

Cybersecurity Siemens AG

ACSC 2026 Kick Off
June 23rd, 2026



SIEMENS

Timeline

	Title	
13:00	Welcome Safety Check-in	Johann Schlaghuber
13:05	Intro	Joe Pichlmayr
13:15	Cybersecurity at Siemens AG	Johann Schlaghuber
13:45	Insights on IT/OT Security	OT SecurityTeam Graz
14:15	(Legacy) Protocols	OT SecurityTeam Graz
14:45	DigiLab / LivingLab (Führung)	Siemens City
16:00	Coffee break / meet & greet	
16:15	Security Advisories	OT SecurityTeam Graz
16:45	Discussion	
17:30	End	

Agenda

Chapters

- 1 Siemens AG Austria
 - 2 Introduction – Cybersecurity in the convergence of IT and OT
 - 3 Challenges at the interfaces between IT and OT
 - 4 Regulatory environment - Joint expertise
 - 5 Development of a collaborative security framework and its implementation at Siemens
 - 6 Holistic approach to security - People - Processes - Technologies Collaboration
 - 7 Cybersecurity Governance
 - 8 Zero Trust
 - 9 Siemens Cybersecurity Offerings
-

Our solutions address the major issues of our time

Siemens



Digital transformation of industry,
infrastructure, and mobility

Siemens Energy



Future-proof
energy technologies

Siemens Healthineers



Functioning
healthcare

Siemens Energy: Listed associated company | Siemens Healthineers: Listed subsidiary of Siemens

Digital transformation has the potential to drive progress and growth and reduce resource consumption in all countries

Industry



Up to **50% material savings** can be realized using digital twins and innovative production technologies such as additive manufacturing.

Infrastructure



Buildings are currently responsible for **39% of global energy related carbon emissions**. Data analytics and automated building management can unlock large saving potentials.

Mobility



Up to **30% higher network capacity** can be achieved through automatic train operation and by optimizing train flows and rail operations.

Businesses and Services of Siemens AG – LC AT CSO View

Industrial Business

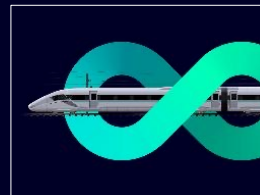
Digital Industries



Smart Infrastructure



Mobility



Siemens Healthineers¹



Siemens Advanta



Services

Siemens Financial Services



Siemens Real Estate



Global Business Services



Foundational Technologies



¹ Publicly listed subsidiary of Siemens; Siemens' share in Siemens Healthineers is 67%



Businesses / Global Services in the scope of Cybersecurity in LC AT



Businesses consulted

Focus on eleven Company Core Technologies Strategic R&D across all Siemens businesses

Siemens R&D
(FY 2025)

€6.6 bn

~ €511 m

Investments in
future technologies



Cybersecurity & Trust



Data & Artificial
Intelligence



Future of Automation



Integrated Circuits &
Electronics



Power Electronics



Simulation &
Digital Twin



Software Systems &
Processes



Sustainable Energy &
Infrastructure



Advanced Manufacturing
& Circularity



Connectivity & Edge



User Experience

A leading technology company

We have set four strategic priorities that guide our mindset, behaviors and actions

Customer impact

We think and act customer first

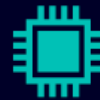
Everything we do is motivated by creating more impact for our customers and accelerating their digitalization and sustainability journey.



Technology with purpose

Solving real-world problems

For more than 175 years, Siemens has been developing technology with purpose.



Empowered people

Better and faster decisions

We are driving progress by empowering our people to take decisions in the best interest of the company.



Growth mindset

Try, learn, improve

We think about the businesses of tomorrow as well as today, always exploring what's possible to expand our technology leadership.



Our digital portfolio



Data analysis



Simulation tools



Secure networking



Artificial intelligence
and Internet of
Things



New business
models



Cybersecurity

Top 10

Siemens is among
the top 10
software
companies

DEGREE – How we measure our impact

2030 ambitions

Decarbonization & energy efficiency	Scope 1 and 2 Reduce by 90% and compensate residual emissions Baseline: 691 kt CO ₂ e FY19	Total Scope 3 Reduce by 30% by 2030 and achieve net-zero by 2050 Baseline: 153 Mt CO ₂ e FY19	Customer Avoided Emissions Achieve >1,000 Mt cumulatively Baseline: 264 Mt CO ₂ e FY23
	Ambition -90% 	Ambition -30% & net-zero 	Ambition >1,000 Mt 
Ethics & Governance	Siemens Integrity Initiative Fight corruption globally by training 50 k people and implement 30 Collective Action initiatives Baseline: 0% FY24	Cybersecurity Cover 100% of our relevant applications with Siemens Zero Trust Baseline: 16% FY24	EU-Taxonomy Increase our EU Taxonomy revenue alignment rate Baseline: 46% FY24
	Ambition 100% 	Ambition 100% 	Ambition Rate increase 
Resource efficiency & circularity	Robust Eco Design Achieve 100% for relevant hardware, software, and service portfolio Baseline: 16% FY21	Waste to landfill Support circularity by pursuing zero waste to landfill Baseline: 0% FY21	Biodiversity Implement a conservation program at 100% of our relevant sites Baseline: 17.7% FY24
	Ambition 100% 	Ambition 100% 	Ambition 100% 
People centricity & society Equity Employability	Pay equity Pursue pay equity by reducing the global adjusted pay gap Baseline: 2.5% FY24	Inclusion level Sustain an inclusion level above 80% Baseline: 80% FY24	Work Well-being Score Maintain a Work Well-being Score above 80 Baseline: 84 FY24
	Ambition Gap reduction 	Ambition >80% 	Ambition >80 
Total learning hours Increase our average to 40 hours per person Baseline: 34.2 h FY24		External learning offerings Reach 3 million people in our business ecosystem and society focused on digitalization and sustainability Baseline: 615 k FY24	
Ambition 40 h 		Ambition 3 m people 	

Regional responsibility for 26 countries¹



Siemens AG Österreich

- 3,100 employees
- €1.3 billion in revenue

Siemens in Austria¹

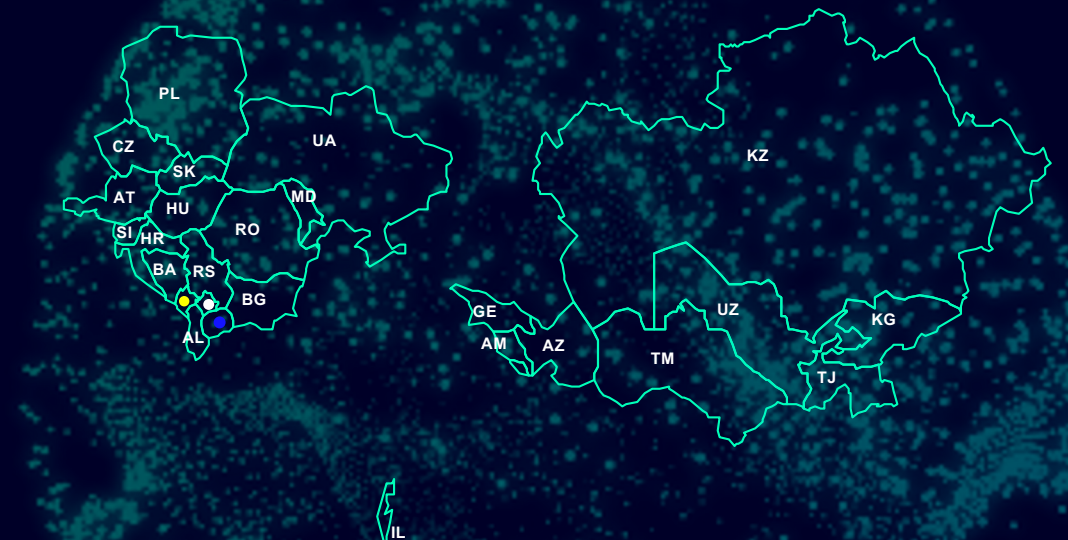
- 9,500 employees
- €3.3 billion in revenue

Lead Country Austria²

- 29,600 employees
- €6.8 billion in revenue

Siemens AG

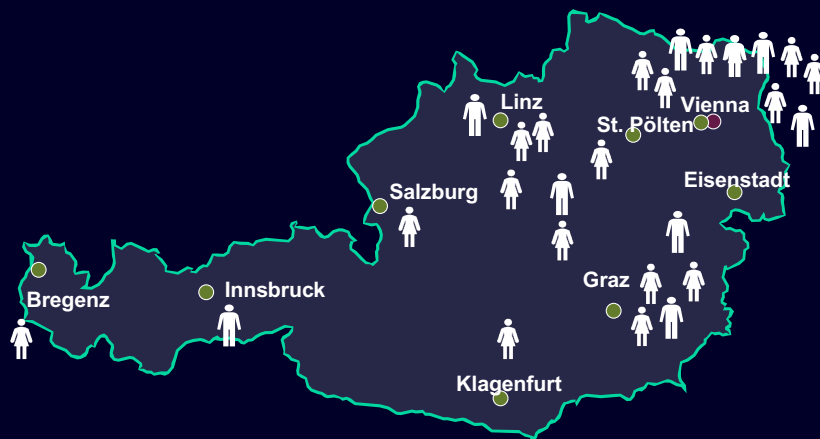
- 318,000 employees
- €78.9 billion in revenue



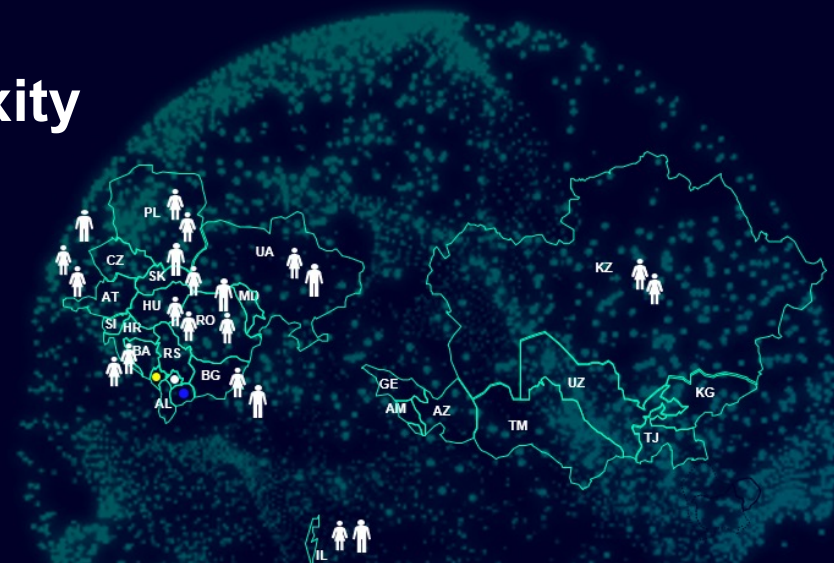
Fiscal year 2024 ¹ Includes Siemens companies in Austria that are majority-owned by the Siemens Group (Siemens AG Österreich [SAGÖ], Siemens Healthcare Diagnostics GmbH, Siemens Mobility Austria GmbH, and others) ² Operational responsibility for 26 countries/ includes Siemens Healthineers, Siemens Mobility, and others
Countries: ● Montenegro, ● Kosovo ● North Macedonia

LC AT – Mastering internal complexity

Cybersecurity Officers
Information Security Professionals
Cybersecurity Experts, ISMS Manager
Collaborative Network



It's all about collaboration!



High number of IT assets
(IT applications and systems)

- Total Assets: > 350
- of which business-critical: > 120



- Clients: > 12,000
- Networks & Servers: > 1,120

- Cloud Accounts: > 20
- Cloud Resources: > 2,920

Over 400 responsible roles for assets & system oversight

Most products from corporate business, but
some products and solutions in local responsibility

SIEMENS

Siemens in Austria



3100
employees



6,900
suppliers



1.1 bn
purchasing volume



13.1 mn
investment volume



33.3 %
export ratio



- 1 Regional headquarter
- 9 Regional Offices (Sales and service)
- 3 R&D sites (T, SMO, SISW)
- 3 Production plants (DI [1], SMO [2])

Businesses and Services of Siemens AG

Industrielles Geschäft

Digital Industries



Smart Infrastructure



Geschäftsbereiche bei Digital Industry (DI) in AT

- Product and Service Business
- Development
- Factory → e.g. Industrial Power Supply, Industrial Firewall
- Show Rooms: DigiLab, Living Lab

General

- Cybersecurity Hardware-/Softwareproduct and Solutions incl. Certificate management solutions

Geschäftsbereiche bei Smart Infrastructure (SI) in AT

- Electrification and Automation → e.g. Grid Automation, Development
- Buildings → e.g. Fire detection systems
- Electronic Products → e.g. low-voltage products (Switchgears)
- Grid Software → SCADA Systems, Development
- E-Mobility → Product- and Systemsolutions
- Show Room: SmartCity

DigiLab



Edge und Cloud Computing



Artificial Intelligence



Simulation



Cyberphysische Produktionssysteme



Intelligentes Energiemanagement



Fahrerlose Transportfahrzeuge



Industrial Security



Industrial Communication & Real Time Location System



Introduction

Cybersecurity in the convergence of IT and OT

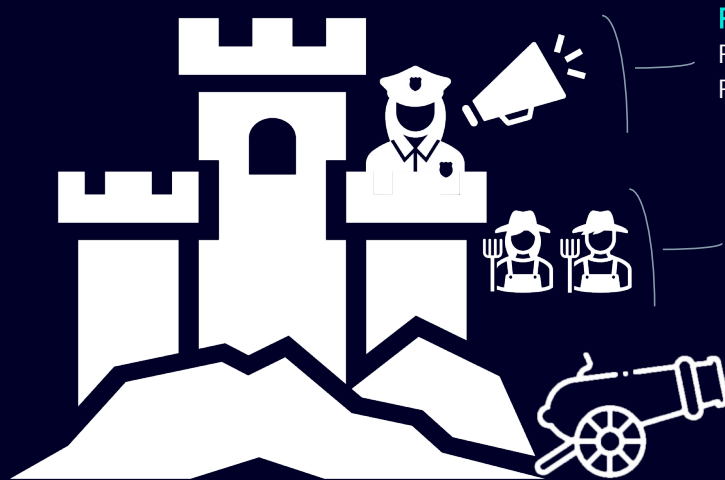
Introduction

Cybersecurity and the convergence of IT and OT



Cybersecurity

The ensemble of **technologies, processes** and **people** to protect individuals and organizations against **cybercrime**.



Processes

Procedures in case of alarms
Procedures for Incident Management

People

Trainees
Experts
...

Technology

Camera surveillance
Firewall
Antivirus
....



Cybercrime

- Criminal organizations
- States
- Terrorists
- Amateurs

Various
motivations

Financial profit
espionage

Destabilization
Fame / Fun

Introduction

Cybersecurity and the convergence of IT and OT



Data-driven decisions

- Continuous data analysis
- Best possible decision - concrete action
- Continuous improvement



Transparency

- Real-time analysis of workflows and processes
- Increase in performance



Sustainable development

- Identify energy & cost wastage
- Optimization of material availability

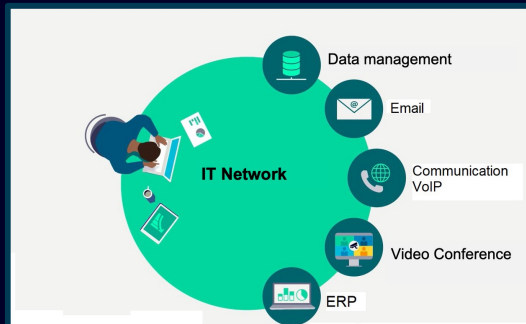


Innovation & Agility

- Continuous monitoring of production processes
- Continuous improvement
- Adequate support

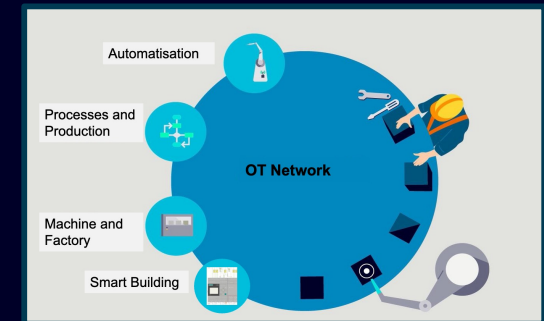
Introduction

Cybersecurity and the convergence of IT and OT



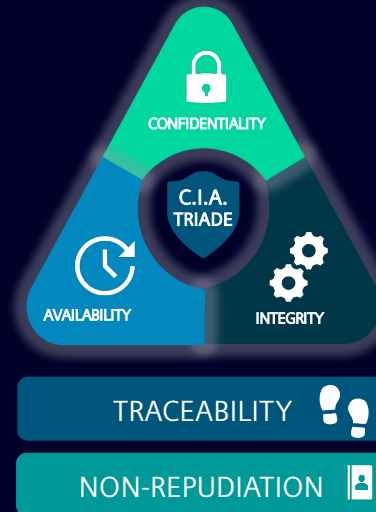
Requirements of IT

- Controlled environment**
E. g.: Air-conditioned data center
- Performance**
Efficient & secure communication
- Authentication**
of all users – Industrial espionage
- Confidentiality**
Mobile working + BYOD



Requirements of OT

- Challenging environment**
Need for rugged devices
- Quick response times**
Production: orders in milliseconds
- High availability**
Safety of people and machines
- Defense in depth**
Availability and integrity





Challenge at the interfaces of IT and OT

Challenges at the interface of IT and OT

Complexity of digital twin integration



Special requirements on both sides

Interconnection of systems



Increase in the attack surface
Distribution of malware
Unauthorized access

Mobile terminals | BYOD



Increased connectivity
Delimitation of personal / professional data

Converging threats



Cyberattacks can also
have a physical impact

Emerging threats



Data-oriented decisions
Effects on operating performance



Regulatory environment - Joint expertise

Regulatory environment and joint expertise

Standards

Cybersecurity IT

- ISO 27001
- TISAX

Cybersecurity OT

- IEC 62443

Security (Functional Safety)

- IEC 61508
- IEC 61511

Guidelines

GDPR

NIS 2 Guideline / NISG2026

CRA - Cyber Resilience Act

CER – Resilience in Critical Infrastructures

DORA – Dig. Operational Resilience Act

Machinery Regulation

AI Act



Development of a collaborative security framework

The development of a collaborative security framework

A collaborative framework between Cybersecurity, IT/OT & security
Goal: guarantee a uniform, coherent & coordinated approach

Information sharing

Sharing information for a better understanding of threats and vulnerabilities

Emerging threats, empowers all teams to strengthen their defenses

Coordination of security activities

Joint audit and compliance plan

Identifying security gaps that require immediate action

Response to non-conformities

Having an incident response plan in place that involves both Cybersecurity and security teams

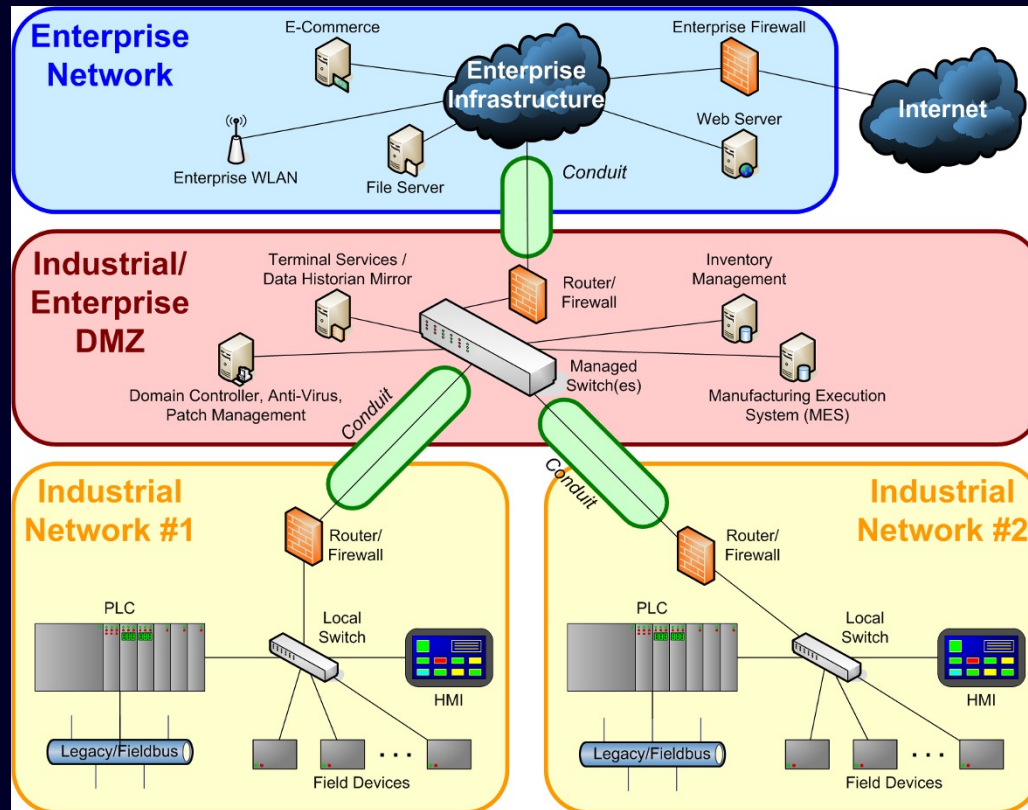
More effective and comprehensive crisis management

Continuous training

Maintaining expertise and raising awareness of new threats

Understanding each other's challenges | Keeping up to date with the latest trends | Crisis management training

Scope of the IEC 62443 Standards



IT Security Policies & Pract.
(e.g. ISO 2700x, etc.)

Process Safety
(e.g. IEC 61508)

ISA/IEC 62443

OT Security Policies & Practices

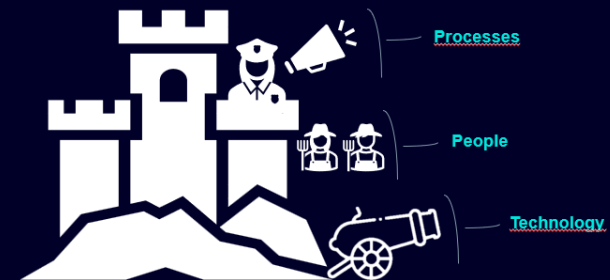
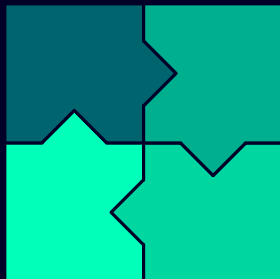




Holistic security approach

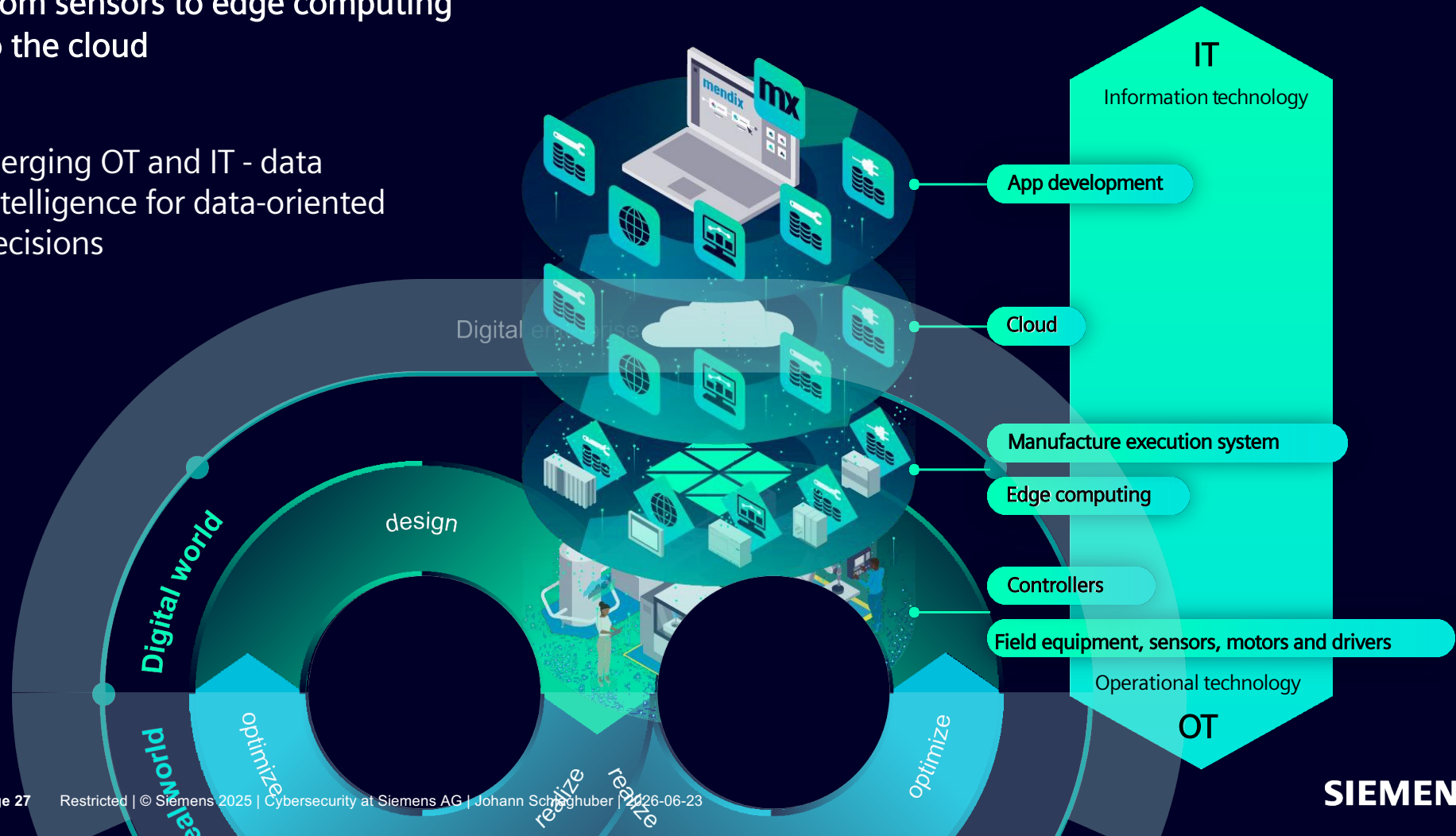
People – Processes – Technology

Collaboration



From sensors to edge computing to the cloud

Merging OT and IT - data
intelligence for data-oriented
decisions



Cybersecurity Governance at Siemens

Our Mission

- **Secure** the IT/OT infrastructure, to **ensure information security along the lifecycle** of Siemens products, solutions and services, as well as in all internal business processes.

- **Provide transparency** on the status of cybersecurity and risk exposure.
- **Offer a risk-based approach** and comprehensively cover cybersecurity for

IT – Information Technology

OT – Operational Technology

Products, Solutions/Services Security (PSS)



Cybersecurity Governance (publicly available [link](#)):

Importance of Cybersecurity is emphasized in our Cybersecurity Policy



SIEMENS

Cybersecurity Policy

Siemens Lead Country Austria

Cybersecurity (CYS) is an important issue for the future – for companies and society. It is a key prerequisite for organizations to safeguard critical infrastructure, protect sensitive information and assure business continuity. Siemens takes this responsibility very seriously and is therefore a co-founder and active partner of the „Charter of Trust“ (<https://www.charteroftrust.com>).

The objectives of Cybersecurity at Siemens are to secure the IT/OT infrastructure (Information Technology / Operational Technology), to ensure information security along the lifecycle of Siemens products, solutions and services, as well as in all internal business processes.

Cybersecurity affects and is affected by every employee of Siemens. Consequently, Cybersecurity is a collaborative task where the degree of involvement and responsibility depends on the individual roles and functions.

We are committed to fulfilling our responsibility in this regard.
This is ensured by the following principles:

- Compliance with external legislation and the specifications of major Cybersecurity standards like ISO 27001, ISO 62443 or TISAX as well as adherence to internal company-wide Cybersecurity regulations
- Definition of an organizational structure with clear responsibilities and measurable objectives of Cybersecurity
- Provision of adequate resources to plan, implement, monitor as well as continuously improve the operational effectiveness of the ISMS (Information security management system)
- Offer of internal communications and training to continuously promote appropriate behavior of all employees
- Strengthening of resilience to ensure optimal Business Continuity (BCM)
- Implementation of Cybersecurity is an integral part of the business strategy

For our society, customers and Siemens, we are a trusted partner – both in the real and the digital world.

Patricia Neumann
Chief Executive Officer

Bernd Ulbricht
Chief Financial Officer

Please visit our website to get further information about Cybersecurity Governance:

Version 1.0 Vienna February 2025 © Siemens AG

Cybersecurity (CYS) is an important issue for the future – for companies and society. It is a key prerequisite for organizations to safeguard critical infrastructure, protect sensitive information and assure business continuity. Siemens takes this responsibility very seriously and is therefore a co-founder and active partner of the „Charter of Trust“ (<https://www.charteroftrust.com>).

The objectives of Cybersecurity at Siemens are to secure the IT/OT infrastructure (Information Technology / Operational Technology), to ensure information security along the lifecycle of Siemens products, solutions and services, as well as in all internal business processes.

Cybersecurity affects and is affected by every employee of Siemens. Consequently, Cybersecurity is a collaborative task where the degree of involvement and responsibility depends on the individual roles and functions.

We are committed to fulfilling our responsibility in this regard.
This is ensured by the following principles:

- Compliance with external legislation and the specifications of major Cybersecurity standards like ISO 27001, ISO 62443 or TISAX as well as adherence to internal company-wide Cybersecurity regulations
- Definition of an organizational structure with clear responsibilities and measurable objectives of Cybersecurity
- Provision of adequate resources to plan, implement, monitor as well as continuously improve the operational effectiveness of the ISMS (Information security management system)
- Offer of internal communications and training to continuously promote appropriate behavior of all employees
- Strengthening of resilience to ensure optimal Business Continuity (BCM)
- Implementation of Cybersecurity is an integral part of the business strategy

For our society, customers and Siemens, we are a trusted partner – both in the real and the digital world.

Patricia Neumann
Chief Executive Officer

Bernd Ulbricht
Chief Financial Officer

Please visit our website to get further information about Cybersecurity Governance:

Vienna, February 2025



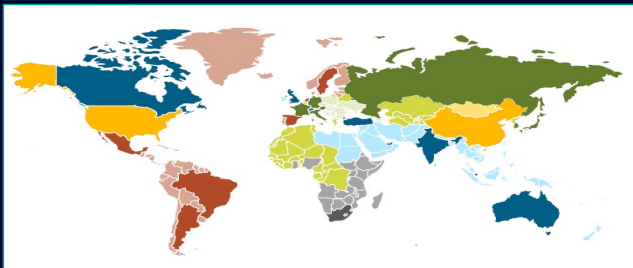
How we protect our company

SIEMENS CERT INCIDENT RESPONSE ([int](#)) ([ext](#)) ([dash](#))

Siemens CERT: cert@siemens.com
24/7 Emergency telephone: +49 89 7805 28999

Siemens ProductCERT: productcert@siemens.com
24/7 Emergency telephone: +49 89 7805 27883

Cybersecurity in the Countries



CYS Defense



Siemens CERT



CYS Governance



- › Policy Framework
- › SFeRA - Security Framework and Regulations Application
- › Standards, Processes & Guidelines
- › Baselines, Instructions and Guides
- › Governance Announcements



- › ISMS - Information Security Management System
- › Certification according ISO 27001
- › Reporting and Controlling



- › PSS Initiative
- › PSS Guide
- › PSS Curriculum



- › WBT - Awareness & Training
- › PSS - Awareness Material
- › Cybersecurity Cards



- › Caremore (Access restricted)
- › CISOZARE List



- › Cybersecurity Risk Management
- › ACP Governance for D&I and IT/IOT
- › Supplier Risk Management incl. Cybersecurity Contract Clauses for external Providers
- › Exception Handling

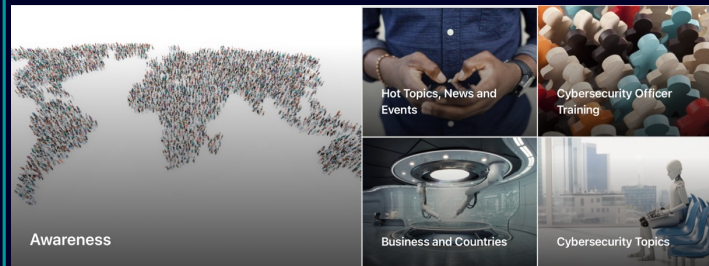
[Cybersecurity Governance \(publicly available link\)](#)

Cybersecurity at Siemens

- Cybersecurity Management – High Level Responsibilities, Accountable Managers
- ISO 27001 and other certifications – ISMS, Accredited Standards
- Cybersecurity Enterprise Architecture – Data-driven, Resilience
- Cybersecurity Policy Framework – Policies, Standards, Baselines
- Product and Solution Security (PSS) – Secure Environment, Binding Requirements
- Security Awareness – Trainings
- Cybersecurity Status Monitoring – CyberMart
- Cybersecurity Risk Management – ERM, ACP, ...
- Second Line of Defense – TLoD Model
- Information Security Incident Handling – CIA, Incident Response, ...
- Cybersecurity and Artificial Intelligence – Anomaly Detection

CYS Awareness & Knowledge

Cyber Sense



Annual Cybersecurity Training

^ Annual Cybersecurity Training (mandatory)



AI technology is revolutionizing many industries, and cybersecurity is no different. While integrating AI into daily operations offers numerous benefits, it's crucial to understand how to protect against cybercriminals who might use the same technology for more effective attacks.

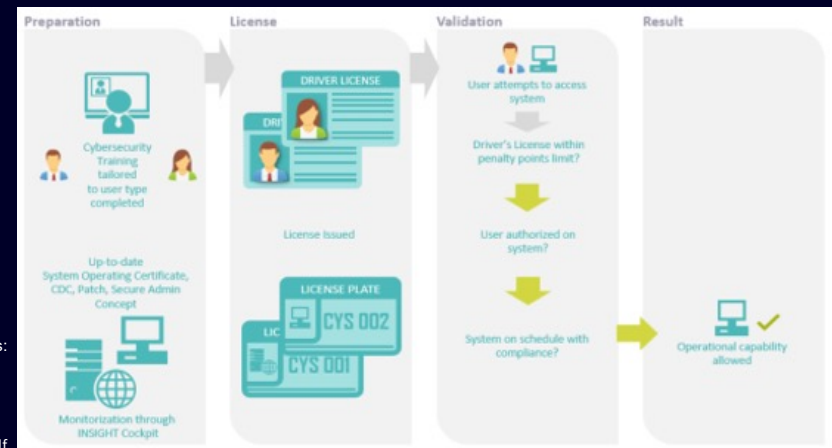
On this training you will meet Lisa, your AI-generated host, who will be joined by other avatars as we delve into the role of AI in your everyday business environment.

Cybersecurity Executive Training: [link](#)

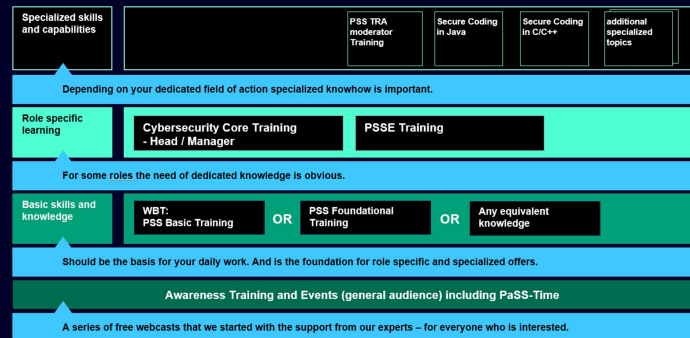
Driver's License

- Siemens has introduced the Driver's License and License Plate concept that provides a set of cybersecurity regular trainings and certifications.
- Certification is mandatory for Asset Owners, Asset Managers, and System Administrators.
- The Driver's license is also mandatory for those who are owning, managing, and operating Cloud environments:

Source:
SC236Common_Appendix_IT_OT.pdf



PSS Curriculum



Addressing all roles in ITAM

- System Owners / Admins
- Application Owner / Manager

[Cyber Sense](#)

[Knowledgeboard Austria](#)

[Knowledgeboard Österreich](#)

Addressing all PSSO/PSSE roles

SIEMENS



Customer Journey **Siemens Cybersecurity** Service Offering in Xcelerator by Siemens Partners



Cybersecurity @ Siemens

Siemens Cybersecurity Internally and for our customers

Cybersecurity for Siemens

We are passionate about enabling a resilient, data-driven Cybersecurity through a robust architecture to protect Siemens.

Security intelligence: We aim to implement an AI-supported and data-driven decision point that provides automatic Siemens Cybersecurity risk identification and mitigation by empowering decision-making.



[Cybersecurity Governance \(publicly available\):](#)

Cybersecurity for our Customers a few examples

- ❖ Certifications (ISO 27001, TISAX, KSV 1870) as maturity evidence, customer questionnaires, audits by customers
- ❖ Customer Awareness
- ❖ Cybersecurity solutions for customers (we sell what we use in our environment)
 - Consulting
 - Training
 - Asset Scan + Inventory / Asset Management
 - Refurbishment (bring cybersecurity up to date)
 - Vulnerability management in Products and Solutions



[Cybersecurity in Austria \(publicly available\):](#)

ACSC 2025 Kick Off bei Siemens Wien



ACSC2026 & Siemens – Timeline



Kick Off OT Security Workshop am 23.06.2026 📍 Siemens AG in Wien

Wettbewerb am 16. und 17. September 2026, in Linz im Rahmen der IKT ➔ <https://seminar.bundesheer.at/>

Wir freuen uns auf spannende Hacking-Events!

Contact

Johann Schlaghuber
Head of Cybersecurity



Siemens AG Österreich
Siemensstraße 90
1210 Wien

johann.schlaghuber@siemens.com



SIEMENS