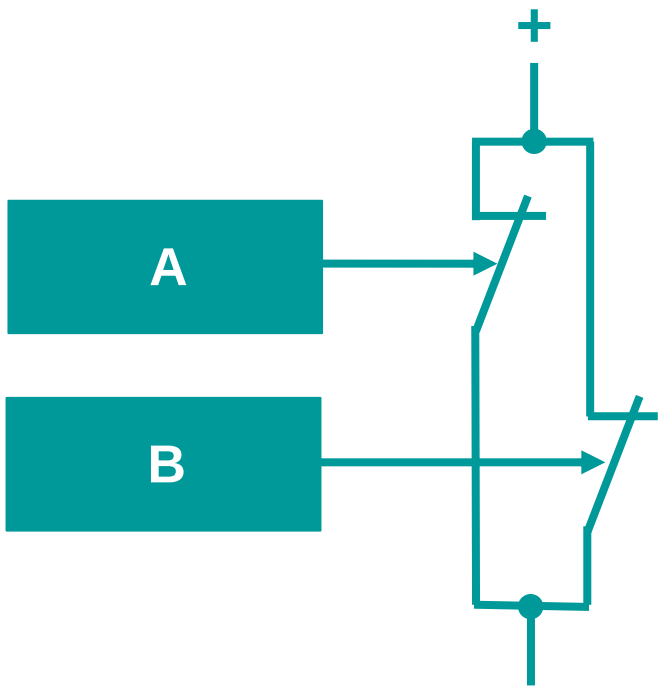
Hardware Fault Tolerance (HFT) – отказоустойчивость аппаратных средств

SIEMENS

2-канал (Dual канал) System:

Выходы подключены **параллельно**.

2 из 2 (2oo2):
Оба канала должны активироваться для выполнения автоматической функции безопасности,
т.е. при отказе одного канала автоматическая функция безопасности не может быть выполнена.
→ Увеличенная оперативная увеличение эксплуатационной готовности
→ снижение доступности безопасности



HFT = 0

здесь: “safe” means de-energized

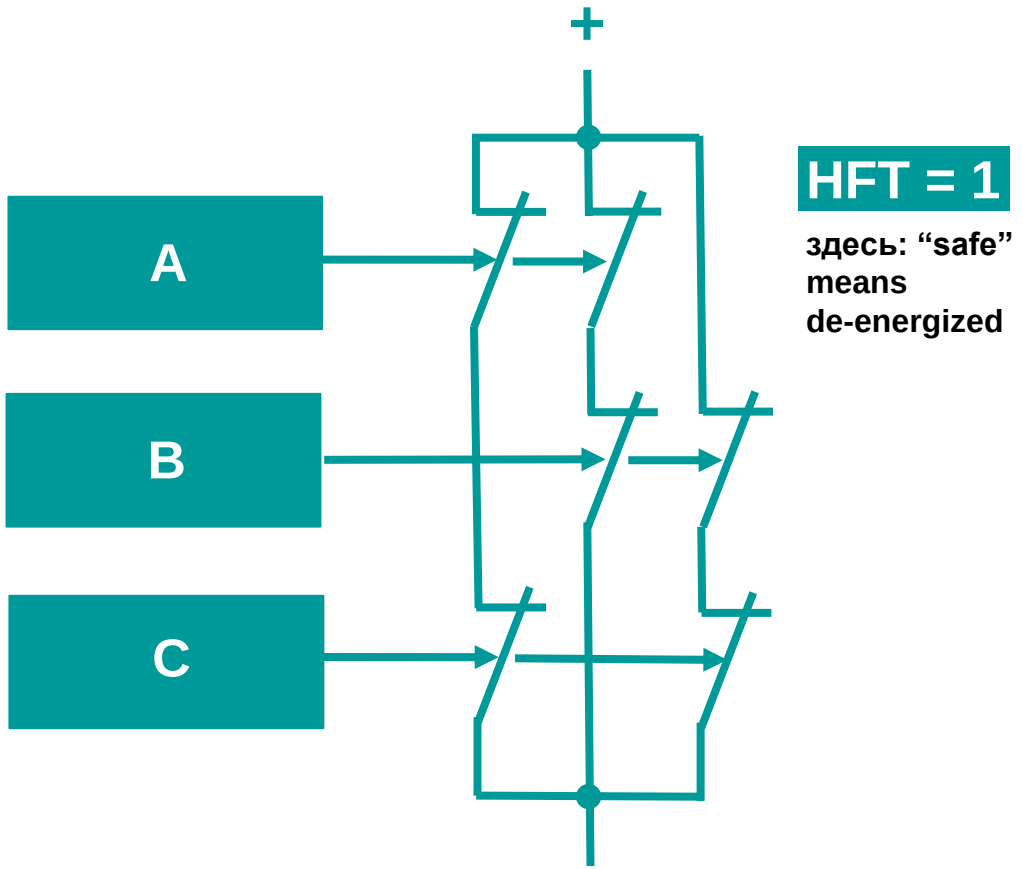
Hardware Fault Tolerance (HFT) – отказоустойчивость аппаратных средств

SIEMENS

Система с 3-каналами (Троирование) - TMR:

Минимум 2 работающих канала требуется для выполнения автоматической функции безопасности
→ увеличение эксплуатационной готовности

При отказе одного канала, автоматическая функция безопасности может продолжать выполняться
→ повышение доступности безопасности



Hardware Fault Tolerance (HFT) – отказоустойчивость аппаратных средств

Сертификация согласно IEC 61508
HFT и SFF в стандартах безопасности

SIEMENS

IEC 61508

HFT = 0
SFF > 99%

1oo1D, SIMATIC S7-400F = SIL 3

SIMATIC S7-400FH = SIL 3
2oo2 из 1oo1D систем

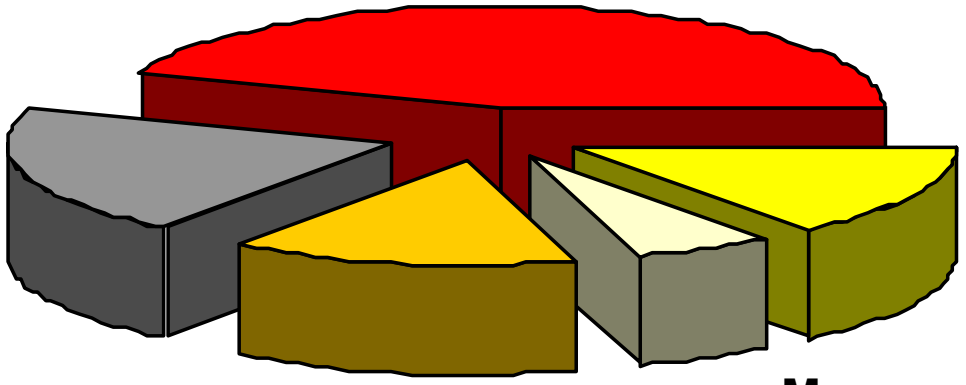
Table 3 – Maximum allowable safety integrity level for a safety function carried out by a type B safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

Hardware Fault Tolerance (HFT) – отказоустойчивость аппаратных средств

Safe Failure Fraction (SFF) – доля безопасных отказов

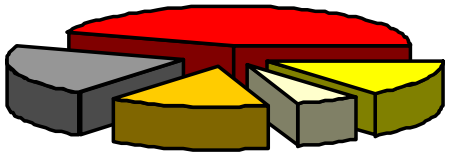
Анализ отказов в системах автоматики



Примечание : На основе 34 исследований в Британии
Health и Safety Executive (GB): from Control. Почему системы работают неправильно и как предотвратить отказы. HSE Books 1995

Распределение сбоев

Ключевые причины отказов



Компетентность людей

+

Управление безопасностью

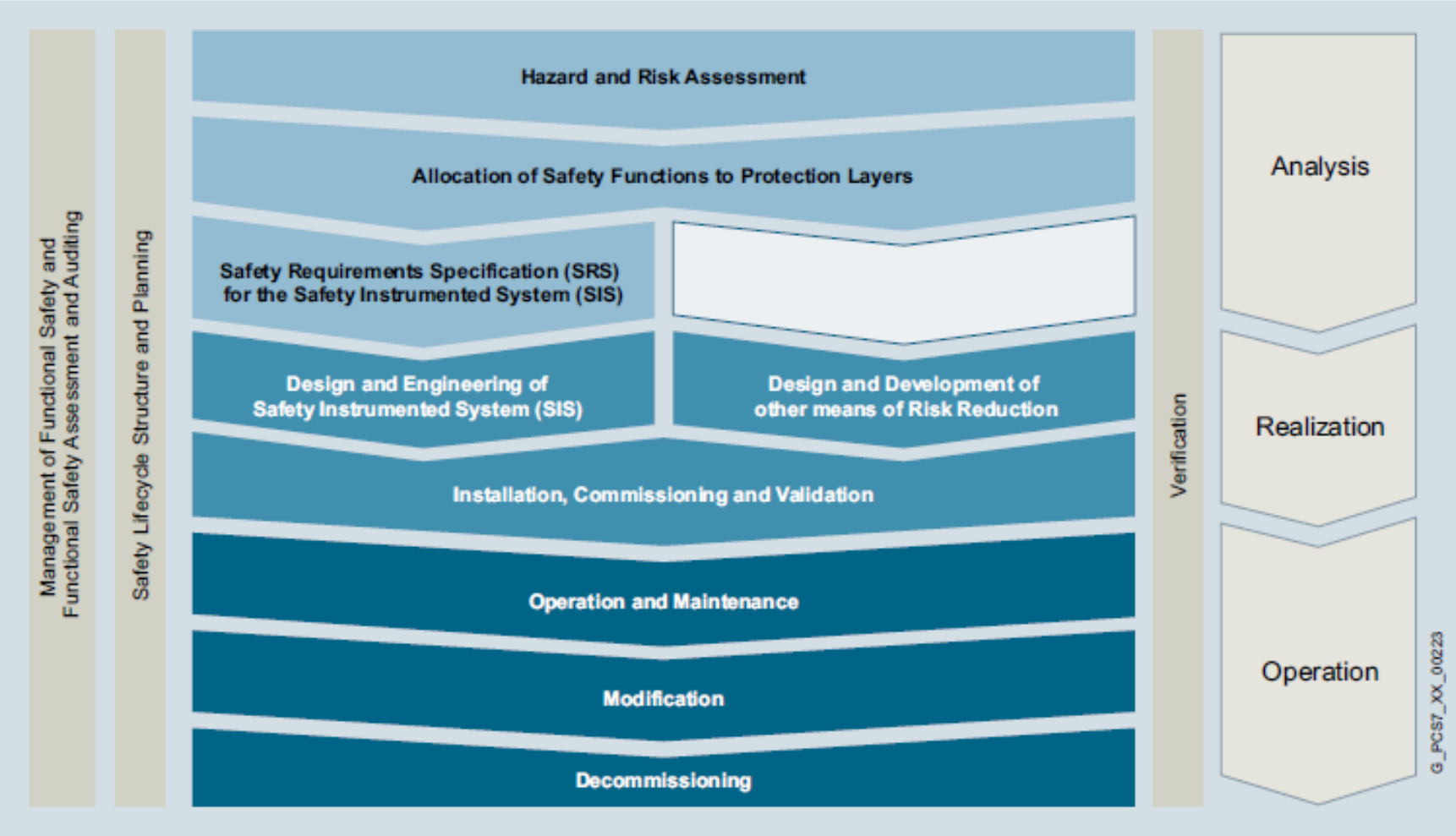
+

Технические требования

Жизненный цикл системы безопасности

- Анализ
- Спецификация
- Разработка и реализация
- Монтаж и пуско-наладка
- Эксплуатация и обслуживание
- Изменения после ввода в эксплуатацию

IEC 61511(ISA S84) Жизненный цикл систем безопасности



Управление функциональной безопасностью
План безопасности и Спецификация требований безопасности

SIEMENS

Functional Safety Management (FSM) Управление функциональной безопасностью	
Не зависимо от проекта FSM	**Зависимо от проекта FSM**
▪ Дополнение к системе контроля качества с интересующей / требуемой функциональной безопасностью ▪ Назначение ответственности ▪ Стандартные операционные процедуры – Standard operation procedures (S.O.P.) ▪ Шаблоны ▪ Квалификация	▪ Дизайн и отслеживание действий по безопасности в соответствующем проекте ▪ Менеджер проекта по безопасности ▪ План безопасности ▪ Проверка и подтверждение ▪ Независимая оценка

Сложность документации зависит от размера проекта и существующей системы менеджмента

Целевые Safety Integrity Level (SIL) – Интегральный уровень безопасности

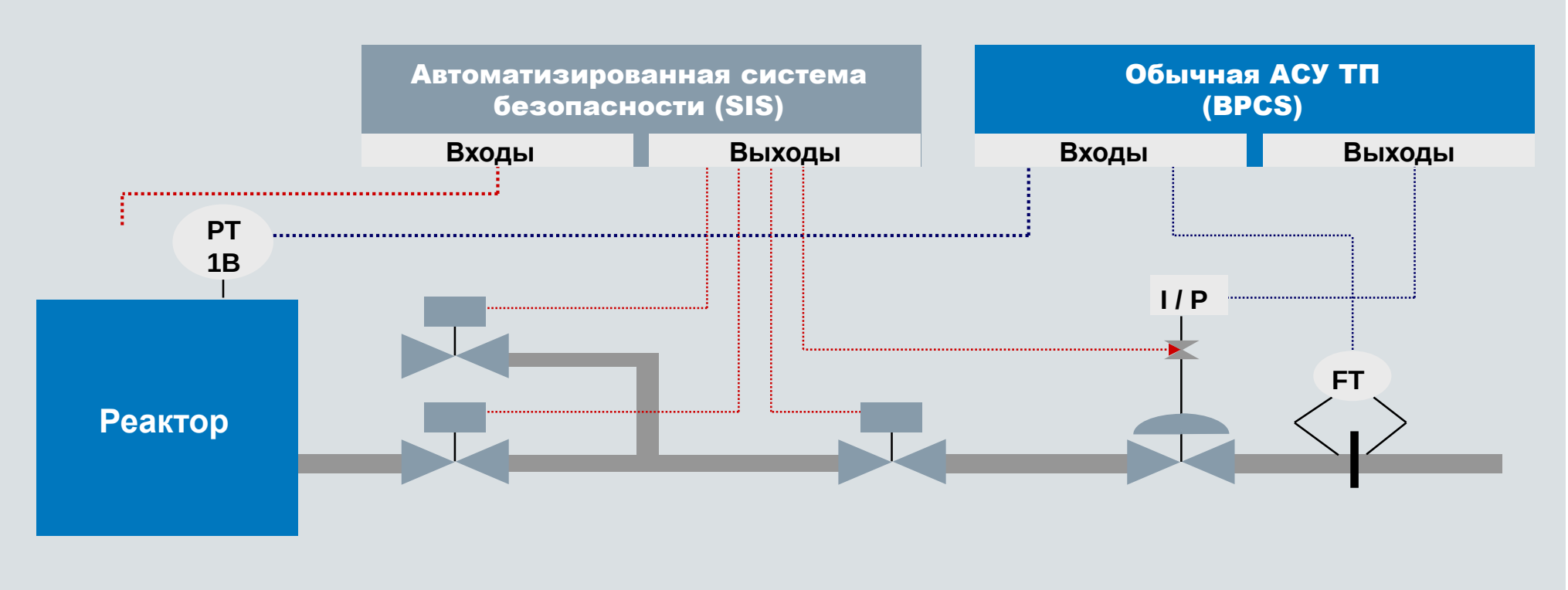
SIEMENS

Safety Integrity Level **Интегральный уровень безопасности**	**Probability of failure on demand (PFD) в год** **(режим спроса)** **Вероятность отказа на запрос**	**Risk Reduction Factor = 1/PFD** **Фактор снижения риска**
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: Критерии эффективности SIS, среди прочих вещей, описывают возможность отказа на запрос.

Автоматизированная система безопасности (SIS)

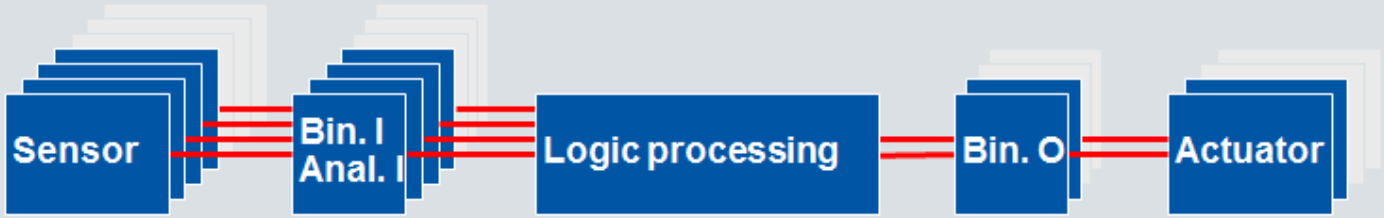
SIS: Комбинация датчикs, логического модуля (напр. контроллера) и исполнительного механизма, который детектирует аномальную робочее сотояние и АВТОМАТИЧЕСКИ возвращает предпритие снова в безопасное состояние.



Функции автоматизированной системы безопасности IEC 61508/11

SIEMENS

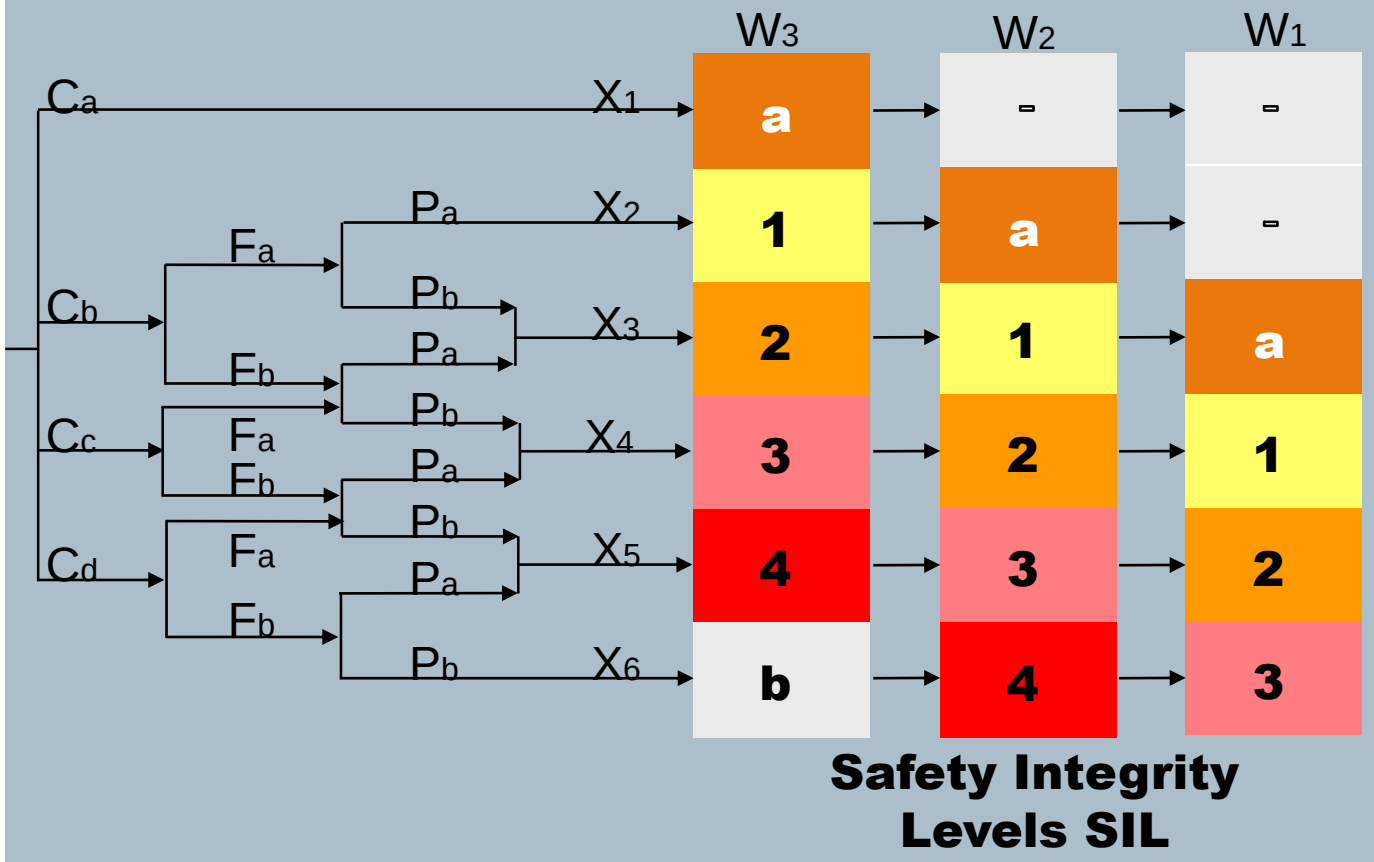
Учитывая полный **контур функциональной безопасности** согласно IEC 61508:



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**

Оценка риска SIL по карте рисков



Safety Integrity Levels SIL

a = нет специальных требований безопасности
b = недостаточно отдельной системы безопасности

Эффект

Ca Незначительная травма
Cb Большие необратимые травмы или смерть одного человека
Cc Смерть нескольких людей
Cd Смерть большого числа людей

Частота и продолжительность

Fa От редких до частых
Fb От частых до постоянных

Предотвращение опасности

Pa Возможно при определенных обстоятельствах
Pb Близко к невозможному

Вероятность возникновения

W1 Очень низкая
W2 Низкая
W3 Относительно высокая

Layer of protection analysis (LOPA) – Анализ уровня защиты

Lopa

Initiating event	PL #1	PL #2	PL #3	PL #4	Consequence
Stirrer drive failed	Batch in Operation	Operator Intervention	Pressure high safety shutdown	Pressure relief value	Tolerable risk
			X		Explosion
		0.1			
	0.5				
0.5/yr					
					No consequence

Tolerable risk according to IEC 61511-3 Table C2
PL = Protection Layer

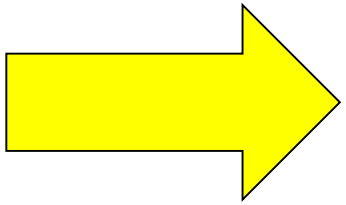
Required PFD ≤ Tolerable risk / Probability of the Event
Example: PFD ≤ $1x10^{-5}$ /(0.5 x 0.5 x 0.1 x 0.07), PFD ≤ 0.006 --> SIL 2

PFD - Probability of failure on demand - Вероятность отказа на запрос

SIEMENS

Спецификация требований безопасности

Требования к функциям безопасности	Требования к целостности безопасности



Должны быть указаны все требования необходимые для разработки автоматических функций безопасности

Приложения для обеспечения безопасности процесса

Приложения безопасности в промышленности

Системы экстренного и останова процесса (ESD/PSD)

- согласно IEC 61508, IEC 61511, ISA S84 и VDI/VDE 2180

Системы управления горением (BMS)

- согласно EN 230, EN 298 и NFPA 85

Пожарные и приложения загазованности (F & G), детектирование пламени и системы пожарной сигнализации

- согласно EN 54, NFPA 72

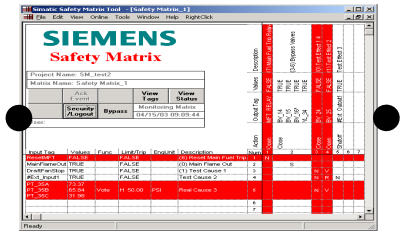
Пример для PFD calculation

SIEMENS

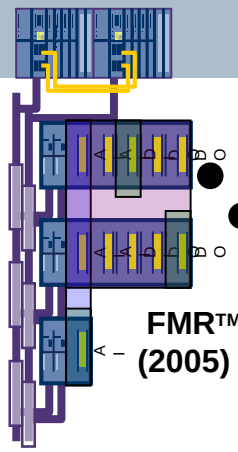
История

Интегрированная безопасность для Автоматизации непрерывных процессов

ИСТОРИЯ SIEMENS в безопасности процессов



SIMATIC
Safety Matrix (2004)

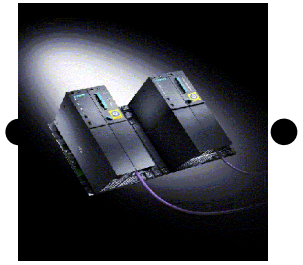


FMR™
(2005)

Safety Fieldbus with
Redundant Ring (2006)

ЦПУ 410
PROFINET
(2013)

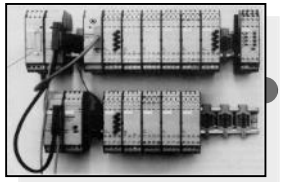
S7 300F/400F PROFIsafe
(2002)



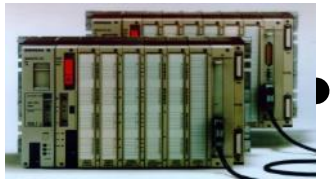
S7-400FH PROFIsafe
(1999)

Safety Matrix
(1999)

QUADLOG
(1995)



SIMATIC S5-110F
(1980)



SIMATIC S5-115F
(1988)

SIMATIC S5-95F
(1994)

Интегрированная безопасность для Автоматизации непрерывных процессов
Полностью интегрированное решение безопасности

SIEMENS

Основные тренды в безопасности процессов

- **Интегрированная архитектура безопасности и контроля процесса**
- **Больше фокус на простоту применени**
- **Больше фокус на безопасность от датчика до исполнительного механизм**
- **Больше важность инструментов менеджмента жизненным циклом**
- **Больше масштабируемость**
- **Более распределенных систем безопасности**
- **Больше гибкости**

SIEMENS

Решение Siemens

Интегрированная безопасность для Автоматизации непрерывных процессов

Интегрированная безопасность для Автоматизации непрерывных процессов Siemens задает моду инновациям

Интегрированное управление и безопасность

- Полная интеграция в SIMATIC PCS 7
- Один интерфейс пользователя для Инжиниринга, Эксплуатации, Диагностики и ЧМИ
- Одна платформа для безопасного и обычного приложения

Интегрированная технология безопасных полевых шин

- Отказоустойчивое и резервированная коммуникация между ЦПУ, распределенным В/В и устройствами безопасности

Flexible Modular Redundancy (FMR) – Гибкое модульное резервирование

- Дает масштабируемое, бюджетное решение под Ваши задачи

Управление жизненным циклом

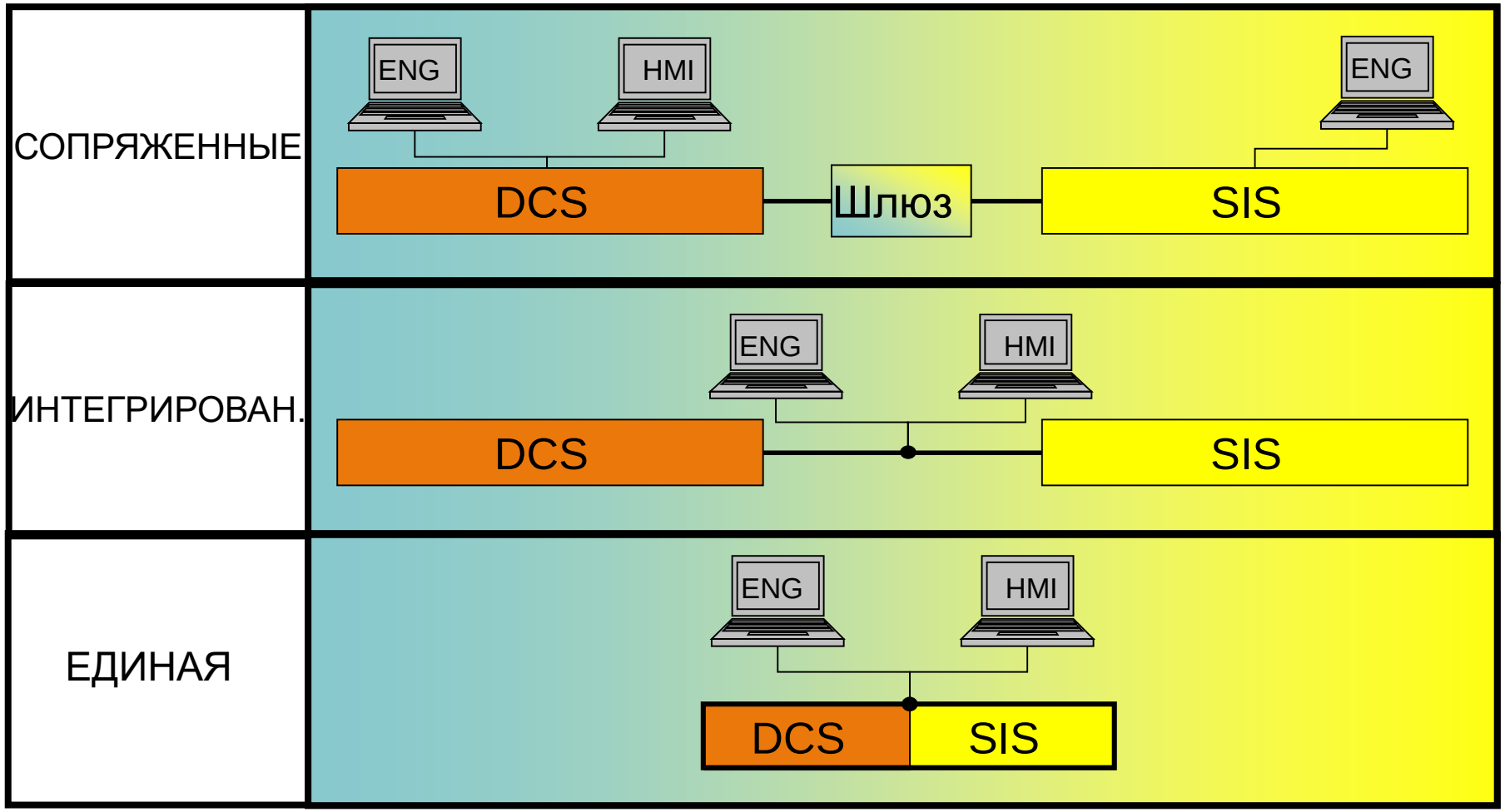
- Простое программирование с CFC и Safety Matrix
- Safety Matrix как инструмент управления жизненным циклом (Lifecycle Management Tool)

SIEMENS

Интегрированные Управление и Безопасность

Интегрированная безопасность для Автоматизации непрерывных процессов

Levels of Integrated Control и Safety



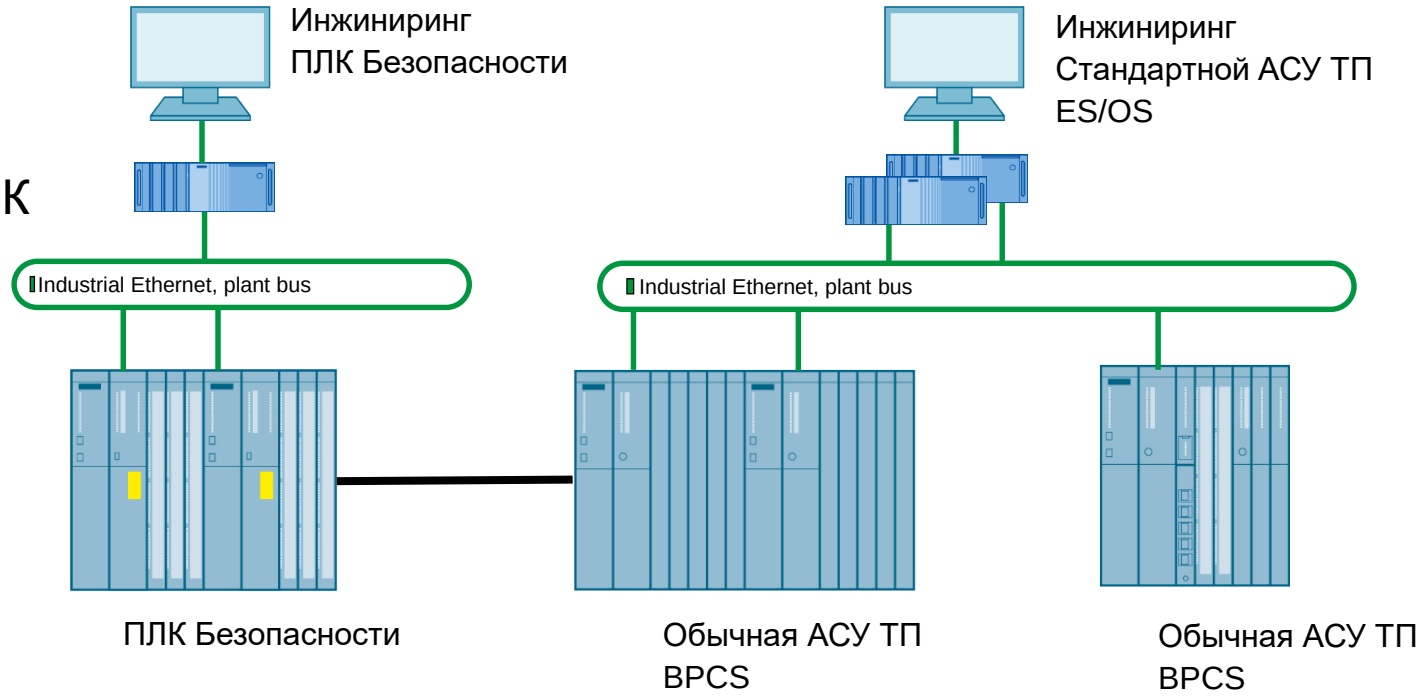
Levels of Integrated Control и Safety

СОПРЯЖЕННЫЕ		Gateway	
ИНТЕГРИРОВАН.			
ЕДИНАЯ			Стандарт-ный B/B

Уровень интеграции Управления и безопасности с S7-400 и PCS 7

Сопряженные

- Отдельные системы
- S7-400F/FH как Safety PLC
- Отдельная станция инжиниринга для ПЛК Безопасности
- AS-410 для PCS 7
- Раздельные ES/OS для РСУ

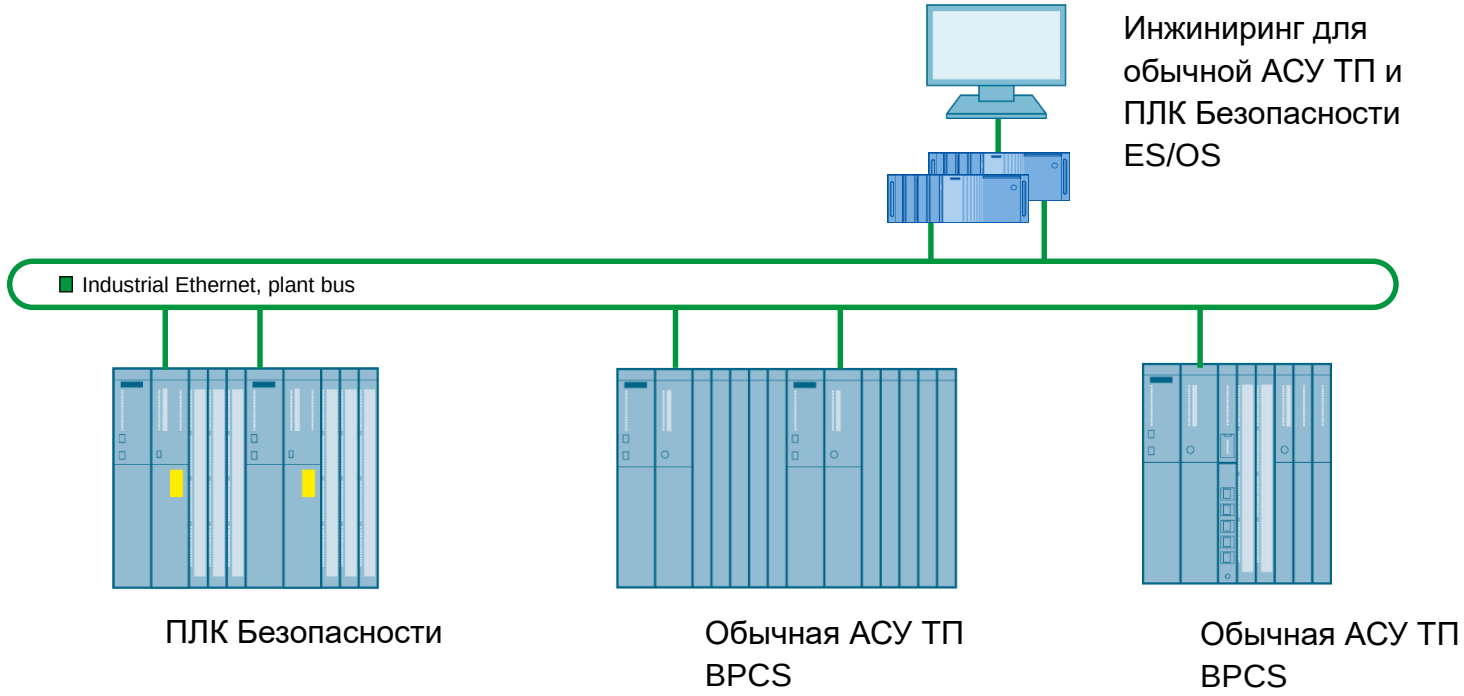


Не требуется дополнительных знаний, поскольку используется подобный инжиниринг ПАЗ и РСУ разделены

SIEMENS

Интегрированные

- Разделенные системы
- Общий инжиниринг
- Общий ЧМИ



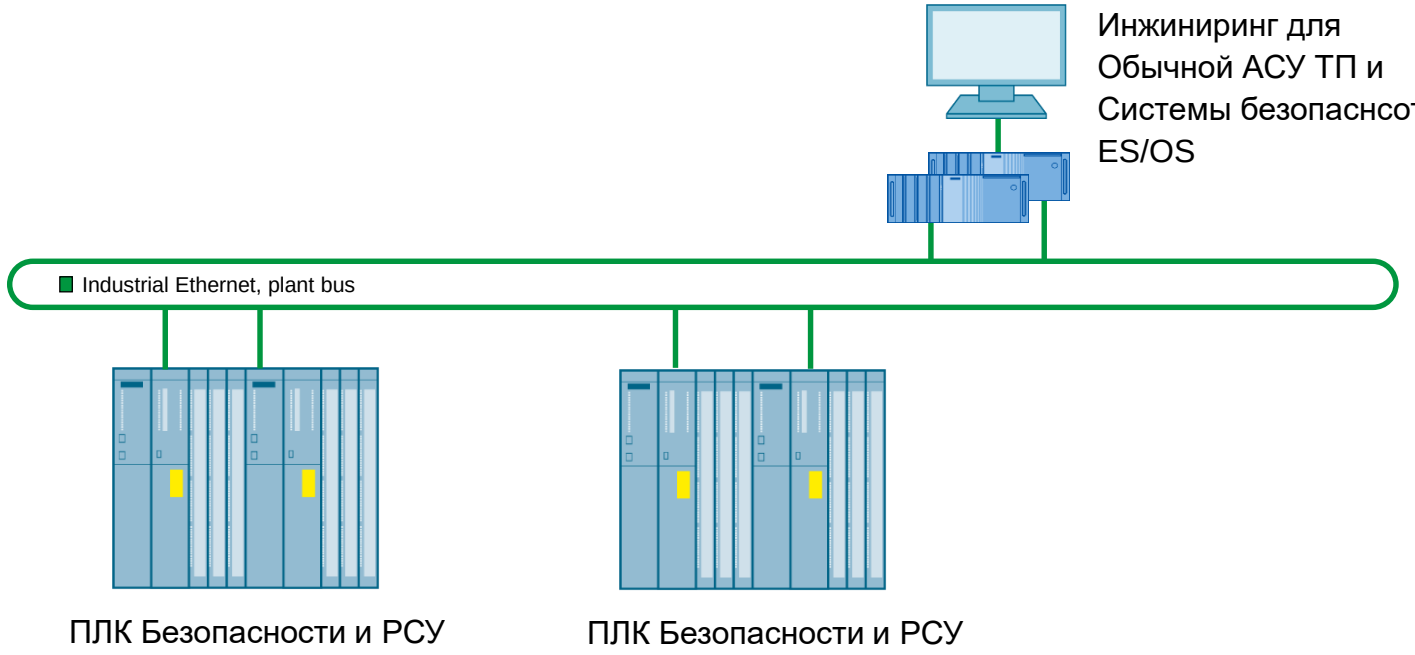
Общий инжиниринг для ПАЗ и РСУ

Уровень интеграции Управления и безопасности с S7-400 и PCS 7

SIEMENS

Единый

- Общая система для ПАЗ и РСУ
- Общий инжиниринг
- Общий ЧМИ



Технология разделения Интегрированной безопасности сертифицирована TÜV вплоть до SIL 3
Меньше требования к ЗИП

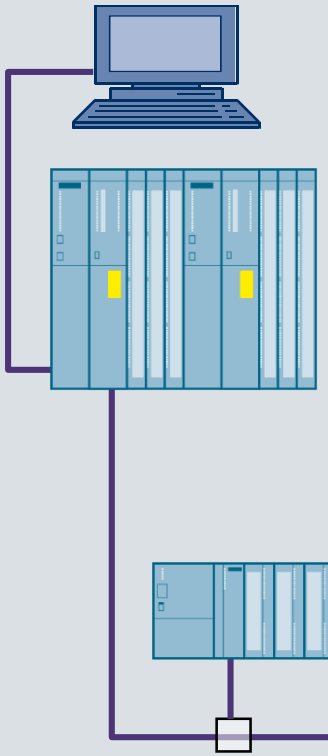
SIMATIC Интегрированная безопасность
Детектирование ошибок и Сдерживание ошибок

Функции безопасности для детектирования и управления ошибками:

- F-ЦПУ
- PROFIsafe коммуникация
- F-I/O модули
- Полевые устройства

SIMATIC Интегрированная безопасность
Концепция

SIEMENS



Стандартное ПО программиро-вания STEP 7	+	Инструмент отказоустойчивого программирования S7 F System
Стандартный ЦПУ F-Аппаратура	+	Отказоустойчивое приложение
Стандартный Удаленный В/В	+	Отказоустойчивый Модуль В/В
Стандартный PROFIBUS DP	+	PROFIsafe

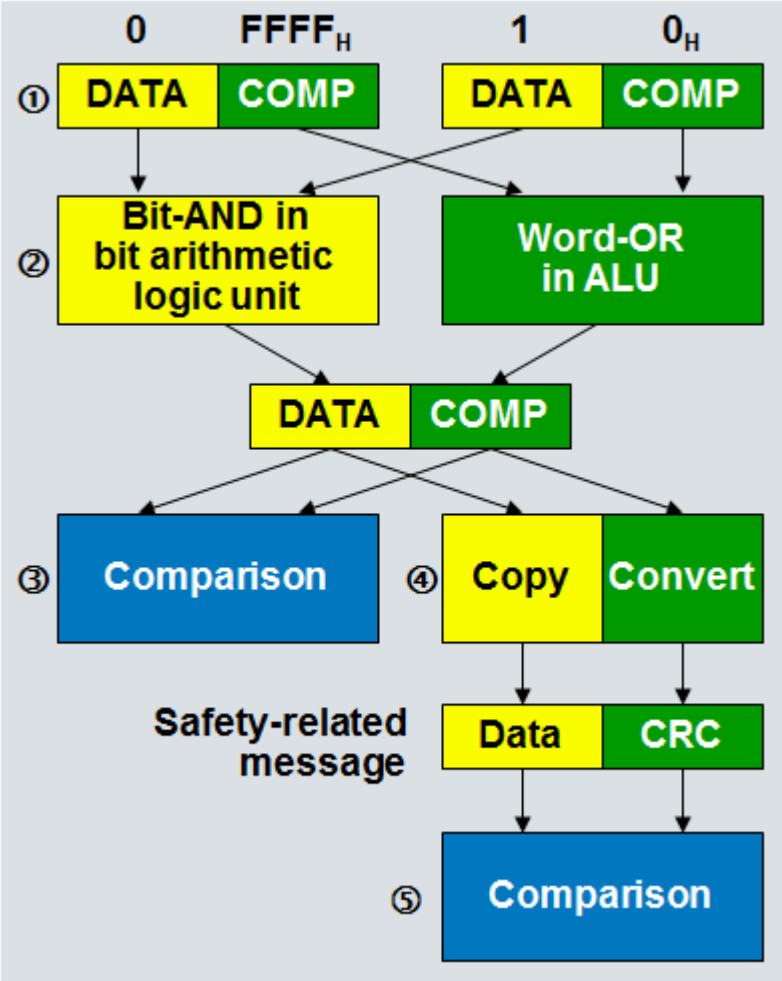
SIMATIC Интегрированная безопасность
Механизмы безопасности

Multi-channel storage of safety-critical data in instance DBs in the CPU, e.g. as word-oriented complement COMP

Multi-channel processing of the safety function in F-FBs by SP7-ASIC of the CPU
- Standard operation on DATA
- Multi-channel operation on COMP

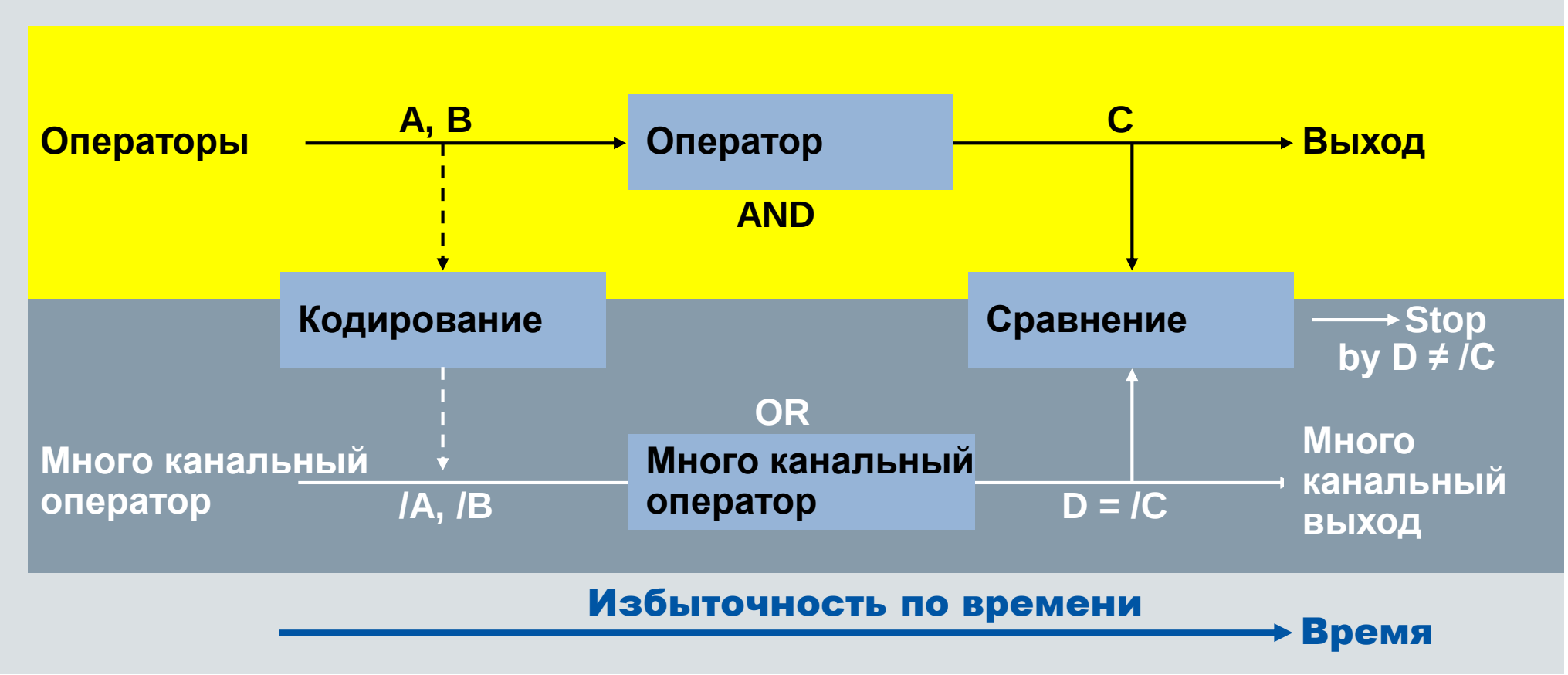
CPU-internal comparison in the output driver to improve error locating
Error handling: disable outputs and stop CPU

CPU-external comparison in receiver (F-output modules and processing F-CPUs)
Error handling: safe substitute values and error message



SIEMENS

Избыточность по времени и многоканальность вместо структурного резервирования



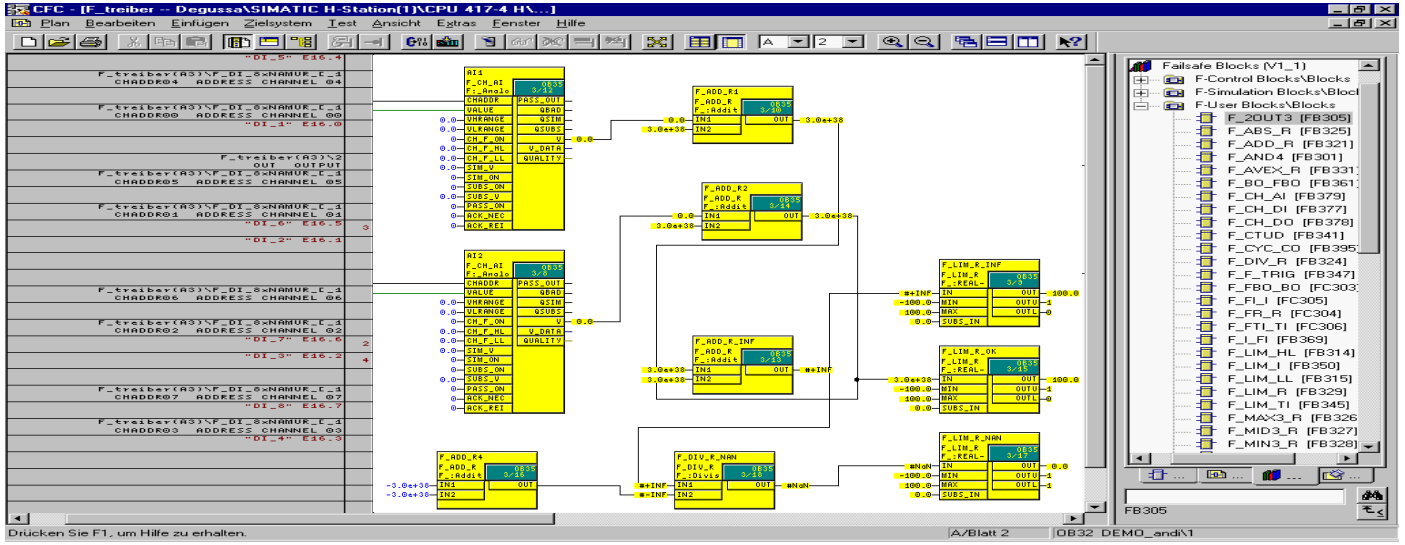
SIMATIC Интегрированная безопасность

Новая технология обеспечивает разделение между безопасностью и стандартным управлением

Невозможно использовать стандартные сигналы в модулях безопасности

Отдельные области данных для сигналов безопасности и стандартных сигналов

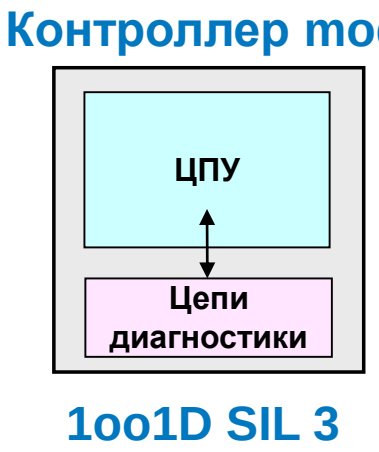
Непрерывная маркировка сигналов безопасности желтым цветом



Общий дизайн системы ЦПУ S7-400 и ЦПУ 410

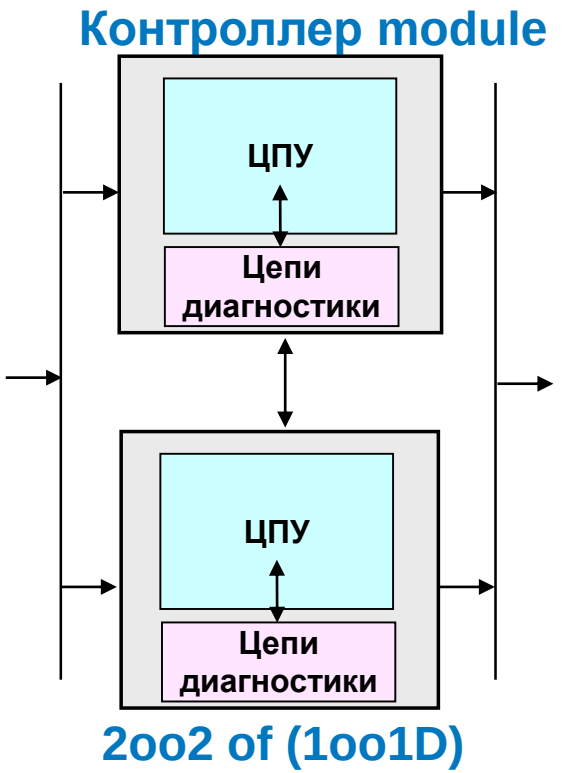
Один ЦПУ

- Структура 1oo1D с разнообразное прикладное ПО
- SIL 3 согласно IEC 61508:2000
- HFT = 0; SFF > 99%



Резервированные ЦПУ

- Структура 2oo2 из 1oo1D с разнообразным прикладным ПО
- Для останова оба ЦПУ должны быть в отказе
- SIL 3 согласно IEC 61508:2000



Harware Fault Tolerance (HFT) - отказоустойчивость аппаратных средств
Safe Failure Fraction (SFF) - доля безопасных отказов

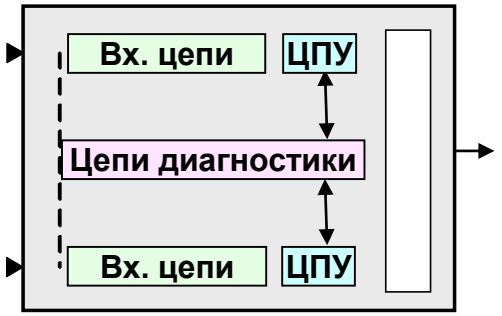
Общий дизайн системы
F-I/O Модули

Модуль дискретного ввода
- 24 – канала SIL 2 с 1oo1D
- 12 – каналов SIL 3 с 1oo2D
- Внутренняя диагностика

Модуль аналогового ввода
- 6 – каналов SIL 3 с 1oo1D
  - Внутри 1oo2
- Внутренняя диагностика

Модуль дискретных выходов
- 10 – каналов SIL 3 с 1oo1D
  - Каждый канал с внутренним 1oo2
- Внутренняя диагностика

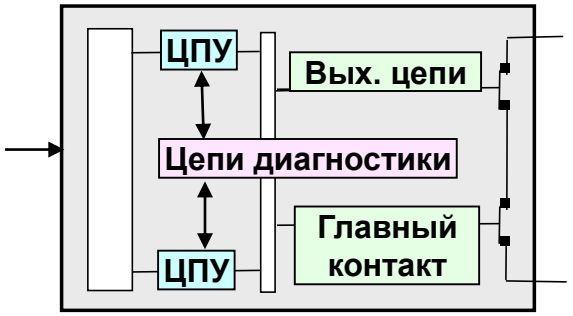
Входной модуль



1oo1D для SIL 2

1oo2D для SIL 3

Выходной модуль



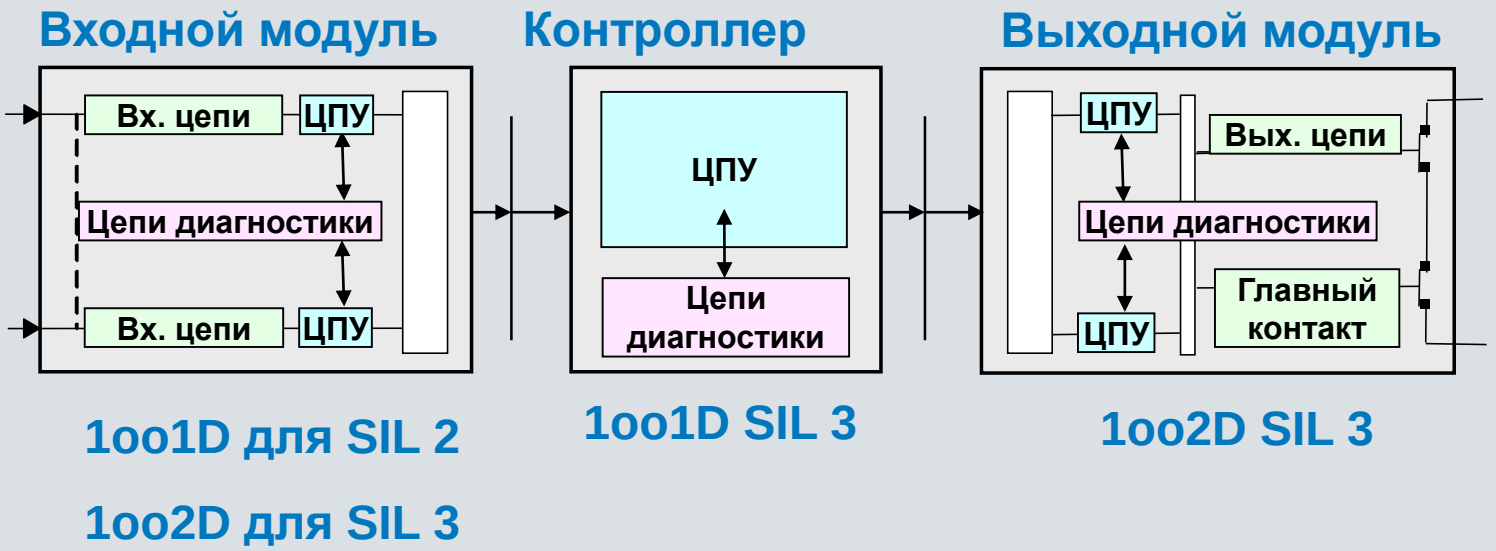
1oo2D SIL 3

Дизайн системы

SIEMENS

Не резервированная система

- Один либо два Датчика на входе
- Резервированная схема внутри модуля B/B
- Резервированные выходные цепи
- С одним контроллером up to SIL 3
  - HFT = 0; SFF > 99%
  - Согласно IEC 61508-2, таблица 3

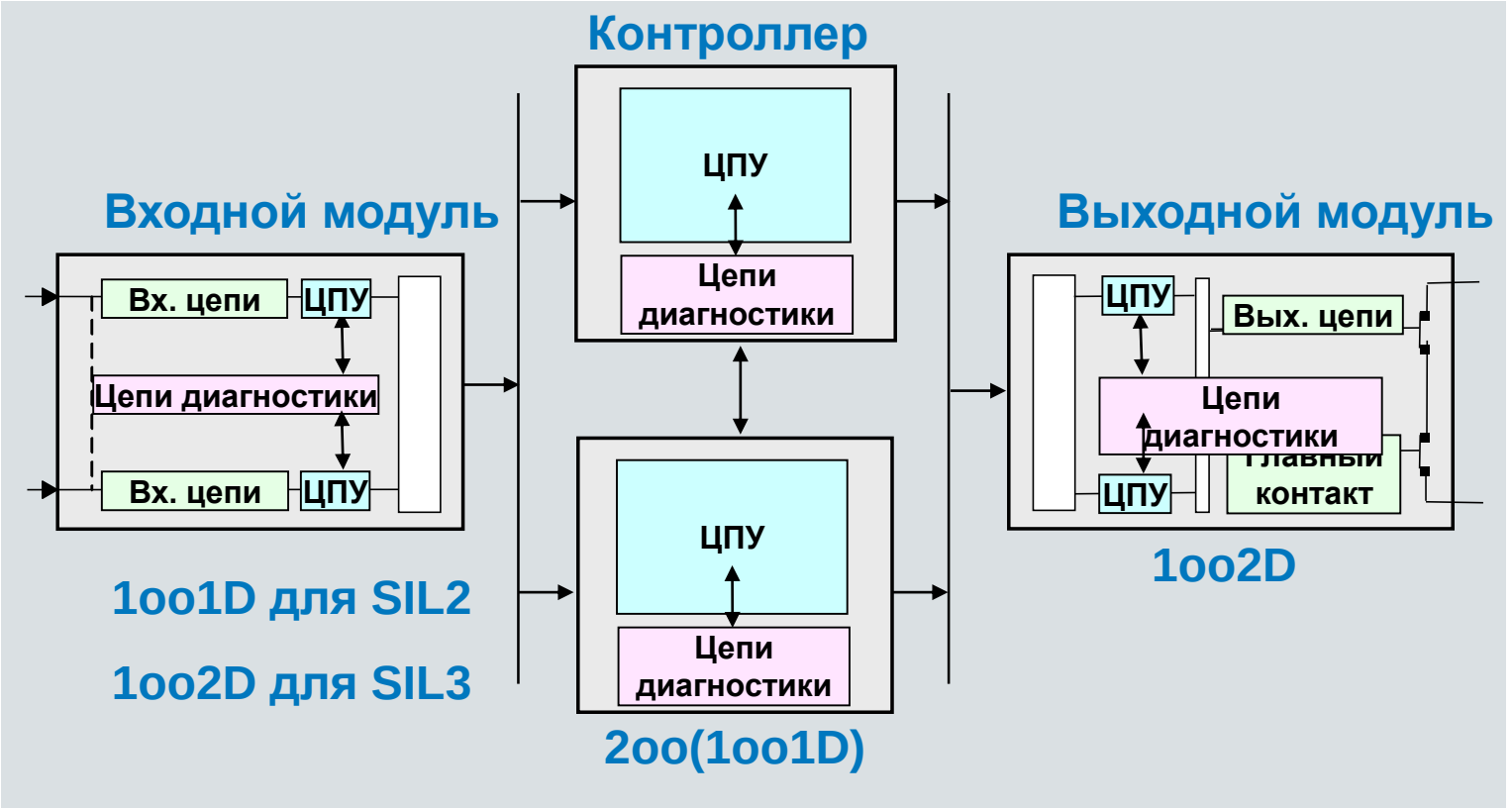


Harware Fault Tolerance (HFT) - отказоустойчивость аппаратных средств
Safe Failure Fraction (SFF) - доля безопасных отказов

SIEMENS

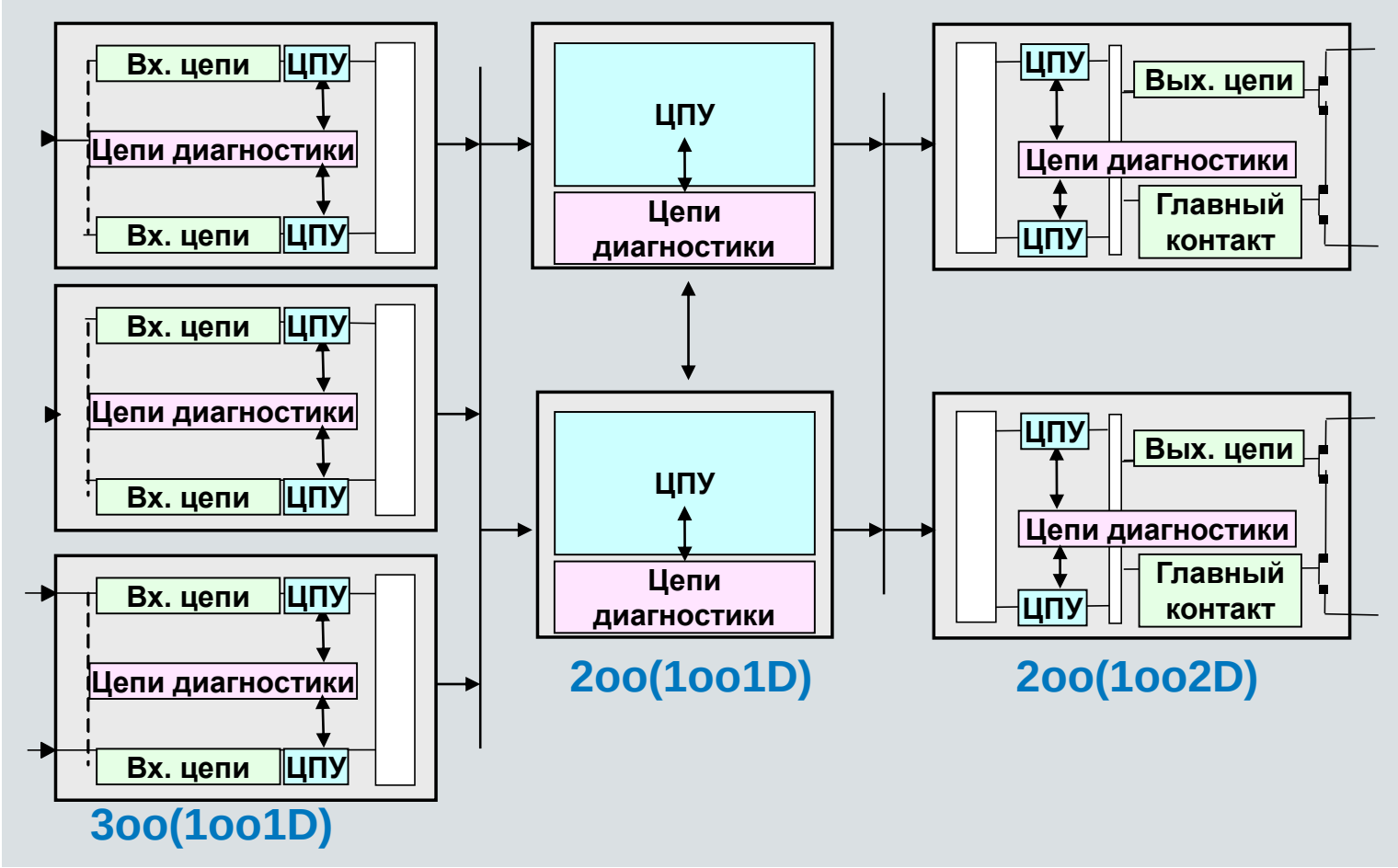
Резервированная система

Структура системы 2oo4,
но доступность выше

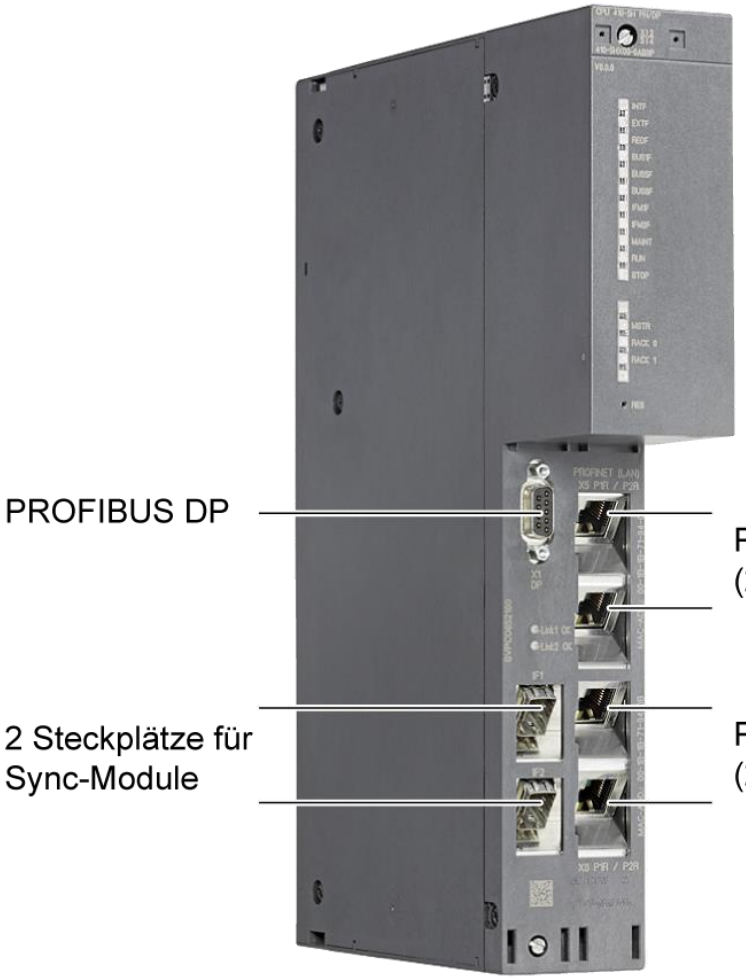


SIEMENS

2oo3 - Голосование



Интегрированная безопасность для автомтизации процессов
Полностью интегрированное решение для обеспечения безопасности



SIL 3

G_PCS7_XX_00376

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

TÜV SÜD

CERTIFICATE

No. Z10 09 07 67803 004

Holder of Certificate: Siemens AG
Industry Sector IA AS
Gleiwitzer Straße 555
90475 Nürnberg
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 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 SN73321C. The report SN73321C and the user documentation in the currently valid revision are mandatory part of this certificate.

Tested according to:
IEC 61508-1:1998; up to SIL 3
IEC 61508-2:2000; up to SIL 3
IEC 61508-3:1998; up to SIL 3
EN 954-1:1997; up to Safety Category 4
ISO 13849-1:2006; up to PL e
EN 60204-1:2006 (to the extent applicable)
IEC 61511:2003
IEC 62061:2005

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.: SN73321 C

Date, 2009-07-20

Page 1 of 1

280497

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

TÜV®

SIEMENS

Контроллер S7-400

CPU type	CPU 410-5H Process Automation	CPU 412-5H PN/DP	CPU 414-5H PN/DP	CPU 416-5H PN DP	CPU 417-5H PN/DP
Component of the AS bundle	AS 410F / AS 410FH	AS 412F / AS 412FH	AS 414F / AS 414FH	AS 416F / AS416 FH	AS 417F / AS 417FH
Technical setup	S7-400 with distributed I/O				
Load memory	integrated 48 MB	integrated 512 KB card up to 64 MB	integrated 512 KB card up to 64 MB	integrated 1 MB card up to 64 MB	integrated 1 MB card up to 64 MB
Main memory	32 MB	1 MB	4 MB	16 MB	32 MB
For program	16 MB	512 KB	2 MB	6 MB	16 MB
For data	16 MB	512 KB	2 MB	10 MB	16 MB
Execution time	7.5 ns	31.25 ns	18.75 ns	12.5 ns	7.5 ns
Prozessobjekte	2600	30	350	1200	2000
Fieldbus interfaces					
MPI/DP	-	32 slaves	32 slaves	32 slaves	32 slaves
DP	96 slaves	64 slaves	96 slaves	125 slaves	125 slaves
PN 1. interface	250 PN/IO devices	256 PN/IO devices	256 PN/IO devices	256 PN/IO devices	256 PN/IO devices
PN 2. interface	250 PN/IO devices	-	-	-	-
Dimensions (W x H x D) in mm	50 x 290 x 219				
MTBF (years)	16.7	23.0	23.0	23.0	23.0
PFD (Proof Test 10 years)	< 1.9E-04	< 1.9E-04	< 1.9E-04	< 1.9E-04	< 1.9E-04
PFD (Proof Test 20 years)	< 3.8E-04	< 3.8E-04	< 3.8E-04	< 3.8E-04	< 3.8E-04

ЦПУ 410-5H

SIEMENS

ET 200M

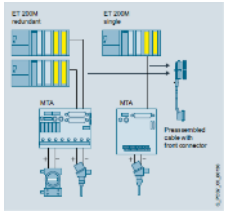
SIL 3

Module type	SM 326 F-DI 24 x DC 24 V	SM 326 F-DI 8 x NAMUR	SM 326 F-DO 8 x DC 24V/2A PM	SM 326 F-DO 10 x DC 24V/2APP	SM 336 F-AI 6 x 0/4 … 20 mA HART
Max. number of inputs/outputs SIL according IEC 61508	24 (1-channel for SIL 2) 12 (2-channel for SIL 3) electrically isolated in groups of 12	8 (1-channel for SIL 2) 4 (2-channel for SIL 3) electrically isolated by channel	10 (intern 2-channel SIL 3) electrically isolated in groups of 5 P/P switching	8 (inter 2-channel SIL 3) electrically isolated in groups of 4 P/M switching	6 (1-channel SIL 3, 1oo1) 3 (2-channel SIL 3, 1oo2) 15 bits + sign 2-wire or 4-wire connection
Input or output current	-	-	2 A per channel with "1" signal	2 A per channel with "1" signal	4 … 20 mA or 0 … 20 mA
Short-circuit-proof sensor supply	4 for 6 channels electrically isolated in groups of 2	8 for 8 channels individually isolated	-	-	6 for 6 channels
Special features	Support of time stamping (SOE) 20 ms resolution	Connection sensors from hazardous areas	"Keep last valid value" parameter, channel-selective passivation	-	HART communication in measuring range 4 … 20 mA
Redundancy	Channel-selective	Channel-selective	Channel-selective	-	Channel-selective
Module and channel diagnostics	●	●	●	●	●
PROFIBUS	●	●	●	●	●
PROFINET	●	-	●	●	●
Dimension (W x H x D in mm)	80 x 125 x 120	80 x 125 x 120	40 x 125 x 120	80 x 125 x 120	40 x 125 x 120
MTBF (years)	22.8	33.8	31.2	28.7	26.5
PFD (Proof Test 20 years)	< 1.0E-05	< 1.0E-05	< 1.0E-05	< 1.0E-05	< 1.0E-05
PFD PROFIsafe communication	< 1.0E-05, once in the evaluation for input and output				

SIEMENS

ET 200M MTA

Terminal module MTA	F-AI HART	F-DI	F-DO	F-DO relays	F-DO relays
Max. number of inputs/outputs SIL according IEC 61508	6 channels 4 … 20 mA (with/without HART 0 … 20 mA (without HART)	24 channels F-DI 24 V DC	10 channels F-DO 24 V DC, 2 A	10 channels F-DO 120 … 230 V AC, 5 A	10 channels F-DO 24 V DC, 5A
ET 200M module	6ES7336-4GE00-0AB0	6ES7326-1BK02-0AB0	6ES7326-2BF10-0AB0	6ES7326-2BF10-0AB0	6ES7326-2BF10-0AB0
I/O Redundancy	●	●	●	●	●
MTBF (years)	92.0	74.0	159.0	130.0	130.0
PFD (Proof Test 10 years)	-	-	-	-	-
PFD (Proof Test 10 years) single channel	3.72E-05	-	-	2.50E-03	1.26E-02
PFD (Proof Test 20 years)	5.00E-04	-	-	5.00E-02	2.50E-01
PFD (Proof Test 20 years) single channel	8.34E-05	-	-	5.10E-03	2.52E-02

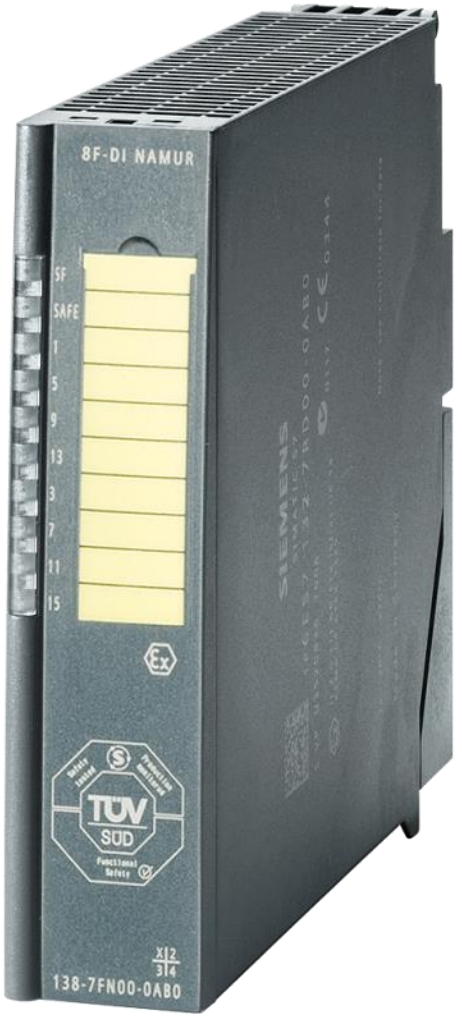


SIEMENS

ET 200iSP с PROFIBUS подключением

SIL 3

Module type	EM 138 F-DI 8 x Namur	EM 138 F-DO 4 x DC 17.4V/40 mA	EM 138 F-AI 4 x Ex HART
Max. number of inputs/outputs SIL according IEC 61508	8 (1-channel SIL 3) or 4 (2-channel SIL 3)	4 (1-channel for SIL 3) P/P switching	4 (1-channel SIL 3) 4 (2-channel, 2 modules, 1oo2 SIL 3) 15 Bit + sign 2-wire or 4-wire connection
Input or output current	-	40 mA per channel 80 mA with parallel connection	4 … 20 mA (with/without HART) or 0 … 20 mA (without HART)
Short-circuit-proof sensor supply	8 for 8 channels individually isolated		4 for 4 channels individually isolated
Special features	Connection sensors from hazardous areas	Connection sensors from hazardous areas	Connection sensors from hazardous areas HART communication
PROFIBUS	●	●	●
PROFINET	-	-	-
Dimension (W x H x D in mm)	30 x 129 x 136.5	30 x 129 x 136.5	30 x 129 x 136.5
MTBF (years)	41.6	52.4	33.9
PFD (Proof Test 20 years)	< 1.0E-05	< 1.0E-05	< 1.0E-04 (1oo1) < 1.0E-05 (1oo2, 2 modules)
PFD PROFIsafe communication	< 1.0E-05, once in the evaluation for input and output		



SIEMENS

Штампы времени

- Точность 30 мс с F-Модулями
- Точность 1 мс со стандартными модулями

Distributed I/O device	Module	Order No.	Used as
ET 200M	SM 321	6ES7 321-7BH01-0AB0 Precision of 1 ms	Module for acquisition of process signals: 16 electrically isolated inputs (24 V DC) and diagnostic messages, redundant signal acquisition possible
ET 200M	SM 321	6ES7 321-7EH00-0AB0 Precision of 1 ms	Module for acquisition of process signals: 16 electrically isolated inputs (24-125 V DC) and diagnostic messages, redundant signal acquisition possible

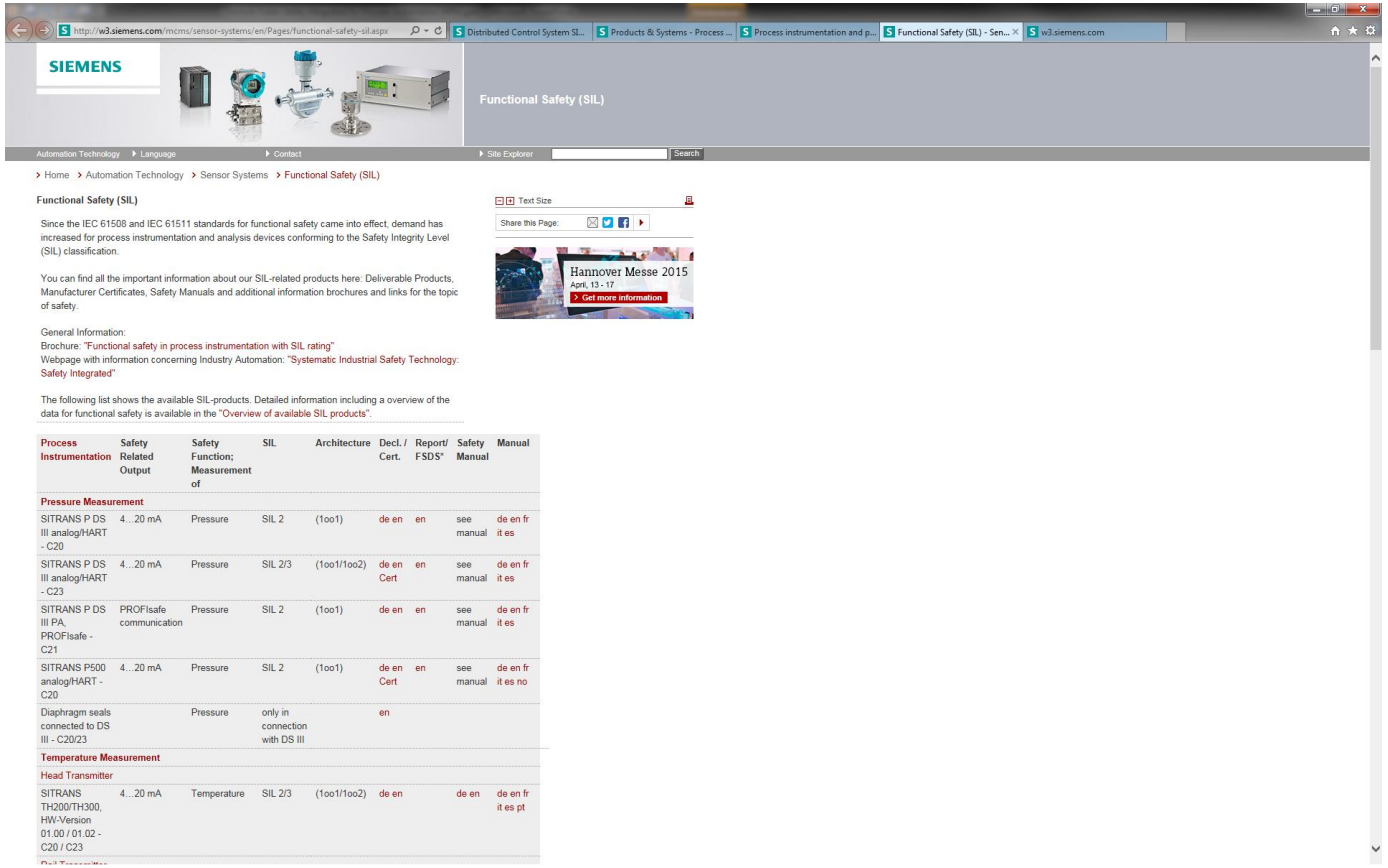
Distributed I/O device	Module	Order No.	Used as
ET 200M	SM 321	6ES7 321-7RD00-0AB0 Precision of 10 ms	Module for acquisition of process signals: 4 inputs (NAMUR), suitable for hazardous areas, redundant signal acquisition possible
ET 200M	SM 321	6ES7 321-7TH00-0AB0 Precision of 10 ms	Module for acquisition of process signals: 16 inputs (NAMUR), redundant signal acquisition possible
ET 200M	SM 326	6ES7 326-1BK02-0AB0 Precision of 20 to 30 ms	Module for acquisition of process signals: • 24 inputs when used – with interface module 6ES7 153-2BAx2 and configuration with F-ConfigurationPack V5.5 SP3 or higher – with interface module 6ES7 153-2BA70-0XB0 and configuration with F-ConfigurationPack V5.5 SP3 or higher • 12 inputs (CH 00 to CH 11) for use with interface module 6ES7 153-2BA01 • redundant signal acquisition and fail-safe signal acquisition possible
ET 200iSP	SM 131	6ES7 131-7RF00-0AB0 Precision of 20 ms	Module for acquisition of process signals: 8 inputs (NAMUR)

Интегрированная безопасность для Автоматизации непрерывных процессов
Полностью интегрированное решение для обеспечения безопасности

SIEMENS

Отказоустойчивые полевые приборы

http://w3.siemens.com/mcms/Датчик-systems/en/Pages/functional-safety-sil.aspx



Интегрированная безопасность для Автоматизации непрерывных процессов

Общая платформа ПЛК для управления процессом и безопасности

- Единое аппаратное решения для всех задач

Одна система инжиниринга систем управления процессом и приложениями безопасности процесса

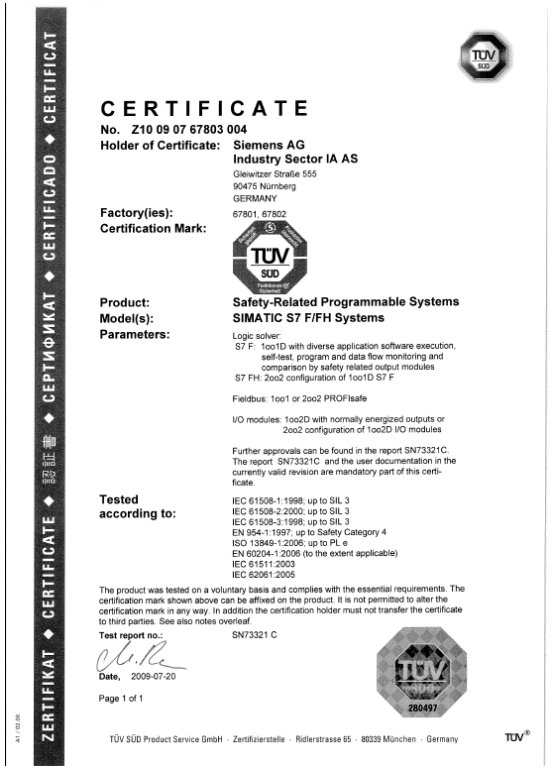
- Меньше обучений и больше использования наработок

Дружественное отображение информации безопасности процесса в PCS 7

Автоматическая интеграция диагностики безопасности процесса в интерфейс оператора

Прямая коммуникация между РСУ и ПАЗ

- Меньше инжиниринга



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

TÜV SÜD

CERTIFICATE

No. Z10 09 07 67803 004

Holder of Certificate: Siemens AG
Industry Sector IA AS
Gleiwitzer Straße 555
90475 Nürnberg
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 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 SN73321C. The report SN73321C and the user documentation in the currently valid revision are mandatory part of this certificate.

Tested according to:
IEC 61508-1:1998; up to SIL 3
IEC 61508-2:2000; up to SIL 3
IEC 61508-3:1998; up to SIL 3
EN 954-1:1997; up to Safety Category 4
ISO 13849-1:2006; up to PL e
EN 60204-1:2006 (to the extent applicable)
IEC 61511:2003
IEC 62061:2005

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.: SN73321 C

Date, 2009-07-20

Page 1 of 1

280497

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

TÜV®

SIEMENS

SIMATIC S7-400FH с S7 F System

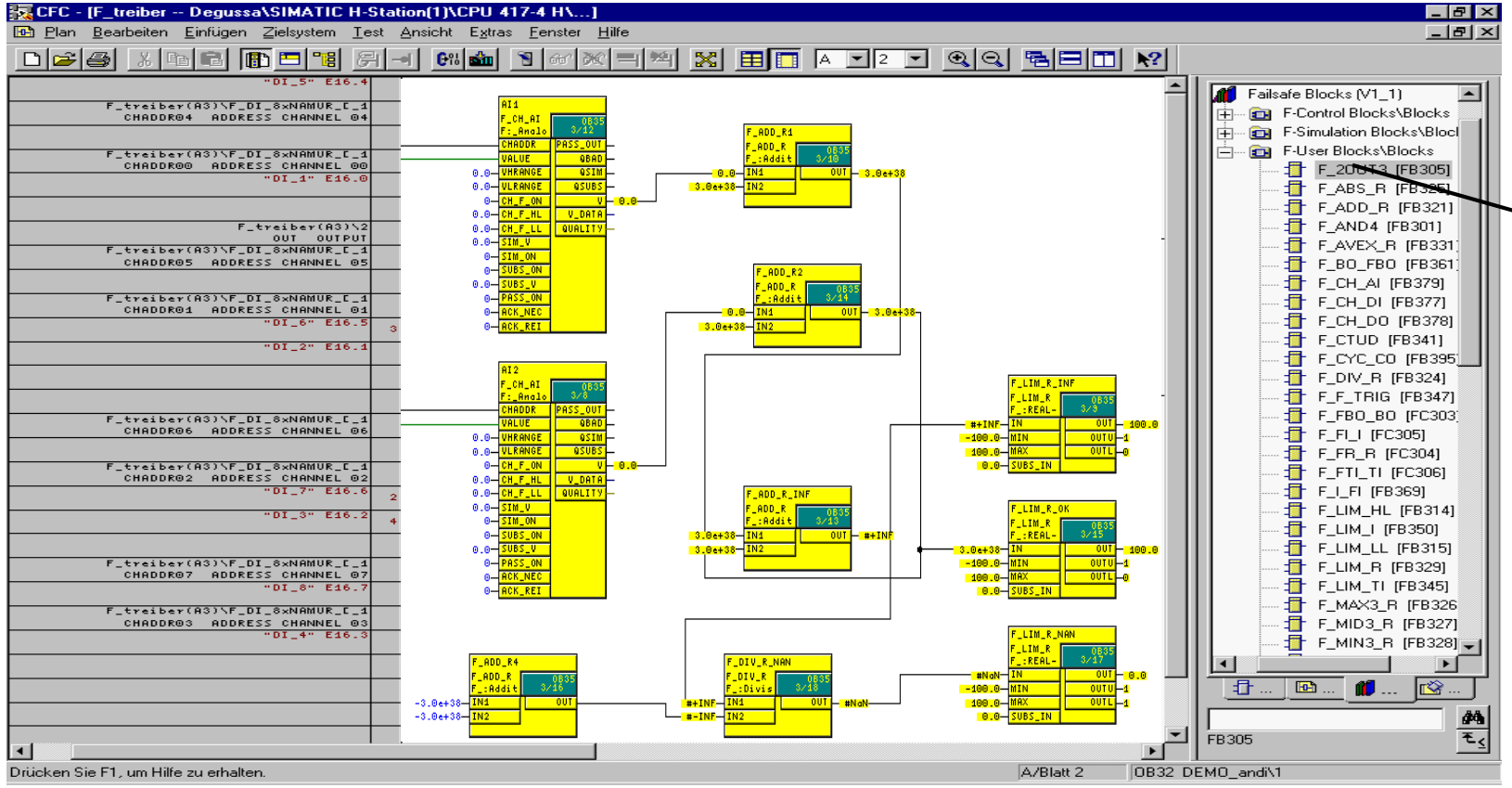
Используется для конфигурации аппаратуры и приложений безопасности согласно IEC 61511

- Опциональный пакет к STEP 7 для конфигурирования S7-400H контроллера с функциональной безопасностью
- Упрощает документацию по программам безопасности, напр. администрированием подписей

➔ **Конфигурирование программ безопасности можно выполнить в CFC или с помощью Safety Matrix**

F программа пользователя
CFC

Генерация F программы пользователя в CFC выбором и соединением блоков F-Библиотеки

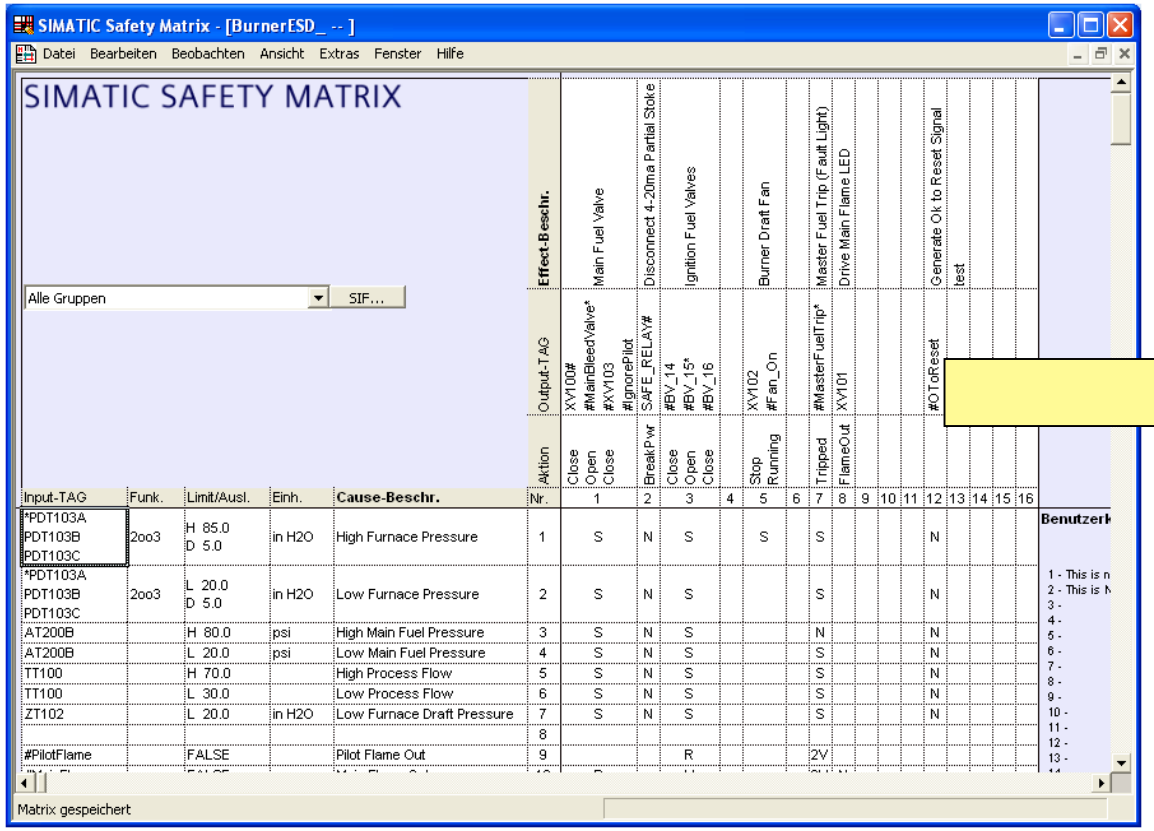


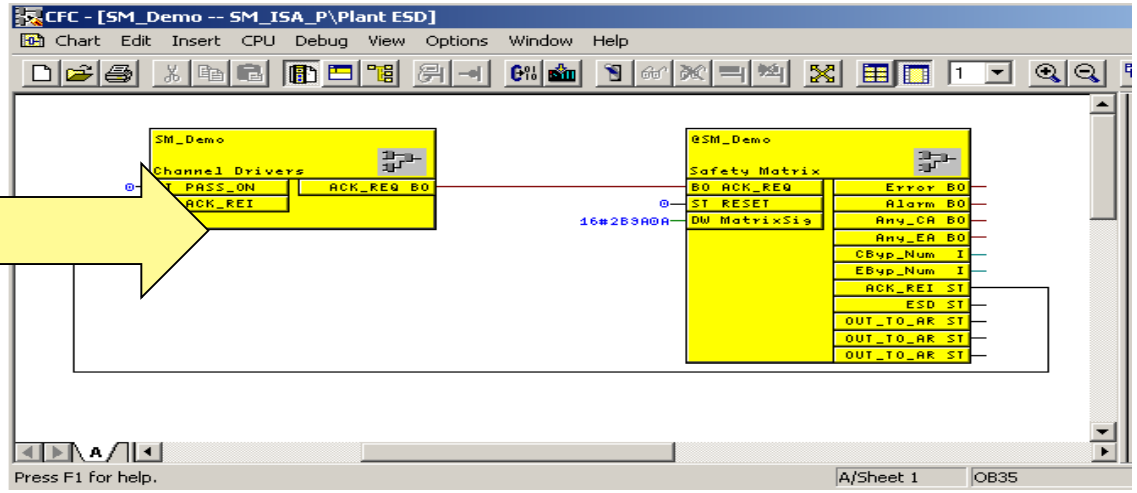
Библиотека F блоков, сертифицированных TÜV

F Программа пользователя
Safety Matrix

SIEMENS

Метод Причин и Эффектов с автоматической генерацией CFC и предупреждений (TÜV-сертифицирован)





SIEMENS

Интегрированное полевое оборудование

Безопасность процесса для Автоматизации непрерывных процессов

Интегрированная безопасность с PROFIsafe

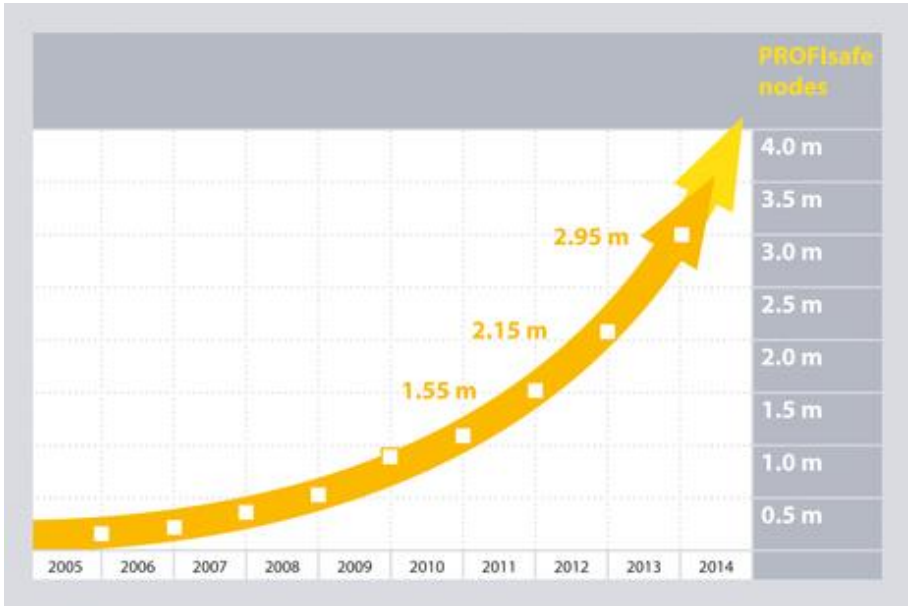
PROFIsafe это профиль уровня приложений, который описывает коммуникацию между отказоустойчивыми устройствами

Опубликован в 1999; текущая версия (V2.61) опубликована в Августе 2014

Поддержка безопасной коммуникации по открытым стандартным шинам PROFIBUS (DP, PA) и PROFINET

TUV сертифицирован
- IEC 61508 SIL 3
- EN 954-1 Cat 4

2.95 Миллионов узлов



PROFIsafe
OSI Модель

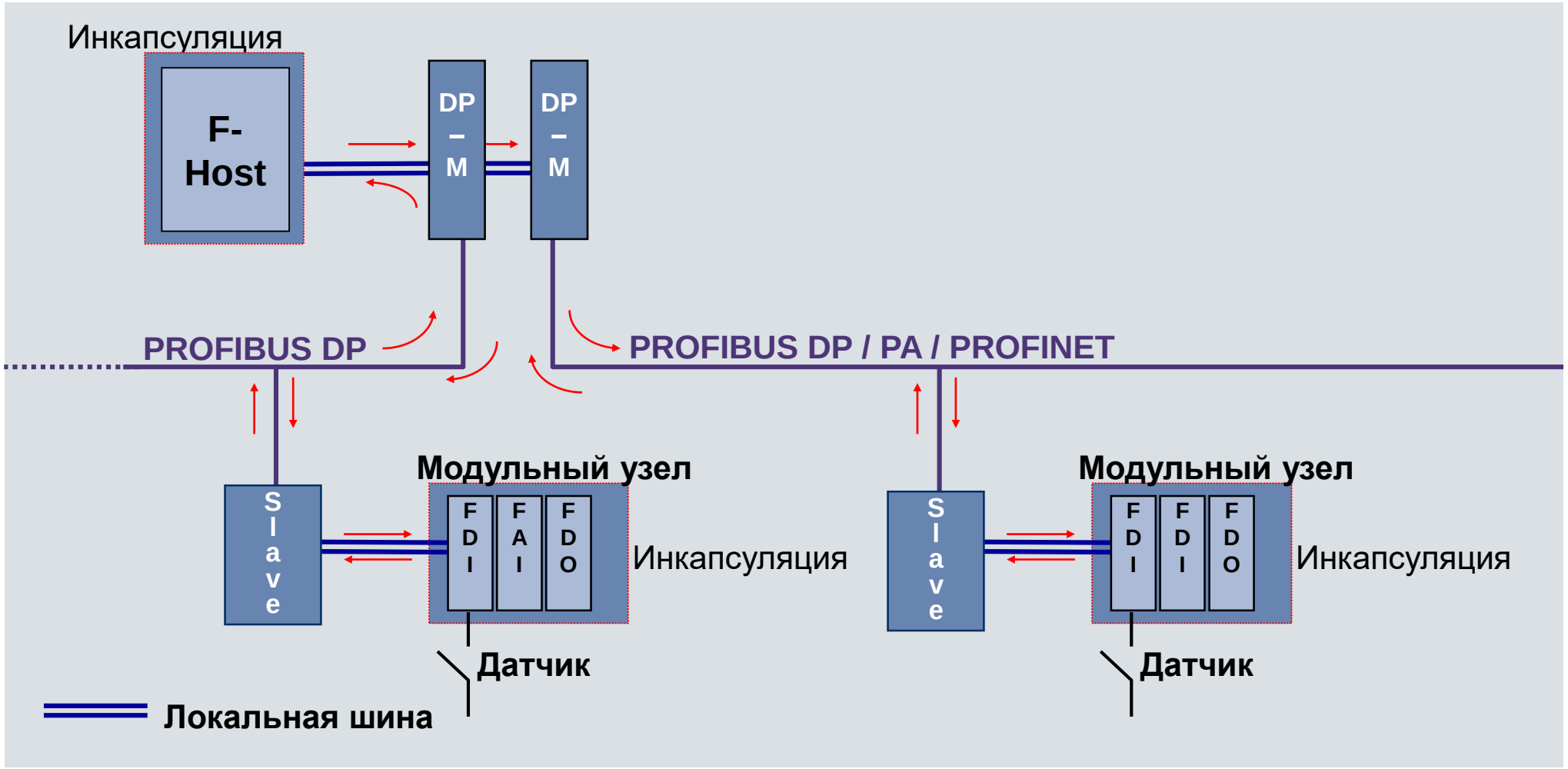
“Черный канал": ASIC, связь, кабели, проч. не относящееся к безопасности

Критические функции не связанные с безопасностью, напр. диагностика

"**PROFIsafe**": Компоненты систем критической коммуникации безопасности : адресация, watchdog таймеры, последовательности, подпись, проч.

Связанные с безопасностью но не часть Profisafe профиля: Безопасный В/В и системы безопасности

PROFIsafe
Линии коммуникации



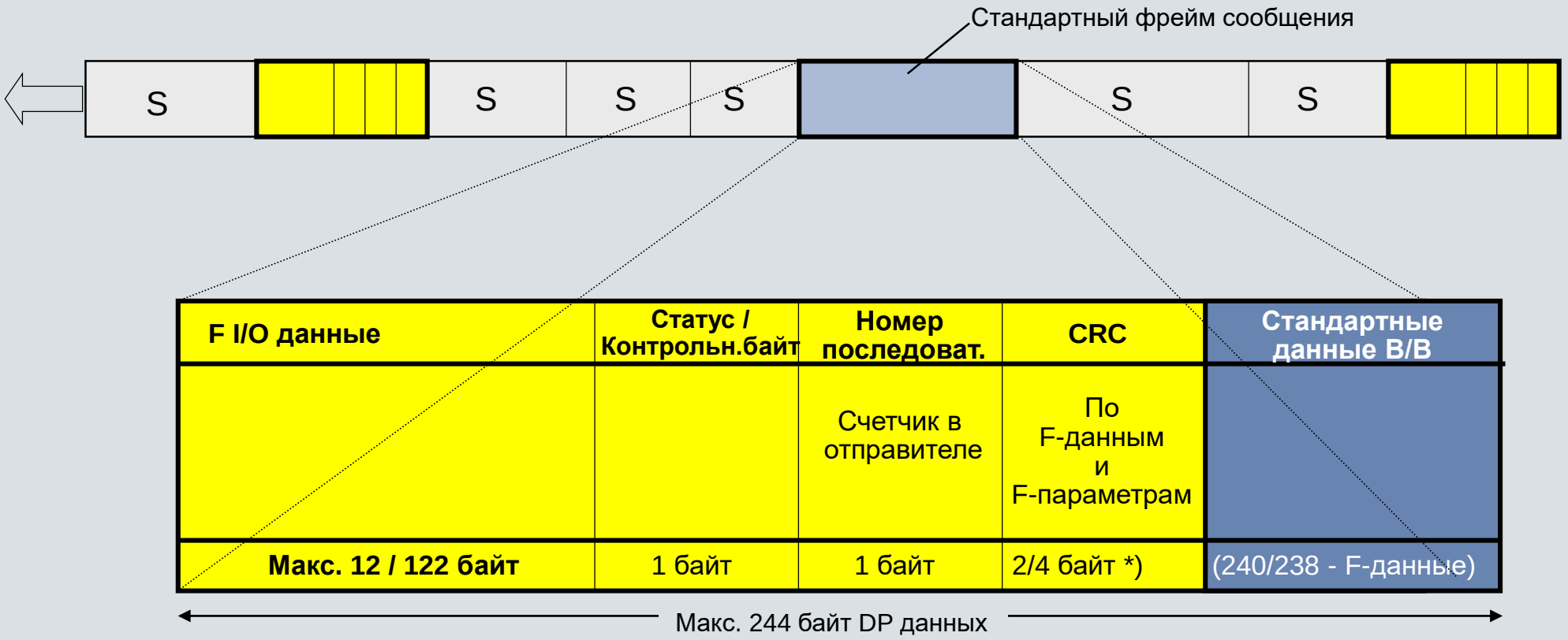
PROFIsafe
Средства выявления ошибок

SIEMENS

Ошибка \ Средство	Номер в последовательности	Ожидание времени с подтверждением	Идентификатор для отправителя и получателя	Рез. Копирование данных CRC
Повтор	X			
Потеря	X	X		
Вставка	X	X	X	
Неправильная последовательность	X			
Повреждение данных				X
Задержка		X		
Связывание безопасных и стандартных сообщений (маскарад)		X	X	X
Ошибка FIFO		X		

Меры должны быть реализованы и контролироваться во всех станциях

PROFIsafe
Протокол



*) 2 байт для макс. 12 байт F I/O данных
4 байт для макс. 122 байт F I/O данных

Шина интегрированной безопасности

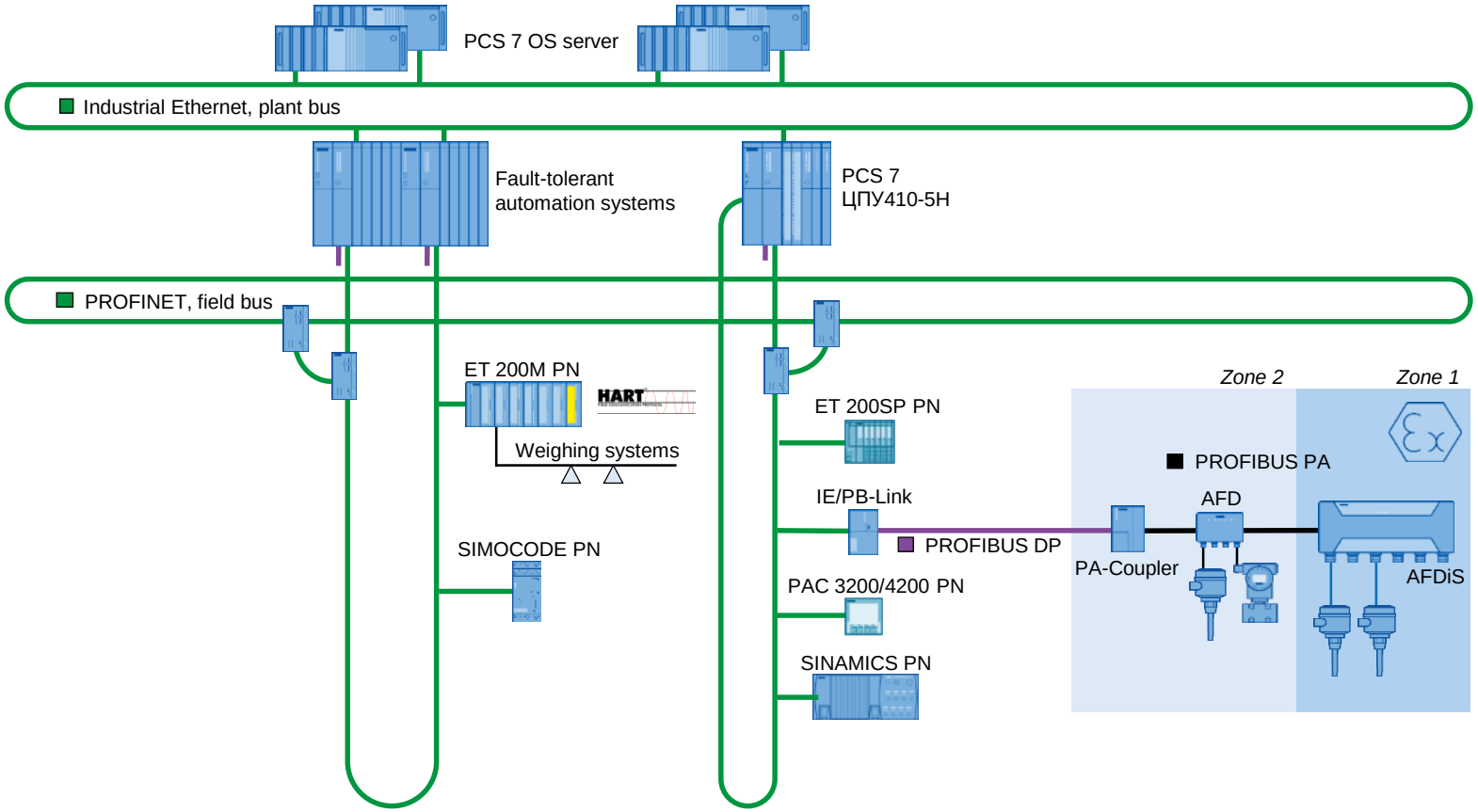
PROFIBUS

- Проверенное решение полевой шины
- Открытый стандарт
- Первая полевая шина с безопасным полевым оборудованием

PROFIsafe по PROFIBUS DP / PA и PROFINET

- FMR (**Гибкое модульное резервирование**), высокая гибкость выбора уровней резервирования и доступности
- Один кабель PROFIBUS для стандартной и безопасной коммуникации PROFIsafe
- Быстрая настройка и ввод в эксплуатацию, благодаря PROFIBUS
- Безопасность от Контроллера через уровень B/B до полевого уровня

PROFINET in SIMATIC PCS 7 и Безопасность процесса



- Два PROFINET IO интерфейса на ЦПУ410-5H включают PROFIsafe
- ET 200M PN с PROFIsafe коммуникация для F-DI, F-DO и F-AI
- Полная интеграция SIMOCODE
- Безопасная коммуникация между контроллерами AS 400

SIEMENS

FMR - Гибкое модульное резервирование

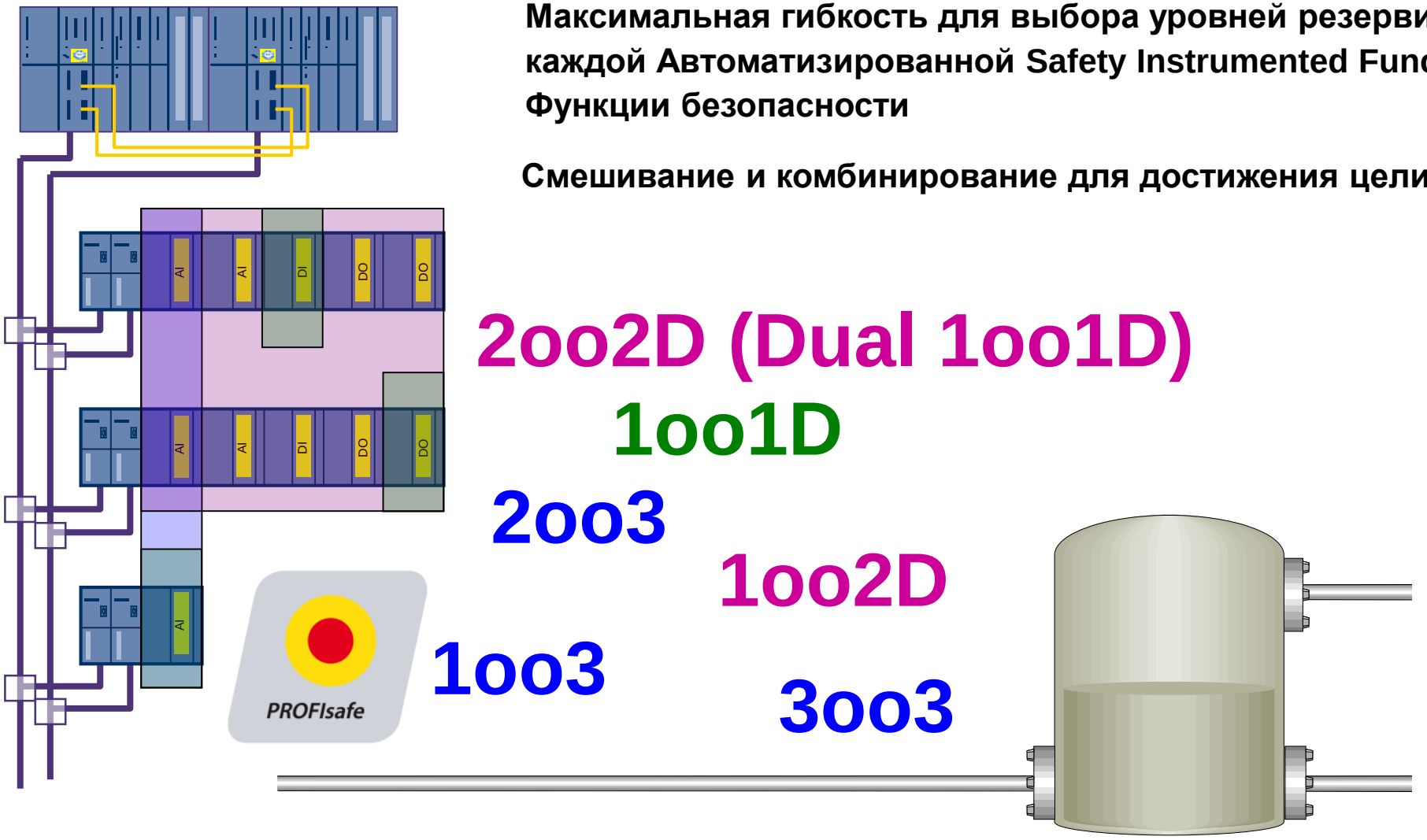
Безопасность процесса для Автоматизации непрерывных процессов

Flexible Modular Redundancy (FMR) - Гибкое модульное резервирование на базе PROFIBUS DP

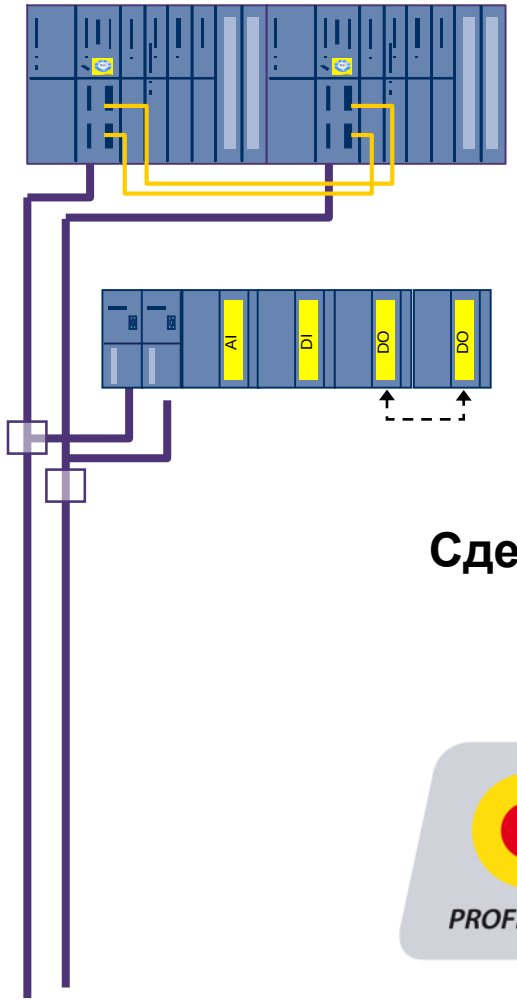
SIEMENS

Максимальная гибкость для выбора уровней резервирования для каждой Автоматизированной Safety Instrumented Function (SIF) – Функции безопасности

Смешивание и комбинирование для достижения цели



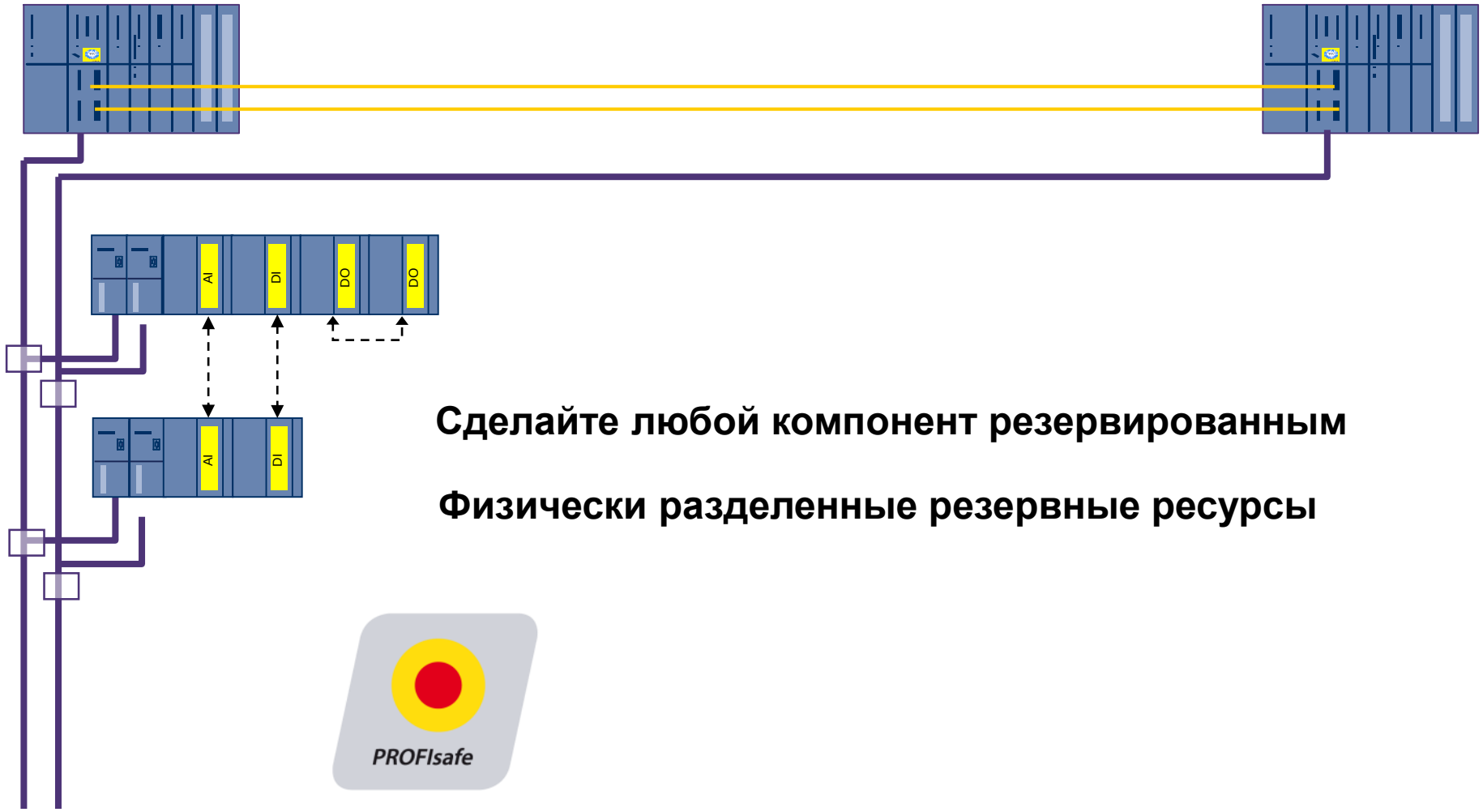
Flexible Modular Redundancy (FMR) - Гибкое модульное резервирование на базе PROFIBUS DP



Сделайте любой компонент резервированным

PROFIsafe

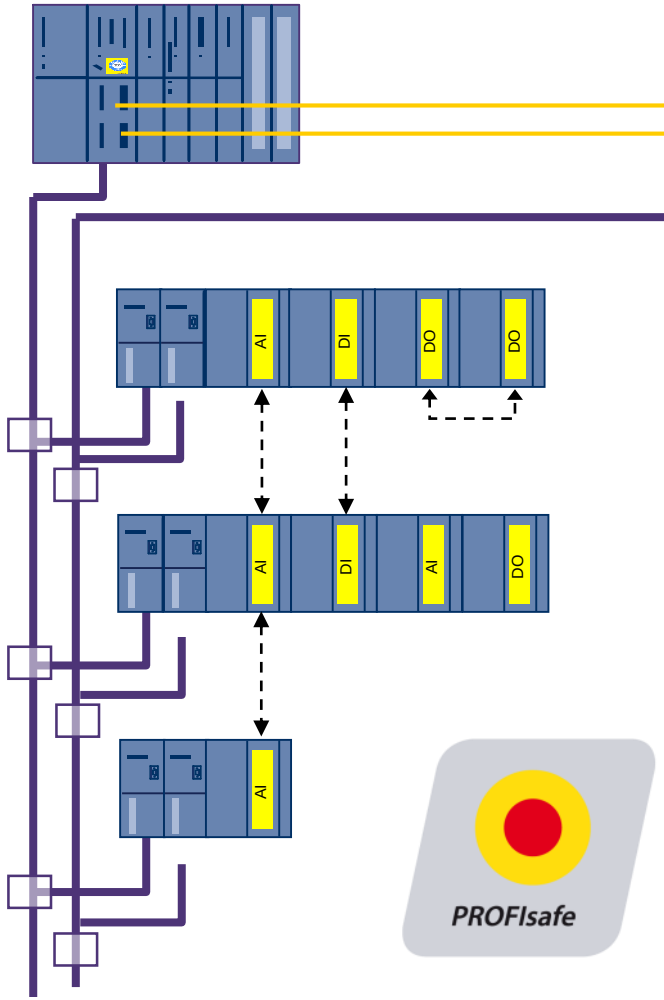
Flexible Modular Redundancy (FMR) - Гибкое модульное резервирование
На базе PROFIBUS DP



Сделайте любой компонент резервированным

Физически разделенные резервные ресурсы

Flexible Modular Redundancy (FMR) - Гибкое модульное резервирование based on PROFIBUS DP

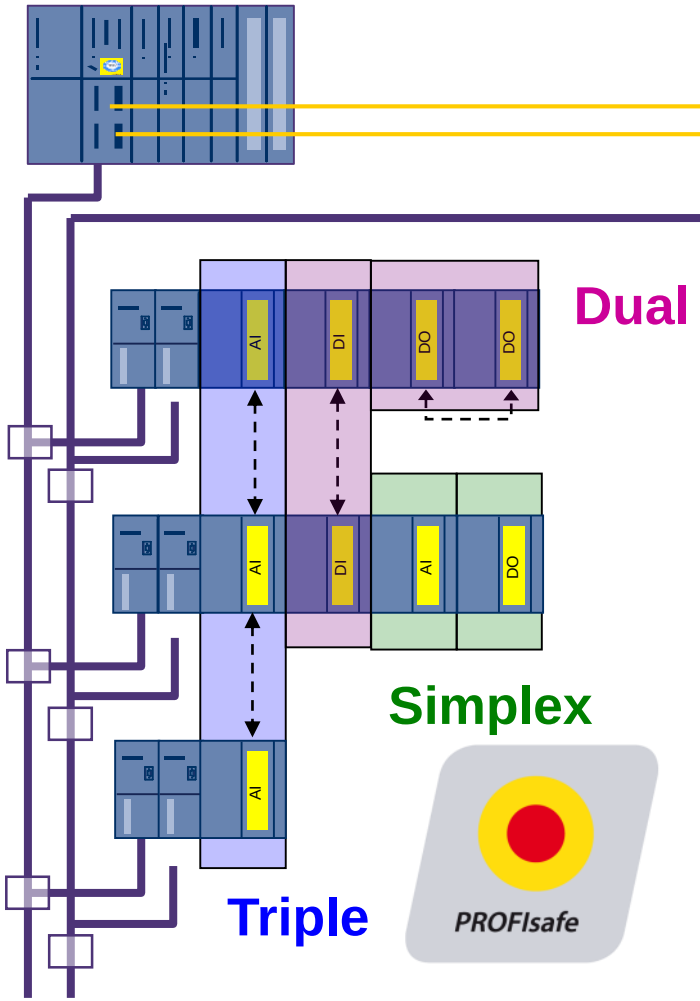


Сделайте любой компонент резервированным

Физически разделенные резервные ресурсы

Смешивание и комбинирование резервирования

Flexible Modular Redundancy (FMR) - Гибкое модульное резервирование based on PROFIBUS DP

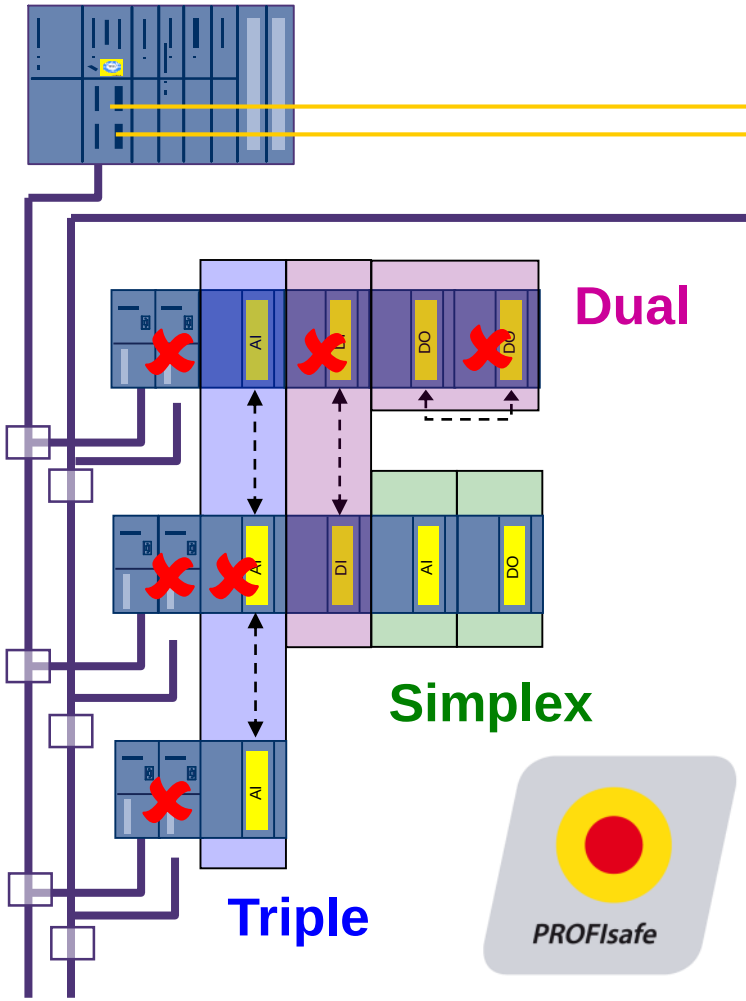


Сделайте любой компонент резервированным

Физически разделенные резервные ресурсы

Смешивание и комбинирование резервирования

Flexible Modular Redundancy (FMR) - Гибкое модульное резервирование based on PROFIBUS DP



Сделайте любой компонент резервированным

Физически разделенные резервные ресурсы

Смешивание и комбинирование резервирования

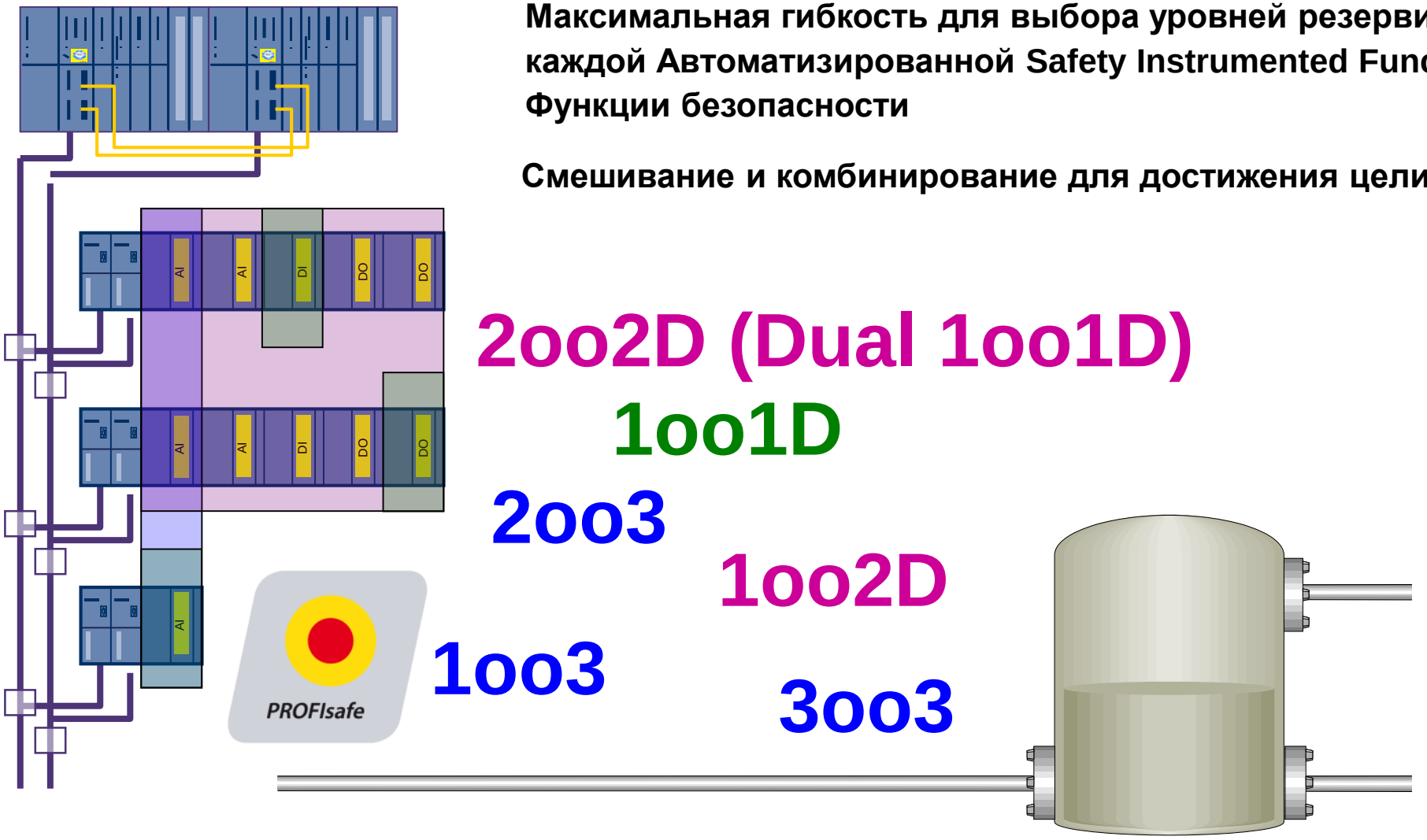
Несколько неисправностей на влияют на безопасность

Flexible Modular Redundancy (FMR) - Гибкое модульное резервирование based on PROFIBUS DP

SIEMENS

Максимальная гибкость для выбора уровней резервирования для каждой Автоматизированной Safety Instrumented Function (SIF) – Функции безопасности

Смешивание и комбинирование для достижения цели



Flexible Modular Redundancy (FMR) - Гибкое модульное резервирование

Safety Integrity Level вплоть до SIL 3 с одним контроллером

- **Наивысший Safety Integrity Level**

Наивысшая гибкость

- **Разделение или комбинация безопасного и стандартного приложения в одном ЦПУ**
- **Использование резервирования для безопасности только там где необходимо**
- **Параллельное использование PROFIsafe по PROFIBUS или PROFINET**

Наивысшая доступность с множественной отказоустойчивостью

- **Архитектура позволяет системе пережить несколько отказов**
- **Резервирование B/B не завить от резервирования ЦПУ**
- **Резервирование B/B и устройств можно сопоставить для максимизации доступности**

Снижение затрат

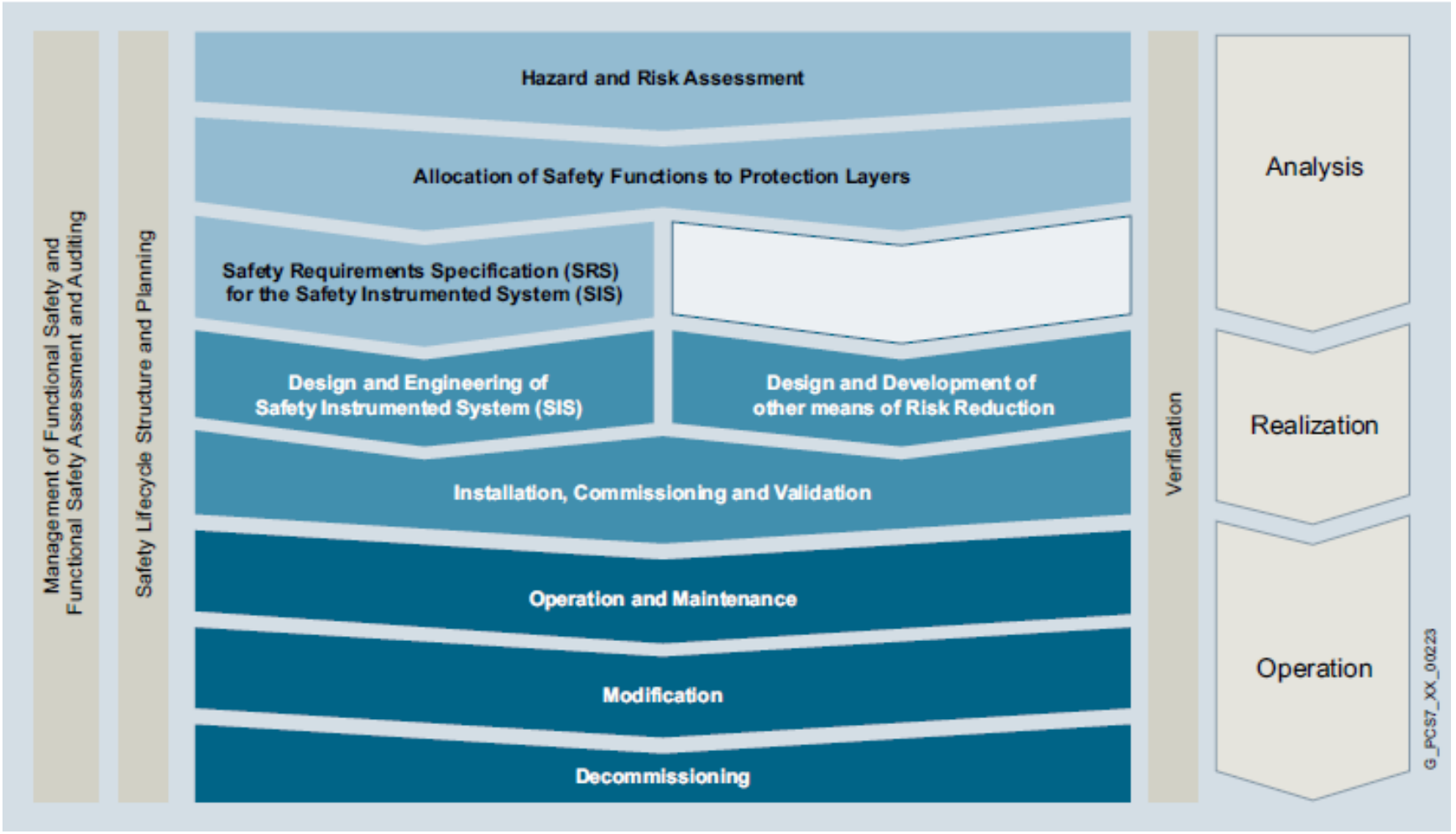
- **Резервирование только там где необходима высокая доступность**
- **параллельное применение PROFIsafe по PROFIBUS или PROFINET**

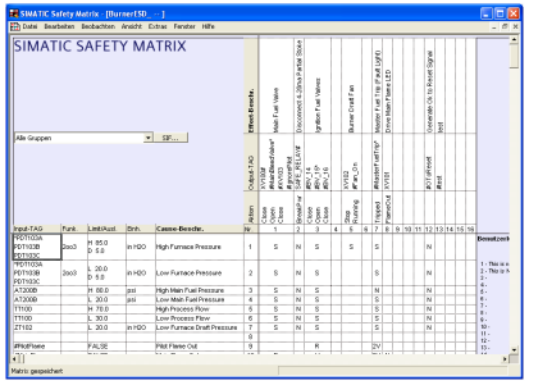
SIEMENS

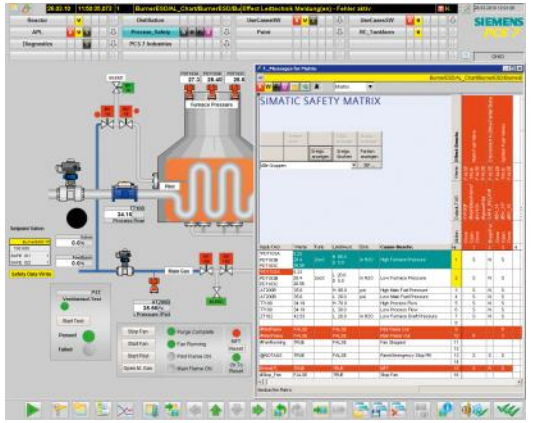
Управление жизненным циклом безопасности

Безопасность процесса для Автоматизации непрерывных процессов

IEC 61511(ISA S84) жизненный цикл безопаности



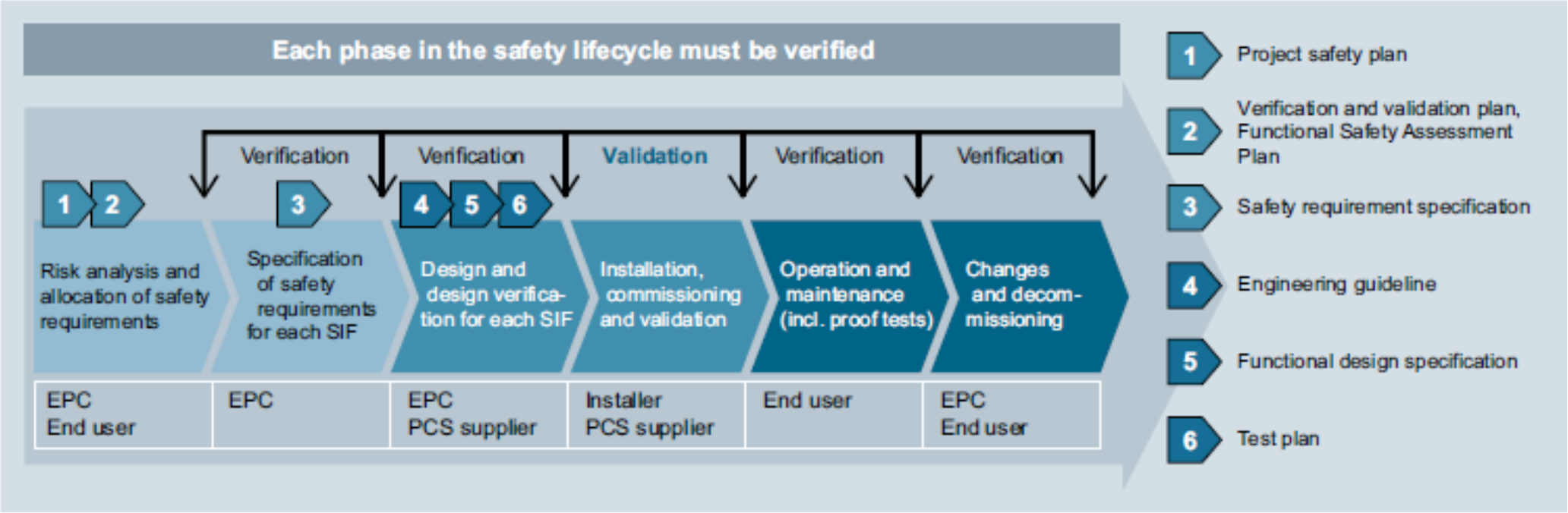




Шаги жизненного цикла безопасности
Управление функциональной безопасностью согласно IEC 61511

SIEMENS

Siemens может Вам помочь



Посмотрите наше предложение
www.siemens.com/processsafety

Управление функциональной безопасностью

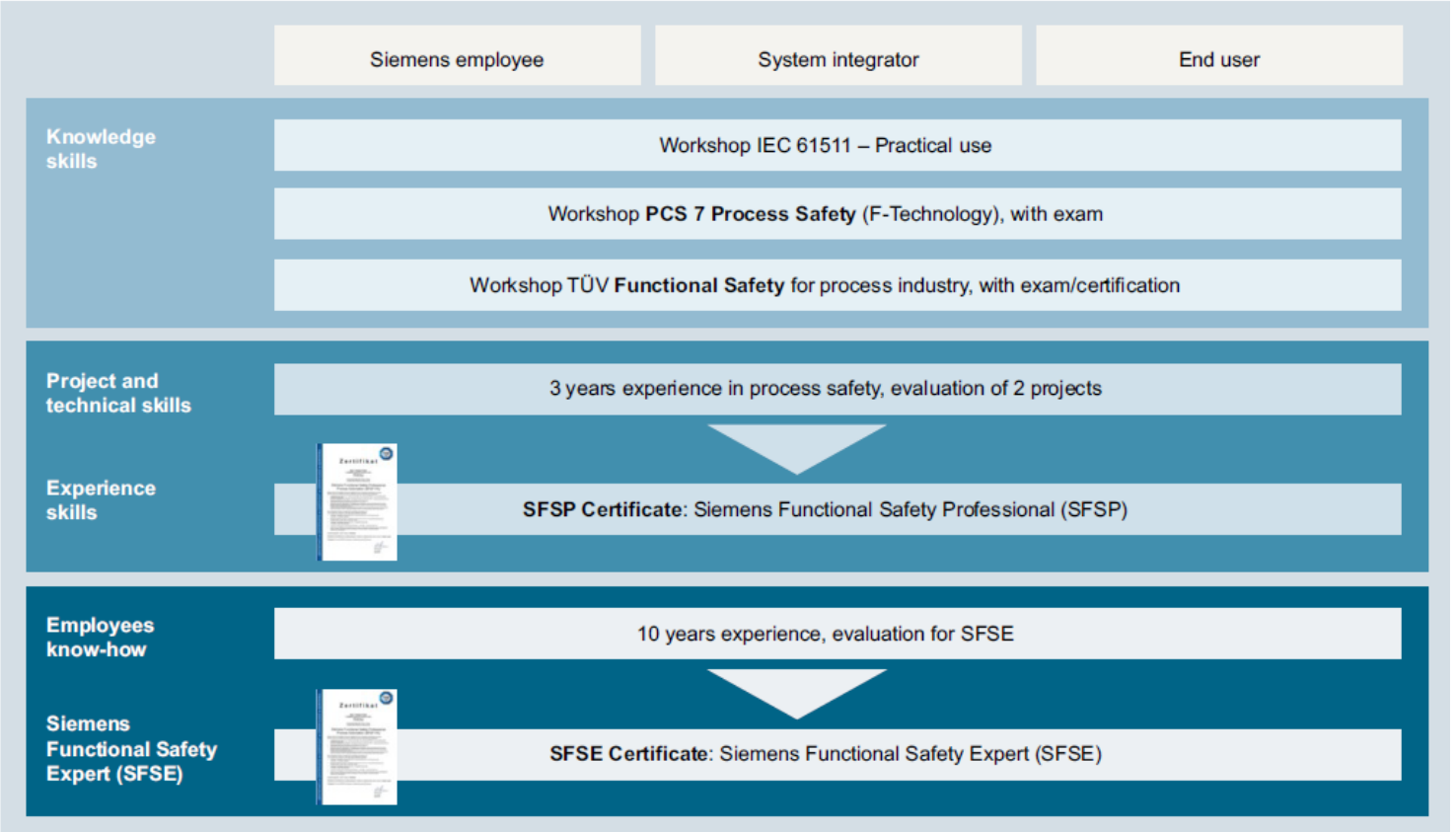
Требуются знания в Безопасности процессов

Обучение по функциональной безопасности Siemens
Информация по курсам SITRAIN
www.sitrain.com

Коды:
ST-WSFSP
ST-WSPUP
ST-PCS7SAF

Станьте Siemens Functional Safety Professional (SFSP)

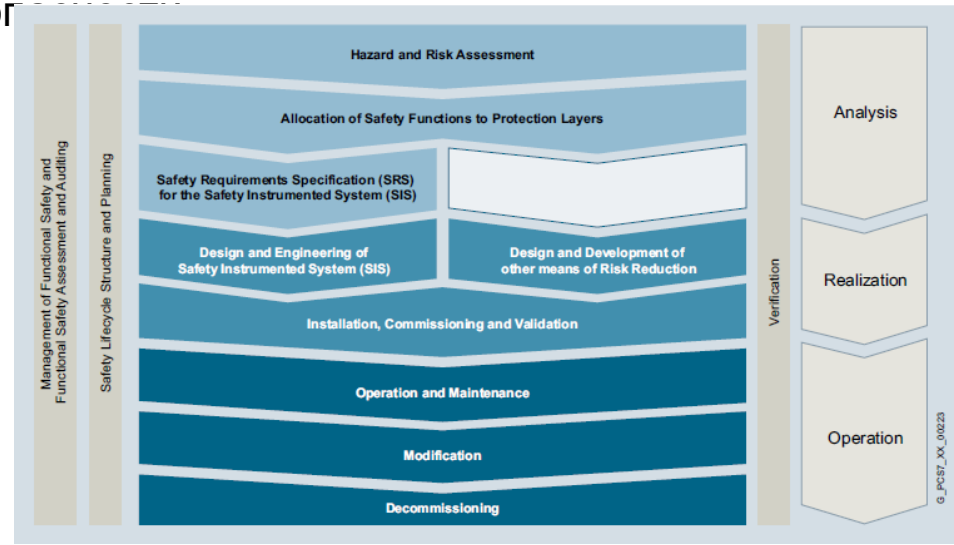
SFSP



IEC 61511(ISA S84) Жизненный цикл безопасности

Разные фазы жизненного цикла безопасности

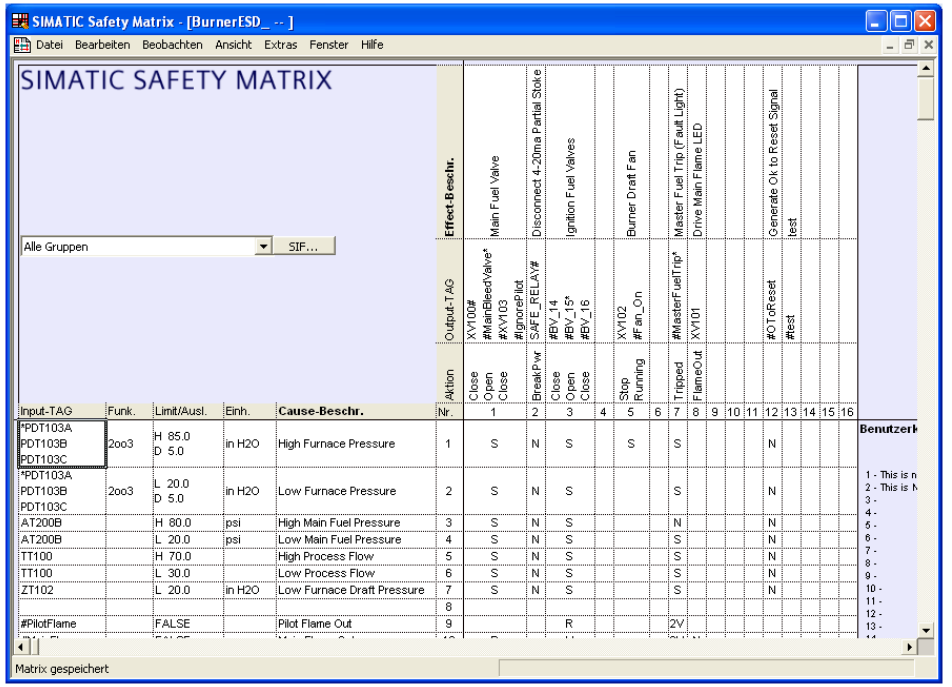
- **Фаза анализа**
  - Идентификация угроз и рисков
  - Разработка Спецификаций требований безопасности для Автоматизированной системы безопасности
  - Распределение функций безопасности на уровни защиты
- **Фаза реализации**
  - Разработка и Инжиниринг Автоматизированная система безоп
  - Дизайн и Разработка других Средства снижения риска
  - Монтаж, Пуско-наладка и Аттестация
- **Фаза эксплуатации**
  - Эксплуатация и техническое обслуживание
  - Внесение изменений
  - Демонтаж



Фаза анализа с Safety Matrix

Фаза анализа

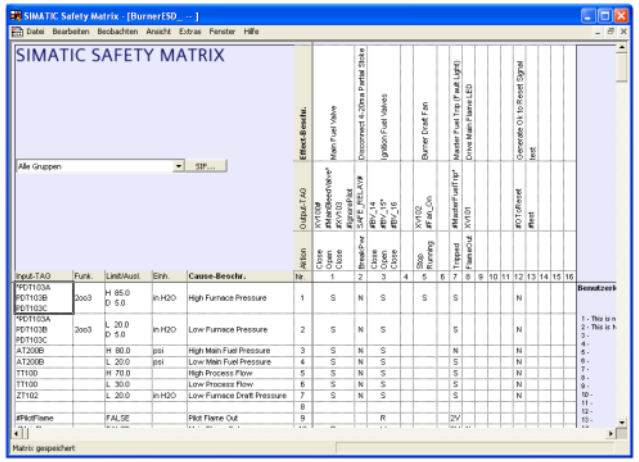
- SIMATIC Safety Matrix как инструмент инжиниринга или редактор
- Разработка Safety Requirement Specification (SRS) - Спецификация требований безопасности для Автоматизированной системы безопасности
- SIMATIC Safety Matrix Editor как инструмент для документировани функций безопасности для SRS (Спецификации требований безоп
- Простое описание Причин и Эффектов
- Простое понимание для всех вовлеченных специалистов

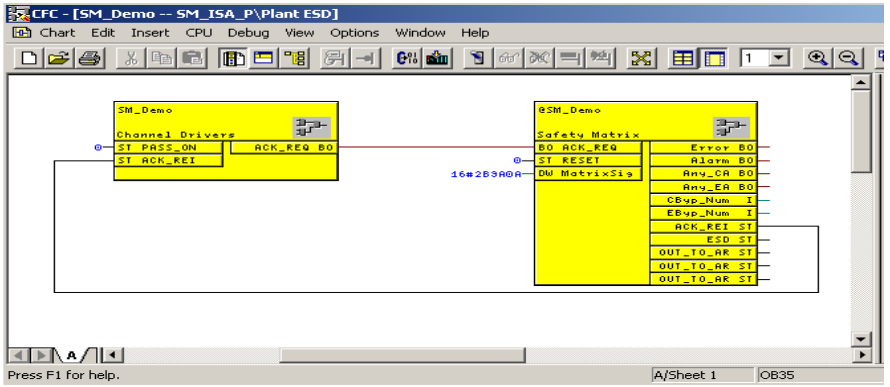


Фаза реализации с Safety Matrix

Фаза реализации

- SIMATIC Safety Matrix как инструмент инжиниринга
- Конфигурация Функций безопасности методом Причин и Эффектов
- Автоматическое создание безопасной логики, сертифицированной TÜV прямо из матрицы Причин и Эффектов
- Простое конфигурирование без специальных навыков программирования





Фаза эксплуатации с Safety Matrix

Фаза эксплуатация

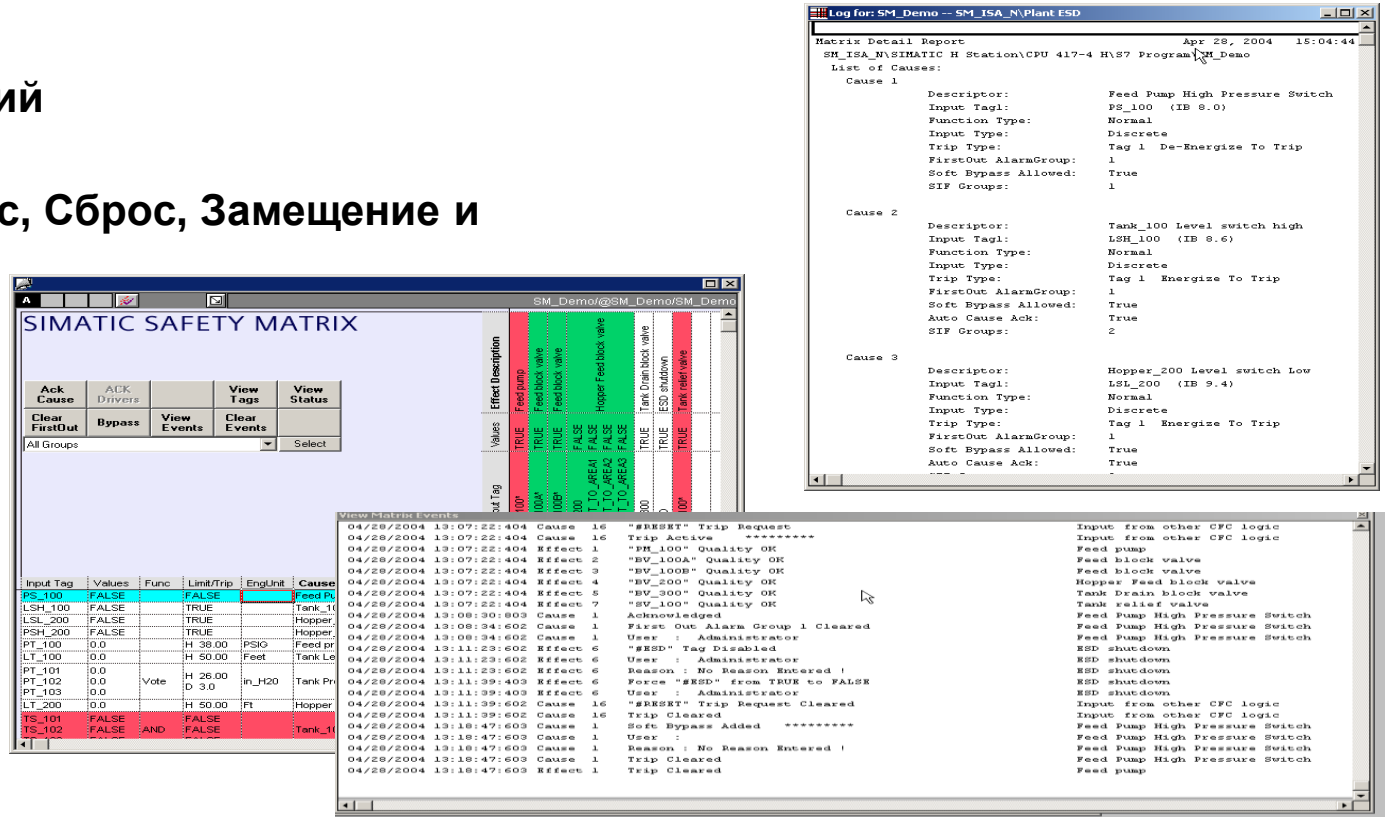
- Online просмотр состяний сигналов, Причин и Эффектов
  Автоматическая интеграция в PCS 7

- Отображение и сохранение предупреждений

- Поддержка функций эксплуатации - Байпас, Сброс, Замещение и изменение параметров

- Запись последовательности событий

- Автоматический отчет эксплуатации
- Автоматическое отслеживание версий
- Автоматическое документирование измеенний



Safety Matrix

Инжиниринг и Дизайн

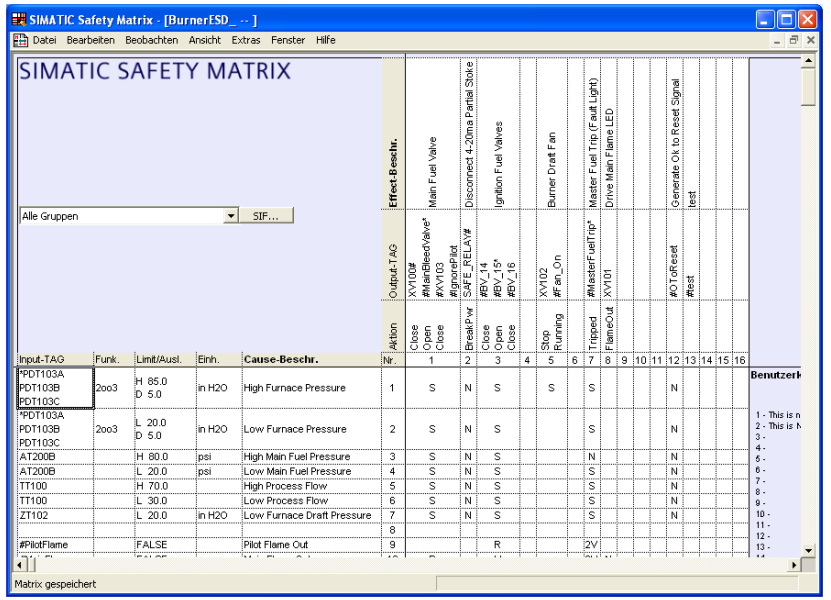
- Простое использование матрицы Причиин и Эффектов
- Авто-генерация безопасной CFC программы для контроллера

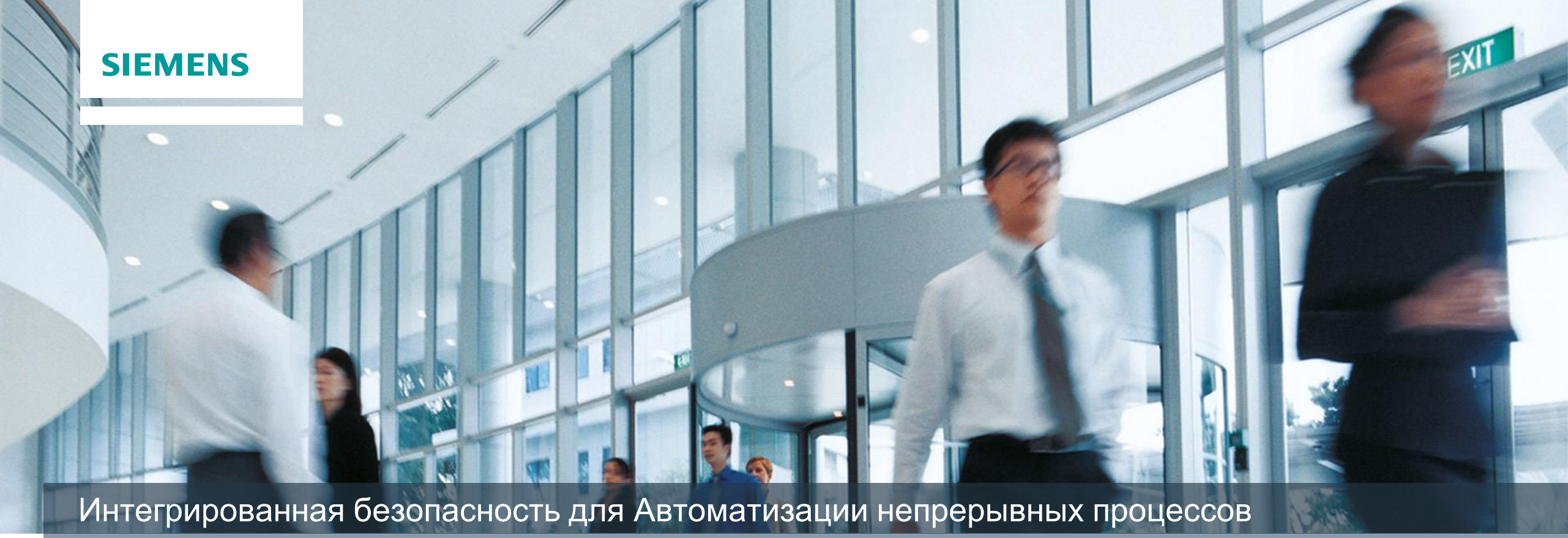
Эксплуатация и обслуживание

- Online просмотр, интеграция в PCS 7
- Поддержка функций Байпаса, Сброса и Замещения
- Запись последовательности событий
- Отображение первой аварии

Инструмент управления жизненным циклом безопасности

- Интегрировано отслеживание версии
- Интегрирована документация действий оператора
- Интегрирована документация изменений



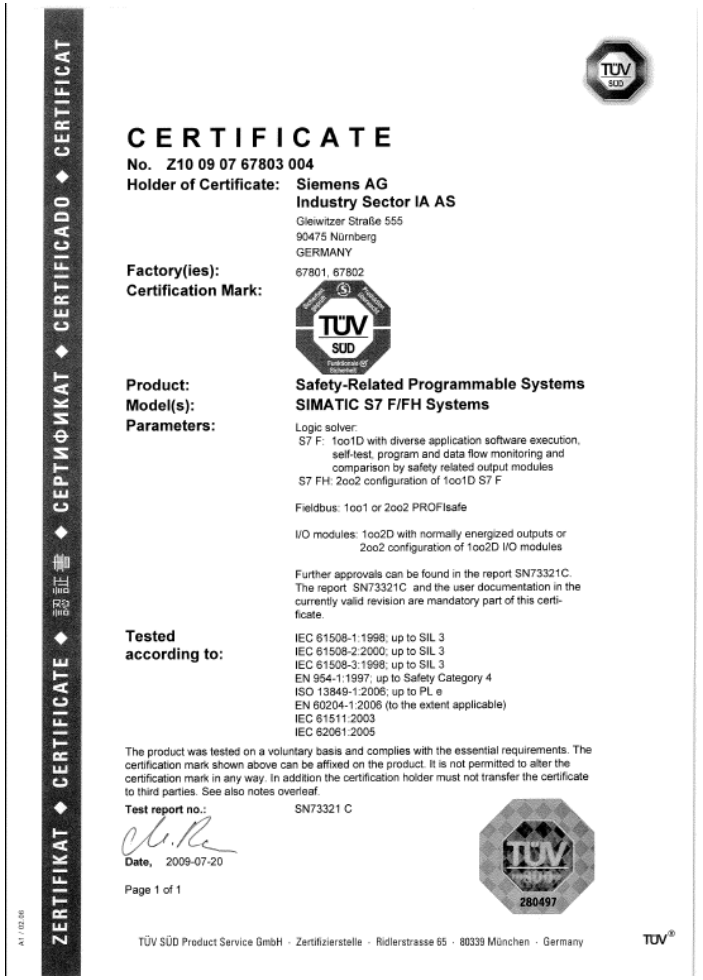


Интегрированная безопасность для Автоматизации непрерывных процессов

Сертификаты

SIEMENS

Здесь можно найти сертификаты



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

TÜV SÜD

CERTIFICATE

No. Z10 09 07 67803 004

Holder of Certificate: Siemens AG
Industry Sector IA AS
Gleiwitzer Straße 555
90475 Nürnberg
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 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 SN73321C. The report SN73321C and the user documentation in the currently valid revision are mandatory part of this certificate.

Tested according to:
IEC 61508-1:1998; up to SIL 3
IEC 61508-2:2000; up to SIL 3
IEC 61508-3:1998; up to SIL 3
EN 954-1:1997; up to Safety Category 4
ISO 13849-1:2006; up to PL e
EN 60204-1:2006 (to the extent applicable)
IEC 61511:2003
IEC 62061:2005

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.: SN73321 C

Date, 2009-07-20

Page 1 of 1

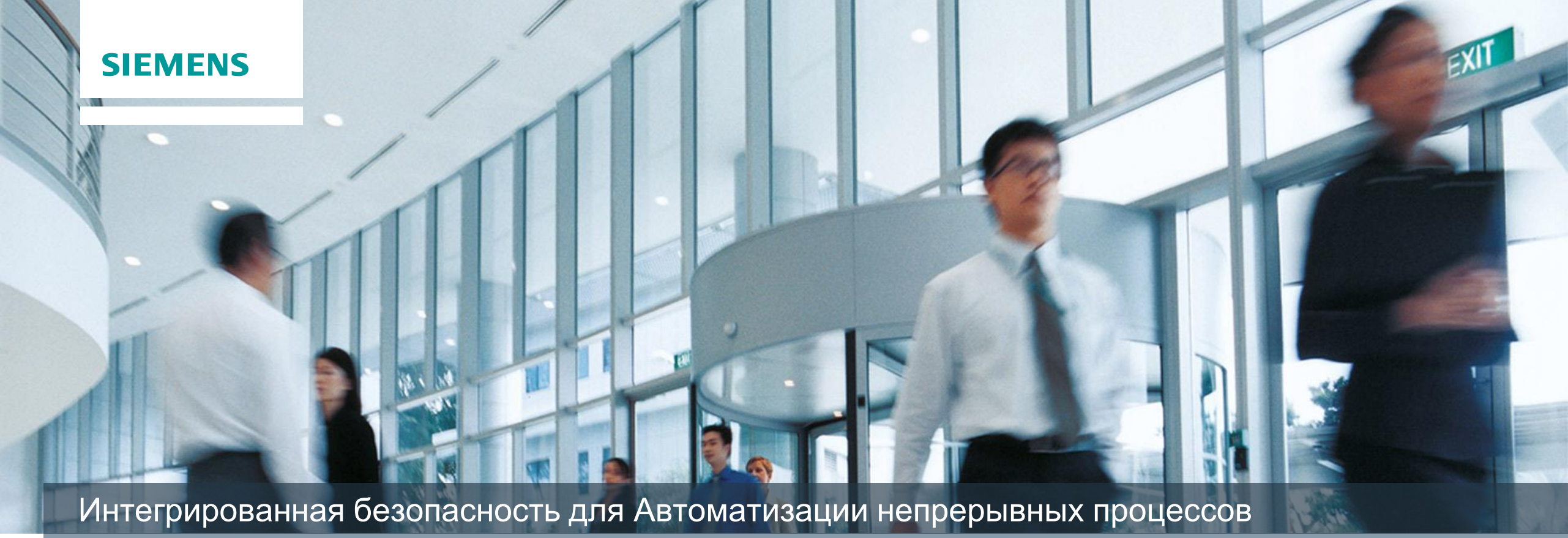
280497

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

TÜV®

Интегрированная безопасность для Автоматизации непрерывных процессов

Дополнительная информация



SIEMENS

Интегрированная безопасность для Автоматизации непрерывных процессов

Безопасность и Защита

Интегрированная безопасность для Автоматизации непрерывных процессов
Безопасность и Защита

SIEMENS

Промышленная защита

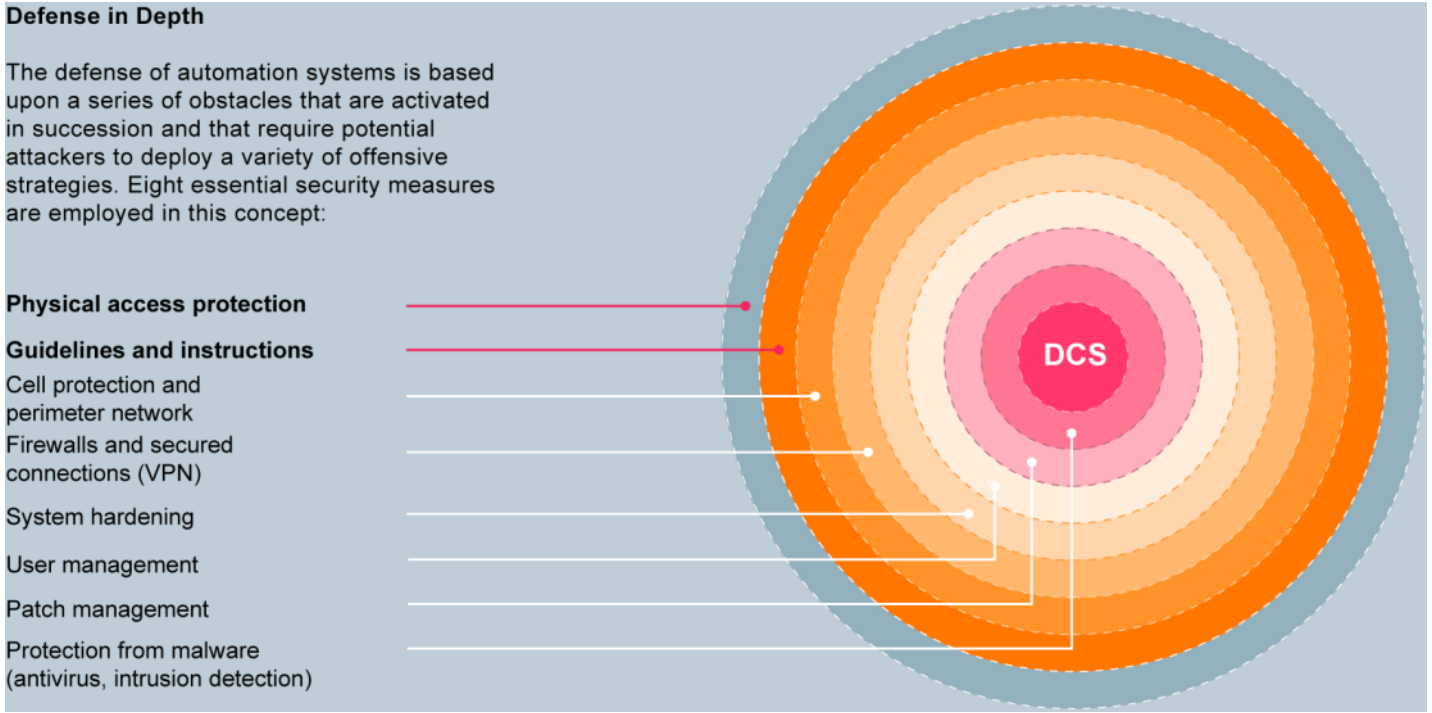
- Становится все более и более важной
- Производство подключено к офисной сети
- Производство подключено к Internet

Что нужно

- Концепции защиты производства
- Особенно Систем безопасности

Существует ли решение

- IEC 62443
- Рабочие группы ISA84
- Сертификация



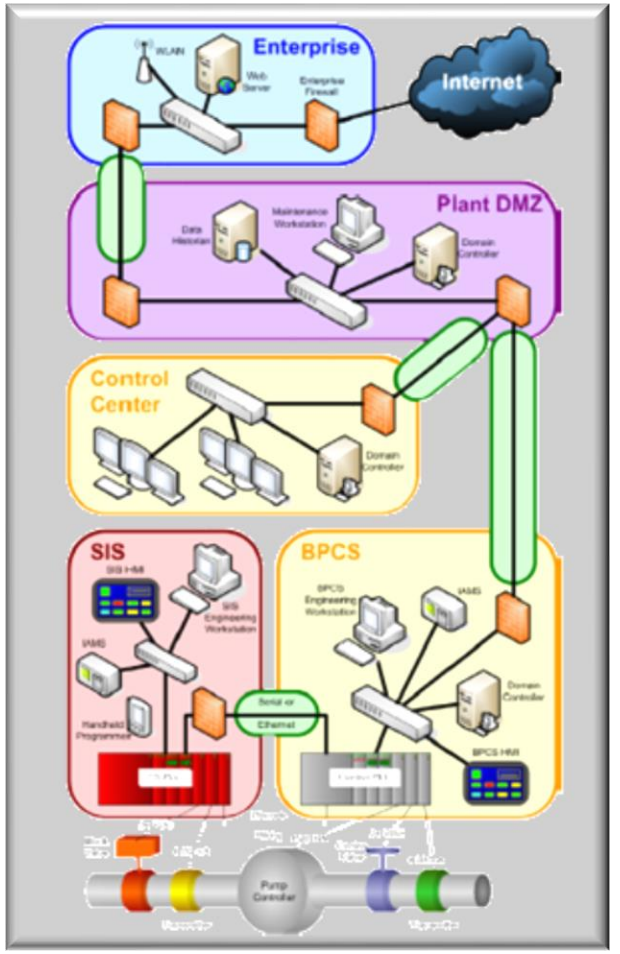
SIEMENS

Часть 3-3: Требования к защите системы и уровни защиты
Приложение A.2.3 Использование уровней защиты

… АСУ ТП и ПАЗ оба используют ПЛК для управления разными аспектами станции загрузки с ПАЗ используя специальные ПЛК Безопасности (FS-PLC) относящиеся к использованию систем безопасности.

Два ПЛК подключены через не маршрутизируемое серийное подключение или Ethernet подключение с устройством защиты периметра.

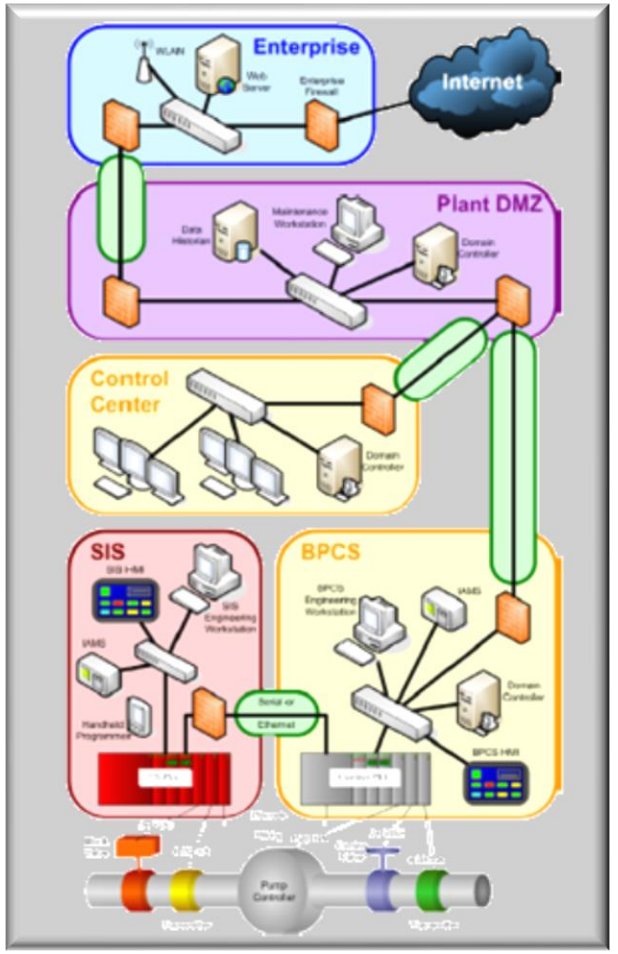
Каждый ПЛК подключается к локальному коммутатору с инженерной станцией для программирования и работы с ЧМИ.



Интегрированная безопасность для Автоматизации непрерывных процессов
Безопасность и Защита ISA84 WG9

- В техническом докладе ISA84 WG9 рассматривается вопрос защиты Автоматизированных систем безопасности
- Приложение А – Пример ПАЗ интерфейса к корпоративной сети описывается после примеров защищенных архитектур реализации ПАЗ: С воздушным зазором, Сопряженные, Интегрированные 1 зона, Интегрированные 2 зоны
- “Примеры концептуальные и не претендуют на шаблон для любой системы. Они предназначены представить разные подходы пользователя по внедрению ПАЗ”

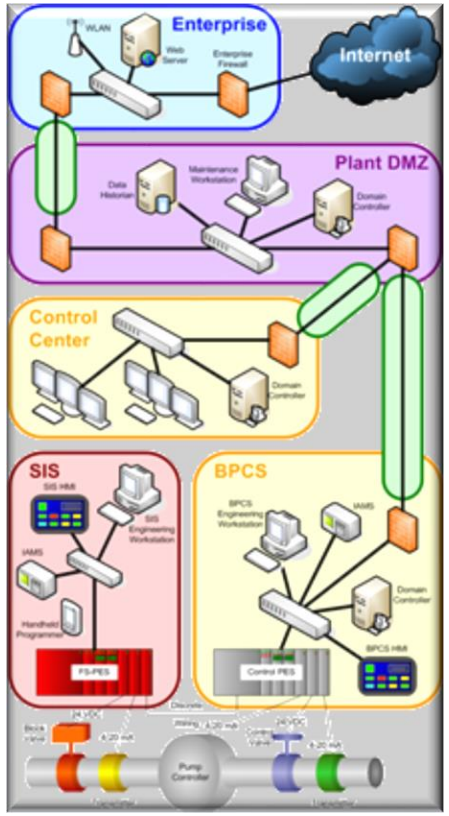
➢ С PCS 7 Интегрированной безопасностью возможно построить рекомендованные Архитектуры



Безопасность и Защита
ISA84 WG9 – Приложение A - Пример ПАЗ интерфейсов к корпоративной сети

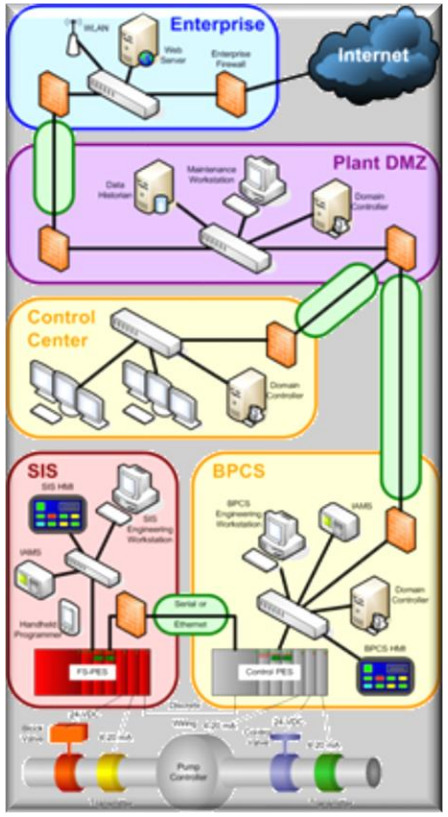
Воздушный зазор

Предусматривается физическая и логическая изоляция ПАЗ от коммуникаций с остальными зонами



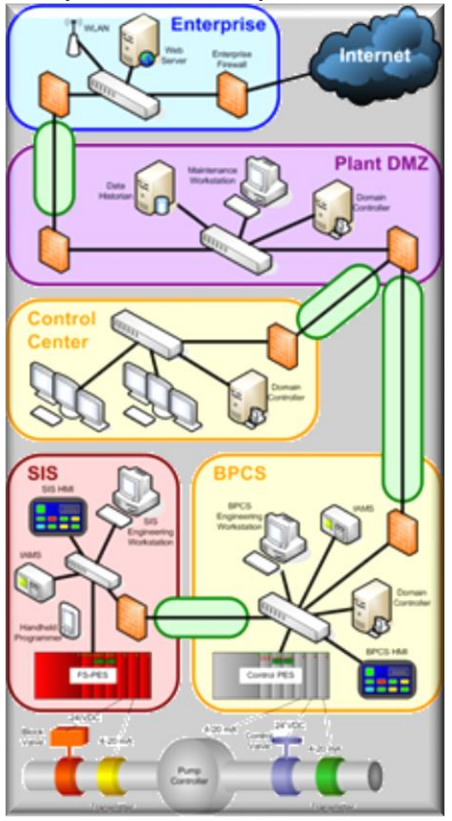
Сопряженные

ПАЗ и АСУ ТП остаются подключенными по прямому подключению точка-точка.



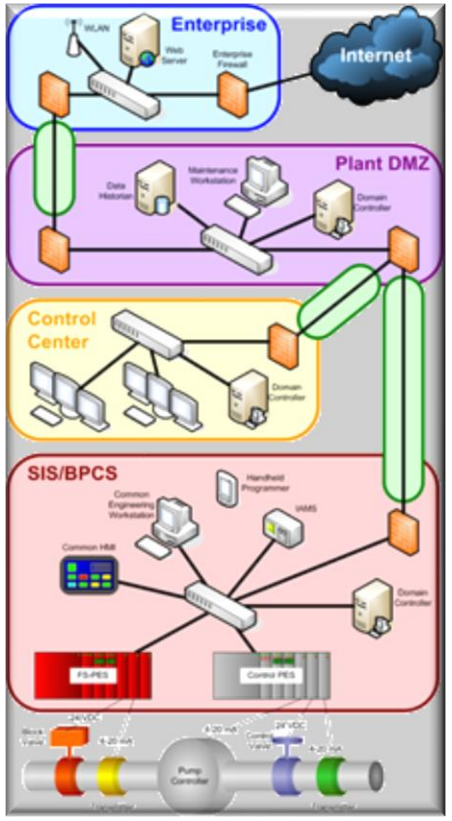
Интеграция 2 зоны

АСУ ТП и ПАЗ системы полностью интегрированы и имеют прямую, real-time коммуникацию между собой.

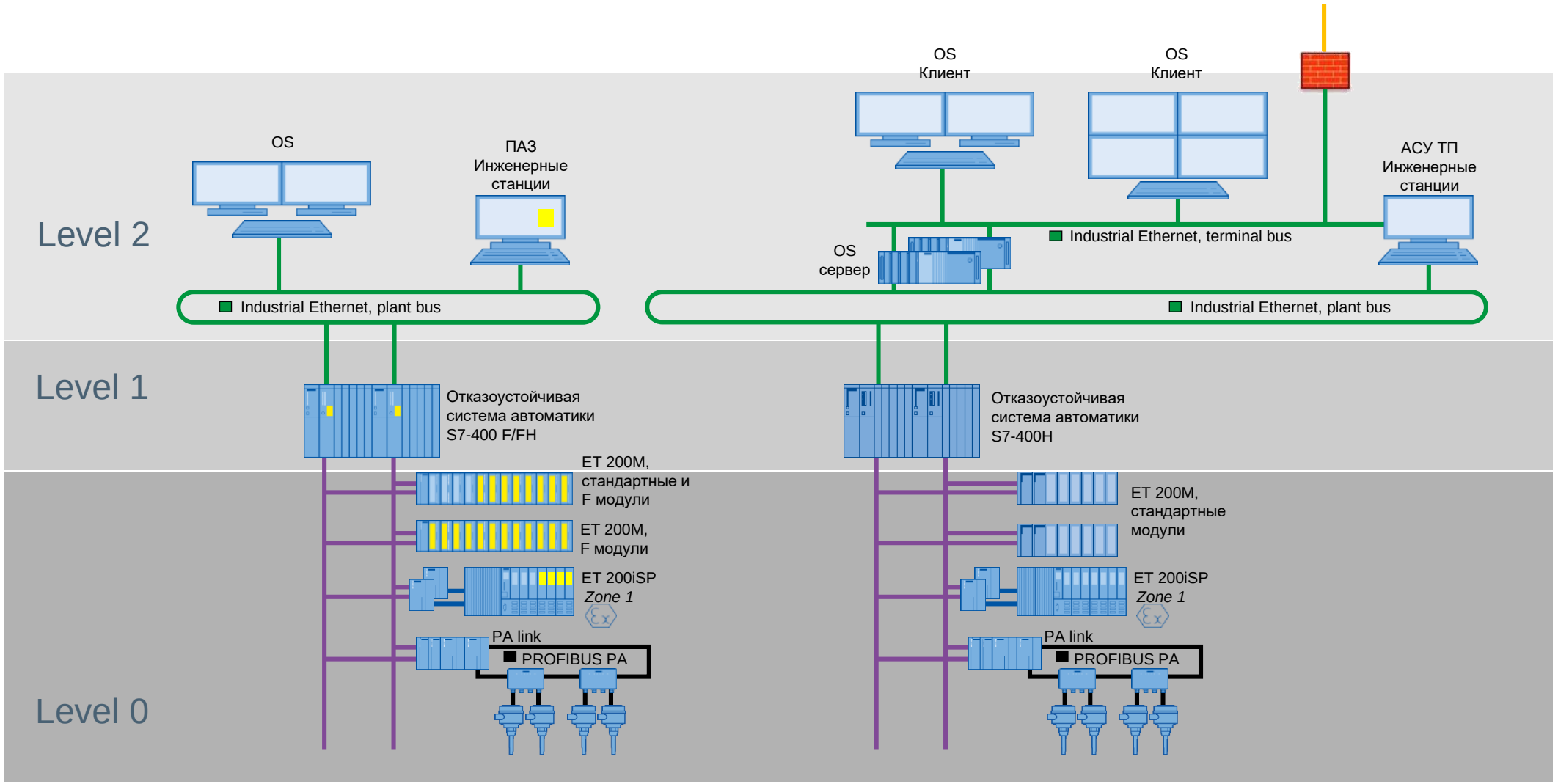


Интеграция 1 зона

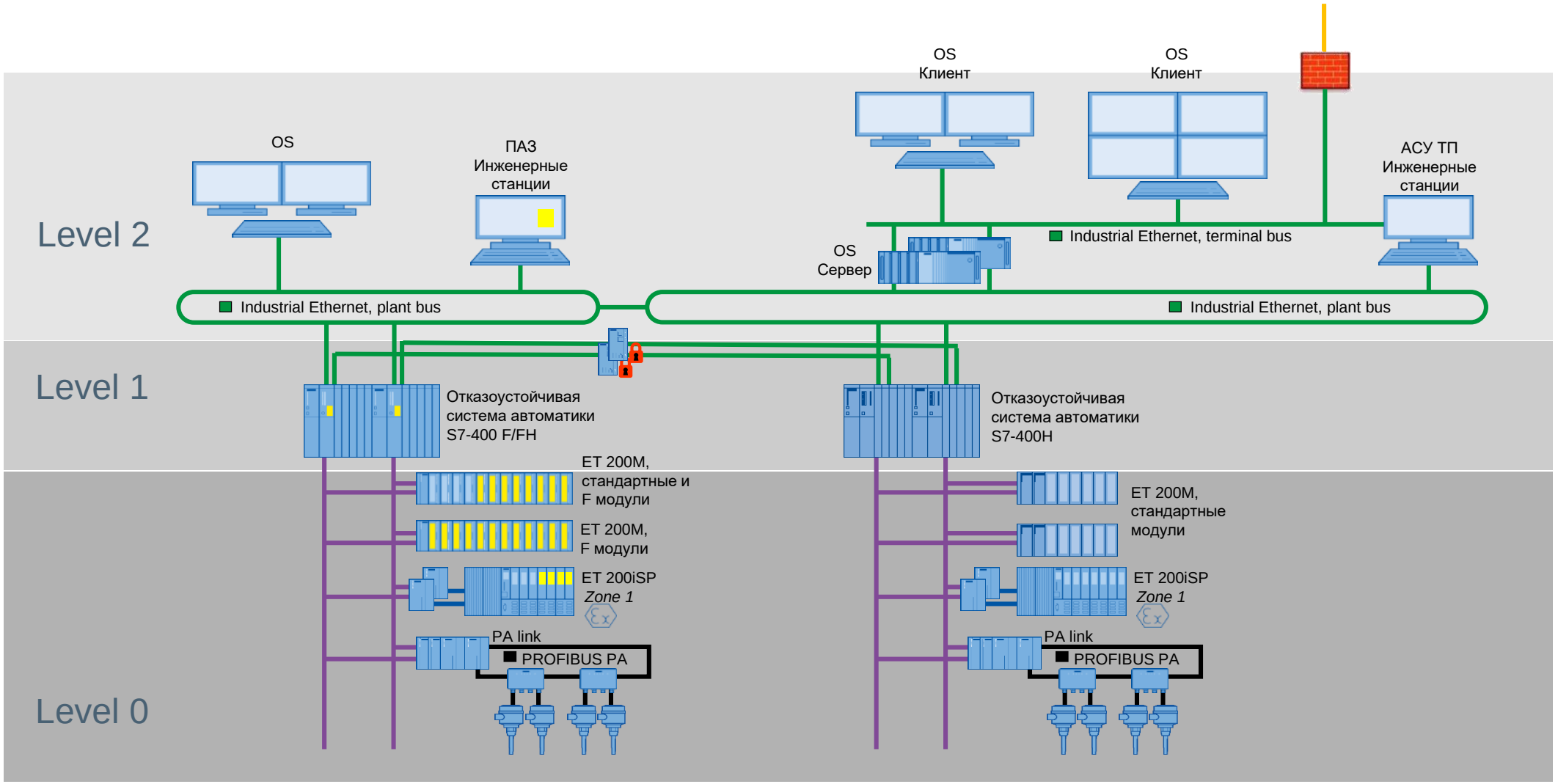
ПАЗ и АСУ ТП интегрированы давая отличное взаимодействие между этими системами



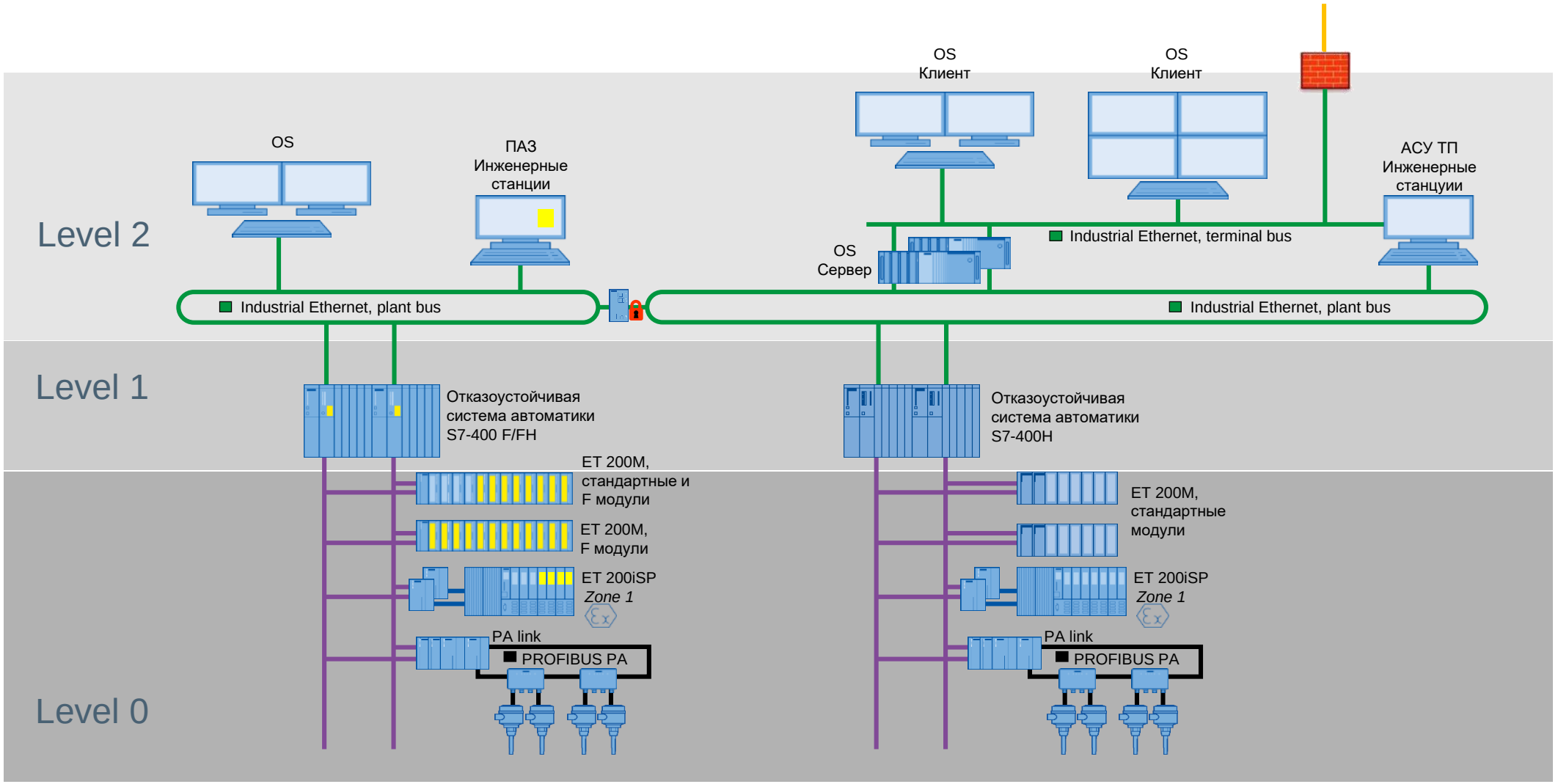
SIMATIC PCS 7
ПАЗ Архитектуры I → Воздушный зазор



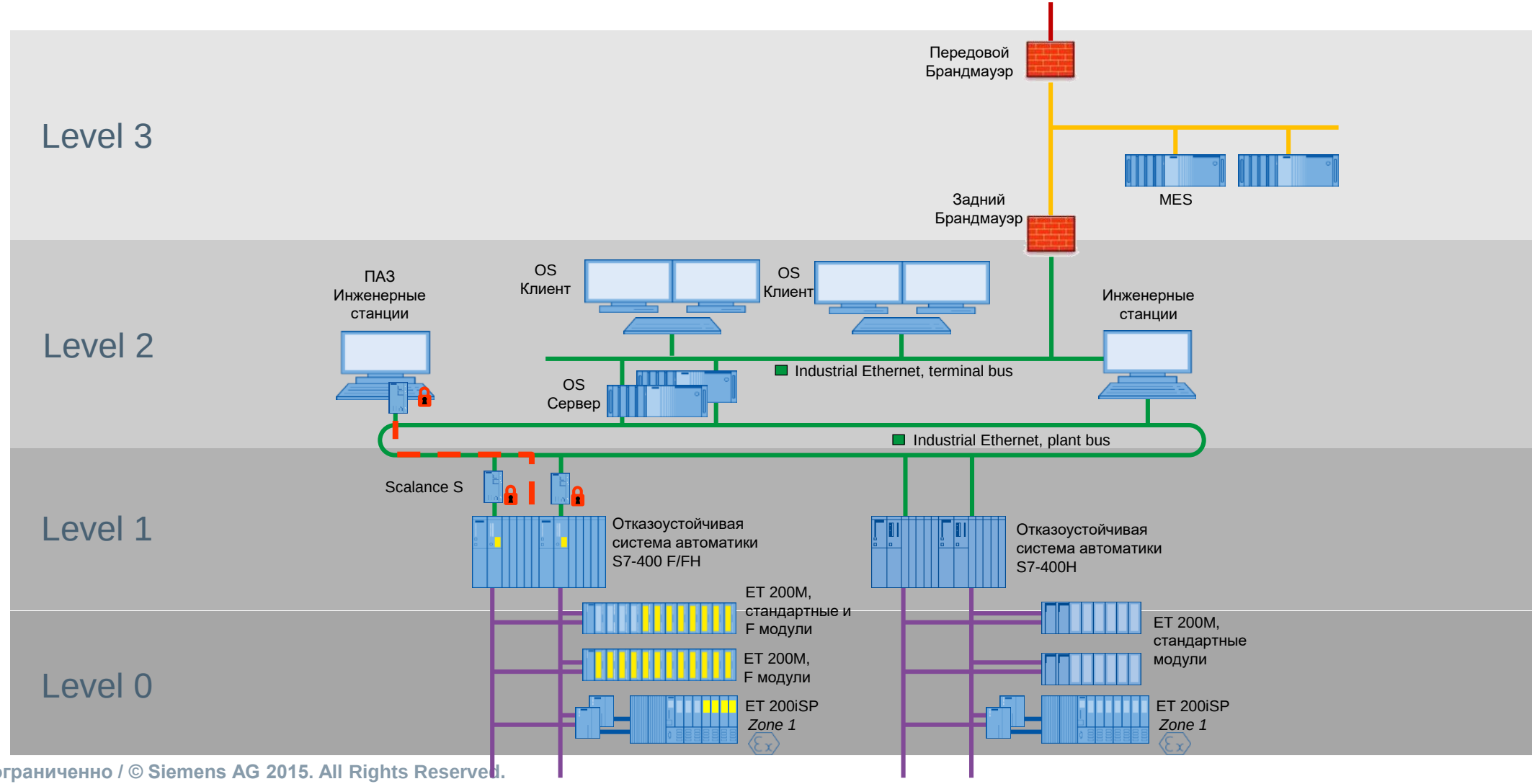
SIMATIC PCS 7
ПАЗ Архитектуры II → Сопряженные



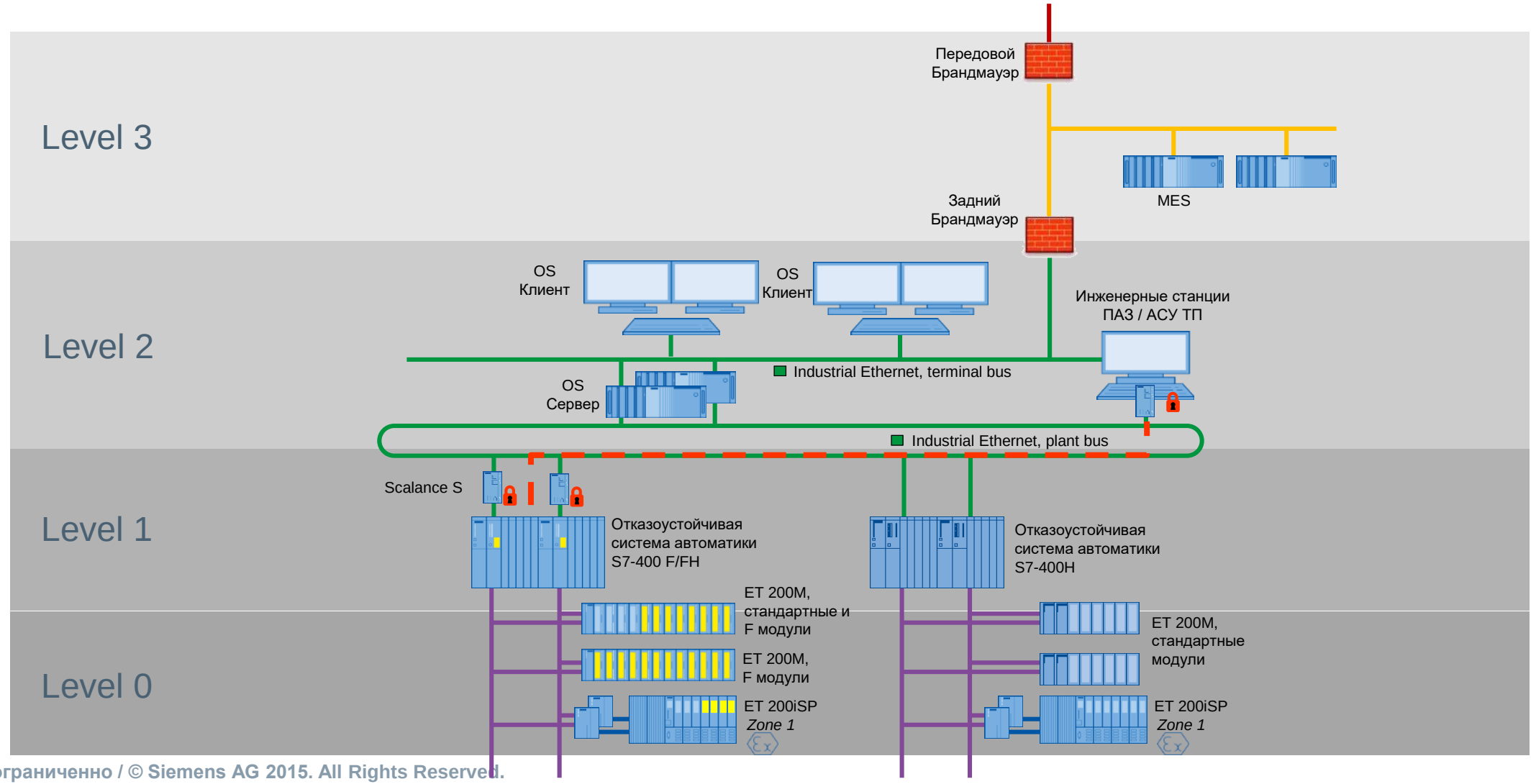
SIMATIC PCS 7
ПАЗ Архитектуры III → Интегрированные в 2 зоны



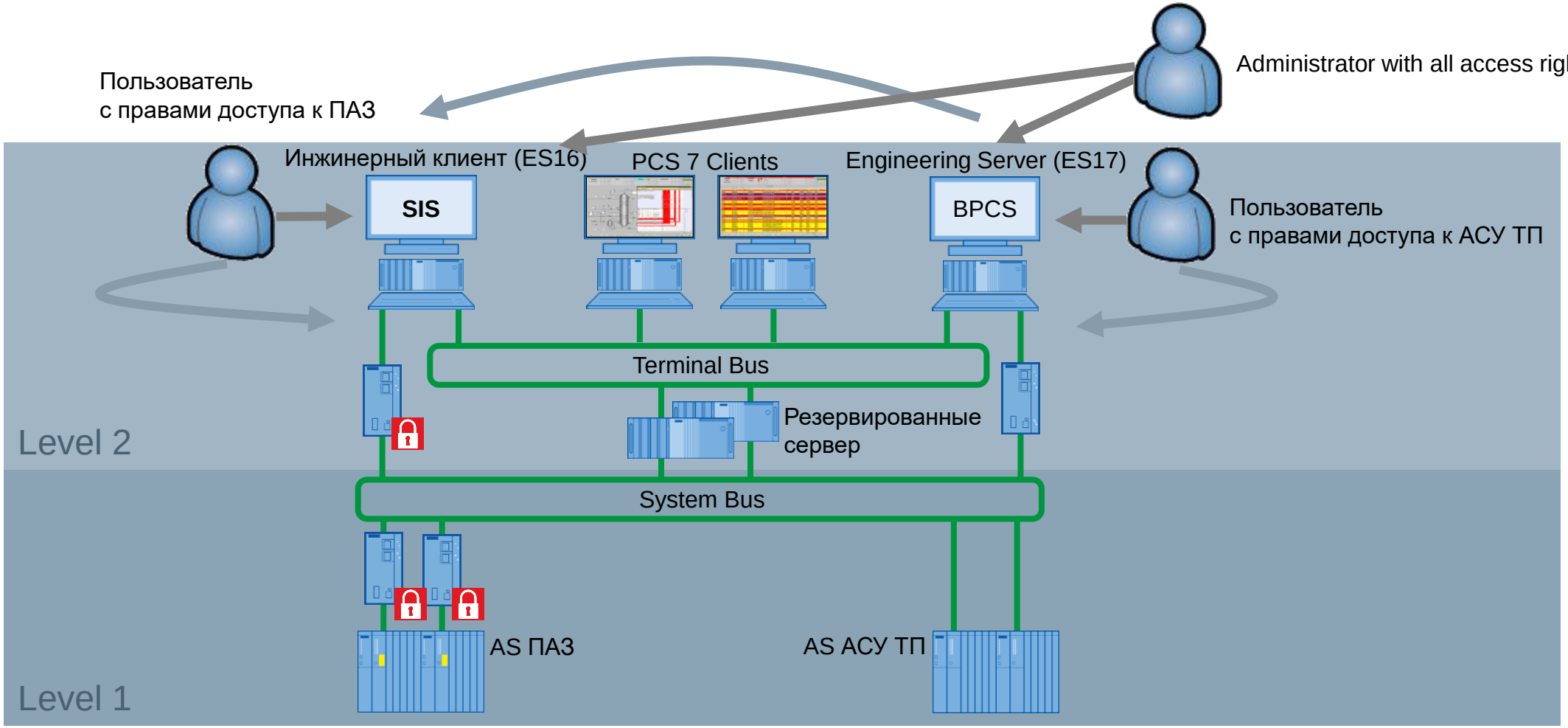
SIMATIC PCS 7
ПАЗ Архитектуры IV - Интегрированные 2 зоны



SIMATIC PCS 7
ПАЗ Архитектуры V – Интегрированные 1 зона



SIMATIC PCS 7
ПАЗ Архитектуры IV

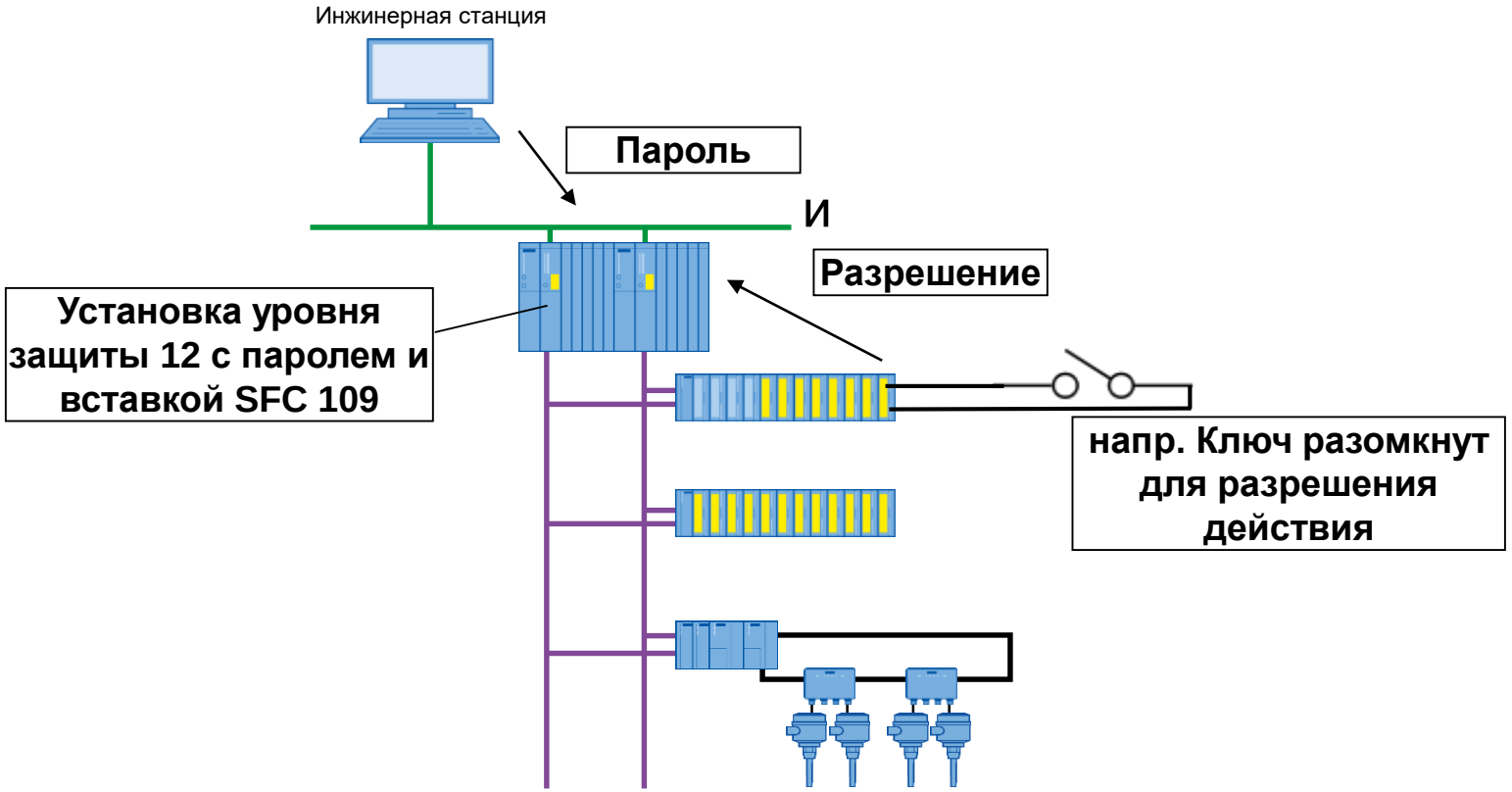


SIEMENS

H-ЦПУ V6 : Дополнительный уровень защиты с SFC 109 "PROTECT“

Для загрузки / Модификации F-Приложения:

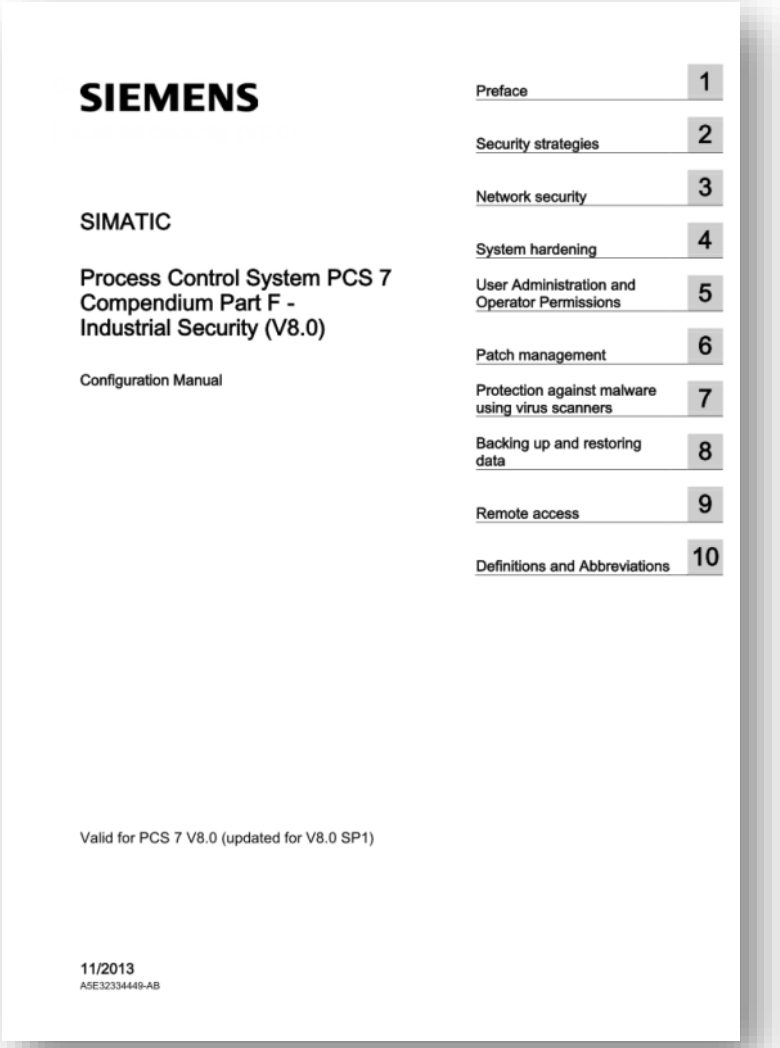
- Пароль ES
  и
- Отключение ключем (*или ЧМИ*)



SIEMENS

PCS 7 Compendium F

http://support.automation.siemens.com/WW/view/en/77507462


SIEMENS

SIMATIC

Process Control System PCS 7 Compendium Part F - Industrial Security (V8.0)

Configuration Manual

Valid for PCS 7 V8.0 (updated for V8.0 SP1)

11/2013
A5E32334449-AB

Безопасность и Защита
Сертификация ситемы

Certificate Of Compliance

This is to certify that the:

SIMATIC PCS 7 CPU 410-5H
Process Automation

Manufactured by:

Siemens AG

Is in compliance with the requirements set forth by:

Achilles Level II Certification

This certificate is restricted to the specified version of the referenced Device (including model number, hardware/firmware/software version, and control protocols) set forth in this Certificate. Any change to the Device might impair the Device's ability to pass the standards referenced in this Certificate. This Certificate is based upon limited testing, and is not a complete or comprehensive certification of the security of the Device. The Device may contain security vulnerabilities and deficiencies that are not covered by the standards referenced in this Certificate. This Certificate is subject to revocation by Wurldtech Security Technologies Inc.

More information regarding this Certificate and the Achilles Level 1 Standard is available at www.wurldtech.com and upon request from Wurldtech Security Technologies Inc.

CERTIFICATE NO. CERT-116-040913

MLFB 6ES7 410-5HX08-0AB0
HARDWARE VERSION

V8.0.x
FIRMWARE VERSION

N/A
CONTROL PROTOCOL

Embedded Device
CATEGORY

Nate Kube, CTO

wurldtech
security technologies

Certificate Of Compliance

This is to certify that the:

SIMATIC PCS 7 (V8.0 SP1) and
Commissioning Services

Manufactured by:

Siemens AG

Is in compliance with the requirements set forth by:

Achilles Practices Certification: Bronze

This certificate is restricted to the specified version of the referenced Device (including model number, hardware/firmware/software version, and control protocols) set forth in this Certificate. Any change to the Device might impair the Device's ability to pass the standards referenced in this Certificate. This Certificate is based upon limited testing, and is not a complete or comprehensive certification of the security of the Device. The Device may contain security vulnerabilities and deficiencies that are not covered by the standards referenced in this Certificate. This Certificate is subject to revocation by Wurldtech Security Technologies Inc.

More information regarding this Certificate and the Achilles Level 1 Standard is available at www.wurldtech.com and upon request from Wurldtech Security Technologies Inc.

CERTIFICATE NO. APC2013-00021

13JS0041; 13JS0073
APC REPORT NUMBER

06-December-2013
DATE OF ISSUE

06-December-2014
DATE OF EXPIRY

Nate Kube, CTO

wurldtech
security technologies

Безопасность и Защита
Сертификация

Achilles Level II Сертификат

- 82 Продуктов
- Контроллер
  - Все S7-400 ЦПУ
- Коммуникационные карты
- Сетевые устройства сертифицированы как брандмауэры

Certificate Of Compliance

This is to certify that the:

SIMATIC PCS 7 CPU 410-5H
Process Automation

Manufactured by:

Siemens AG

Is in compliance with the requirements set forth by:

Achilles Level II Certification

This certificate is restricted to the specified version of the referenced Device (including model number, hardware/firmware/software version, and control protocols) set forth in this Certificate. Any change to the Device might impair the Device's ability to pass the standards referenced in this Certificate. This Certificate is based upon limited testing, and is not a complete or comprehensive certification of the security of the Device. The Device may contain security vulnerabilities and deficiencies that are not covered by the standards referenced in this Certificate. This Certificate is subject to revocation by Wurldtech Security Technologies Inc.

More information regarding this Certificate and the Achilles Level 1 Standard is available at www.wurldtech.com and upon request from Wurldtech Security Technologies Inc.

CERTIFICATE NO. CERT-116-040913

MLFB 6ES7 410-5HX08-0AB0
HARDWARE VERSION

V8.0.x
FIRMWARE VERSION

N/A
CONTROL PROTOCOL

Embedded Device
CATEGORY

Nate Kube, CTO

wurldtech
security technologies

SIEMENS

Примеры

Проверка SIL согласно IEC 61508, IEC 61511 и VDI 2180-4

Проверка SIL согласно IEC 61508, IEC61511 и VDI 2180-4

Пример элементов и оборудования

- Датчик
  - Расходомер, λ_{DU} = 1.26E-7, поверка T = 12 мес (8760 час), доказано практикой
  - Барьер, λ_{DU} = 3.60E-8, поверка T = 12 мес (8760 час)

- Логика
  - B/B, SIL 3 сертифицирован, PFD = 1.00E-5
  - ЦПУ, SIL 3 сертифицирован, резервированный контроллер, PFD = 3.80E-4
  - Коммуникация, PFD = 1.00E-5

- Исполнительный элемент
  - Реле, λ_{DU} = 4.67E-9, поверка T = 12 мес, доказано практикой
  - Силовой выключатель, λ_{DU} = 4.00E-7, поверка T = 12 мес, доказано практикой

Проверка SIL согласно IEC 61508, IEC61511 и VDI 2180-4

Архитектура и Аппаратная отказоустойчивость

- Часть датчика
  - Трансмиттер HFT = 0, доказано практи
    - => SIL 2
  - Блок питания HFT = 0
    - => SIL 1

Часть датчика = SIL 1

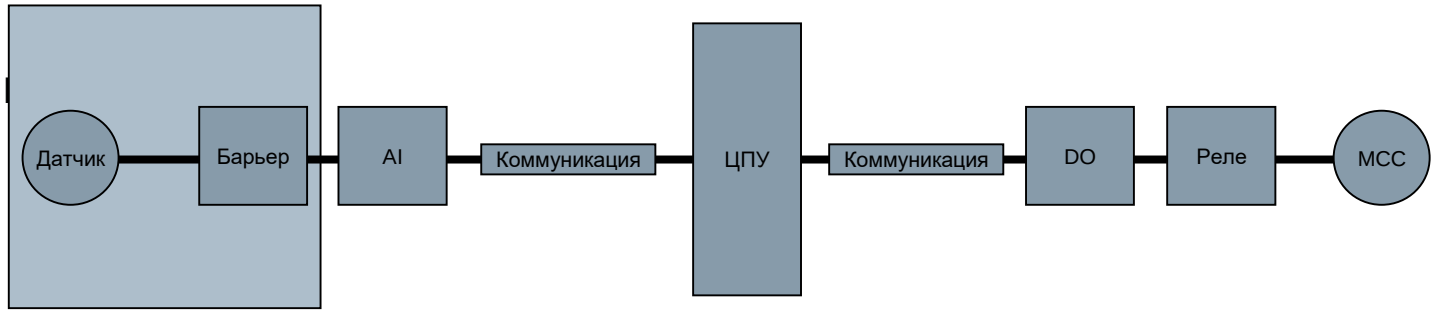


Table 1. Minimum *HFT* and examples for architectures of field devices with given SIL of the SIF

SIL	*HFT*	Examples of architectures for field devices
1	0	1oo1, 2oo2
2	1	1oo2, 2oo3
3	2	1oo3
4	not recommended	

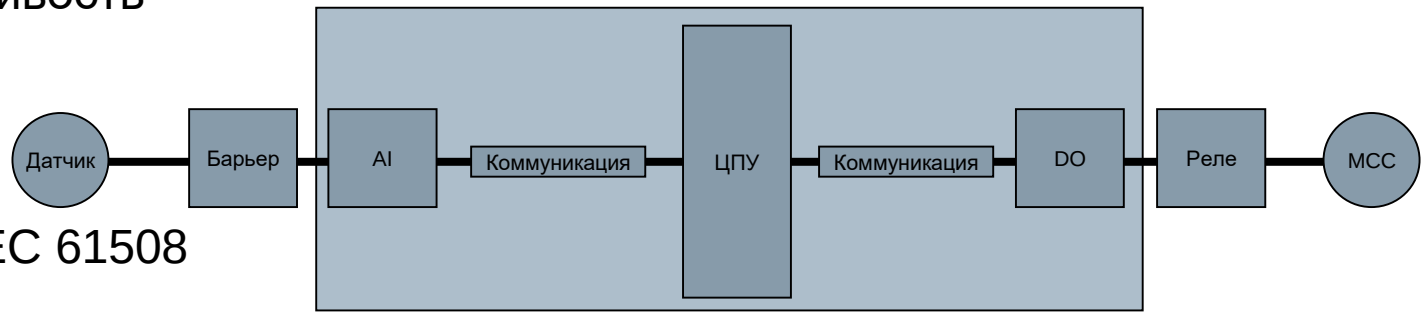
Table 2. Minimum *HFT* and examples of architectures for especially qualified field devices (proven-in-use) with a given SIL of the SIF

SIL	*HFT*	Examples of architectures for especially qualified field devices (proven-in-use)
1	0	1oo1, 2oo2
2	0	1oo1, 2oo2
3	1	1oo2, 2oo3
4	not recommended	

Hardware Fault Tolerance (HFT) – отказоустойчивость аппаратных средств

Проверка SIL согласно IEC 61508, IEC61511 и VDI 2180-4

Архитектура и Аппаратная отказоустойчивость



- Логическая система (Контроллер и IO)
  - IO SIL 3 сертифицирован согласно IEC 61508
    - => SIL 3
  - Контроллер SIL 3 сертифицирован согласно IEC 61508
    - => SIL 3
  - Коммуникация SIL 3 сертифицирована согласно IEC 61508
    - => SIL 3

Логическая система = SIL 3

Проверка SIL согласно IEC 61508, IEC61511 и VDI 2180-4

Архитектура и Аппаратная отказоустойчивость

- Исполнительный элемент
  - Реле HFT = 0, доказано практикой
    - => SIL 2
  - MCC HFT = 0, доказано практикой
    - => SIL 2

Исполнительный элемент= SIL 2

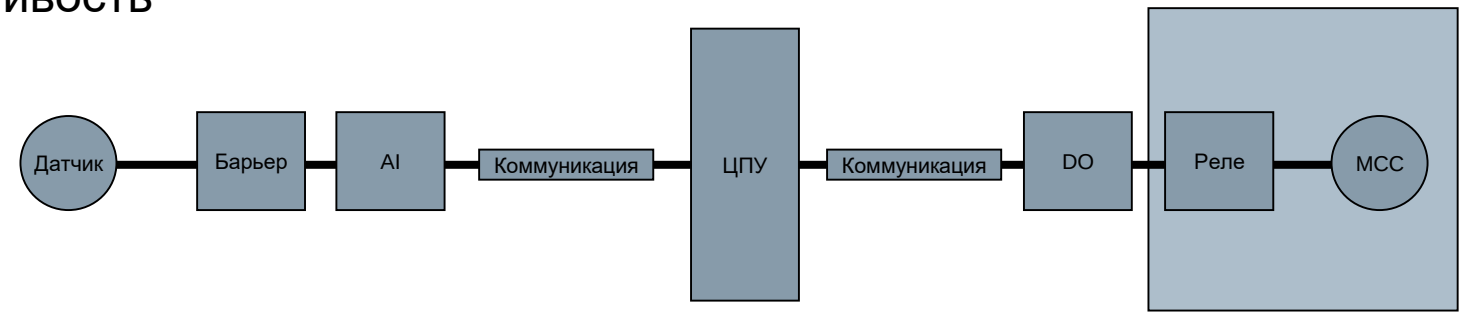


Table 2. Minimum *HFT* and examples of architectures for especially qualified field devices (proven-in-use) with a given SIL of the SIF

SIL	*HFT*	Examples of architectures for especially qualified field devices (proven-in-use)
1	0	1oo1, 2oo2
2	0	1oo1, 2oo2
3	1	1oo2, 2oo3
4	not recommended	

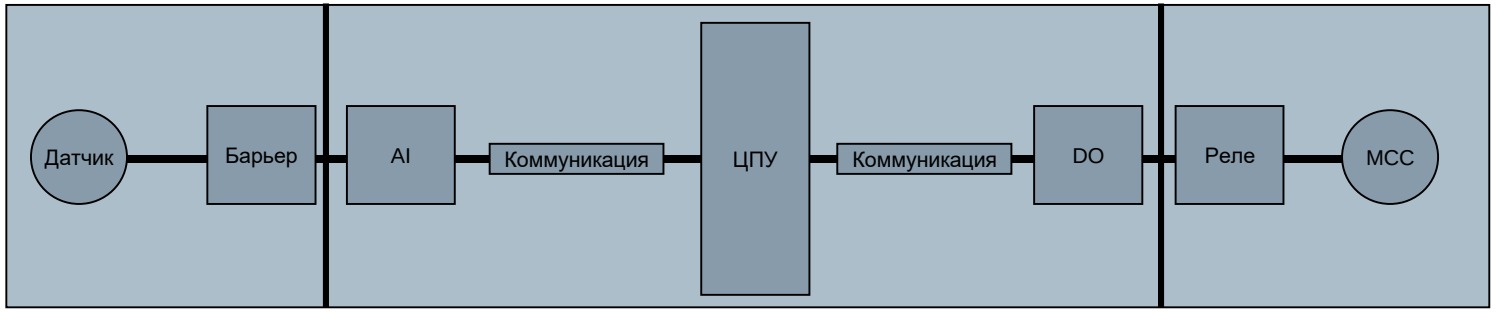
Hardware Fault Tolerance (HFT) – отказоустойчивость аппаратных средств

Проверка SIL согласно IEC 61508, IEC61511 и VDI 2180-4

Архитектура и Аппаратная отказоустойчивость

- Вся система
  - Часть датчика = SIL 1
  - Логическая система = SIL 3
  - Исполнительный элемент= SIL 2

Вся система = SIL 1



– 28 – 61508-2 © IEC:2010

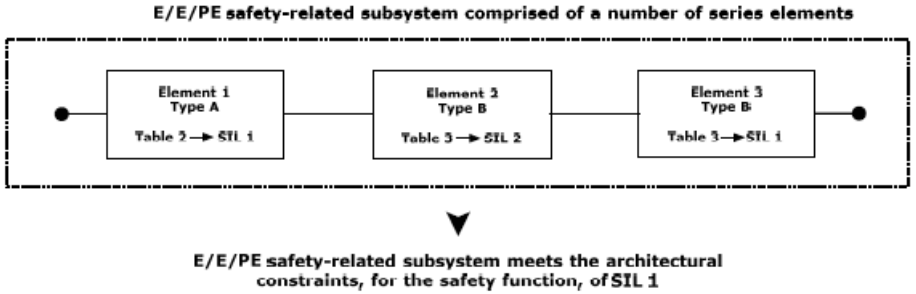


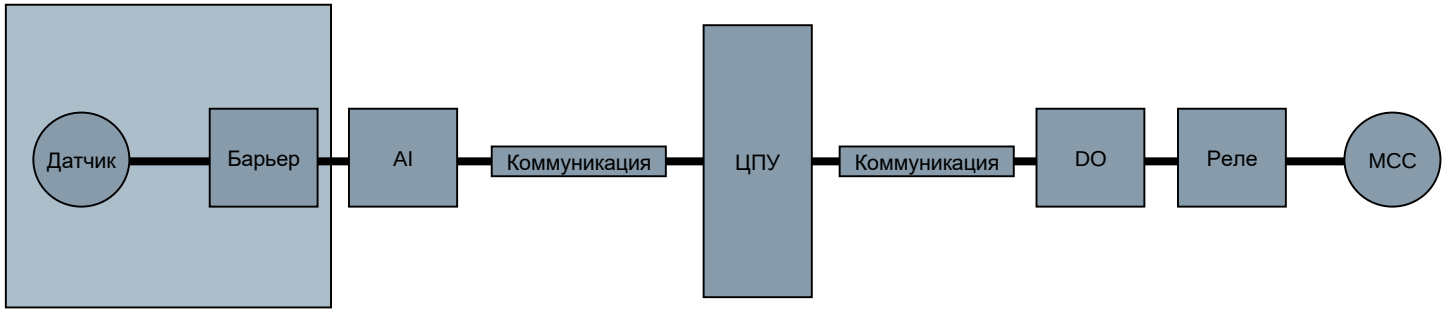
Figure 5 – Determination of the maximum SIL for specified architecture (E/E/PE safety-related subsystem comprising a number of series elements, see 7.4.4.2.3)

Проверка SIL согласно IEC 61508, IEC61511 и VDI 2180-4

Аппроксимация Probability of Failure on Demand (PFD) - вероятность отказа на запрос

- Часть датчика
  - Расходомер, λ_{DU} = 1.26E-7, поверка T = 12 мес (8760 час), доказано практикой
  - Барьер, λ_{DU} = 3.60E-8, поверка T = 12 мес (8760 час)
  - $PFD_S = PFD_{Датчик} + PFD_{Блок\ питания}$
  - PFD_S = 0.5 * 1.26E-7 *8760 + 0.5 * 3,60E-8 8760
  - PFD_S = 5.52E-4 + 1.58E-5
  - PFD_S = 5.68E-4

$$PFD_{1oo1} = \frac{1}{2}\lambda_{DU} \cdot T_1$$

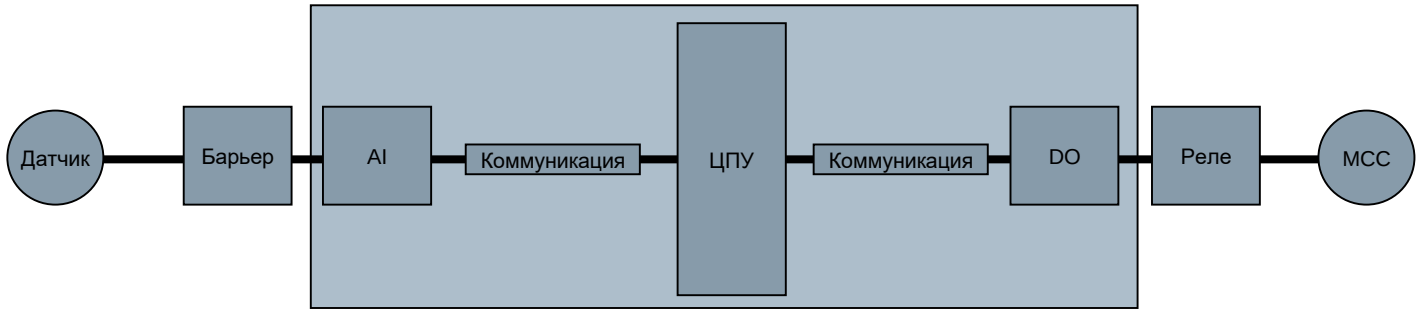


Проверка SIL согласно IEC 61508, IEC61511 и VDI 2180-4

Probability of Failure on Demand (PFD) - вероятность отказа на запрос

Логическая система

- Вход, SIL 3 сертифицирован, PFD = 1.00E-5
- Выход, SIL 3 сертифицирован, PFD = 1.00E-5
- ЦПУ, SIL 3 сертифицирован, PFD = 3.80E-4
- Коммуникация, PFD = 1.00E-5
- $PFD_L = PFD_{AI}+PFD_{ЦПУ}+PFD_{DO}+PFD_{Com}$
- PFD_L = 1.0E-5 + 3.8E-4 + 1.0E-5 + 1.0E-5
- PFD_L= 4.1E-4



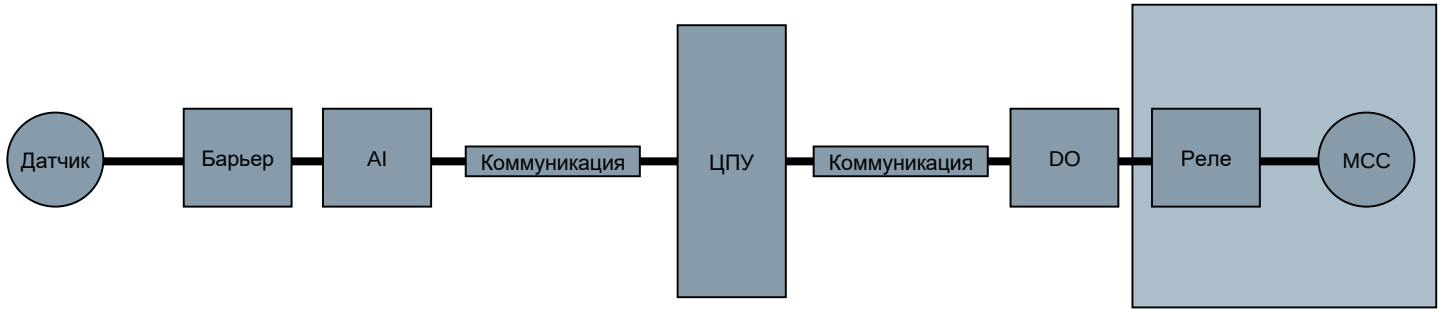
Проверка SIL согласно IEC 61508, IEC61511 и VDI 2180-4

Probability of Failure on Demand (PFD) - вероятность отказа на запрос

Выходной элемент

- Реле, λ_{DU} = 4.67E-9, поверка T = 12 мес (8760 час), доказано практикой
- Power circuit breaker, λ_{DU} = 4.00E-7, поверка T = 12 мес (8760 час), доказано практикой
- $PFD_{FE} = PFD_{Реле} + PFD_{MCC}$
- PFD_{FE} = 0.5 * 4.67E-9 *8760 + 0.5 * 4.00E-7 * 8760
- PFD_{FE} = 2.05E-5 + 1.75E-3
- PFD_{FE} = 1.77E-3

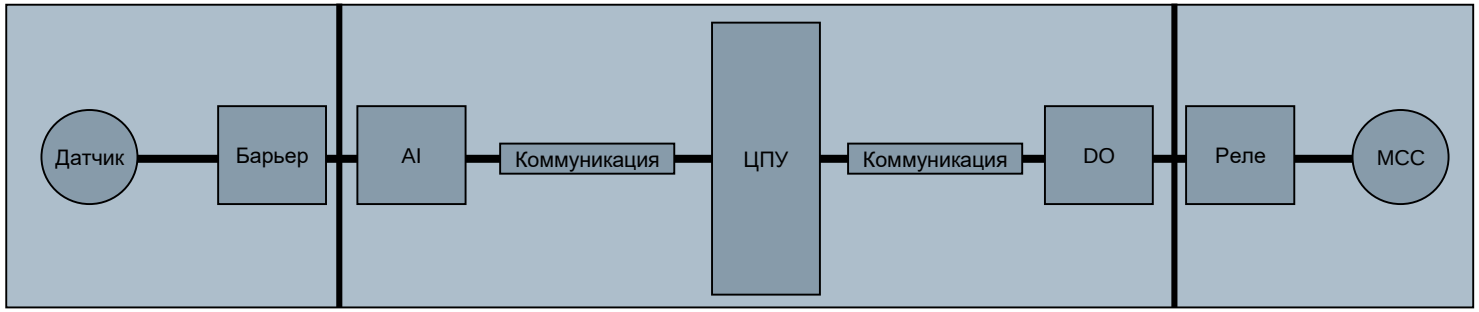
$$PFD_{1oo1} = \frac{1}{2}\lambda_{DU} \cdot T_1$$



Проверка SIL согласно IEC 61508, IEC61511 и VDI 2180-4

Probability of Failure on Demand (PFD) – вероятность отказа на запрос

- PFD общий
  - PFD_S = 5.68E-4
  - PFD_L= 4.10E-4
  - PFD_{FE} = 1.77E-3



$$PFD_{\text{Total}} = PFD_S + PFD_L + PFD_{FE} \qquad (6)$$

- PFDTotal = 5.68E-4 + 4.10E-4 + 1.77E-3
- PFDTotal = 2.75E-3

Вся система = SIL 2

Table 2 – Safety integrity levels – target failure measures for a safety function operating in low demand mode of operation

Safety integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function (PFD_{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Проверка SIL согласно IEC 61508, IEC61511 и VDI 2180-4

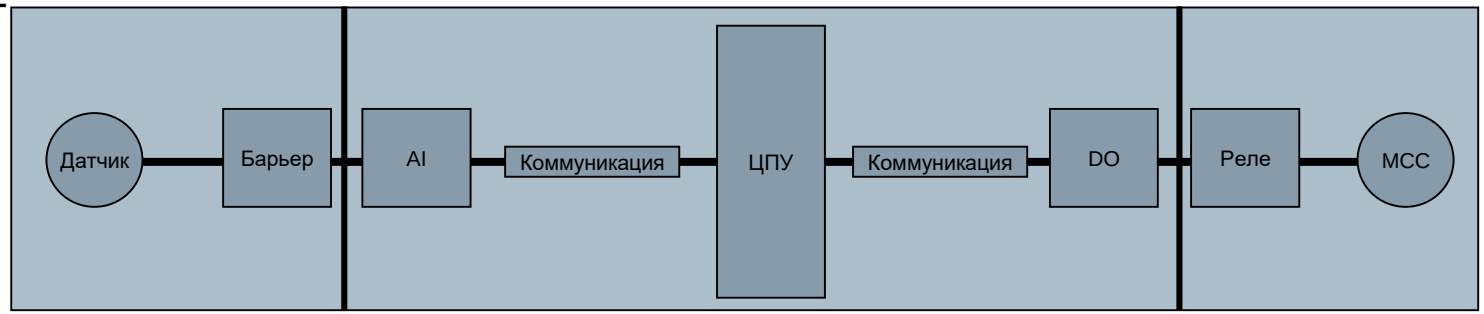
Архитектура и Аппаратная отказоустойчивость

- Результат SIL 1

Probability of Failure on Demand (PFD) – вероятность отказа на запрос

- Результат SIL 2

Вся система SIL 1

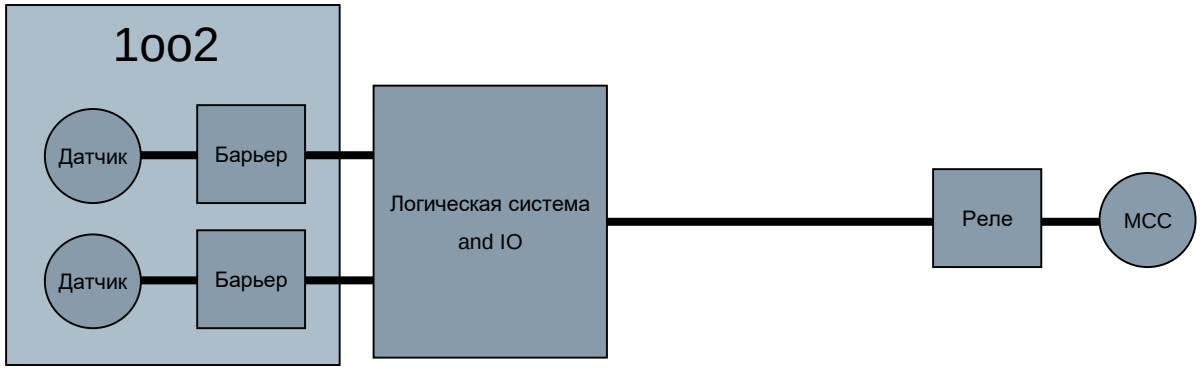


Архитектура должна быть изменена, например, для соответствия SIL 2

Проверка SIL согласно IEC 61508, IEC61511 и VDI 2180-4

Архитектура и Аппаратная отказоустойчивость

- Часть датчика
  - Трансмиттер HFT = 1, доказано практикой
    - => SIL 3
  - Барьер HFT = 1
    - => SIL 2
- Логическая система и Исполнительный элемента остается без изменений SIL 3 и SIL 2



Вся система SIL 2

Table 1. Minimum *HFT* and examples for architectures of field devices with given SIL of the SIF

SIL	*HFT*	Examples of architectures for field devices
1	0	1oo1, 2oo2
2	1	1oo2, 2oo3
3	2	1oo3
4	not recommended	

Table 2. Minimum *HFT* and examples of architectures for especially qualified field devices (proven-in-use) with a given SIL of the SIF

SIL	*HFT*	Examples of architectures for especially qualified field devices (proven-in-use)
1	0	1oo1, 2oo2
2	0	1oo1, 2oo2
3	1	1oo2, 2oo3
4	not recommended	

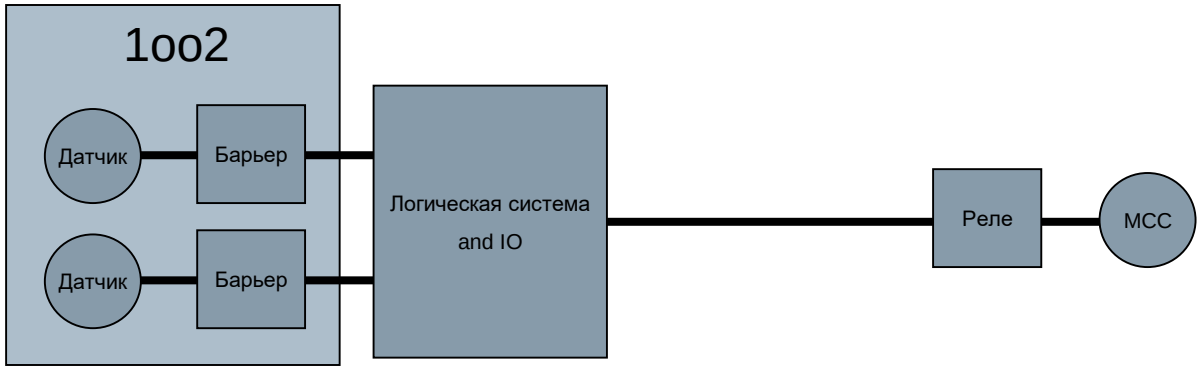
Hardware Fault Tolerance (HFT) – отказоустойчивость аппаратных средств

Проверка SIL согласно IEC 61508, IEC61511 и VDI 2180-4

Probability of Failure on Demand (PFD) – вероятность отказа на запрос

- PFD Общий
  - ß = 10%
  - PFD_S = 4/3 * (5.68E-4)² + 0.1 * 5.68E-4
  - PFD_S = 5.72E-5
  - PFD_L= 4.10E-4
  - PFD_{FE} = 1.77E-3
  - PFDTotal = 5.72E-5 + 4.10E-4 + 1.77E-3
  - PFDTotal = 2.24E-3

Вся система = SIL 2



$$PFD_{Total} = PFD_S + PFD_L + PFD_{FE} \qquad (6)$$

$$PFD_{1oo2} = \frac{4}{3} \cdot PFD_{1oo1}{}^2 + \beta \cdot PFD_{1oo1}$$

Table 2 – Safety integrity levels – target failure measures for a safety function operating in low demand mode of operation

Safety integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function (PFD_{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Проверка SIL согласно IEC 61508, IEC61511 и VDI 2180-4

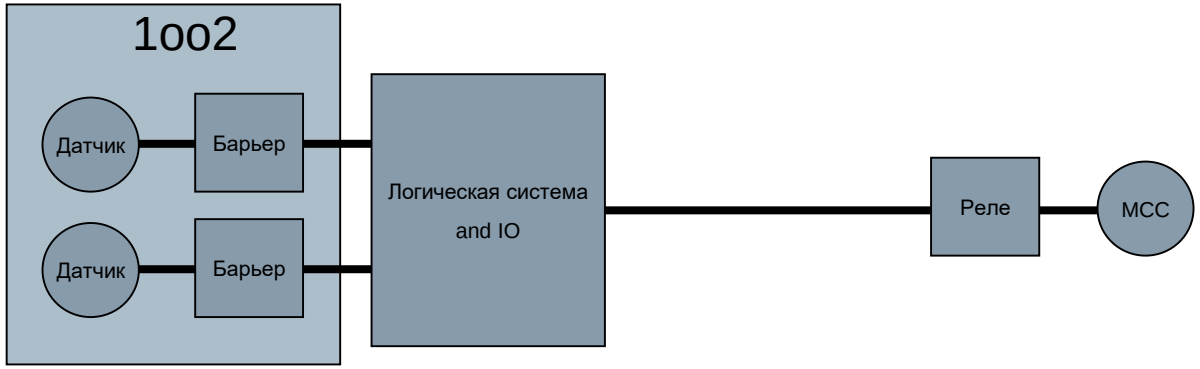
Архитектура и Аппаратная отказоустойчивость

- Результат SIL 2

Probability of Failure on Demand (PFD) - вероятность отказа на запрос

- Результат SIL 2

Вся система
SIL 2



Спасибо за внимание!

Сергей Степанюк

PCS7 Leading specialist

100% foreign owned subsidiary Siemens Ukraine
RC-UA PD P&S
Ул. Ярославская 58
04071 Киев, Украина
Тел.: +380 44 392-2322
Моб.: +380 68 538-2322
E-Mail: serhii.stepaniuk@siemens.com

siemens.com/process-safety