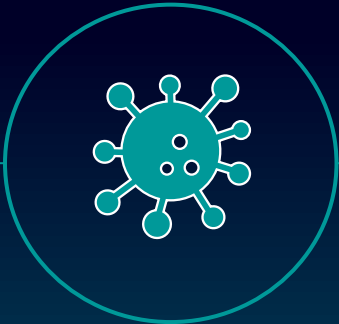




Cybersecurity: challenges and opportunities for a large corporation like Siemens

Key global trends driving cybersecurity demand



Growing cyberrisk for businesses



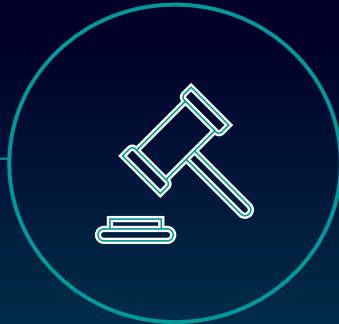
Fundamental technological changes



Workforce gap is widening



Increasing professional hacking



More laws and regulations worldwide



Challenging local vs global regulation

There is a strong need to act!

Cybersecurity at Siemens: InfoSec and PSS

Siemens follows a holistic and comprehensive approach to secure its products, solutions, services, and IT infrastructure.



Siemens sees cybersecurity as an enabler for digital transformations and strong competitiveness factor.

Product and Solution Security – Holistic Lifecycle View

Secured Product Development

- Security Standards & Processes
- Secured Architecture, Design & Coding
- Threat & Risk Assessment
- Security Testing
- Data Privacy
- Component Vulnerability Monitoring
- Adherence to state-of-the-art international standards (IEC 62443) and compliance to regional regulatory frameworks

Incident & Vulnerability Handling

- Siemens ProductCERT (24/7 hotline)
- Support for handling of security incidents and vulnerabilities
- Forensic Support
- Task Force



Secured Installation

- Secured Network Design
- Hardening
- Antivirus

Secured Operation

- Monitoring
- Scanning
- Patching

Company-wide key pillars



People



Process



Tools

Vulnerability and incident handling



Report

Analysis

Handling

Disclosure



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

<https://new.siemens.com/global/en/products/services/cert.html>

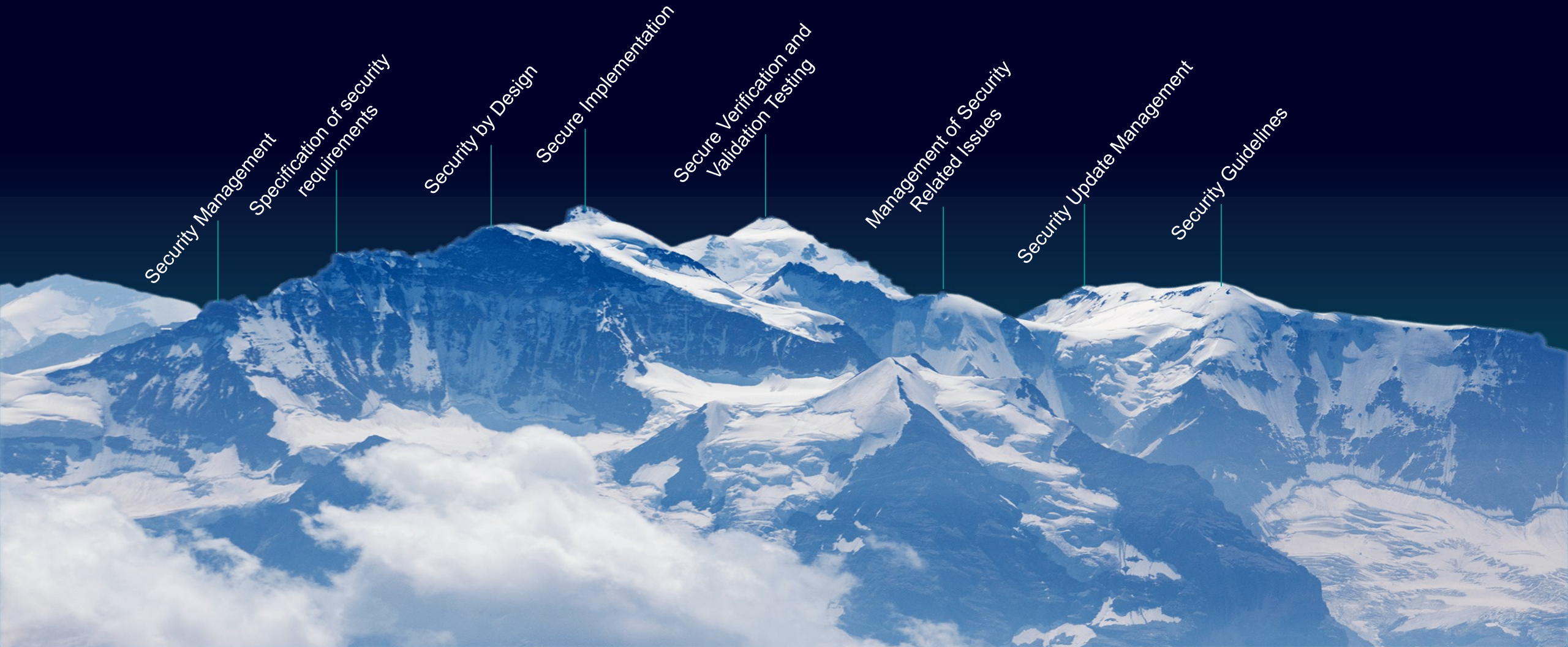
Report Security Issue

Siemens Security Advisories

Hall of Thanks

Certification by independent 3rd party

It is like climbing a mountain.... the assessment is based on more than four dozen "peaks":



Example: IEC62443 certification

ZERTIFIKAT • CERTIFICATE • 認證證書 • CERTIFICADO • CERTIFICAT • CERTIFICATE




Product Service

CERTIFICATE

No. IITS1 113879 0001 Rev. 00

Holder of Certificate: Siemens Schweiz AG
SI BP
Theilerstrasse 1a
6300 Zug
SWITZERLAND

Site(s): Siemens Schweiz AG
SI BP
Theilerstrasse 1a, 6300 Zug, SWITZERLAND

Siemens AG
SI BP
Siemensallee 84, 76187 Karlsruhe, GERMANY

Certification Mark: 

Type: Industrial IT Security

Scope of Certificate: Secure Development Lifecycle Process

Applied Standard(s): IEC 62443-4-1:2018
PPP 15003B:2021 (IEC 62443-4-1: Full ML3 Process Profile)

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report.
See <http://www.tuvsud.com/ps-cert> for details.

Report No.: 21CR02S027

Valid until: 2024-08-29

Date, 2021-09-14 
(Enrico Seidel)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany



- Siemens Smart Infrastructure Building Products was certified by TÜV SÜD on IEC62443-4-1 development process certification:
 - the process is fully compliant with international standard
 - achieved maturity level 3: the process is lived by existing projects
- IEC62443 4-2 product certification:
 - X200 & X300 edge gateways
 - SIPORT- Access control system
 - Desigo CC and Cerberus DMS
 - ASD+ – Aspirating smoke detectors
 - More products to follow...

ZERTIFIKAT • CERTIFICATE • 認證證書 • CERTIFICADO • CERTIFICAT • CERTIFICATE




Product Service

CERTIFICATE

No. ITS2 113879 0002 Rev. 02

Holder of Certificate: Siemens Schweiz AG
SI BP
Theilerstrasse 1a
6300 Zug
SWITZERLAND

Certification Mark: 

Product Type: Connect Gateway

Model(s): X200 & X300, Edge OS: V5.0.10 or higher

Tested according to: IEC 62443-4-1:2018
IEC 62443-4-2:2019
PPP 15003B:2021 (IEC 62443-4-1: Full ML3 Process Profile)

The secure development lifecycle and the resulting product(s) were assessed on a voluntary basis and comply 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 transfer the certificate to third parties. See <http://www.tuvsud.com/ps-cert> for details.

Test report no.: 22CR03013
Valid until: 2024-11-02

Date, 2022-11-02 
(Nadia Patricia Stefan)



ZERTIFIKAT • CERTIFICATE • 認證證書 • CERTIFICADO • CERTIFICAT • CERTIFICATE




Product Service

CERTIFICATE

No. ITS2 113880 0001 Rev. 00

Holder of Certificate: Siemens AG
Siemensallee 84
76187 Karlsruhe
GERMANY

Certification Mark: 

Product Type: IACS components

Model(s): SIPORT – Access Control System MP 3.x

Tested according to: IEC 62443-4-1:2018
IEC 62443-4-2:2019
PPP 15003B:2021 (IEC 62443-4-1: Full ML3 Process Profile)

The secure development lifecycle and the resulting product(s) were assessed on a voluntary basis and comply 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 transfer the certificate to third parties. See <http://www.tuvsud.com/ps-cert> for details.

Test report no.: 22CR03020
Valid until: 2025-07-08

Date, 2022-09-08 
(Nadia Patricia Stefan)



ZERTIFIKAT • CERTIFICATE • 認證證書 • CERTIFICADO • CERTIFICAT • CERTIFICATE




Product Service

CERTIFICATE

No. ITS2 113879 0003 Rev. 00

Holder of Certificate: Siemens Schweiz AG
SI BP
Theilerstrasse 1a
6300 Zug
SWITZERLAND

Certification Mark: 

Product Type: Aspirating Smoke Detector

Model(s): FDA261/FDA262/FDA222/FDA242
FDA261-CN/FDA262-CN
FDA222-CN/FDA242-CN

Tested according to: IEC 62443-4-1:2018
IEC 62443-4-2:2019
PPP 15003B:2021 (IEC 62443-4-1: Full ML3 Process Profile)

The secure development lifecycle and the resulting product(s) were assessed on a voluntary basis and comply 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 transfer the certificate to third parties. See <http://www.tuvsud.com/ps-cert> for details.

Test report no.: 22CR03072
Valid until: 2024-03-16

Date, 2023-05-31 
(Nadia Patricia Stefan)



ZERTIFIKAT • CERTIFICATE • 認證證書 • CERTIFICADO • CERTIFICAT • CERTIFICATE




Product Service

CERTIFICATE

No. ITS2 113879 0004 Rev. 00

Holder of Certificate: Siemens Schweiz AG
SI BP
Theilerstrasse 1a
6300 Zug
SWITZERLAND

Certification Mark: 

Product Type: IACS components

Model(s): Desigo CC and Cerberus DMS V6 and higher

Tested according to: IEC 62443-4-1:2018
IEC 62443-4-2:2019
PPP 15003B:2021 (IEC 62443-4-1: Full ML3 Process Profile)

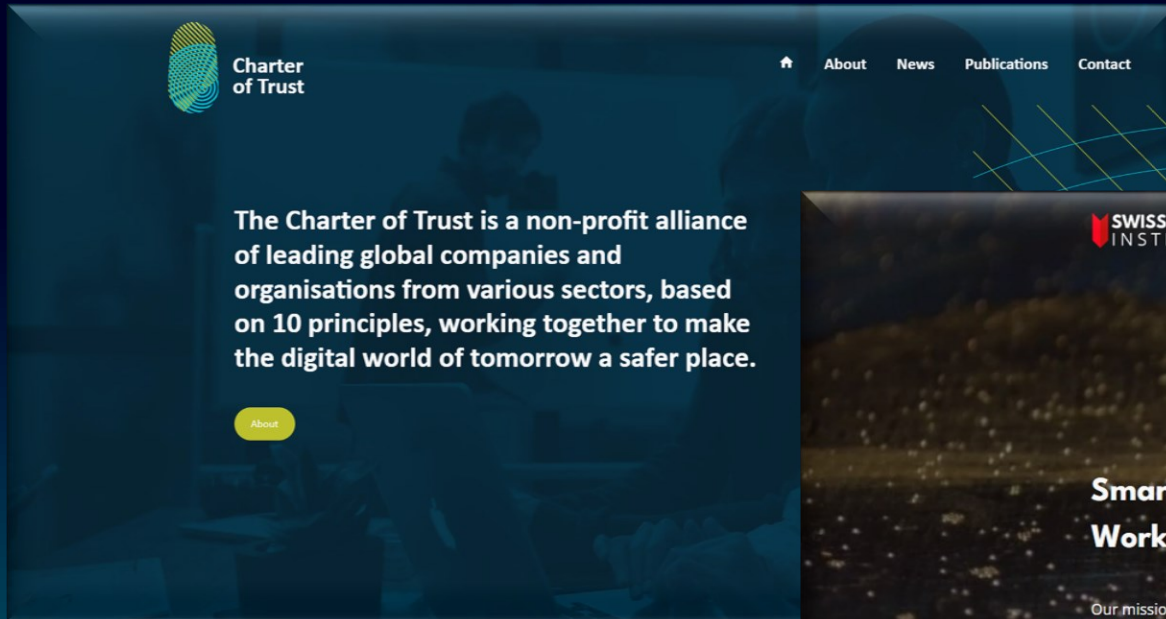
The secure development lifecycle and the resulting product(s) were assessed on a voluntary basis and comply with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition, the certification holder must transfer the certificate to third parties. See <http://www.tuvsud.com/ps-cert> for details.

Test report no.: 22CR03082
Valid until: 2025-09-24

Date, 2023-05-14 
(Nadia Patricia Stefan)



Sharing is caring: collaboration and communication

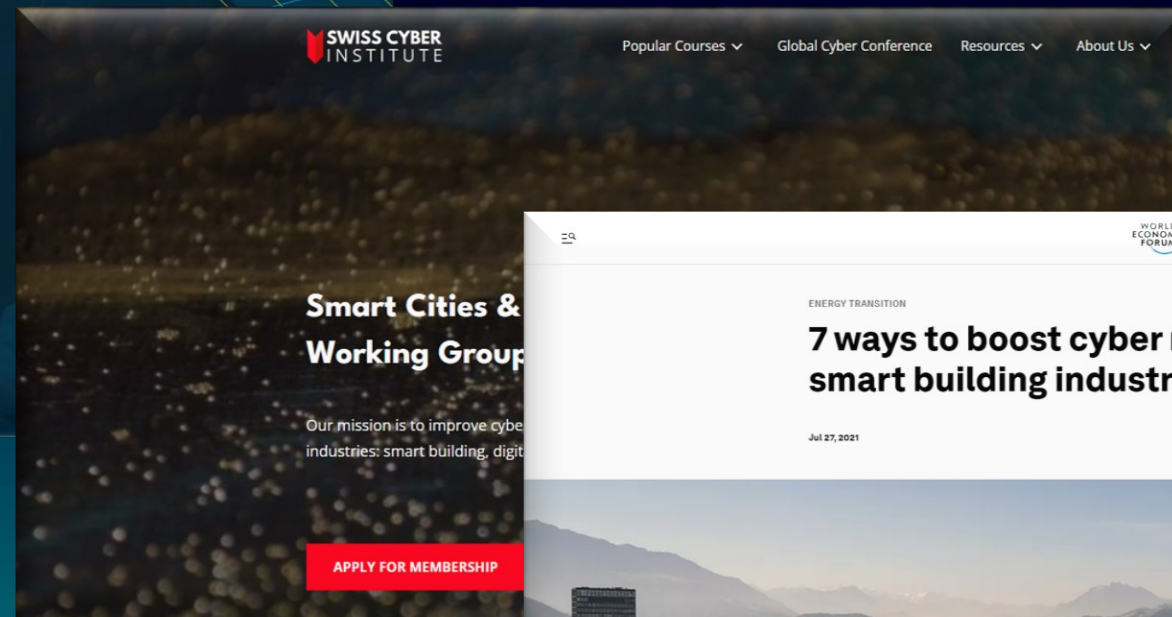


Charter of Trust

↑ About News Publications Contact

The Charter of Trust is a non-profit alliance of leading global companies and organisations from various sectors, based on 10 principles, working together to make the digital world of tomorrow a safer place.

About



SWISS CYBER INSTITUTE

Popular Courses ▾ Global Cyber Conference Resources ▾ About Us ▾

Smart Cities & Working Group

Our mission is to improve cyber resilience in smart building, digital industries, smart building, digital

APPLY FOR MEMBERSHIP



WORLD ECONOMIC FORUM

ENERGY TRANSITION

7 ways to boost cyber resilience in the smart building industry

Jul 27, 2021



Cybersecurity as a business opportunity



Phase 1: Identify threats and assume responsibility

- Practice responsibility
- Heighten awareness of security risks
- Cultivate a cybersecurity culture in your organization

Phase 2: Take action and embed security

- Embed cybersecurity in your organization
- Embed cybersecurity within products and services

Phase 3: Make the structure of cybersecurity transparent, and be a role model for others

- Share your cybersecurity best-practices
- Join existing cybersecurity communities
- Become active- even outside your own company

<https://www.charteroftrust.com/topic/seeing-cybersecurity-as-an-opportunity/>

I Thank you!