

Cybersecurity for Industrial Operations

How to use IEC 62443 with Examples




SIEMENS

Why is Cybersecurity in OT such an important topic for industry?



SIEMENS

Cyberattacks
The threat is real and growing

 In the past 5 years ...

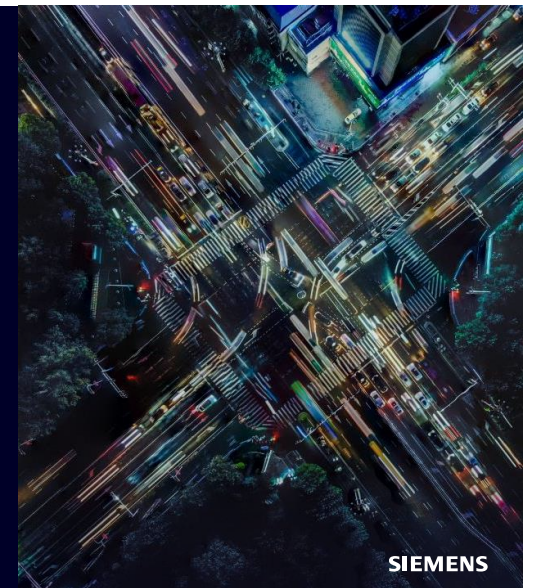
2017	2019	2021
<p>NotPetya/\$10 bn+ in losses</p> <p>Maersk, FedEx, Merck (~\$1.3 bn), Nuance Communications, Reckitt Benckiser and Mondelez (Cadbury) ...</p>	<p>LockerGoga/\$40+ m in loss</p> <p>Norsk Hydro, Norway based aluminum producer and electric power provider hit by a new variant of ransomware</p>	<p>New and evolving threats</p> <p>SolarWinds – Supply chain attacks</p> <p>EKANS – OT/ICS aware ransomware</p> <p>Colonial Pipeline, Steelcase, Honda, etc.</p>



SIEMENS

OT is at the intersection of multiple challenges

- 01 Digitalization**
Need for all types of data, in real-time (LEAN, Predictive Maintenance, etc.)
- 02 Knowledge gaps**
Lack of OT networking and cybersecurity knowledge and experience
- 03 Multiplying adversaries**
Proliferation of cyber-threat actors (insider, external, criminal, nation-state, script kiddies)
- 04 Sophisticated malware infrastructure**
Advancement in malware tools and services (AI, cloud-based tools, etc.)



SIEMENS

So what's this 62443 thing?

SIEMENS

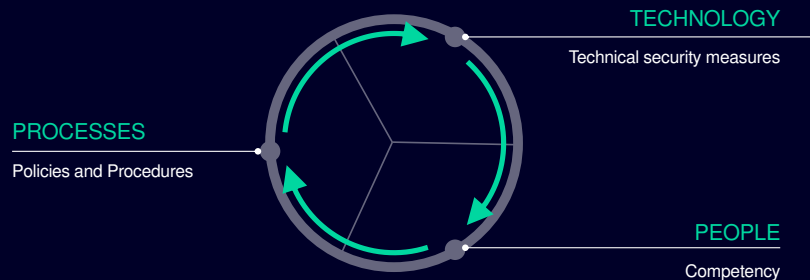
Status IEC 62443

IEC 62443 Security for Industrial Automation and Control Systems					
General	Policies & Procedures	System	Component / Product	Profiles	Evaluation
1-1 Terminology, concepts and models	2-1 Security program requirements for IACS asset owners	3-1 Security technologies for IACS	4-1 Secure Product Development Lifecycle Requirements	5-x Profile x	6-1 Security Evaluation Methodology for IEC 62443-2-4
1-2 Master glossary of terms and abbreviations	2-2 IACS Security Protection	3-2 Security Risk Assessment for System Design	4-2 Technical security requirements for IACS components		6-2 Security Evaluation Methodology for IEC 62443-4-2
1-3 Performance metrics for IACS security	2-3 Patch management in the IACS environment	3-3 System security requirements and security levels			
1-4 IACS security lifecycle and use-cases	2-4 Security program requirements for IACS service providers				
1-5 Scheme for IEC 62443 Cyber Security Profiles	2-5 Implementation guidance for IACS asset owners				

■ Published
■ Under revision
■ In development / planned

SIEMENS

A holistic Cybersecurity approach is guided by three main pillars
People, Technology and Processes



A holistic security protection concept has to include technology, processes and people

SIEMENS

Legislation – The When, What and Who?

SIEMENS



Legislation is underway in many parts of the world

CIRCA and SEC regulations in US will change how companies address cybercrime
Focus is on: reporting, disclosure criteria and transparency

Source: [McKinsey, 2022](#)

Tightening cybersecurity obligations across **Europe** - the **NIS2** directive
Focus is on: new rules, more sectors included

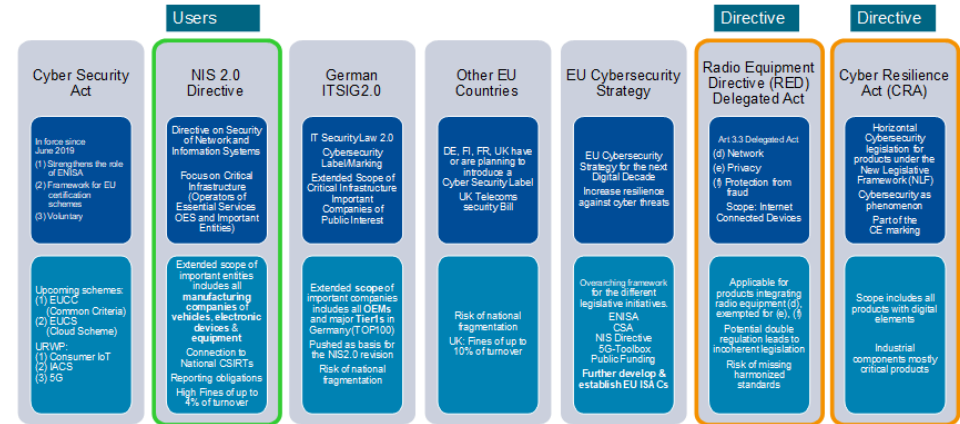
Source: [European Parliament, 2023](#)

Key changes in data privacy and cyber security laws across **Southeast Asia** in 2022

Source: [Harvest Smith Freehills, 2022](#)

SIEMENS

Guidance for Europe



Quelle: Bosch

Seite 4 | 08.03.2023

Entities

Essential entities
 (Sectors of High Criticality)

Included in Annex I
 + Annual turnover >€50 m

Fines:
 Max. **€10 m up to 2%**
 total worldwide annual turnover



On-site inspections and off-site supervision, including random checks, and regular audits

[Find more here](#) →

Important entities
 (Other Critical Sectors)

Included in Annex II

Fines:
 Max. **€7 m up to 1.4%**
 total worldwide annual turnover



On-site inspections and off-site ex post supervision

SIEMENS

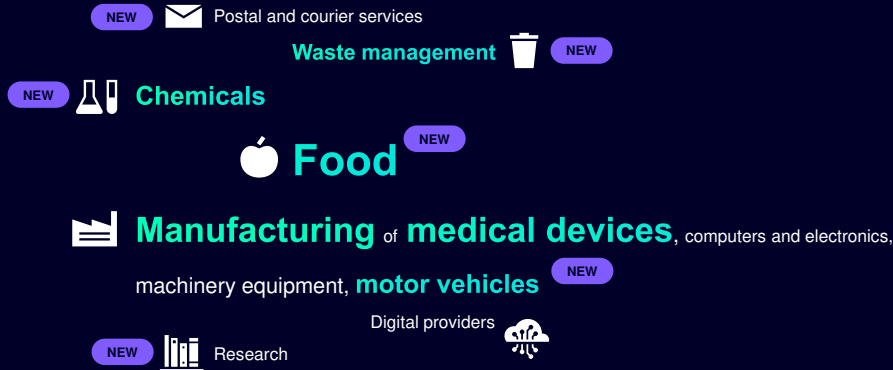
Essential entities Annex I¹



¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555&from=EN#d1e32-143-1>

SIEMENS

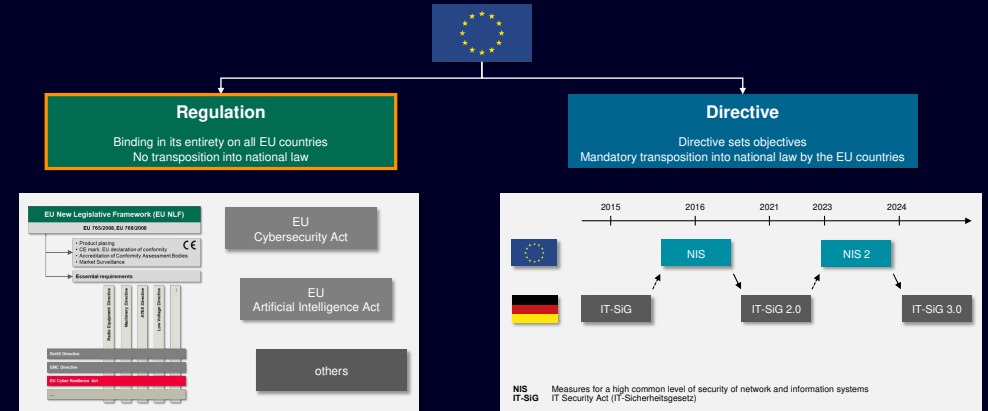
Important entities Annex II¹



¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555&from=EN&id=32-143-1>

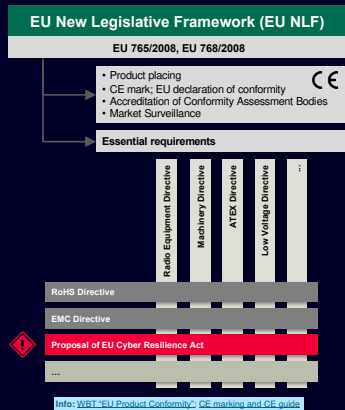
SIEMENS

EU Regulation v. EU Directive



SIEMENS

New Legislative Framework (NLF)



- Product** (e.g. EU CRA: "product" = "product with digital elements")
 - Union harmonisation legislation applies to
 - finished products as defined by the scope of each legislation
 - newly manufactured products
 - used and second-hand products imported from a third country when they enter the Union market for the first time
 - A product which has been **subject to important changes or overhauls** aiming to modify its original performance, purpose or type **may be considered as a new product**
- Making available on the market**
 - A product is made available on the market when supplied for distribution, consumption or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge
 - The concept of making available **refers to each individual product**
- Placing on the market**
 - A product is placed on the market when it is **made available for the first time** on the Union market
 - Each individual product can only be placed once on the Union market
 - Products made available on the market **must comply with the applicable Union harmonisation legislation at the moment of placing on the market**
- Responsibilities**
 - The **manufacturer is always solely responsible for the conformity of the product**
 - Applies also in case of a 3rd party ("notified body") involvement on a mandatory or voluntary basis

SIEMENS

Develop an Action Plan For OT Cyber Security



- Appoint and advisor to the Board (A trusted company, a Competent person) Trust is key.
- Start with a baseline Audit, Understand your operational estate. Create a concise and current inventory of your networks.
- Appoint a senior member of staff the responsibility of defining the companies action plan. Provide them with the money and tools to establish the plan.
- Define a key Risk measurement matrix for Cyber Security reporting. Monthly reports should be the norm across IT and OT. Define clear processes.
- Access your supply chain, KNOW your supply chain.
- Manage your security, know your threats, be proactive.

SIEMENS

The OT Security Journey by Gartner

60% of orgs. are here 30% of orgs. are here

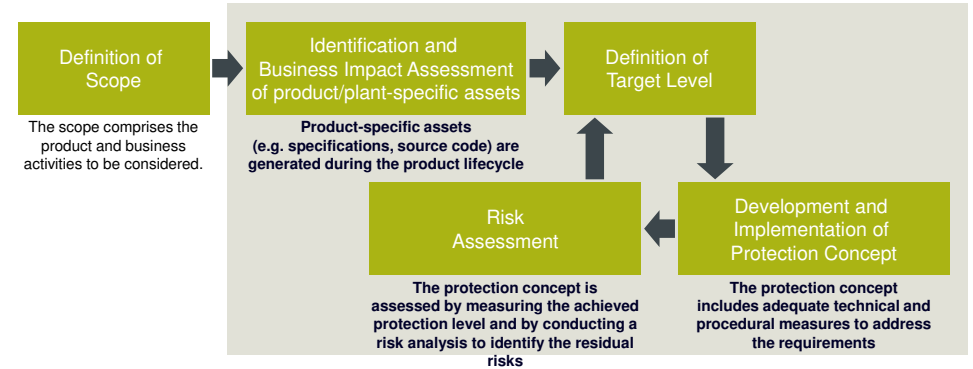


Source: Gartner OT Security Journey adapted by Securityweek.com, 2022

SIEMENS

General workflow for the protection of product/plant-specific assets. (Holistic Security Concept)

IEC62443/ISO27001 Based Method



Key Decisions To Be Made.....

... by answering key questions and addressing five levers for security in business including IT

“What in my business do I need to protect?”

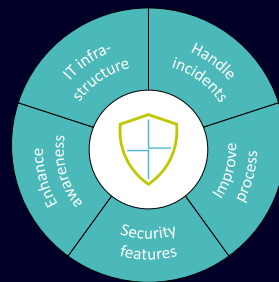
Identification of the critical business assets

“Which level of security do I need?”

Security level drives requirements, i

“How do I protect the specific assets?”

Standards based security solutions are applied to protect and monitor the critical assets

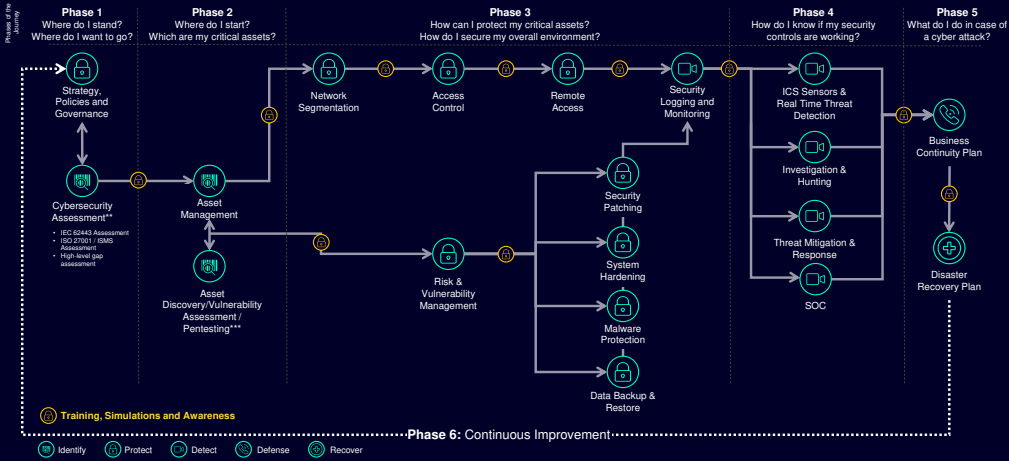


SIEMENS

How does Siemens help you to secure your operations?

SIEMENS

Cybersecurity step by step



SIEMENS

Supplementing Zero Trust

Combining Zero Trust and perimeter protection principles

Defense in depth remains state-of-the-art, ...



... but classical cell protection ...

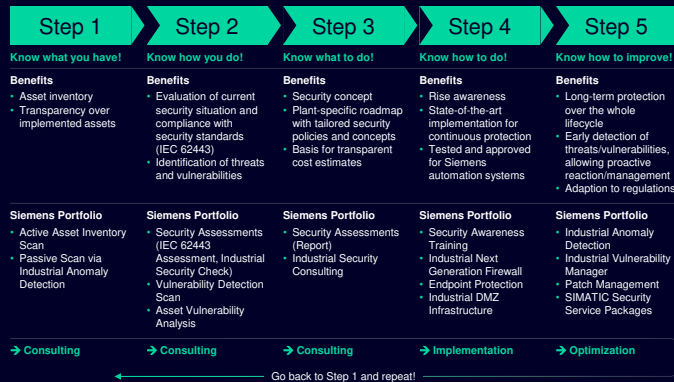


... will be enriched by zero trust principles



SIEMENS

Cybersecurity step by step



Benefits

DI Security overall
Protect the productivity and availability of your plant

Overall
Immediate access to expert know how; Save time and resources

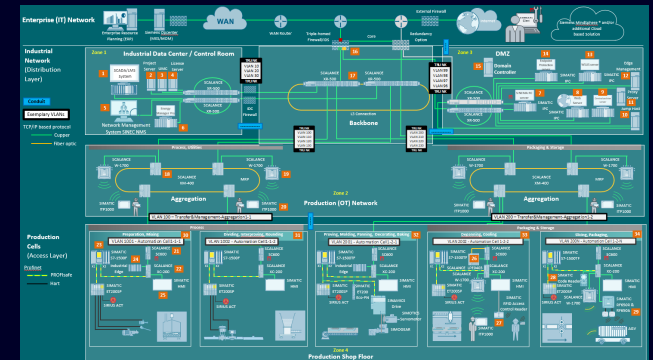
"We make sure that you can focus on your core business!"

SIEMENS

Our Cybersecurity experts enriched with our profound market knowledge support you for building up secure architectures for your industrial operation

Siemens provides end to end security solution from consulting to implementation of dedicated portfolio and optimization of your applications:

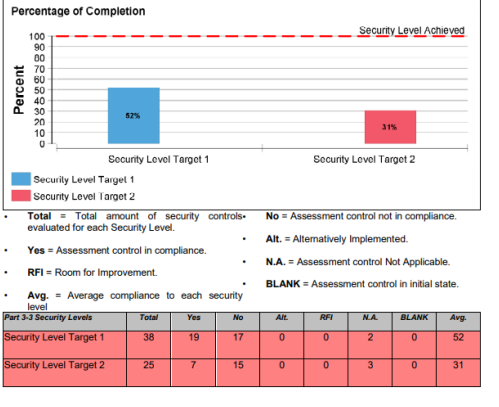
Tailor-made for your complete industrial operations – from sensor to cloud



SIEMENS

Post Assessment Blues

Difficulty to Fix	Moderate	TP02 - Identification Authentication + Authorization	TP07 - Network segmentation
		TP03 - Malware protection	TP08 - Protection of network borders
Easy	Low	TP04 - Whitelisting	TP13 - Monitoring, Logging and Log analysis
		TP05 - System Hardening Measures	TP21 - Emergency Power
		TP06 - System Access protection	
		TP09 - Remote Access protection	
		TP11 - NTP server implementation	
		TP14 - Asset Management and Vulnerability Detection	
		TP15 - Backup + Restore	
		TP16 - Security functionality testing	
		TP17 - Deterministic Output	
		TP19 - Mobile Devices	
		TP20 - Disposal	High



What are we trying to achieve:

- Bring in resilience through Security
- Return of Investment with Security spend – Networks, DMZ, Firewalls
- Access Control – Remote Users
- User Access Control – Fundamental but often a culture change (Identification)
- Asset Management
- Network Protection – People, environment and Machine Safety and Security



SIEMENS

SIEMENS

Digital Industries Industrial Cybersecurity Offering

Use-Cases

Products & Services

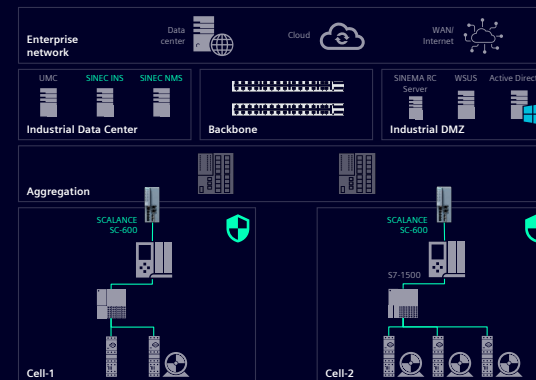
Cybersecurity and with cybersecurity functionality

Network Security	Securing OT/IT integration perimeter-based
	Secure remote access
	End-to-end OT/IT security based on Zero Trust
	Secure OT/IT data exchange
System Integrity	Anomaly detection
	Secure commissioning of Automation Systems
	Central User Management for OT
	Vulnerability and patch management
	Endpoint protection
	Secure communication between automation Systems

Software	Hardware
SINEC NMS	Industrial Firewalls
SINEC INS	Industrial Switches
SINEC Security Monitor	Industrial Routers
SINEC Security Inspector	Industrial WIFI
SINEMA Remote Connect	HM
User Management (UMC)	PLC SIMATIC S7
TIA Portal	Access Control
	Industrial PC
	SCALANCE LPE

SIEMENS

Example of Use-Case Securing OT/IT integration perimeter-based



Solution

The key points of this approach are:

- Network segmentation
- Protection of zone boundaries
- Securing the communication between the security zones
- Centralized management

Current State

- No separation between IT and OT
- No boundary Control
- Flat Networks – routing, Mobile devices, Modems
- User Access is uncontrolled

SIEMENS

Network Security

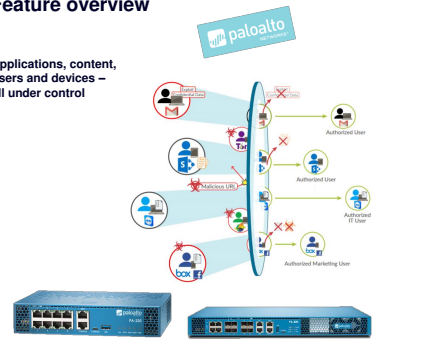
Perimeter protection with Industrial Next Generation Firewall

Our solution

- Based on **Palo Alto Networks Next-Generation Firewall Appliances**
- Palo Alto Networks is a "Gartner Magic Quadrant Leader" for Enterprise Network Firewalls for the 10th consecutive year
- Application layer and stateful inspection firewall
- IPSec VPN gateway
- Threat Prevention (additional subscription required)
- Advanced Malware Protection (additional WildFire subscription required)
- Prevents against known and unknown threats
- High availability (active/active and active/passive) modes
- Redundant power input for increased reliability (PA-220 and PA-850) and fan-less design (for PA-220 model)

Feature overview

Applications, content, users and devices – all under control



SIEMENS

Use cases for more network security

Network segmentation and „demilitarized zone“ (DMZ)

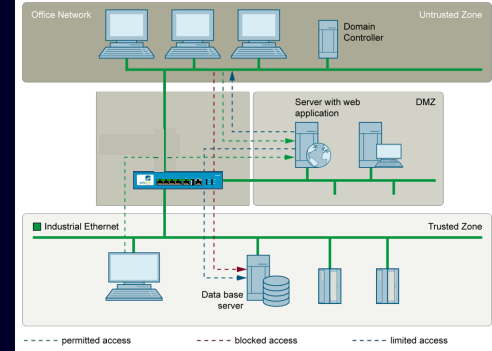
Task

The industrial network shall be divided into several security zones. Also, a deep inspection of the data flow is required.

Solution

With the Industrial Next Generation Firewall based on the firewalls of **Palo Alto Networks** a flexible security zone concept can be realized, containing:

- Different security zones such as DMZ, and automation cells
- Remote access only to specific and selected network cells
- Application Layer Firewall
- Deep Packet Inspection

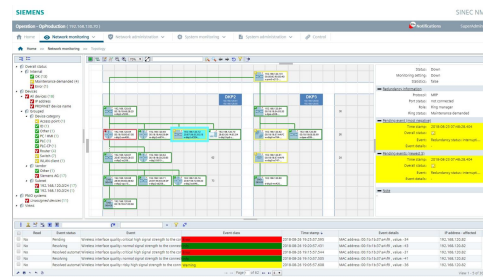


SIEMENS

Use cases for more network security

Network management and -diagnostics

- Network Visibility!!!!!!**
- Management**
- Logs/Events**
- Diagnostics**
- Device Management**
- Rule**
- Time Sync**



SIEMENS

Network Security

Network cells, Firewalls and VPN

Separation in network cells

SIMATIC PCS neo is designed to operate in separated network cells which is made possible by simple cross-firewall communication

The communication within and across network cells, e.g. between PCS neo servers and clients, is secured by using HTTPS.

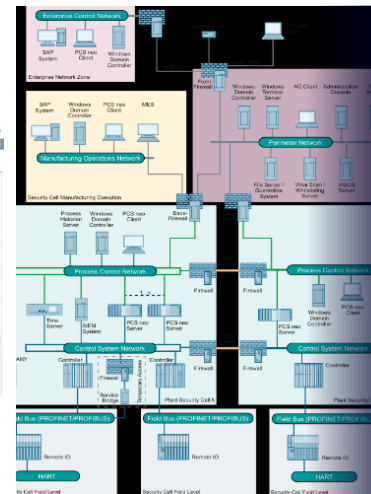
Multiple firewall layers

- Front firewall to control and restrict the data exchange with the office network
- Perimeter network (DMZ) to allow service and support access to the plant with controlled and restricted data exchange with the process control network
- On every host Windows firewall automatically configured by SIMATIC PCS neo

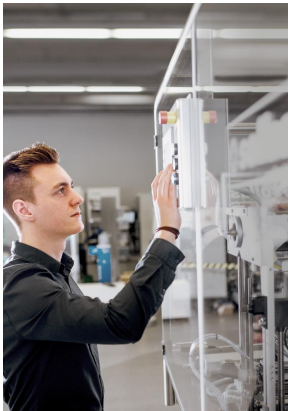
Virtual Private Network (VPN) as a solution for manipulation protection, e.g. when transferring data via untrusted networks.

PCS neo provides proven add-on partner products which are tested on compatibility.

SIEMENS



Continuous protection against malware with Endpoint Protection



Endpoint Protection

- The threat of malware in form of viruses, rootkits and trojans is growing exponentially – also for endpoint devices in industrial environments (e.g. IPC).
- Endpoint Protection provides different approaches – each has its advantages depending on the use case.

How does it work?

- Antivirus:** The execution of known malicious applications is blocked based on continuously updated signature files
- Application Whitelisting:** Only trusted applications are allowed to run based on a positive list
- Endpoint Detection and Response:** Interoperability test for the specific configuration of PCS 7 version and 3rd party EDR software version



SIEMENS

Network Security Mechanical closing of unused ports with IE RJ45 Port Lock

Main value drivers



Protection against known and unknown threats caused by malware



Easy, centralized operation via management server



Approved versions with tailor-made configurations for Siemens products

SIEMENS



IE RJ45 Port Lock

Feature / function

- Mechanical closing** of unused RJ45 interfaces of network components and end devices

Security functionalities:

- RJ45 port can also lock non-configurable network components
- Robust, industrial-suited construction
- Easy installation without additional tools due to RJ45 compatible design
- Removal of port lock only after unlocking with a mechanical key

Benefit

Secures physically open, unused RJ45 interfaces to prevent unauthorized network access

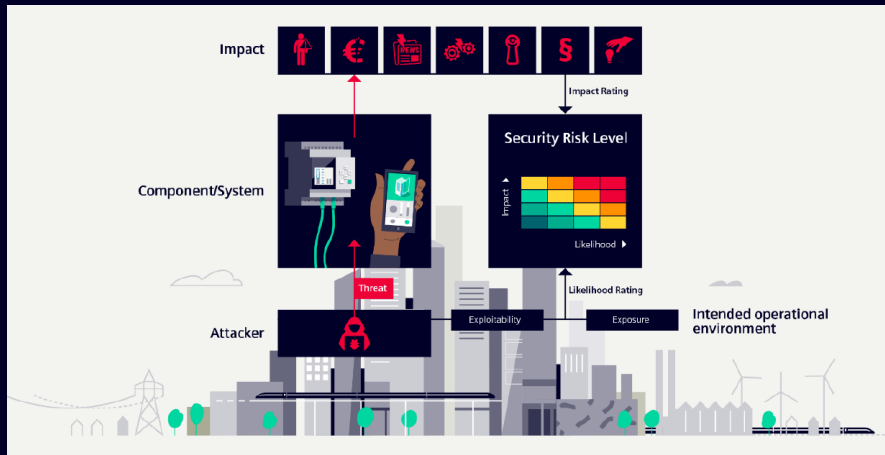
Temporary **network disconnections** (plant shutdown for maintenance) can be implemented directly on site

Protection of the critical network components:

- unauthorized network access
- espionage or data manipulation

SIEMENS

TRA Process



SIEMENS

TRA Process

Threat and Risk Analysis (TRA)

Preparation

- Create system overview
- Specify scope and intended operational environment
- Specify protection goals and impacts
- Document components

Involved roles:

- Product management, project leader
- Architect
- PSSE or Security specialist
- TRA Moderator

Workshop

- Identify and analyze threats
- Rate likelihood and impact to derive risk

Threat description	Likelihood	Impact	Risk
Threat 1	Very likely	Critical	Red
Threat 2	Possible	Disastrous	Yellow
Threat 3	Possible	Negligible	Green

Involved roles:

- Product management, project leader
- Architect, solution designer, developers, tester
- Service engineer
- Installation / commissioning expert
- PSSE or Security specialist
- TRA Moderator

Risk treatment

Definition of technical, physical and organizational security measures, specified in:

- Requirements
- Design
- User documentation

Tracking of risk treatment

Management sign-off for residual risks

SIEMENS

Industrial Security

Certification for the process control system SIMATIC PCS 7

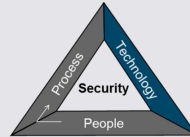
First product certification according to IEC 62443

TÜV SÜD certifies that the SIMATIC PCS 7 process control system conforms with the security standards IEC 62443-4-1 and IEC 62443-3-3



Highlights

- With this certificate, the company documents its security approach to automation products, and gives integrators and operators a transparent insight into its industrial security measures.
- The process control system offers comprehensive security measures and functions to protect plant operation



- 4-1 Product Development Lifecycle of SIMATIC PCS 7
- 3-3 Functional security capabilities of SIMATIC PCS 7

SIEMENS

Siemens Vulnerability Handling and Disclosure Process

Handling of Security Vulnerabilities in Siemens Products

Reporting of Vulnerabilities

To report a security vulnerability affecting a Siemens product, solution or infrastructure component, please contact Siemens CERT (contact information, see below). Siemens usually responds to incoming reports within one business day (reference: Munich, Germany).

Everyone is encouraged to report discovered vulnerabilities, regardless of service contracts or product lifecycle status. Siemens urges reporting parties to perform a coordinated disclosure, as immediate public disclosure causes a 'zero-day situation' which puts Siemens' customer systems at unnecessary risk.



Siemens ProductCERT – Contact for Products, Solutions and Services

PGP Public Key and Fingerprint: 7F04 6EDA 338E 6D94 A3AA 4974 BB67 95EA 8E55 D52E
Email: productcert@siemens.com

Siemens CERT – Contact for Infrastructure

PGP Public Key and Fingerprint: A3D1 8E40 D104 DEAD A112 3FF6 B485 0E2E 1AA2 2CD8
Email: cert@siemens.com

SIEMENS

How to find Information about Security Incidents?

Security advisories are official statements

Security Publications

Siemens Security Advisories

Siemens ProductCERT investigates all reports of security issues and publishes Security Advisories for validated security vulnerabilities that directly involve Siemens products and require applying an update, performing an upgrade, or other customer action. As part of the ongoing effort to help operators manage security risks and help keep systems protected, Siemens ProductCERT discloses the required information necessary for operators to assess the impact of a security vulnerability.

SSA-232418	5.3	Vulnerabilities in SIMATIC S7-1200 and SIMATIC S7-1500 CPU families	i	V1.0	2019-08-13	PDF	↓	TXT
SSA-307392	7.5	Denial-of-Service in OPC UA in Industrial Products	i	V1.3	2019-07-09	PDF	↓	TXT
SSA-254686	7.9	Foreshadow / L1 Terminal Fault Vulnerabilities in Industrial Products	i	V1.5	2019-06-11	PDF	↓	TXT
SSA-179516	5.9	OpenSSL Vulnerability in Industrial Products	i	V1.5	2019-04-09	PDF	↓	TXT

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

Subscribe to Security Advisories

Stay Informed

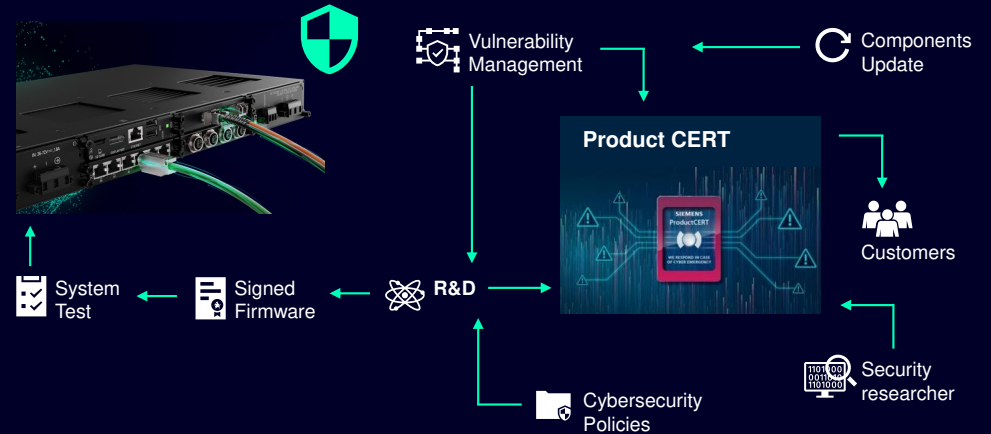
Follow us on Twitter, register to our advisory mailing list, or subscribe to our RSS feeds to stay informed with Siemens ProductCERT. Our Twitter handle is @ProductCERT. Register to our advisory mailing list and we will notify you via email on newly released or updated Security Advisories.

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

SIEMENS

Keeping products secure through whole product life cycle is essential

From ex works till vulnerability patching with Siemens' solutions



SIEMENS



Thank You!

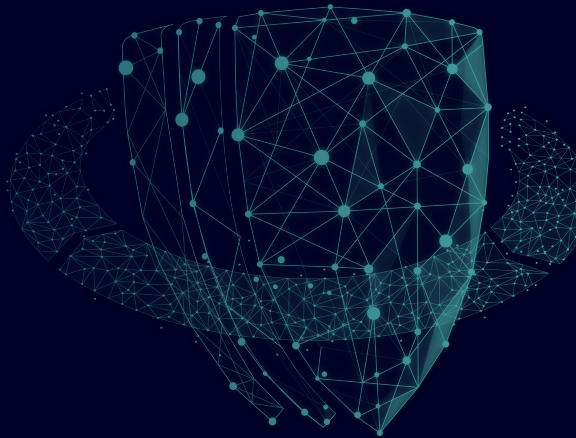


SIEMENS

SIEMENS



Published by Siemens Ireland
Wayne Bursey
Industrial Network and Cyber Security Lead
Siemens Ireland
DCU Innovation Campus
Dublin
Ireland
Mobile +353 86 4651693
E-mail wayne.bursey@siemens.com



SIEMENS