Safety & Securtiy

www.siemens.com/process-safety

Safety Integrated for Process Automation

Basics and Standards

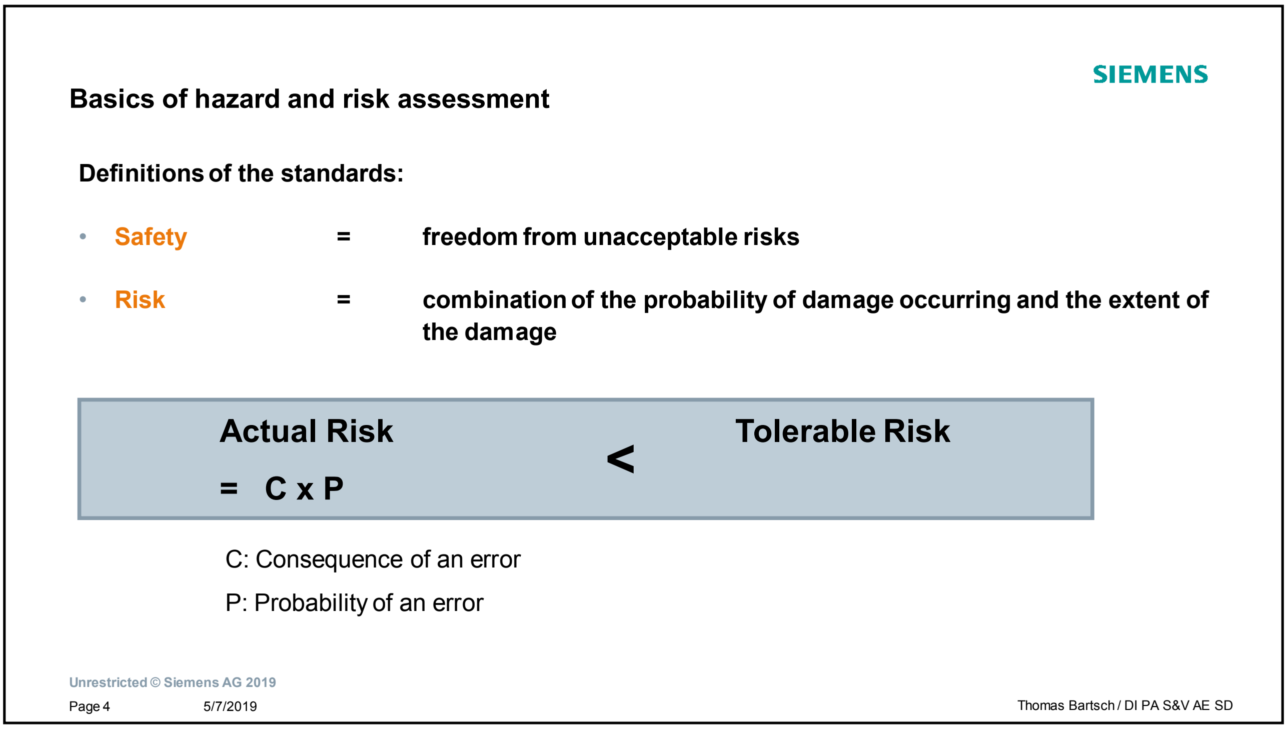
siemens.com/process-safety

Safety Approach

SIEMENS

Functional Safety reduces the risk of process related accidents and ensures maximum safety for:

People
Process
Environment



Basics of hazard and risk assessment

SIEMENS

Definitions of the standards:

- **Safety** = **freedom from unacceptable risks**
- **Risk** = **combination of the probability of damage occurring and the extent of the damage**

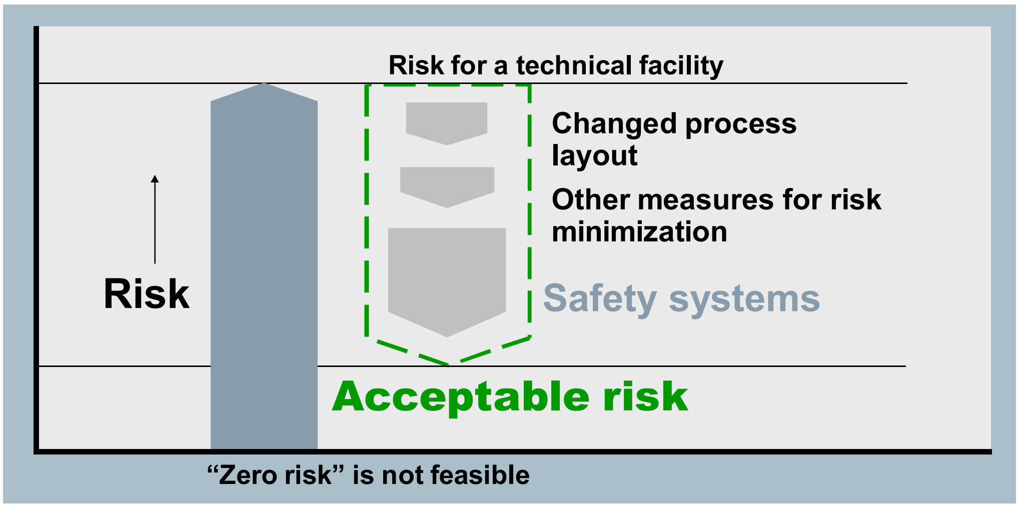
Actual Risk = C x P < Tolerable Risk

C: Consequence of an error

P: Probability of an error

Risk Reduction
The Approach of Safety

SIEMENS



Risk for a technical facility

Risk

Changed process layout

Other measures for risk minimization

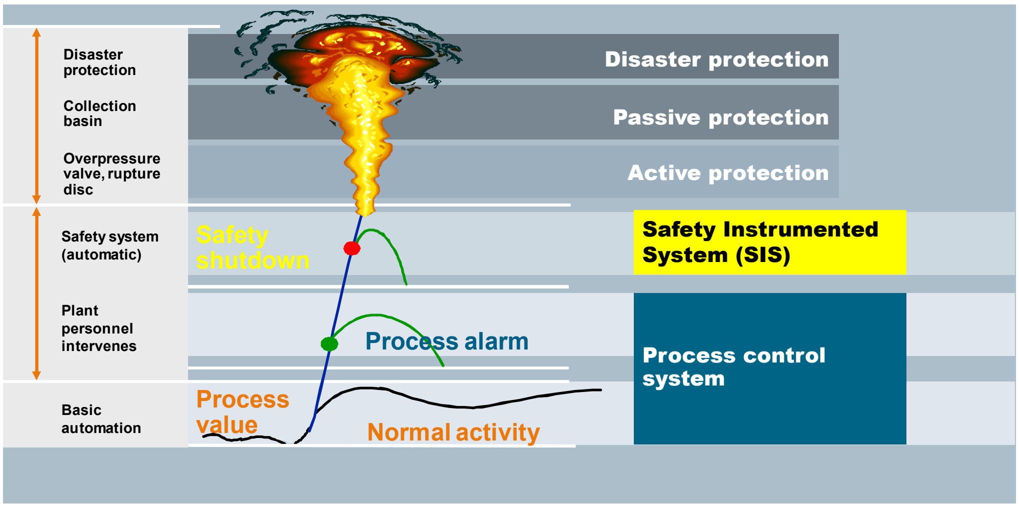
Safety systems

Acceptable risk

“Zero risk” is not feasible

Safety concept

SIEMENS



Disaster protection

Collection basin

Overpressure valve, rupture disc

Safety system (automatic)

Plant personnel intervenes

Basic automation

Disaster protection

Passive protection

Active protection

Safety shutdown

Safety Instrumented System (SIS)

Process alarm

Process value

Normal activity

Process control system

International safety standards

INTERNATIONAL ELECTROTECHNICAL COMMISSION

IEC61508

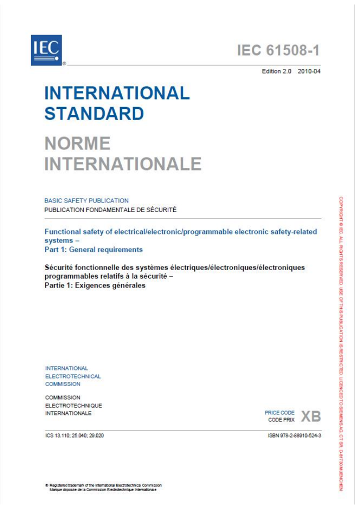
INTERNATIONAL ELECTROTECHNICAL COMMISSION

IEC61511

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.

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

International safety standards



IEC 61508-1

Edition 2.0 2010-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

BASIC SAFETY PUBLICATION
PUBLICATION FONDAMENTALE DE SÉCURITÉ

Functional safety of electrical/electronic/programmable electronic safety-related systems –
Part 1: General requirements

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité –
Partie 1: Exigences générales

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE
CODE PRIX XB

ICS 13.110; 25.040; 29.020

ISBN 978-2-88910-524-3

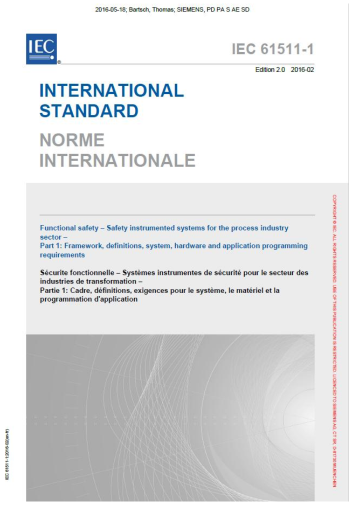
® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

COPYRIGHT © IEC. ALL RIGHTS RESERVED. USE OF THIS PUBLICATION IS RESTRICTED. LICENCED TO SIEMENS AG, CT SR, D-81730 MUENCHEN

Part	Functional Safety of electrical/programmable electronic safety-related systems
IEC 61508-1	General requirements
IEC 61508-2	Requirements for electrical/electronic/programmable electronic safety-related systems
IEC 61508-3	Software requirements
IEC 61508-4	Definitions and abbreviations
IEC 61508-5	Examples of methods for the determination of safety integrity lefels
IEC 61508-6	Guidelines on the application of the IEC 61508-2 and IEC 61508-3
IEC 61508-7	Overview of techniques and measures

SIEMENS

International safety standards



2016-05-18; Bartsch, Thomas; SIEMENS, PD PA S AE SD

IEC 61511-1

Edition 2.0 2016-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Functional safety – Safety instrumented systems for the process industry sector –
Part 1: Framework, definitions, system, hardware and application programming requirements

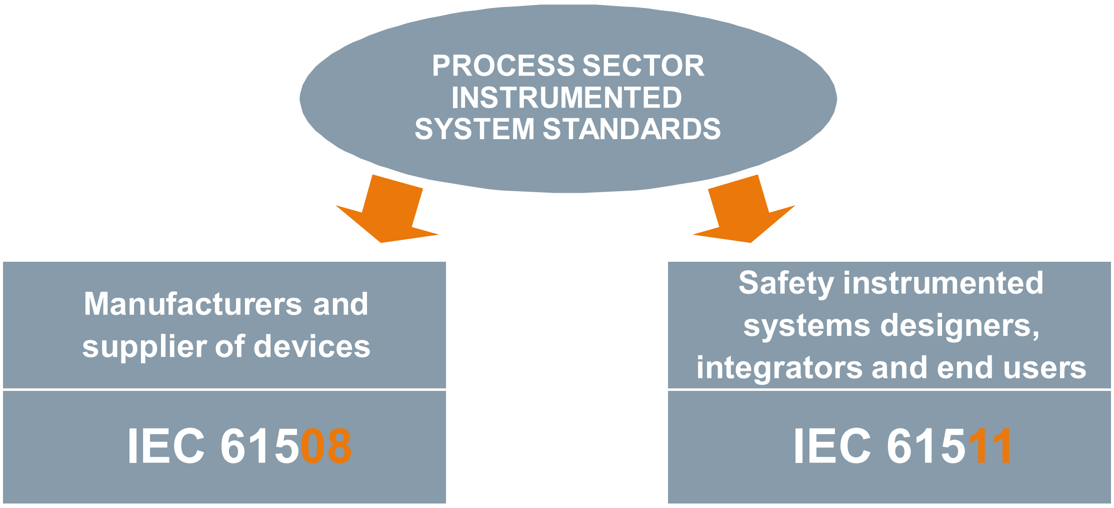
Sécurite fonctionnelle – Systèmes instrumentes de sécurité pour le secteur des industries de transformation –
Partie 1: Cadre, définitions, exigences pour le système, le matériel et la programmation d'application

IEC 61511-1:2016-02(en-fr)

Part	Functional safety - Safety instrumented systems for the process industry sector
IEC 61511-1	Framwork, definitions, system, hardware and application programming requirements
IEC 61511-2	Guidelines for the application of IEC 61511-1
IEC 61511-3	Guidance for the determination of the required safety integrity levels

SIEMENS

International safety standards



PROCESS SECTOR INSTRUMENTED SYSTEM STANDARDS

Manufacturers and supplier of devices

IEC 61508

Safety instrumented systems designers, integrators and end users

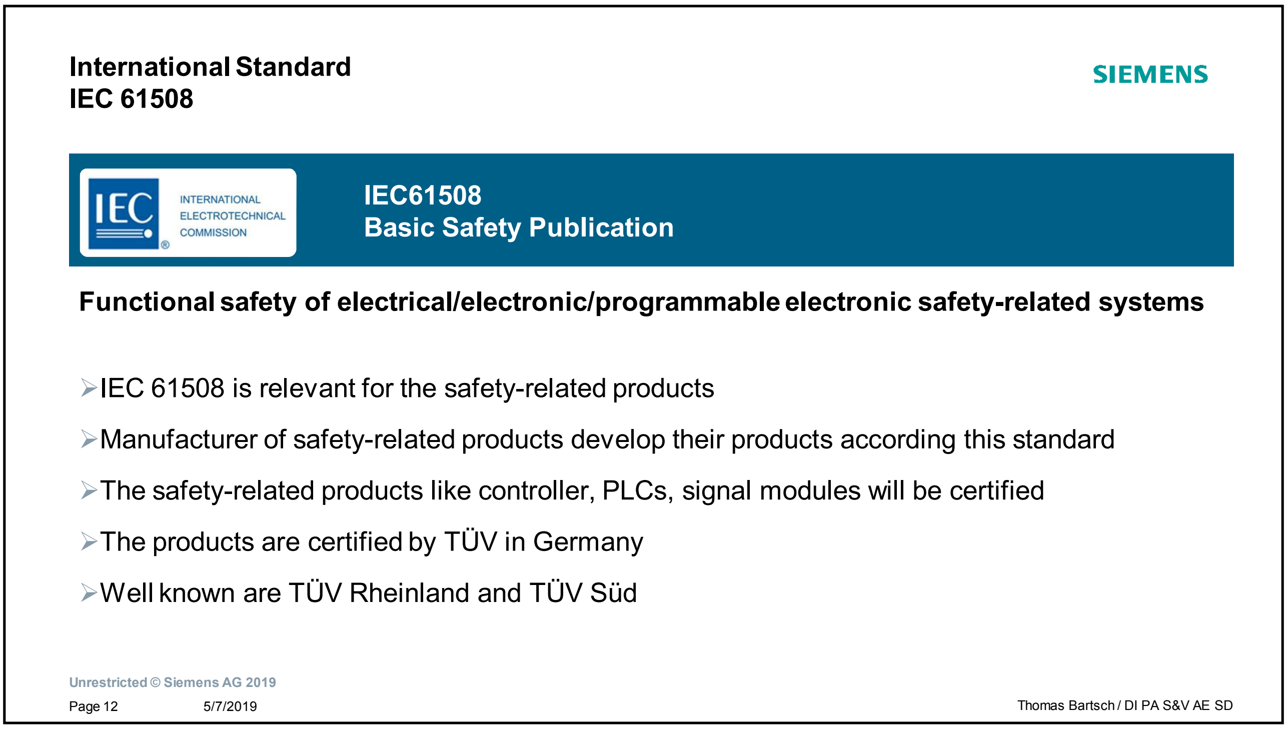
IEC 61511

SIEMENS
Ingenuity for life

Safety Integrated for Process Automation

Certified products of Siemens

Unrestricted © Siemens AG 2019 siemens.com/process-safety



International Standard IEC 61508

SIEMENS

IEC INTERNATIONAL ELECTROTECHNICAL COMMISSION

IEC61508
Basic Safety Publication

Functional safety of electrical/electronic/programmable electronic safety-related systems

- ➢IEC 61508 is relevant for the safety-related products
- ➢Manufacturer of safety-related products develop their products according this standard
- ➢The safety-related products like controller, PLCs, signal modules will be certified
- ➢The products are certified by TÜV in Germany
- ➢Well known are TÜV Rheinland and TÜV Süd

Unrestricted © Siemens AG 2019

Page 12 5/7/2019 Thomas Bartsch / DI PA S&V AE SD

International Standard
IEC 61508 – Certification bodies

SIEMENS

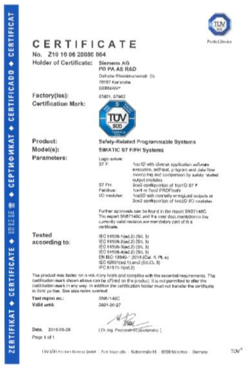
INTERNATIONAL ELECTROTECHNICAL COMMISSION

IEC61508
Certification according IEC 61508

exida®

TÜV SÜD

TÜVRheinland®



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): 07801, 07802

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 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. [illegible])

Page 1 of 1

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

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ CEPTИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

International Standard
IEC 61508 – Certification bodies

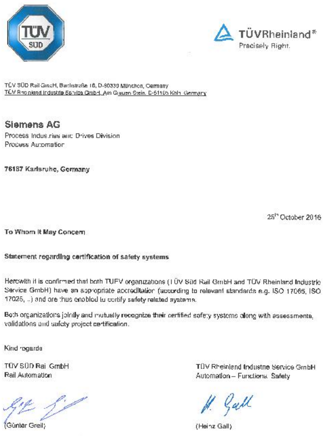
SIEMENS

The local TÜVs belong to one organization

- They accept each other

TÜV SÜD

TÜVRheinland®



TÜVRheinland®
Precisely Right.

TÜV SÜD Rail GmbH, Barthstraße 16, D-80339 München, Germany
TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, D-51105 Köln, Germany

Siemens AG
Process Industries and Drives Division
Process Automation

76187 Karlsruhe, Germany

25th October 2016

To Whom It May Concern

Statement regarding certification of safety systems

Herewith it is confirmed that both TUEV organizations (TÜV Süd Rail GmbH and TÜV Rheinland Industrie Service GmbH) have an appropriate accreditation (according to relevant standards e.g. ISO 17065, ISO 17025, ..) and are thus enabled to certify safety related systems.

Both organizations jointly and mutually recognize their certified safety systems along with assessments, validations and safety project certification.

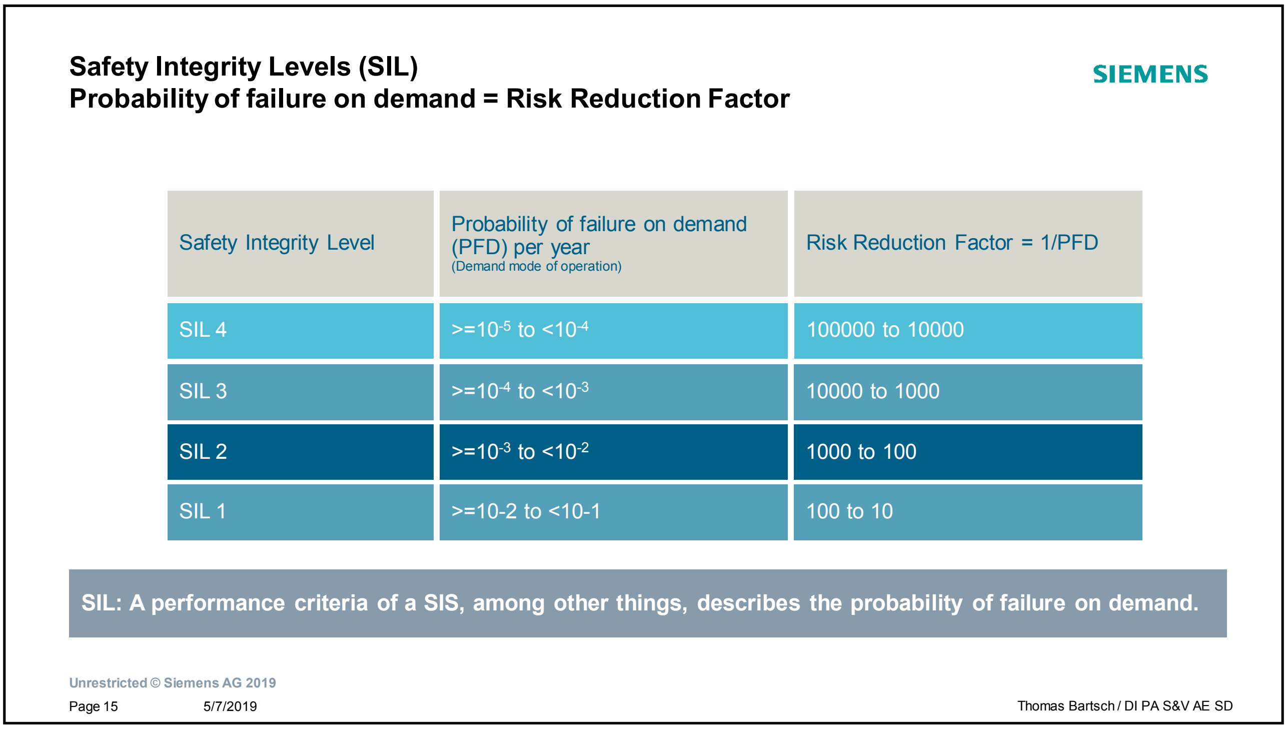
Kind regards

TÜV SÜD Rail GmbH
Rail Automation

(Günter Greil)

TÜV Rheinland Industrie Service GmbH
Automation – Functional Safety

H. Gall
(Heinz Gall)

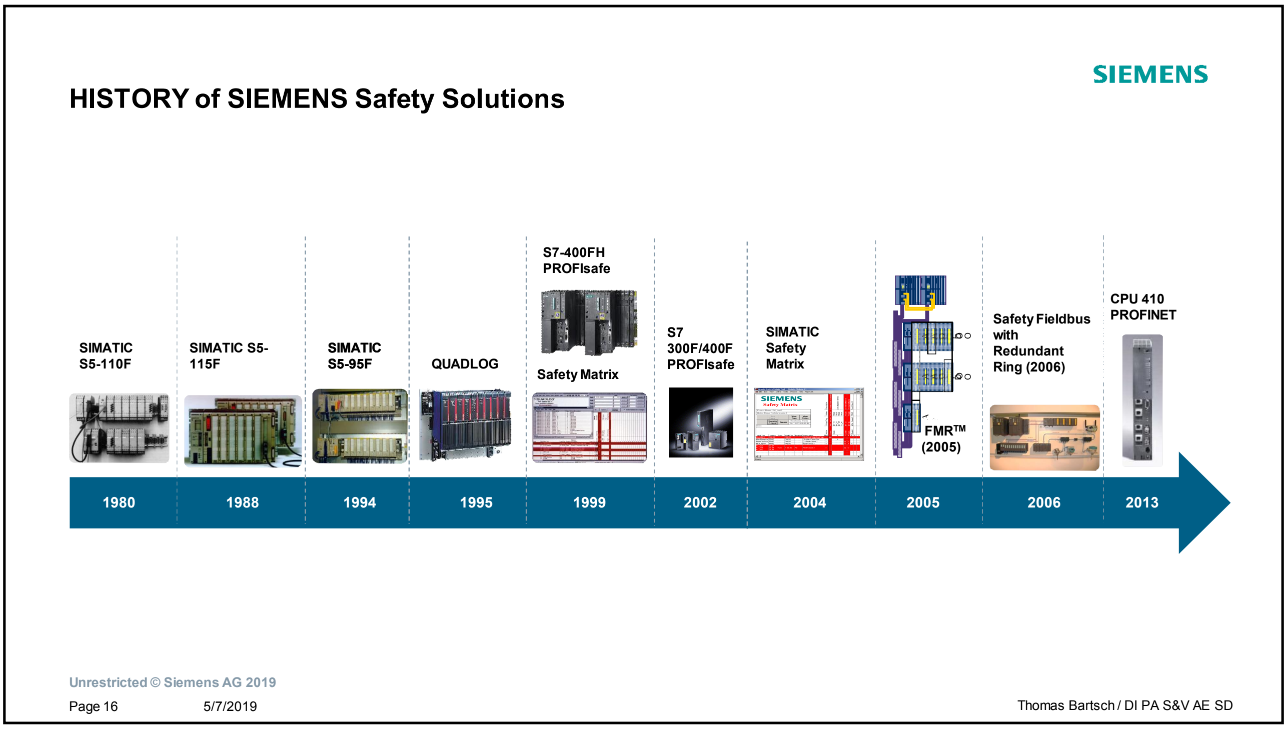


Safety Integrity Levels (SIL)
Probability of failure on demand = Risk Reduction Factor

SIEMENS

Safety Integrity Level	Probability of failure on demand (PFD) per year (Demand mode of operation)	Risk Reduction Factor = 1/PFD
SIL 4	>=10^{-5} to <10^{-4}	100000 to 10000
SIL 3	>=10^{-4} to <10^{-3}	10000 to 1000
SIL 2	>=10^{-3} to <10^{-2}	1000 to 100
SIL 1	>=10-2 to <10-1	100 to 10

SIL: A performance criteria of a SIS, among other things, describes the probability of failure on demand.



HISTORY of SIEMENS Safety Solutions

SIEMENS

Siemens
Scalable Range of Safety Controllers

The fail-safe S7-400F/FH is a powerful controller for system solutions in process and manufacturing industries:

- Based on SIMATIC F Systems Library
- Physical separation of controllers possible
- Extremely high-speed processing and communications performance
- Changes to the configuration during operation
- Failsafe and high availability versions
- Hot swapping
- The S7-410 controller is the default controller for PCS7 Safety but smaller controllers such as the S7-412 and S7-414 are available
- SIMATIC SIS compact for separated safety solutions Usable with any SCADA and DCS system

Redundant systems

Certified for the use up to SIL 3

Remote IO
Overview SIMATIC ET 200M Failsafe Modules

Features

- Two-channel I/O with integrated signal and line test and diagnostics
- Single-channel, switched, can be redundant
- Can also be used for standard operation

Modules	Features
SM 326 DI 24 24 V DC	Max. 12 x 2-channel inputs, SIL 3/Cat. 4 or. Max. 24 x 1-channel inputs, SIL 2
SM 326 DO 10 24 V DC/2A	10 x current sourcing/sourcing outputs, SIL 3/Cat. 4
SM 326 D0 8 PM	8 x current sourcing/sinking outputs, SIL 3/Cat. 4
SM 336 AI 6 13-bit	6 x 2-channel inputs, SIL 3 , HART, 0-20ma 4- 20 mA
SM 326 DI 8 NAMUR	4 x 2-channel inputs, SIL 3/Cat. 4 or 8 x 1-channel inputs, SIL 2

Remote IO for the Hazardous Area
SIMATIC ET 200iSP

SIEMENS

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, 17,4V DC 40mA
  - Analogue Input Module F-AI4 HART

Scan QR code to learn more about ET200iSP

Customer benefits:

- Reduced installation effort by using ET 200iSP compared to traditional solutions (with Ex barriers)
- Diagnostics (i.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

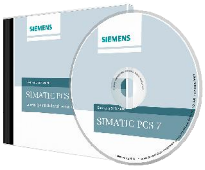
Software
SIMATIC S7 F-Systems and S7 Safety Matrix

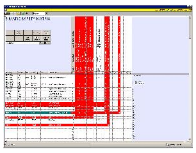
SIEMENS

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

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

- STEP 7 option package for configuring S7-400H Controller with safety functionality
- 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 CFC or on the other hand with SIMATIC S7 Safety Matrix**

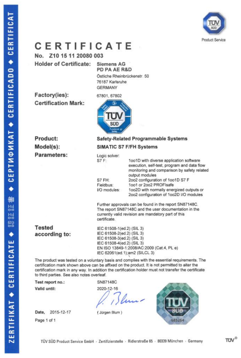
SIEMENS

Certificates

Where can you find the TUEV certificates relevant for SIMATIC S7 F/FH systems?

- ➢ https://support.industry.siemens.com/cs/ww/en/view/73192008

Scan QR code to find the relevant certificates



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

Product Service

CERTIFICATE

No. Z10 15 11 20080 003

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 comparison by safety related output modules S7 FH: 2oo2 configuration of 1oo1D S7 F Fieldbus: 1oo1 or 2oo2 PROFIsafe I/O modules: 1oo2D with normally energized outputs or 2oo2 configuration of 1oo2D I/O modules Further approvals can be found in the report SN87148C. The report SN87148C and the user documentation in the currently valid revision are mandatory part of this certificate.
Tested according to:	IEC 61508-1(ed.2) (SIL 3) IEC 61508-2(ed.2) (SIL 3) IEC 61508-3(ed.2) (SIL 3) IEC 61508-4(ed.2) (SIL 3) EN ISO 13849-1:2008/AC:2009 (Cat.4, PL e) IEC 62061(ed.1);am2 (SILCL 3)

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:	2020-12-16

Date, 2015-12-17

(Jürgen Blum)

685264

Page 1 of 1

A1 / 04.11

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

SIEMENS
Ingenuity for life

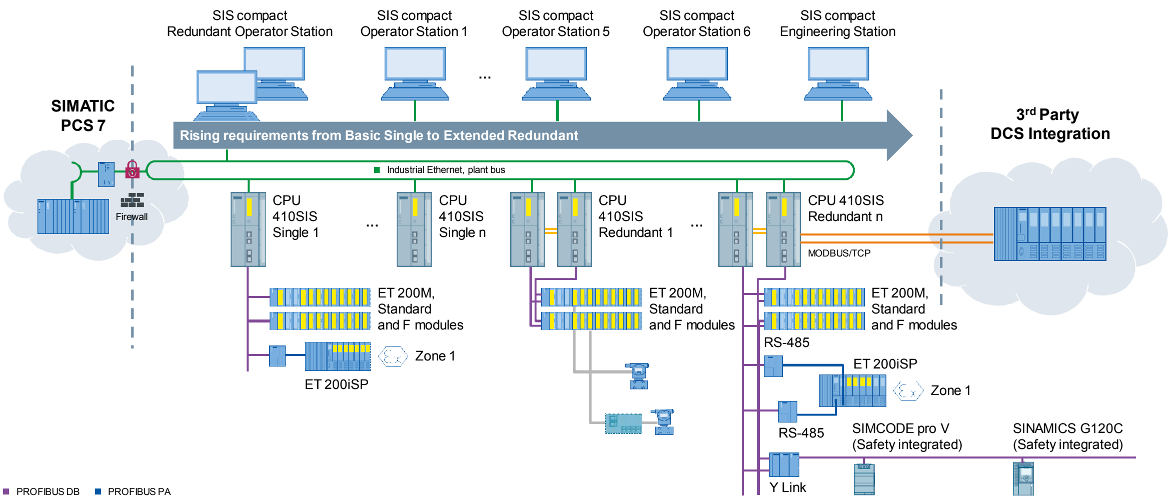
Safety Integrated for Process Automation

SIMATIC SIS compact

siemens.com/process-safety

SIMATIC SIS compact
Overview

SIEMENS

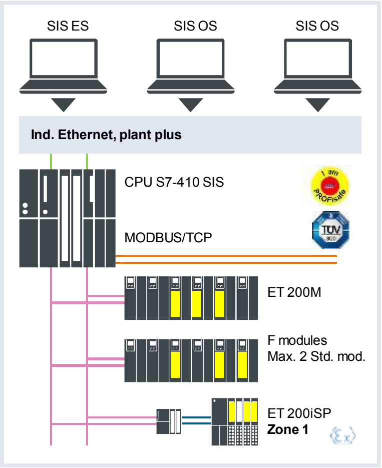


SIMATIC SIS compact
Description

SIEMENS

SIMATIC SIS compact

- ... is designed as a dedicated, lean Safety Instrumented System (SIS) offering, based on the SIMATIC portfolio
- … consists of SIS hardware and software
- … is streamlined in its functionality and price structure
- … meets the market requirements of small to mid-size safety applications
- … covers 4 preconfigured bundles for different use cases



Key Benefits

✓ Increased safety → Tailored to your requirements
✓ Flexible implementation → Independent from DCS system
✓ Cost efficient → Through specific bundles

SIMATIC SIS compact
Hardware

SIEMENS

SIMATIC CPU 410SIS

- Standalone safety controller
- Based on CPU410
- 4MB work memory
- Same communication and IO limits like CPU 410E
- Exclusively for SIMATIC SIS compact

Highlights

- Non-volatile load memory
- SysLog Support
- Conformal Coating
- Usage up to 70°C
- Innovations via Firmware update

SEC E4MB

SIMATIC SIS compact
Software

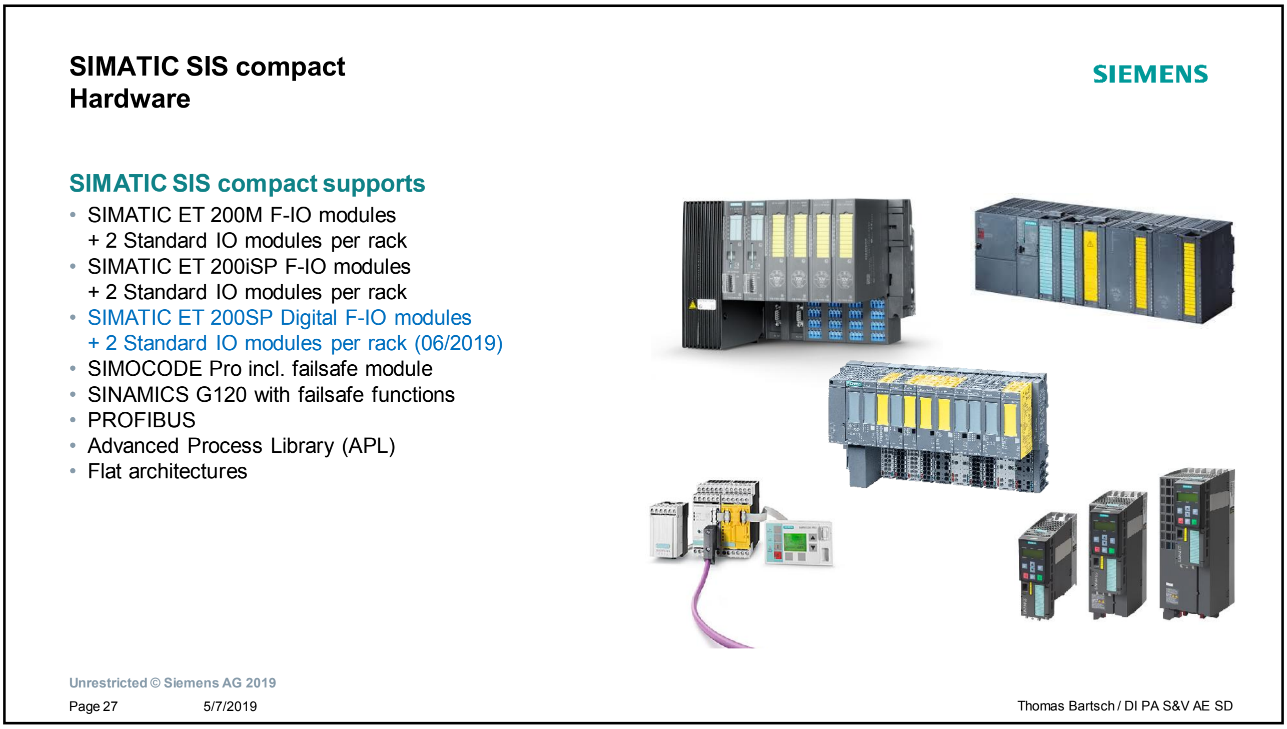
SIEMENS

ES Single Station SIS (AS/OS: PO 200)

- APL Support
- No SFC
- No Batch and Route Control
- Upgrade with SIMATIC PCS 7 PO licenses

AS Engineering Package SIS (PO unlim.)

- APL Support
- No SFC
- No Batch and Route Control



SIMATIC SIS compact
Hardware

SIEMENS

SIMATIC SIS compact supports

- SIMATIC ET 200M F-IO modules
  + 2 Standard IO modules per rack
- SIMATIC ET 200iSP F-IO modules
  + 2 Standard IO modules per rack
- SIMATIC ET 200SP Digital F-IO modules
  + 2 Standard IO modules per rack (06/2019)
- SIMOCODE Pro incl. failsafe module
- SINAMICS G120 with failsafe functions
- PROFIBUS
- Advanced Process Library (APL)
- Flat architectures

Page 27 5/7/2019 Thomas Bartsch / DI PA S&V AE SD

DRAFT

SIEMENS
Ingenuity for life

SIMATIC S7 Safety Matrix

The Management Tool for all Phases of the Safety Lifecycle

siemens.com/process-safety

SIMATIC S7 Safety Matrix
Safety Engineering and Monitoring made easy

SIEMENS

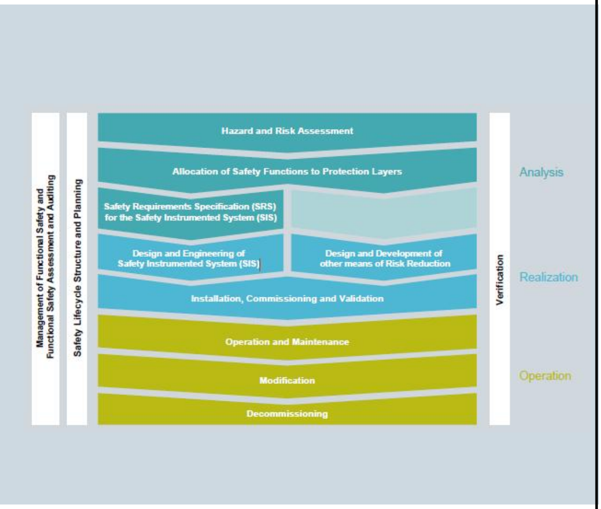
SIMATIC S7 Safety Matrix – the Safety Management Tool

Functional safety and Safety Lifecycle Management

The installation and operation of potentially dangerous plants in the process industry are subject to the international standard IEC 61511, the standard for the functional safety of Safety Instrumented Systems (SIS).

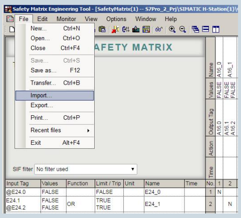
The procedure for implementing functional safety is described in this standard in accordance with the safety lifecycle of the plant, which is usually divided into the following three phases:

- **Analysis/Specification**
- **Realization/Engineering**
- **Operation/Maintenance**


Management of Functional Safety and Functional Safety Assessment and Auditing
Safety Lifecycle Structure and Planning
Hazard and Risk Assessment
Allocation of Safety Functions to Protection Layers
Safety Requirements Specification (SRS) for the Safety Instrumented System (SIS)
Design and Engineering of Safety Instrumented System (SIS)
Design and Development of other means of Risk Reduction
Installation, Commissioning and Validation
Operation and Maintenance
Modification
Decommissioning
Verification
Analysis
Realization
Operation

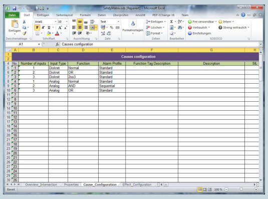
SIMATIC S7 Safety Matrix
At a glance

SIEMENS



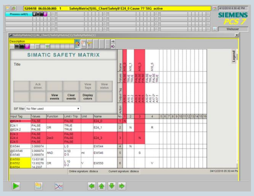
Input Tag	Values	Function	Limit / Trip	Unit	Name	Time	No.	1	2
@E24.0	FALSE		FALSE		E24_0		1	N	
E24.1 @E24.2	FALSE FALSE	OR	TRUE TRUE		E24_1		2		N

Easy understandable engineering due Cause & Effect matrix with new bypassing and degraded voting



Import and Export to a spreadsheet for simplified, effective and cost-efficient engineering

Usable with SIMATIC PCS 7 and SIMATIC SIS compact



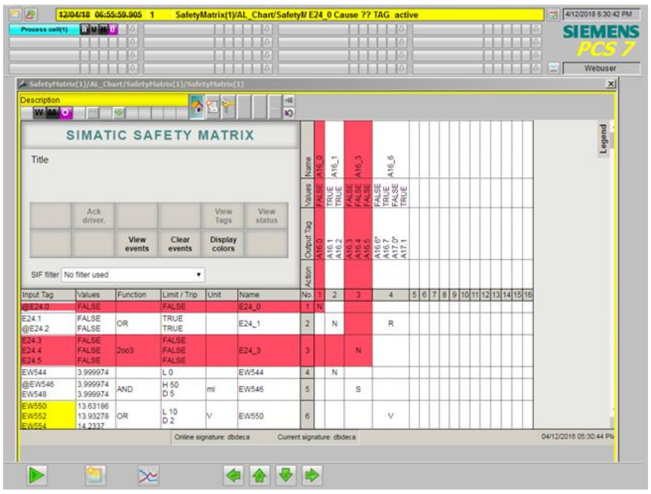
OS Web Client support for SIMATIC Safety Viewer with optional release via key switch

Improved monitoring function: new dynamic color schemes, acknowledgement and central simulation deactivation

SIMATIC Safety Matrix V6.3
Overview

SIEMENS

- SM Viewer web enabled
- Tag Bypass & Degraded Voting
- Import / Export
- Multiple Ack & Reset
- Time limited Cause Bypass
- Improved print function
- Support of bulk engineering



Name	Values	Output Tag	Action	No.
A16_0	FALSE	A16.0		1
A16_1	TRUE TRUE	A16.1 A16.2		2
A16_3	FALSE FALSE FALSE	A16.3 A16.4 A16.5		3
A16_6	FALSE TRUE FALSE TRUE	A16.6* A16.7 A17.0* A17.1		4

Input Tag	Values	Function	Limit / Trip	Unit	Name	No.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
@E24.0	FALSE		FALSE		E24_0	1	N															
E24.1 @E24.2	FALSE FALSE	OR	TRUE TRUE		E24_1	2		N		R												
E24.3 E24.4 E24.5	FALSE FALSE FALSE	2oo3	FALSE FALSE FALSE		E24_3	3			N													
EW544	3.999974		L 0		EW544	4		N														
@EW546 EW548	3.999974 3.999974	AND	H 50 D 5	ml	EW546	5			S													
EW550 EW552 EW554	13.63186 13.93278 14.2337	OR	L 10 D 2	V	EW550	6				V												

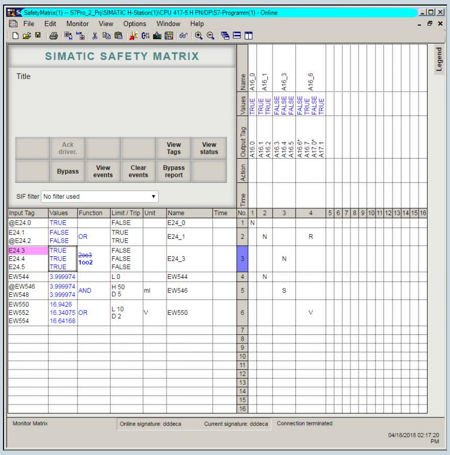
Online signature: dbdeca Current signature: dbdeca 04/12/2018 05:30:44 PM

SIMATIC S7 Safety Matrix
Safety Engineering and Monitoring made easy

SIEMENS

SIMATIC S7 Safety Matrix easy engineering

- operational in SIMATIC PCS 7 and SIMATIC SIS compact
- Fully integrated or separated, it is your choice
- No programming knowledge required
- Easy understandable for everyone with engineering due Cause & Effect matrix (C&E)
- Concise overview of the safety function (SIF)



Name	Values	Output Tag	Action	Time	No.
A16_0	TRUE	A16.0			1
A16_1	TRUE TRUE	A16.1 A16.2			2
A16_3	FALSE FALSE FALSE	A16.3 A16.4 A16.5			3
A16_6	FALSE TRUE FALSE TRUE	A16.6* A16.7 A17.0* A17.1			4

Input Tag	Values	Function	Limit / Trip	Unit	Name	Time	No.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
@E24.0	TRUE		FALSE		E24_0		1	N															
E24.1 @E24.2	FALSE FALSE	OR	TRUE TRUE		E24_1		2		N		R												
E24.3 E24.4 E24.5	TRUE TRUE TRUE	~~2oo3~~ 1oo2	FALSE FALSE FALSE		E24_3		3			N													
EW544	3.999974		L 0		EW544		4		N														
@EW546 EW548	3.999974 3.999974	AND	H 50 D 5	ml	EW546		5			S													
EW550 EW552 EW554	16.9426 16.34075 16.64168	OR	L 10 D 2	V	EW550		6				V												
							7																
							8																
							9																
							10																
							11																
							12																
							13																
							14																
							15																
							16																

Monitor Matrix Online signature: dddeca Current signature: dddeca Connection terminated 04/18/2018 02:17:20 PM

SIMATIC S7 Safety Matrix
Safety Engineering and Monitoring made easy

SIEMENS

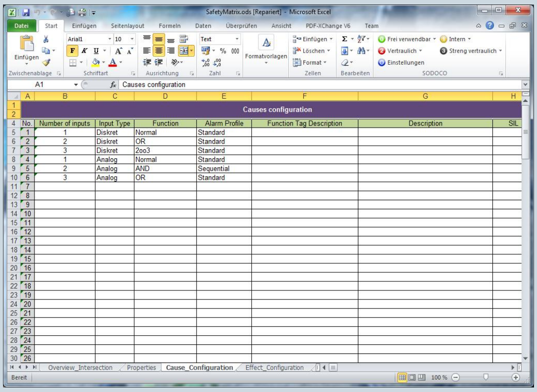
Effective and cost-efficient engineering

Import and Export for simplified and cost-efficient engineering

Import and Export
Cause & Effect matrix can be imported and exported via a spreadsheet in “Open Office Calc”-Format

Spreadsheet
For a better handling the spreadsheet is split in several sheets, general information and C&E relevant information.

Bulk-engineering is part of the SIMATIC S7 Safety Matrix
Pre-definition of the safety loops and function
Implementation of base template in the spreadsheet
Duplication and adaption of the safety functions
Safe time during engineering and start-up earlier



SafetyMatrix.ods [Repariert] - Microsoft Excel

A1 Causes configuration

Causes configuration

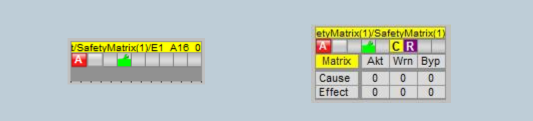
No.	Number of inputs	Input Type	Function	Alarm Profile	Function Tag Description	Description	SIL
1	1	Diskret	Normal	Standard			
2	2	Diskret	OR	Standard			
3	3	Diskret	2oo3	Standard			
4	1	Analog	Normal	Standard			
5	2	Analog	AND	Sequential			
6	3	Analog	OR	Standard			
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							
22							
23							
24							
25							
26							

SIMATIC S7 Safety Matrix
Safety Engineering and Monitoring made easy

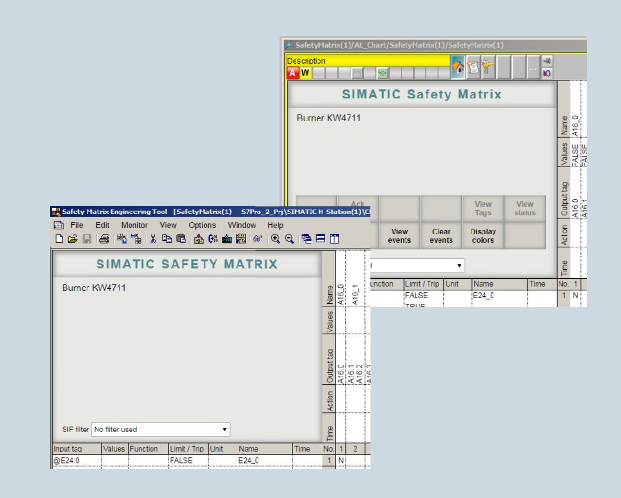
SIEMENS

SIMATIC S7 Safety Matrix easy engineering

- Multiple Safety Matrix in a safety system (SIS)
- 128 causes per matrix
- 128 effects per matrix
- 1024 intersections per matrix
- Up to 3 inputs per cause
- Up to 4 outputs per effect
- New Design, APL style for Safety Matrix



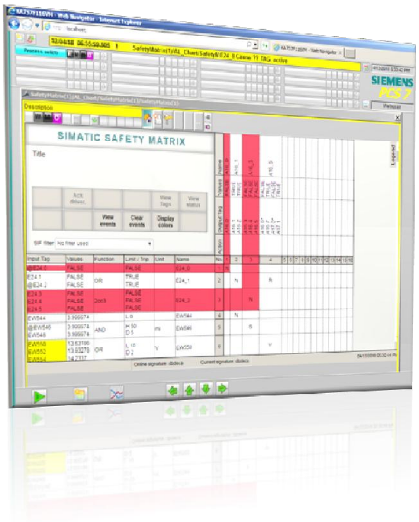
Matrix	Akt	Wrn	Byp
Cause	0	0	0
Effect	0	0	0



SIMATIC Safety Matrix V6.3
Viewer Web enabled

SIEMENS

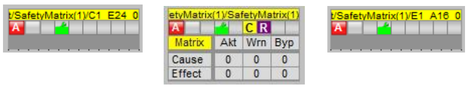
- Safety Matrix Engineering Tool and Viewer completely rebuild based on HTML 5 technology.
- PCS7 OS Web Client support for Safety Matrix Viewer
- Use Case:
  Remote monitoring of a site with Safety System via Web connection.
- Security aspects
    - Two step sequence (initiator/confirmer) including time limitation for remote control
    - Optional local release of via key switch



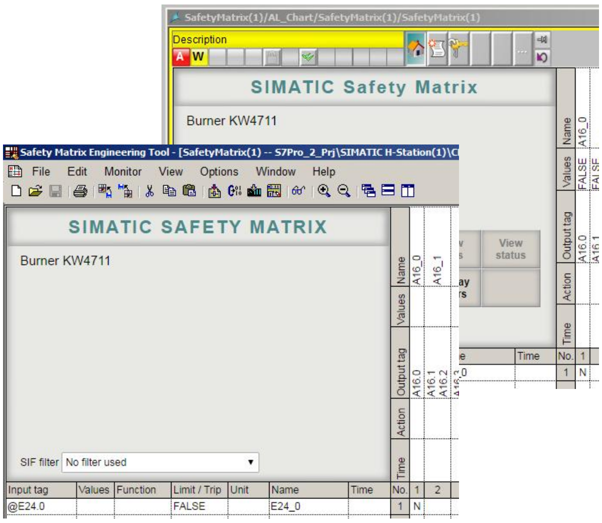
SIMATIC Safety Matrix V6.3
New Design

SIEMENS

- APL style for Safety Matrix Viewer and block icon
    - Faceplate overview and tab selection
    - Alarm control
    - Viewer dialogues
- Simatic Manager Design in SM Engineering Tool


/SafetyMatrix(1)/C1_E24_0
A
etyMatrix(1)/SafetyMatrix(1)
A
C
R
/SafetyMatrix(1)/E1_A16_0
A

Matrix	Akt	Wrn	Byp
Cause	0	0	0
Effect	0	0	0



Burner KW4711

SIF filter: No filter used

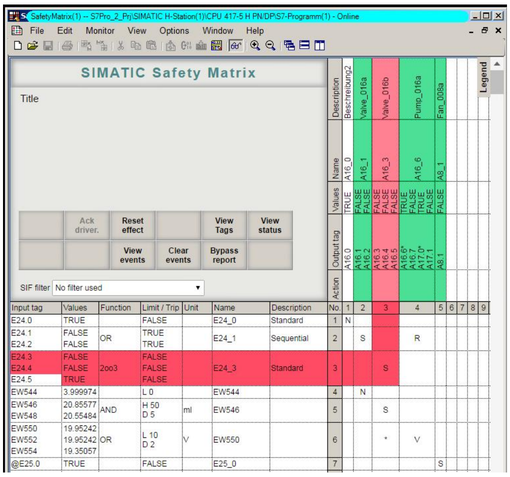
Input tag	Values	Function	Limit / Trip	Unit	Name	Time	No.	1	2
@E24.0			FALSE		E24_0		1	N	

SIMATIC Safety Matrix V6.3

Multiple reset / acknowledgement

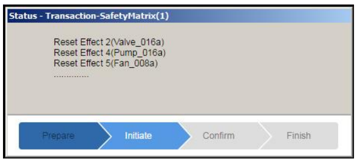
SIEMENS

- Multiple ack of selected acknowledgeable causes via "Ack Cause" button
- Multiple reset of resetable effects via "Reset Effect" button
- Use Case:
  After a plant shut-down with several trip requests it is now possible to bring the matrix back in to "good status" much quicker. No need to invidually ack each single cause, reset each single effect.



No.	1	2	3	4	5	6	7	8	9
Description	Beschreibung2	Valve_016a	Valve_016b	Pump_016a	Fan_008a				
Name	A16_0	A16_1	A16_3	A16_6	A8_1				
Values	TRUE	FALSE FALSE	FALSE FALSE FALSE	TRUE FALSE TRUE FALSE	FALSE				
Output tag	A16.0	A16.1 A16.2	A16.3 A16.4 A16.5	A16.6* A16.7 A17.0* A17.1	A8.1				
Action									

Input tag	Values	Function	Limit / Trip	Unit	Name	Description	No.	1	2	3	4	5	6	7	8	9
E24.0	TRUE		FALSE		E24_0	Standard	1	N								
E24.1 E24.2	FALSE FALSE	OR	TRUE TRUE		E24_1	Sequential	2		S		R					
E24.3 E24.4 E24.5	FALSE FALSE TRUE	2oo3	FALSE FALSE FALSE		E24_3	Standard	3			S						
EW544	3.999974		L 0		EW544		4		N							
EW546 EW548	20.85577 20.55484	AND	H 50 D 5	ml	EW546		5			S						
EW550 EW552 EW554	19.95242 19.95242 19.35057	OR	L 10 D 2	V	EW550		6			*	V					
@E25.0	TRUE		FALSE		E25_0		7					S				


Status - Transaction-SafetyMatrix(1)

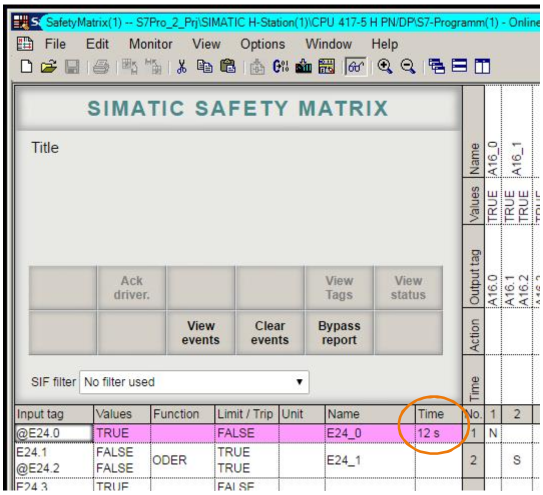
Reset Effect 2(Valve_016a)
Reset Effect 4(Pump_016a)
Reset Effect 5(Fan_008a)
....

SIMATIC Safety Matrix V6.3

Cause: time limited Soft-Bypass Function

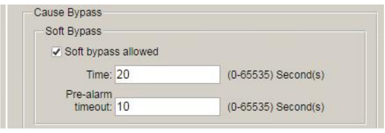
SIEMENS

- time limit and pre-alarm timeout now available for Soft Bypass function
- Cause configuration dialogue (Cause details -> Options)
- Use Cases for temporary bypasses:
  - Bypassing plant conditions like start-ups, shutdowns, and process transitions
  - Bypassing of safety critical equipment for maintenance or repair



No.	1	2
Name	A16_0	A16_1
Values	TRUE	TRUE TRUE
Output tag	A16.0	A16.1 A16.2
Action		
Time		

Input tag	Values	Function	Limit / Trip	Unit	Name	Time	No.	1	2
@E24.0	TRUE		FALSE		E24_0	12 s	1	N	
E24.1 @E24.2	FALSE FALSE	ODER	TRUE TRUE		E24_1		2		S
E24.3	TRUE		FALSE						


Cause Bypass

Soft Bypass

☑ Soft bypass allowed

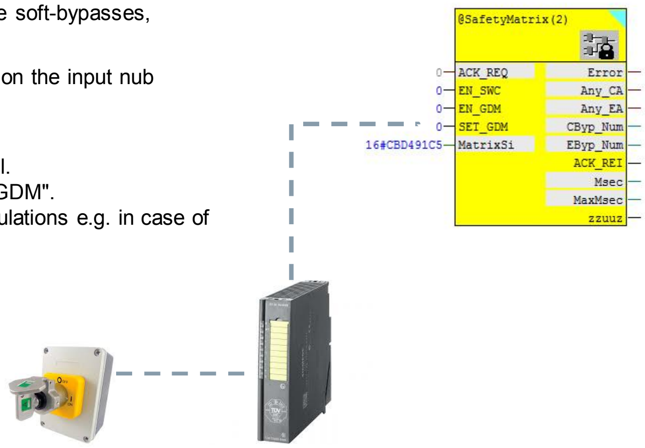
Time: 20 (0-65535) Second(s)

Pre-alarm timeout: 10 (0-65535) Second(s)

SIMATIC Safety Matrix V6.3
Central deactivation of simulation and bypasses

SIEMENS

- New inputs EN_GDM, SET_GDM on @Matrix block
- EN_GDM enables the external reset of all active soft-bypasses, simulations and overrides for causes/effects.
- The reset function is activated by a High signal on the input nub SET_GDM.
- Use Case:
  Hardware key switch connected to F-DI channel.
  Signal connected to the new block nub " SET_GDM".
  Possible to deactivate the made bypasses /simulations e.g. in case of unavailabilty of the visualisation.



Safety vs. Standard applications

SIEMENS

WhenShouldIuseSafety.mp4

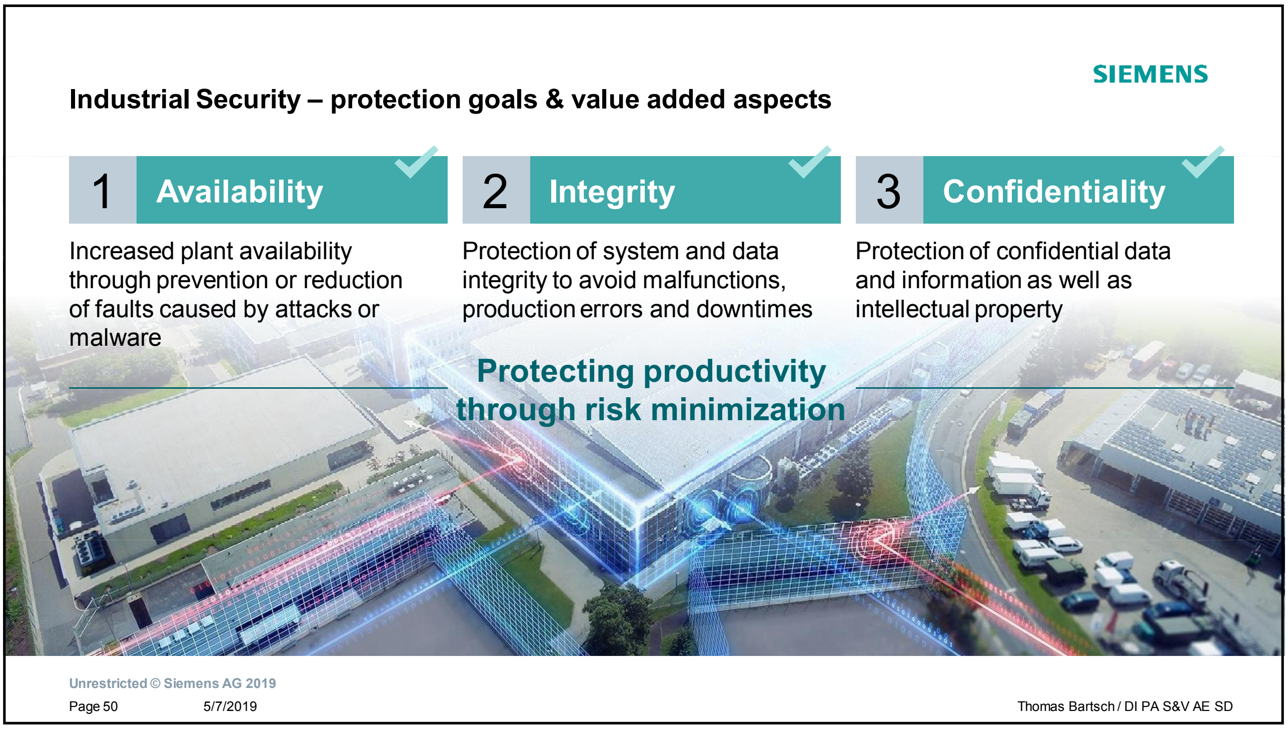
Industrial Security

Protecting Productivity

siemens.com/industrial-security

Safety Approach

Functional Safety reduces the risk of process related accidents and ensures maximum safety for:



SIEMENS

Industrial Security – protection goals & value added aspects

1 **Availability** ✓

Increased plant availability through prevention or reduction of faults caused by attacks or malware

2 **Integrity** ✓

Protection of system and data integrity to avoid malfunctions, production errors and downtimes

3 **Confidentiality** ✓

Protection of confidential data and information as well as intellectual property

Protecting productivity through risk minimization

Unrestricted © Siemens AG 2019

Page 50 5/7/2019 Thomas Bartsch / DI PA S&V AE SD

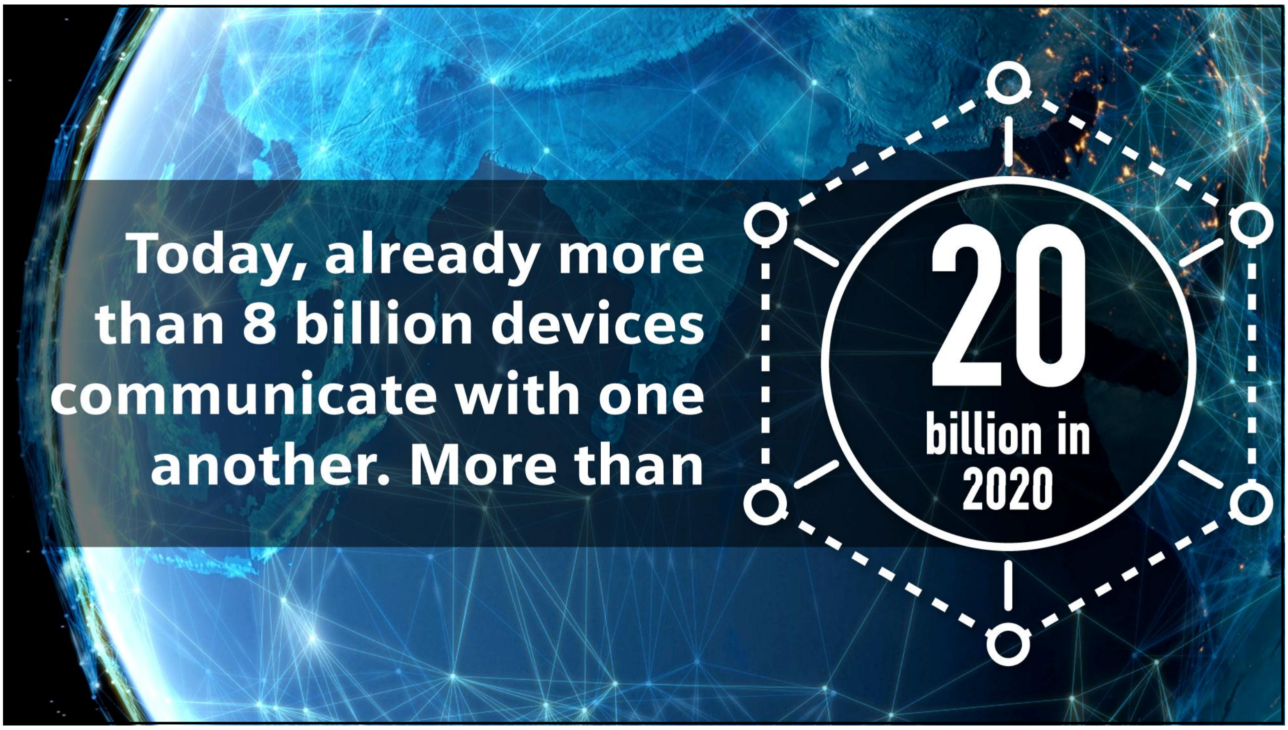
SIEMENS
Ingenuity for life

Stay secure in the age of digitalization

Cyber crime is wide spread and costs the global economy US$400 billion by annually.[1]
Cyber attacks are impacting companies of all sizes, in all markets

[1] Estimate by Center for Strategic and International Studies, Washington, D.C.

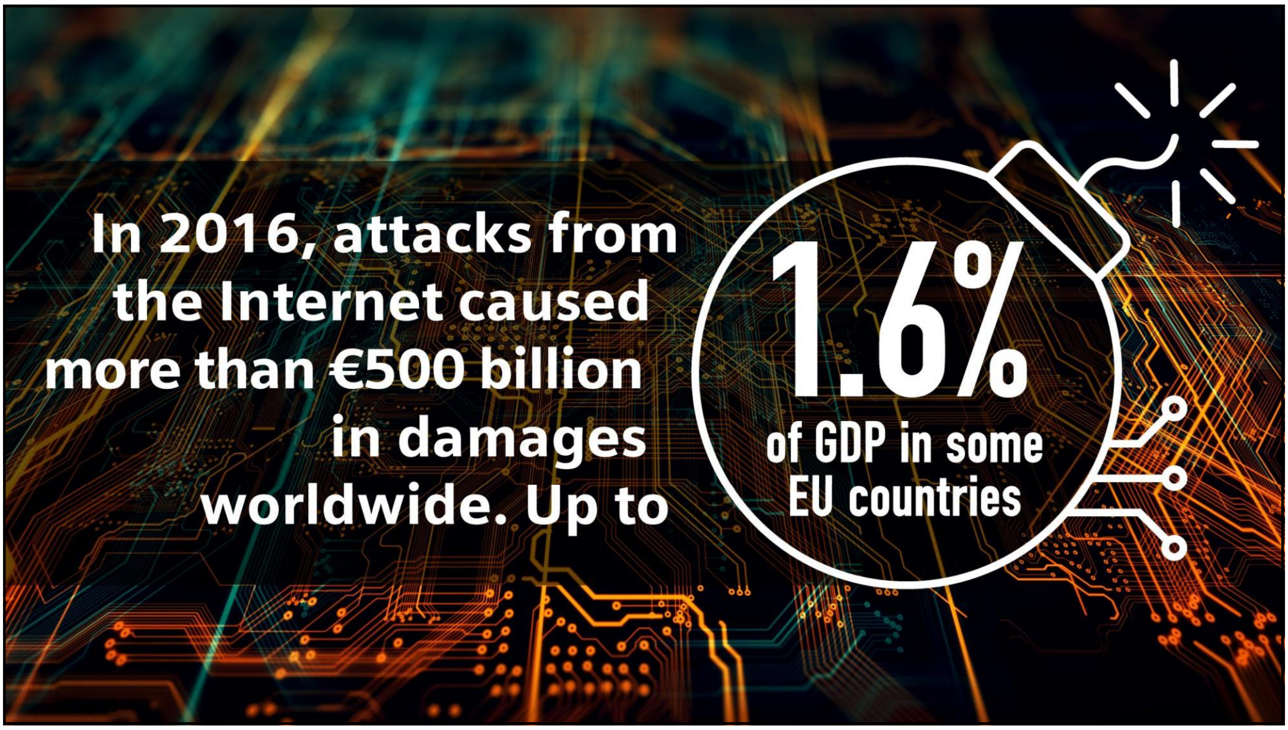
Page 51



Today, already more than 8 billion devices communicate with one another. More than

20

billion in 2020

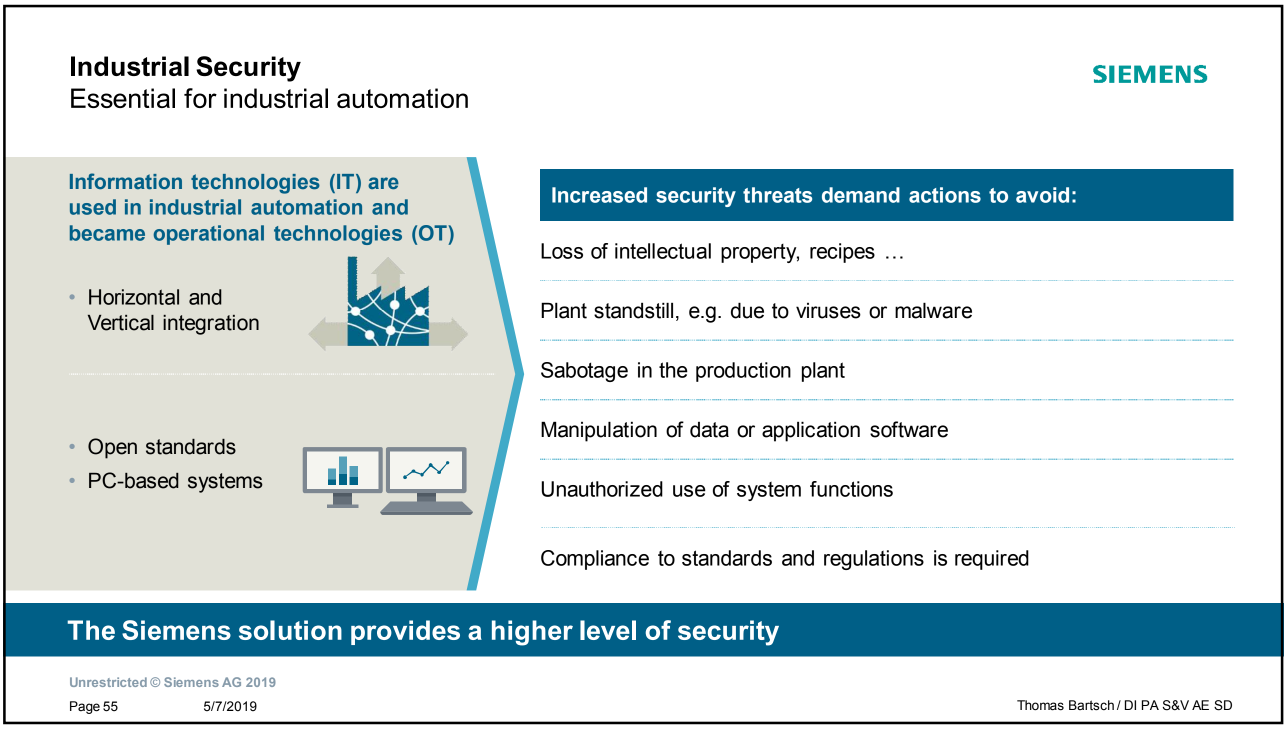


In 2016, attacks from the Internet caused more than €500 billion in damages worldwide. Up to

1.6%

of GDP in some EU countries

Malware, malicious code, denial of service and industrial espionage are the common types of cyber attacks.



Industrial Security

Essential for industrial automation

SIEMENS

Information technologies (IT) are used in industrial automation and became operational technologies (OT)

- Horizontal and Vertical integration

- Open standards
- PC-based systems

Increased security threats demand actions to avoid:

Loss of intellectual property, recipes …

Plant standstill, e.g. due to viruses or malware

Sabotage in the production plant

Manipulation of data or application software

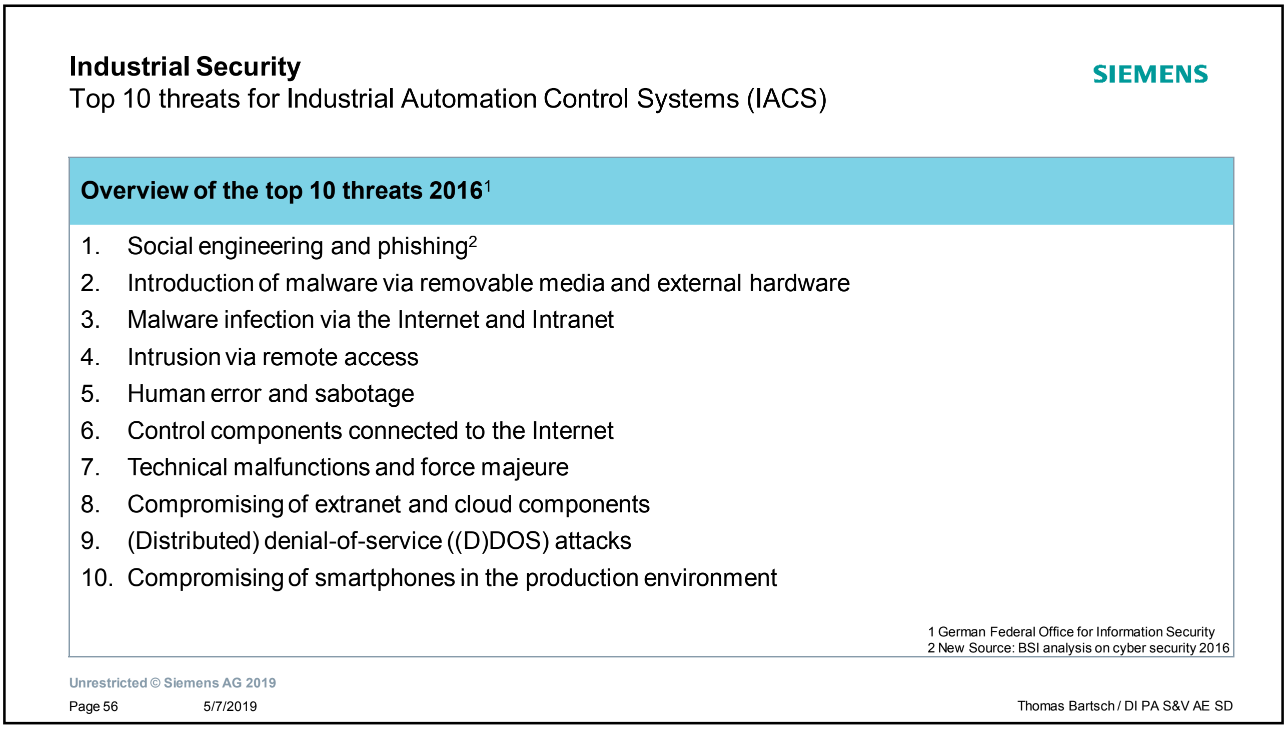
Unauthorized use of system functions

Compliance to standards and regulations is required

The Siemens solution provides a higher level of security

Unrestricted © Siemens AG 2019

Page 55 5/7/2019 Thomas Bartsch / DI PA S&V AE SD



Industrial Security

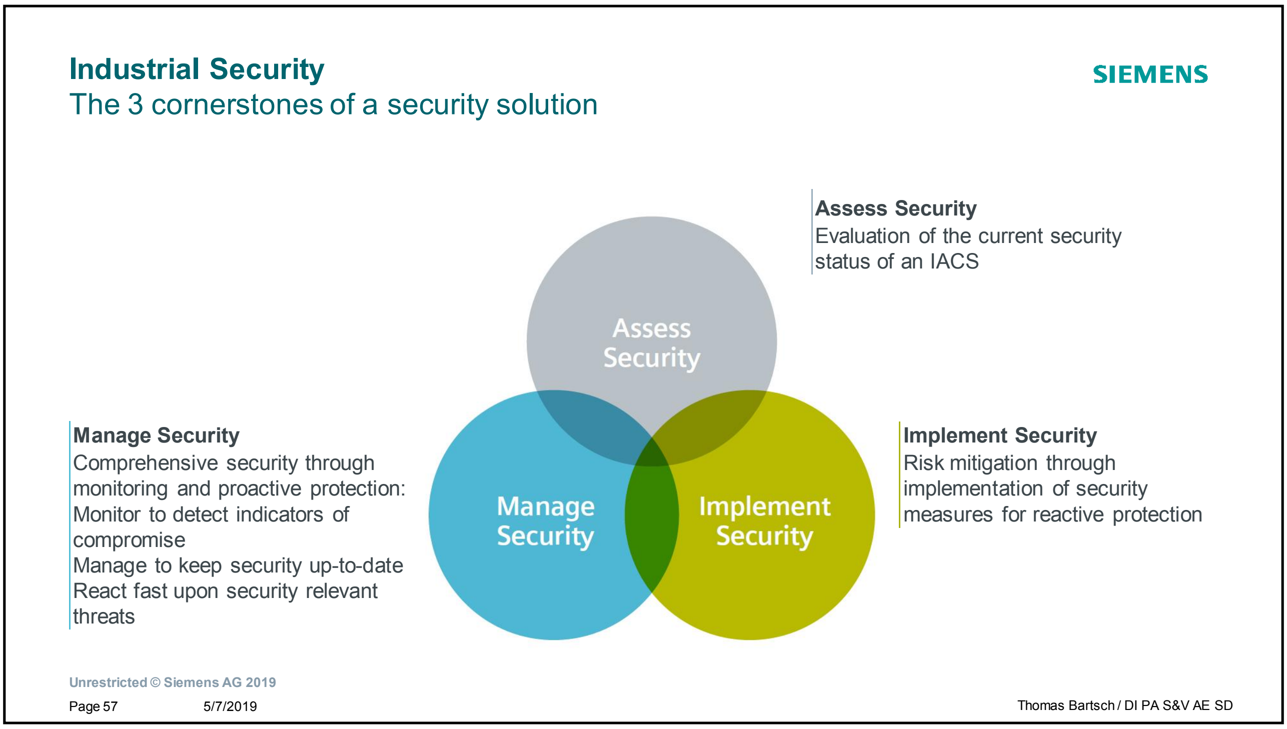
Top 10 threats for Industrial Automation Control Systems (IACS)

SIEMENS

Overview of the top 10 threats 2016[1]

1. Social engineering and phishing[2]
2. Introduction of malware via removable media and external hardware
3. Malware infection via the Internet and Intranet
4. Intrusion via remote access
5. Human error and sabotage
6. Control components connected to the Internet
7. Technical malfunctions and force majeure
8. Compromising of extranet and cloud components
9. (Distributed) denial-of-service ((D)DOS) attacks
10. Compromising of smartphones in the production environment

[1] German Federal Office for Information Security
[2] New Source: BSI analysis on cyber security 2016



Industrial Security

The 3 cornerstones of a security solution

SIEMENS

Assess Security
Evaluation of the current security status of an IACS

Manage Security
Comprehensive security through monitoring and proactive protection:
Monitor to detect indicators of compromise
Manage to keep security up-to-date
React fast upon security relevant threats

Implement Security
Risk mitigation through implementation of security measures for reactive protection

Scope of IEC 62443

Security is about technology, processes and people

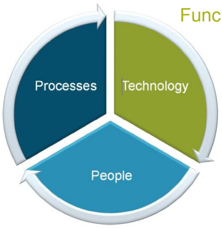
SIEMENS

The standard IEC 62443 addresses the security of an:

- Industrial Automation and Control System (IACS)

The definition of an IACS includes everything

- The technical automation solution
- The policies and procedures (Processes) required for the operation and maintenance of the automation solution and process plant
- The personnel involved in the operation and maintenance of the process plant



Functional security measures

Policies and Procedures

Competency

Important parts of IEC 62443
Defense in Depth Concept

SIEMENS

IEC 62443-3-3 System security and security levels

- Specifies the technical requirements for control systems and addresses the **Product Suppliers**

IEC 62443-2-4 Requirements for IACS solution suppliers

- Specifies the requirements for the policies and procedures of **System Integrators** and **Maintenance Service Providers**

IEC 62443-2-1 Requirements for an IACS security management system

- Specifies the organizational measures and processes for the **Asset Owners**

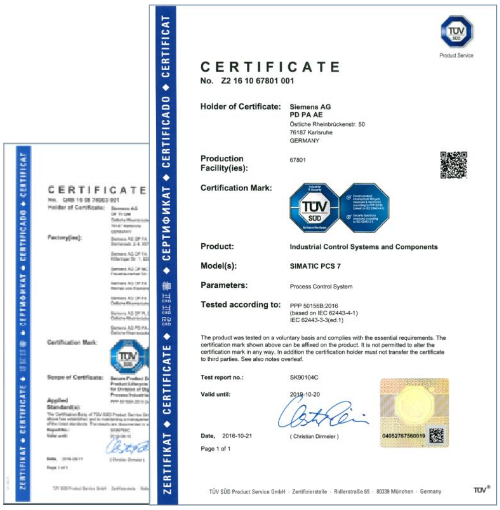
Defense in Depth involves all stakeholders:
Asset Owner, System Integrator and Product Supplier

TÜV certification according to IEC 62443 for SIMATIC PCS 7
IEC 62443-3-3 and IEC 62443-4-1

SIEMENS

TÜV SÜD certifies the Siemens SIMATIC PCS 7 process control system

- Conformity with the security standards IEC 62443-4-1 and IEC 62443-3-3
- SIMATIC PCS 7 is the first product to be certified by TÜV SÜD according to IEC 62443
- Comprehensive security measures and functions for securing plant operation



CERTIFICATE

No. Z2 16 10 67801 001

Holder of Certificate: Siemens AG
PD PA AE
Östliche Rheinbrückenstr. 50
76187 Karlsruhe
GERMANY

Production Facility(ies): 67801

Certification Mark:

Product: Industrial Control Systems and Components

Model(s): SIMATIC PCS 7

Parameters: Process Control System

Tested according to: PPP 50156B:2016
(based on IEC 62443-4-1)
IEC 62443-3-3(ed.1)

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.: SK90104C

Valid until: 2019-10-20

Date, 2016-10-21

(Christian Dirmeier)

04052767560019

Page 1 of 1

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

ZERTIFIKAT ◆ CERTIFICATE ◆ 認証証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT
TÜV SÜD
Product Service

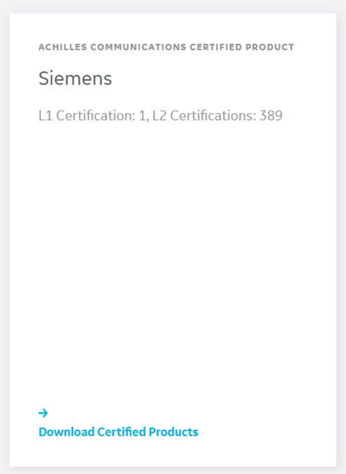
Certified Products

SIEMENS

Achilles Communications Certified Products

- https://www.ge.com/digital/applications/achilles-communications-certified-products

	SIMATIC S7-400 CPU 412-2 PN SIMATIC S7-400 CPU 414-3 PN/DP SIMATIC S7-400 CPU 416-3 PN/DP SIMATIC S7-400 CPU 414F-3 PN/DP SIMATIC S7-400 CPU 416F-3 PN/DP	Apr 18	6ES7412-2EK07-0AB0 6ES7414-3EM07-0AB0 6ES7416-3ES07-0AB00 6ES7414-3FM07-0AB0 6ES7416-3FS07-0AB0	V7.0x
	SIMATIC PCS 7 CPU 410-5H Process Automation SIMATIC PCS 7 CPU 410E Process Automation SIMATIC PCS 7 CPU 410SMART Process Automation	Apr 18	6ES7410-5HX08-0AB0 6ES7410-5HM08-0AB0 6ES7410-5HN08-0AB0	V8.2x
	SIMATIC S7 CPU 410SIS Safety Controller	Apr 18	6ES7410-5FM08-0AB0	V8.2x



ACHILLES COMMUNICATIONS CERTIFIED PRODUCT

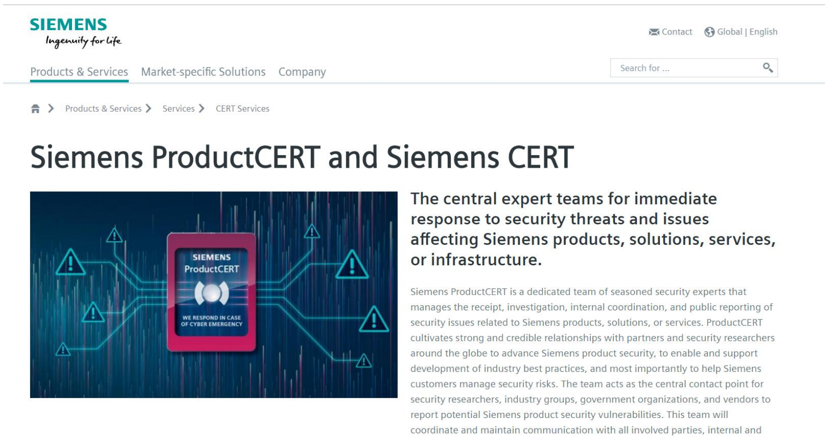
Siemens

L1 Certification: 1, L2 Certifications: 389

→
Download Certified Products

SIEMENS

https://new.siemens.com/global/en/products/services/cert.html#SecurityPublications



SIEMENS
Ingenuity for life

Siemens ProductCERT and Siemens CERT

The central expert teams for immediate response to security threats and issues affecting Siemens products, solutions, services, or infrastructure.

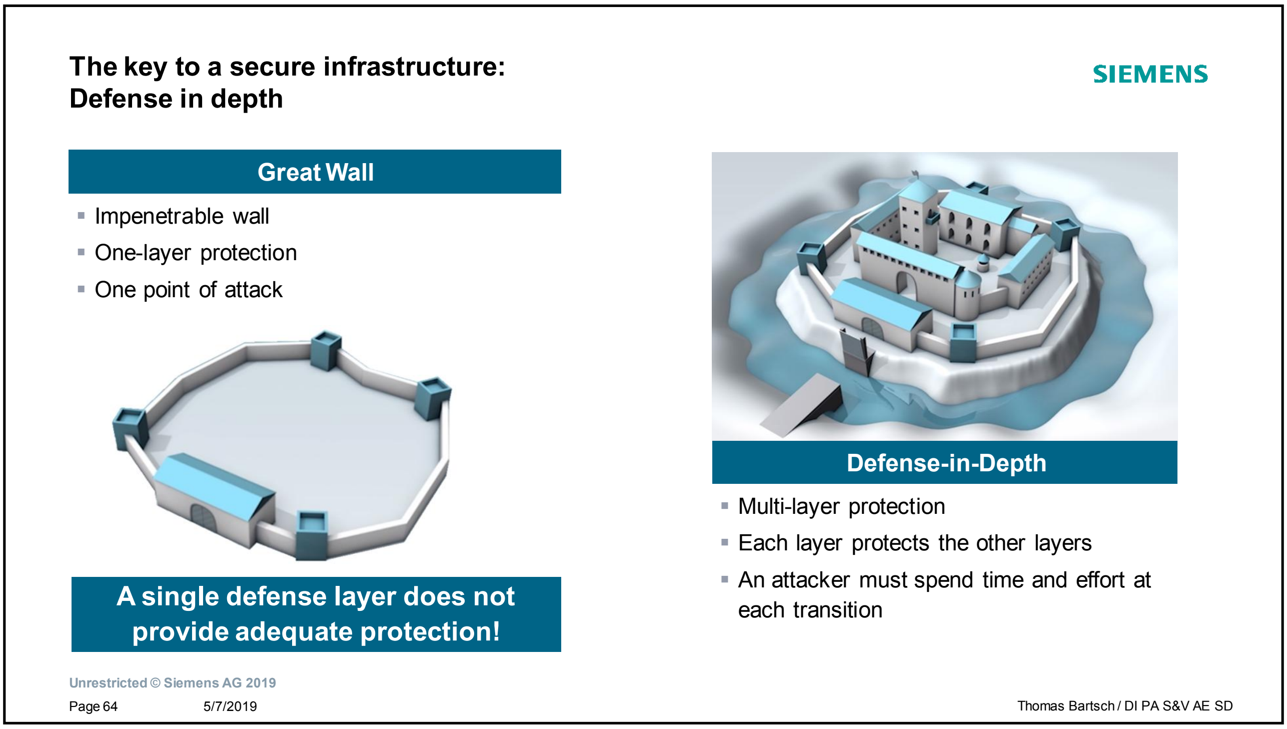
Siemens ProductCERT is a dedicated team of seasoned security experts that manages the receipt, investigation, internal coordination, and public reporting of security issues related to Siemens products, solutions, or services. ProductCERT cultivates strong and credible relationships with partners and security researchers around the globe to advance Siemens product security, to enable and support development of industry best practices, and most importantly to help Siemens customers manage security risks. The team acts as the central contact point for security researchers, industry groups, government organizations, and vendors to report potential Siemens product security vulnerabilities. This team will coordinate and maintain communication with all involved parties, internal and

Charter of Trust

We sign for cybersecurity!
We sign the Charter of Trust.

SIEMENS AES AIRBUS Allianz Atos CISCO DAIMLER DELL Technologies

enel IBM Munich Security Conference Münchner Sicherheitskonferenz msc NXP SGS T · · TOTAL TÜV SÜD



The key to a secure infrastructure: Defense in depth

SIEMENS

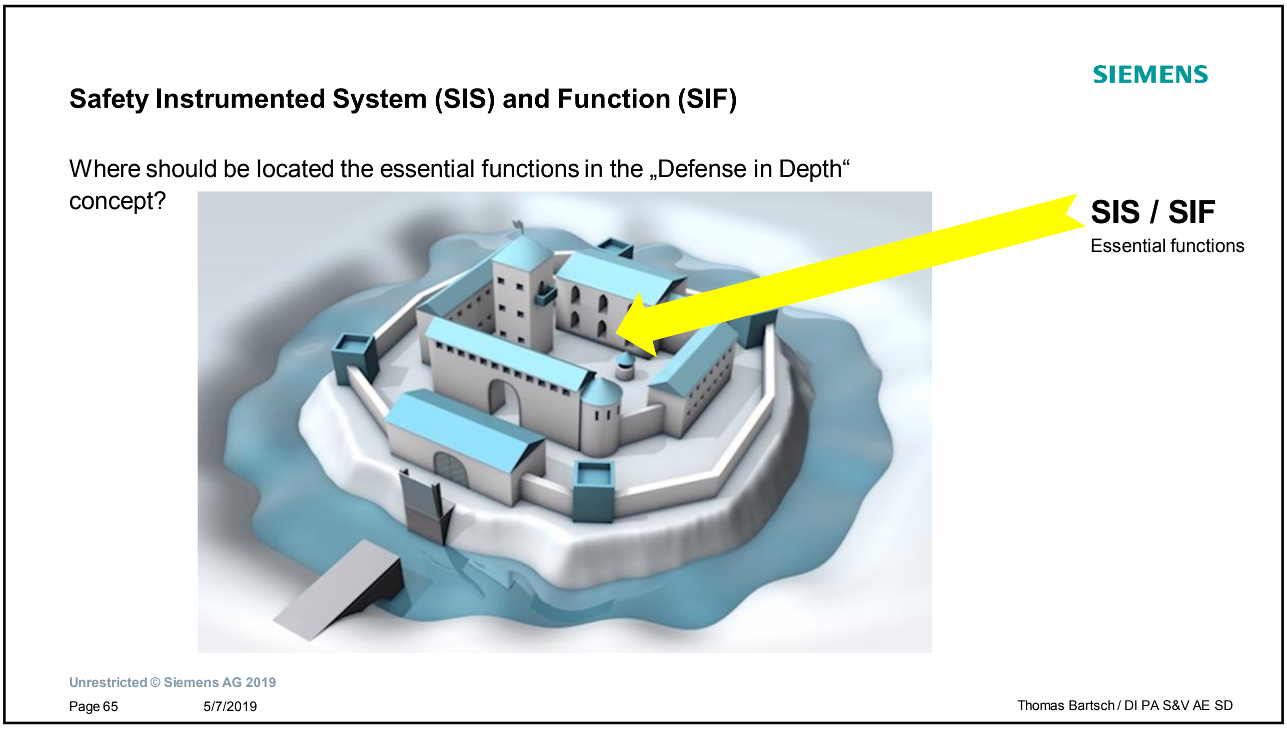
Great Wall

- Impenetrable wall
- One-layer protection
- One point of attack

A single defense layer does not provide adequate protection!

Defense-in-Depth

- Multi-layer protection
- Each layer protects the other layers
- An attacker must spend time and effort at each transition



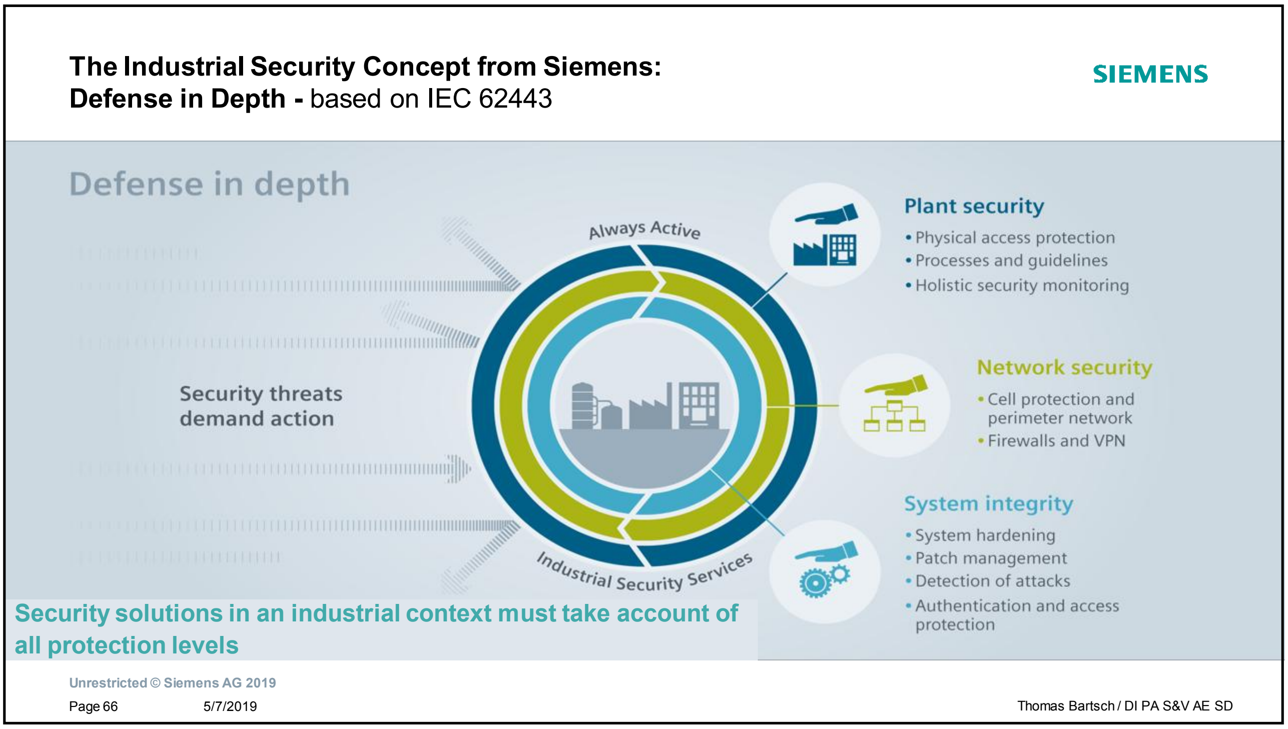
Safety Instrumented System (SIS) and Function (SIF)

SIEMENS

Where should be located the essential functions in the „Defense in Depth“ concept?

SIS / SIF

Essential functions



The Industrial Security Concept from Siemens: Defense in Depth - based on IEC 62443

SIEMENS

Defense in depth

Always Active

Security threats demand action

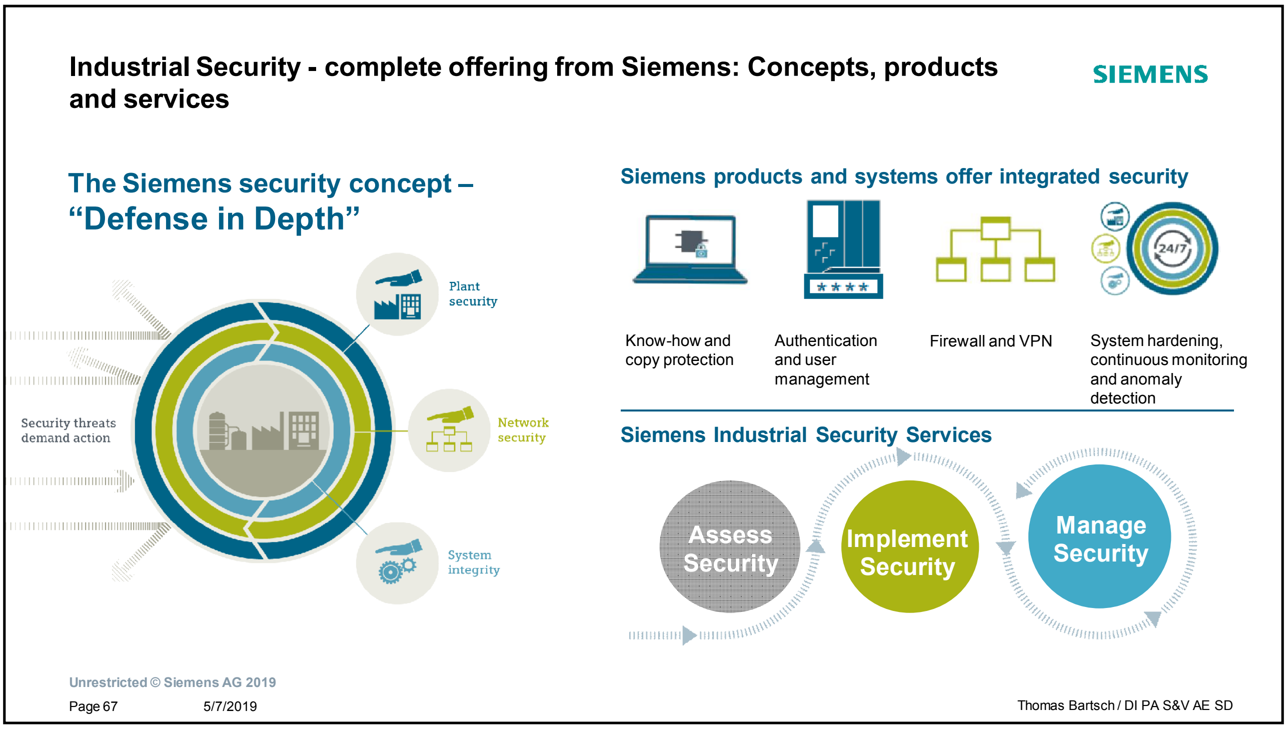
Industrial Security Services

Plant security
- Physical access protection
- Processes and guidelines
- Holistic security monitoring

Network security
- Cell protection and perimeter network
- Firewalls and VPN

System integrity
- System hardening
- Patch management
- Detection of attacks
- Authentication and access protection

Security solutions in an industrial context must take account of all protection levels



Industrial Security - complete offering from Siemens: Concepts, products and services

SIEMENS

The Siemens security concept – "Defense in Depth"

Security threats demand action

Plant security

Network security

System integrity

Siemens products and systems offer integrated security

Know-how and copy protection

Authentication and user management

Firewall and VPN

System hardening, continuous monitoring and anomaly detection

Siemens Industrial Security Services

Assess Security → Implement Security → Manage Security

SIEMENS

IEC 62443-2-4 Requirements for IACS Solution Suppliers

Security Concept
PCS 7 and WinCC

Basic document

- PCS 7 & WinCC security concept (A5E39251019-AA)

Detailed documents

- Virus scanner administration
- Patch management and security updates
- Support and remote dial-up
- Application whitelisting

Defense in Depth security architecture

Division into segments and security cells

Network subnets, IP adresses and name resolution

Active directory and Windows work groups

Windows security patch management

Support access and remote service (VPN, IPsec)

Virus scan and firewalls

User and access rights

Time synchronization

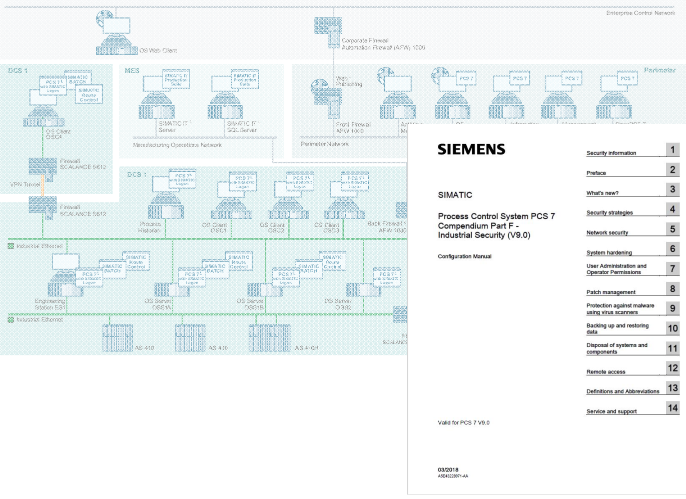
All documents are available online in the Customer Support Portal

SIEMENS

IEC 62443-2-4 Requirements for IACS Solution Suppliers

PCS 7 Compendium Part F
IT security configuration guidelines

- Network security
- System hardening
- User administration & Operator authorizations
- Patch management
- Protection against malware using virus scanners
- Backup and restoration of data
- Remote access



SIEMENS

SIMATIC

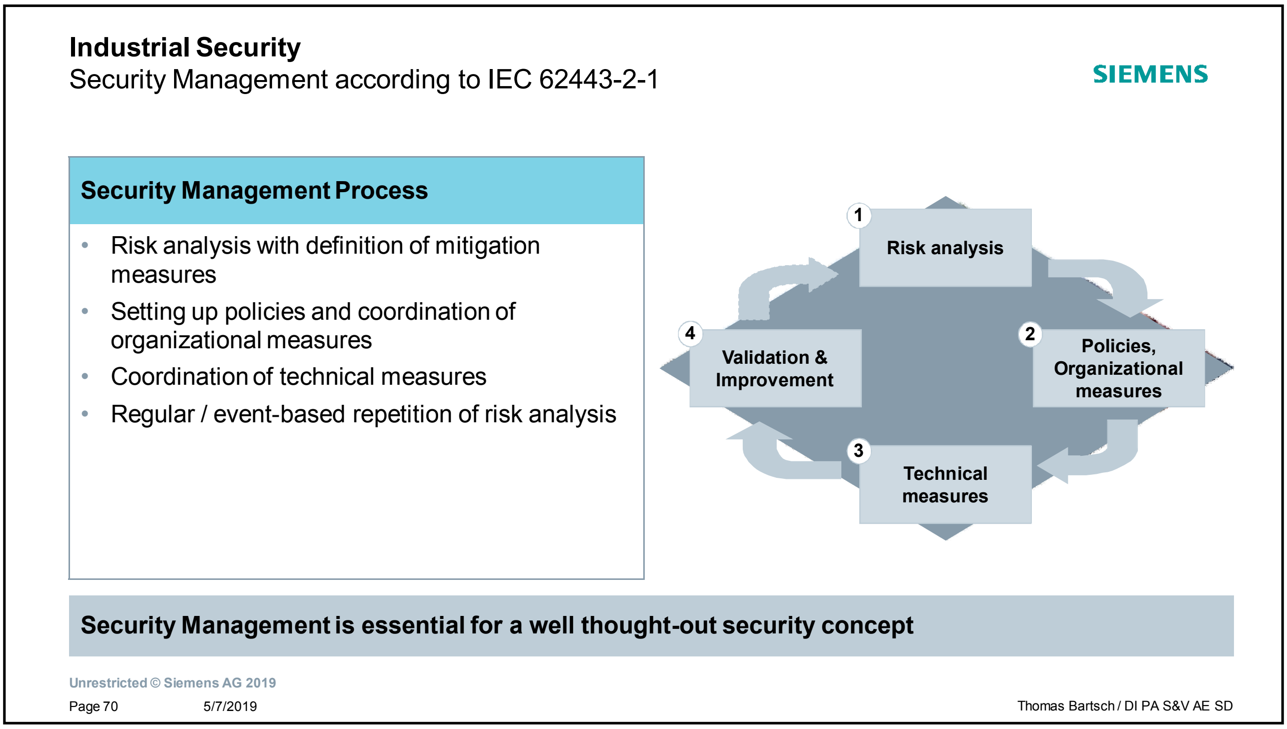
Process Control System PCS 7
Compendium Part F -
Industrial Security (V9.0)

Configuration Manual

Security information	1
Preface	2
What's new?	3
Security strategies	4
Network security	5
System hardening	6
User Administration and Operator Permissions	7
Patch management	8
Protection against malware using virus scanners	9
Backing up and restoring data	10
Disposal of systems and components	11
Remote access	12
Definitions and Abbreviations	13
Service and support	14

Valid for PCS 7 V9.0

03/2018
A5E43228971-AA



Industrial Security

Security Management according to IEC 62443-2-1

SIEMENS

Security Management Process

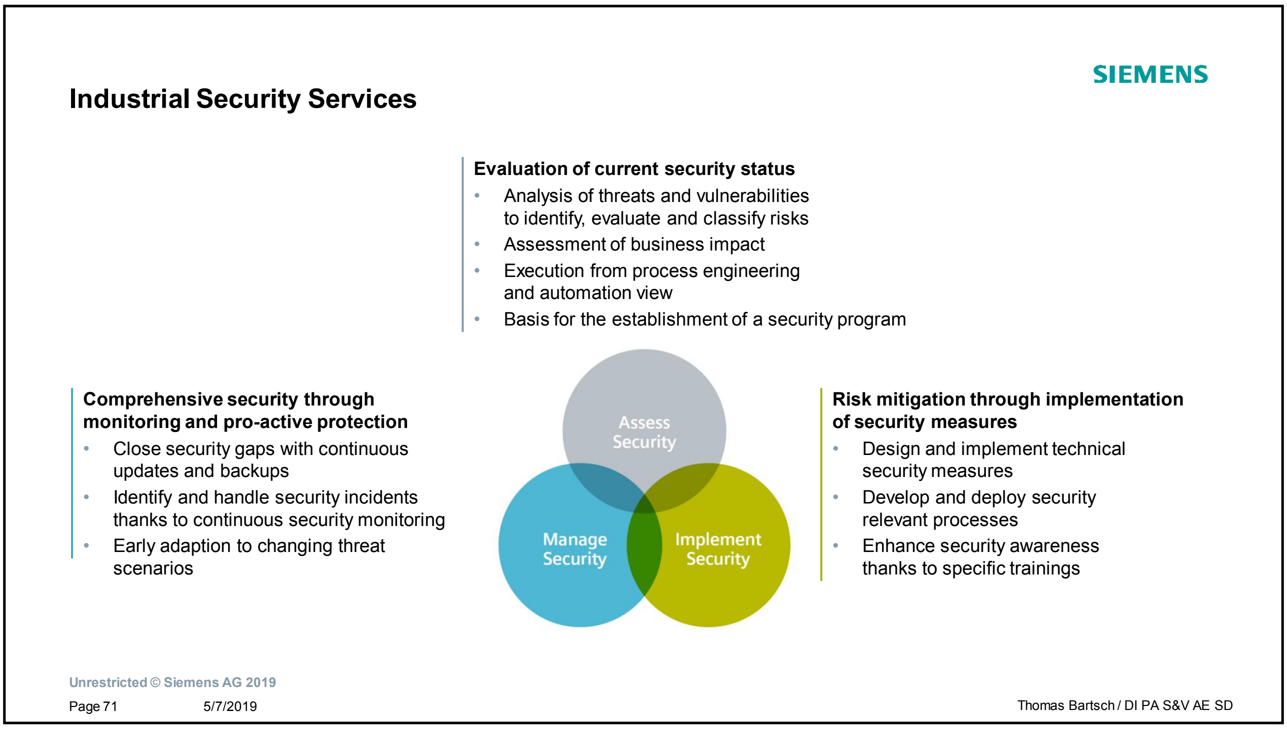
- Risk analysis with definition of mitigation measures
- Setting up policies and coordination of organizational measures
- Coordination of technical measures
- Regular / event-based repetition of risk analysis

1
Risk analysis
2
Policies, Organizational measures
3
Technical measures
4
Validation & Improvement

Security Management is essential for a well thought-out security concept

Unrestricted © Siemens AG 2019

Page 70 5/7/2019 Thomas Bartsch / DI PA S&V AE SD



SIEMENS

Industrial Security Services

Evaluation of current security status

- Analysis of threats and vulnerabilities to identify, evaluate and classify risks
- Assessment of business impact
- Execution from process engineering and automation view
- Basis for the establishment of a security program

Comprehensive security through monitoring and pro-active protection

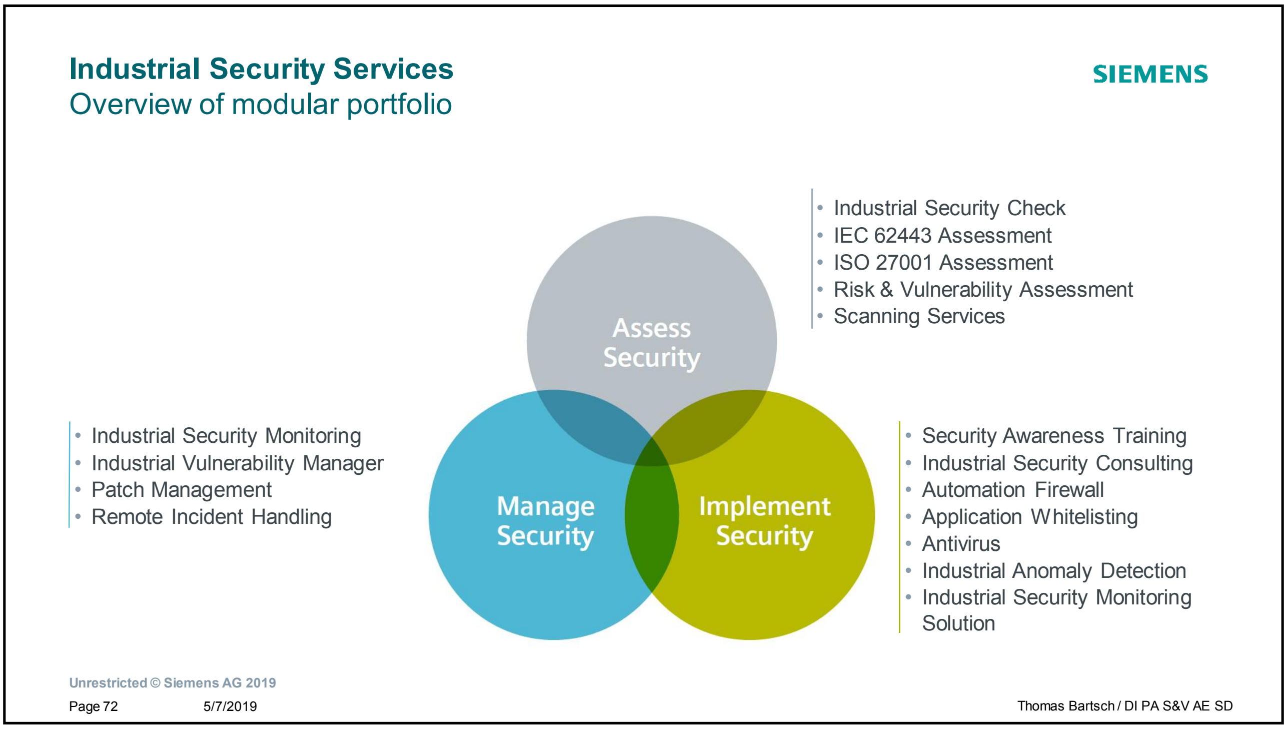
- Close security gaps with continuous updates and backups
- Identify and handle security incidents thanks to continuous security monitoring
- Early adaption to changing threat scenarios

Risk mitigation through implementation of security measures

- Design and implement technical security measures
- Develop and deploy security relevant processes
- Enhance security awareness thanks to specific trainings

Unrestricted © Siemens AG 2019

Page 71 5/7/2019 Thomas Bartsch / DI PA S&V AE SD



Industrial Security Services

Overview of modular portfolio

SIEMENS

Assess Security

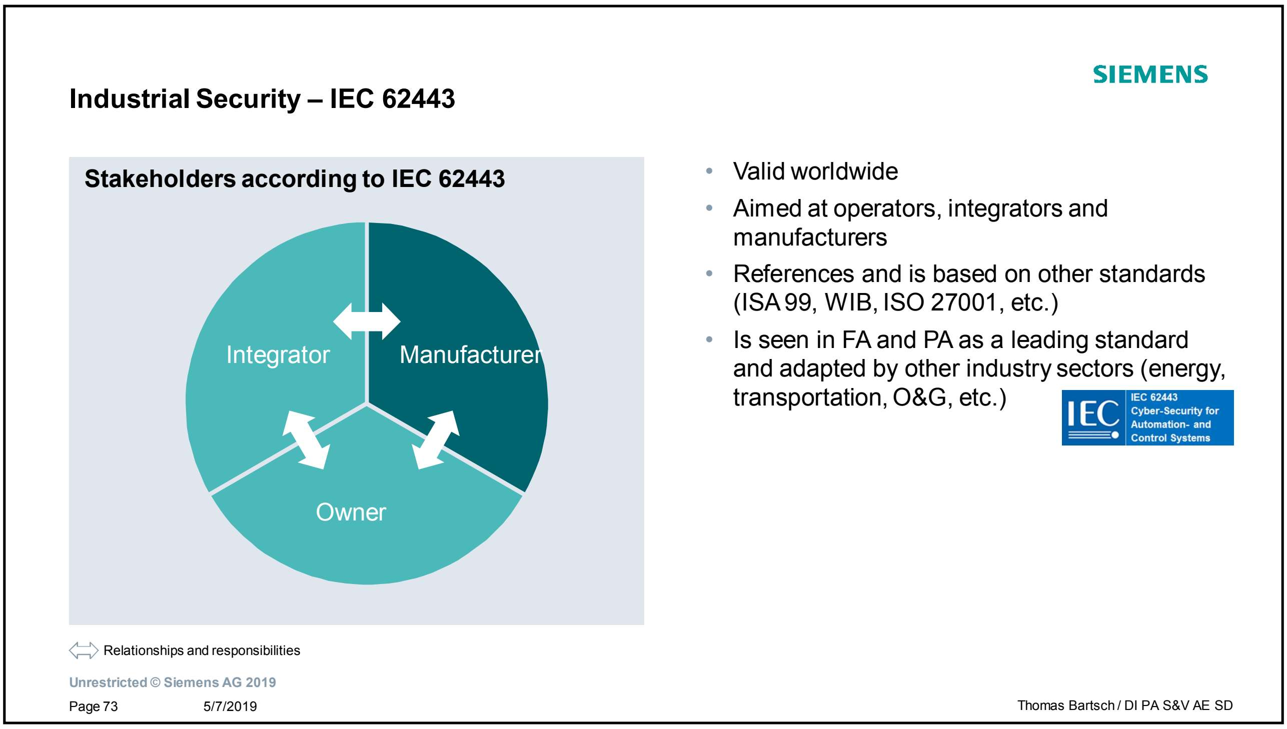
- Industrial Security Check
- IEC 62443 Assessment
- ISO 27001 Assessment
- Risk & Vulnerability Assessment
- Scanning Services

Manage Security

- Industrial Security Monitoring
- Industrial Vulnerability Manager
- Patch Management
- Remote Incident Handling

Implement Security

- Security Awareness Training
- Industrial Security Consulting
- Automation Firewall
- Application Whitelisting
- Antivirus
- Industrial Anomaly Detection
- Industrial Security Monitoring Solution



Industrial Security – IEC 62443

SIEMENS

Stakeholders according to IEC 62443

Integrator

Manufacturer

Owner

⟺ Relationships and responsibilities

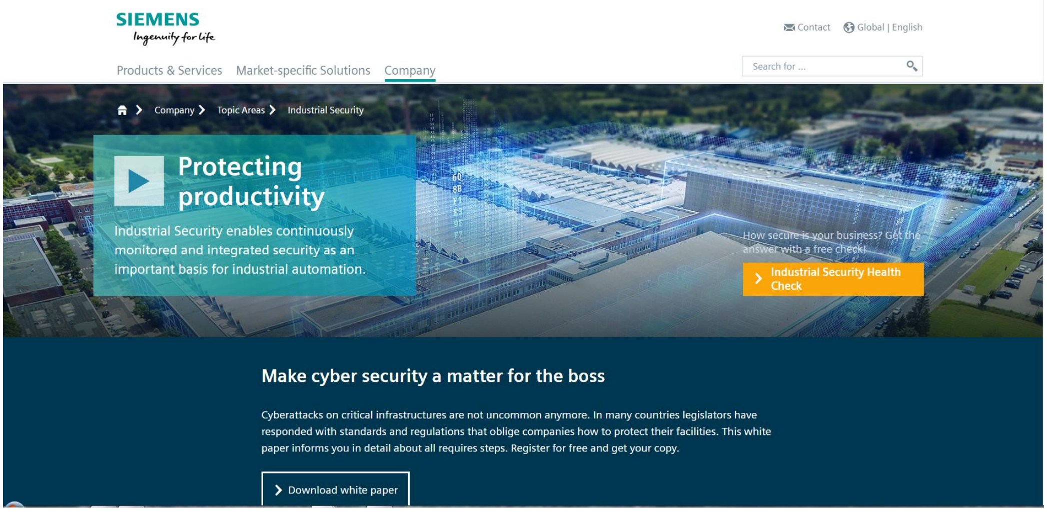
- Valid worldwide
- Aimed at operators, integrators and manufacturers
- References and is based on other standards (ISA 99, WIB, ISO 27001, etc.)
- Is seen in FA and PA as a leading standard and adapted by other industry sectors (energy, transportation, O&G, etc.)

IEC | IEC 62443 Cyber-Security for Automation- and Control Systems

Siemens Industrial Security

www.siemens.com/industrial-security

SIEMENS



Protecting productivity

Industrial Security enables continuously monitored and integrated security as an important basis for industrial automation.

How secure is your business? Get the answer with a free check!

Industrial Security Health Check

Make cyber security a matter for the boss

Cyberattacks on critical infrastructures are not uncommon anymore. In many countries legislators have responded with standards and regulations that oblige companies how to protect their facilities. This white paper informs you in detail about all requires steps. Register for free and get your copy.

Download white paper

Contact page

SIEMENS
Ingenuity for life

Thomas Bartsch
Sales Development
DI PA S&V AE SD

Gleiwitzer Straße 555
90475 Nuremberg

Mobile: +49 173 7074436

E-mail:
thomasbartsch@siemens.com

siemens.com/process-safety