Digitalizacija in izzivi pri konvergenci IT in OT storitev

4. april 2023

SIEMENS

“Megatrends” shaping consumer behavior are having a major impact on the industry

Climate change

Reduction of carbon-footprint. Leads to CO_2 neutrality in production.

Individualization

The need for individual products leads to lot size one in the production.

Globalization

Global crises put supply chains under pressure. Leads to better security of supply in production.

Digitalization

Technologies enable seamless data management flow and connected systems.

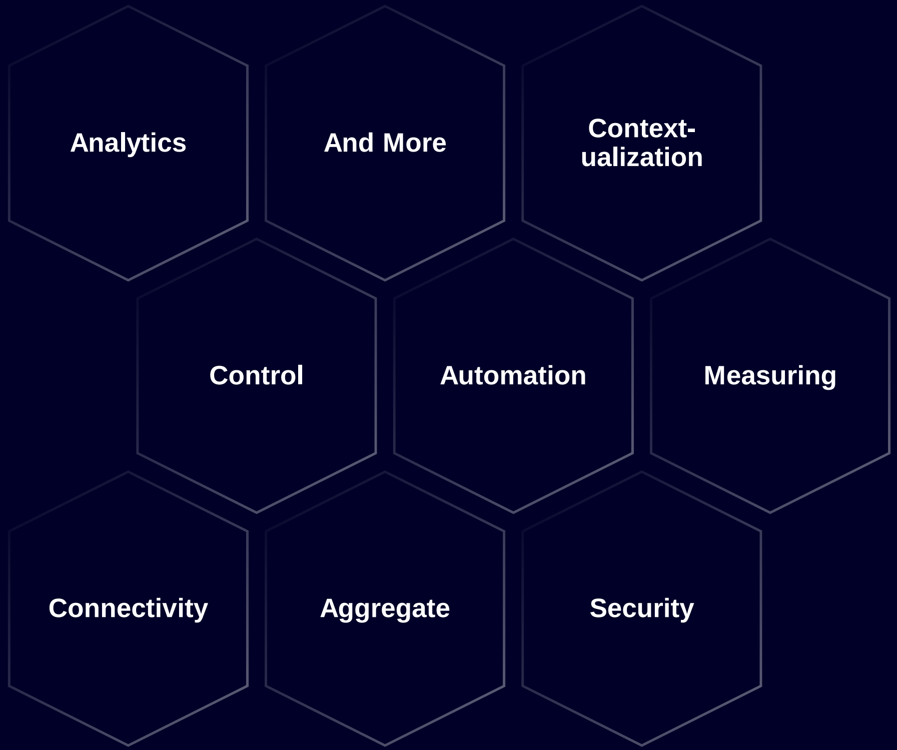
More Sustainability

More Flexibility

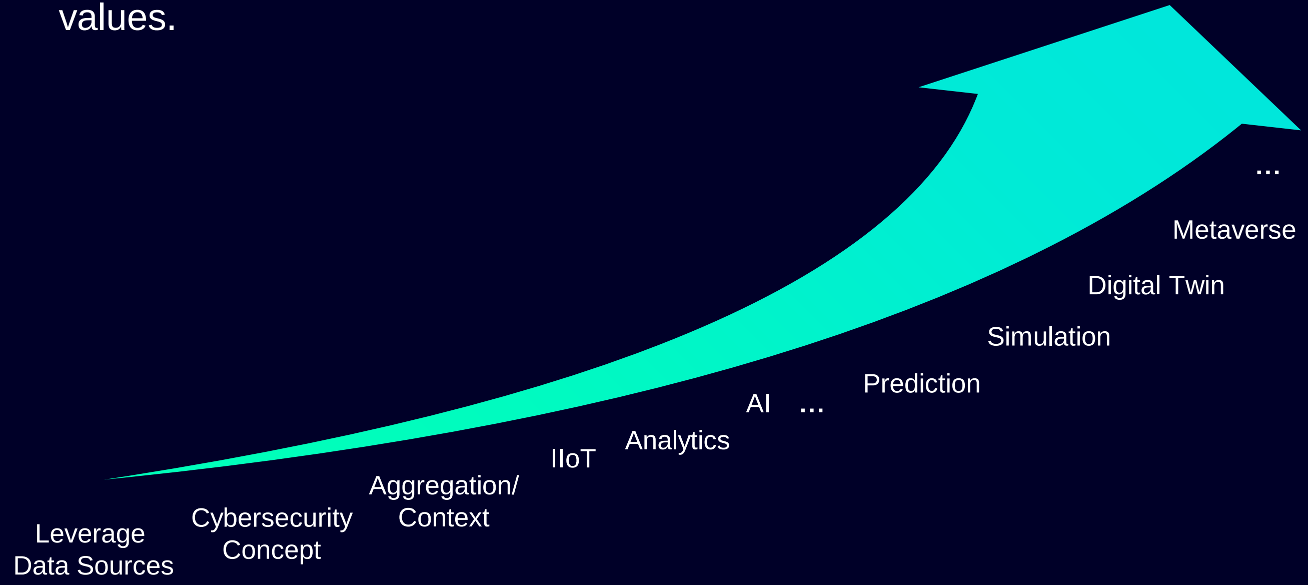
More Efficiency & Resilience

More Transparency & Quality

Digital Transformation can only be enabled by the Integration of technologies and domains across OT and IT



OT and IT still separated systems leveraging own values.



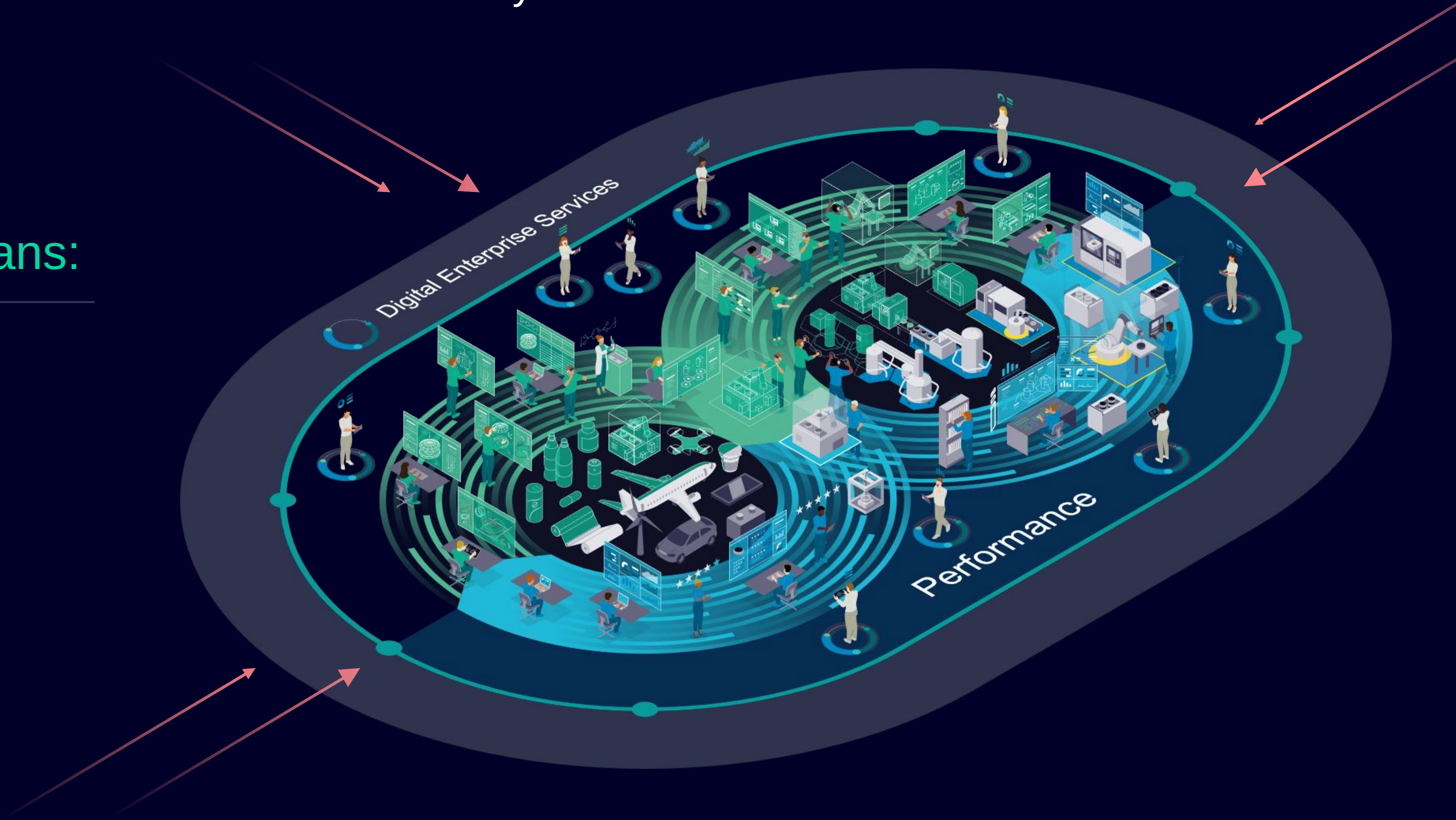
OT and IT must come together in an orchestrated integration Journey. Manufacturers are in different stages in this Journey.

Machines & automation systems are part of the IoT

This means OT/IT integration across all areas and layers

OT/IT converge means:

- 👍 **More connectivity**
- 👍 **More data**
- 👎 **New cyber-risks**



SIEMENS

Next gen automation

Transformation of our TIA pyramid to higher IT share

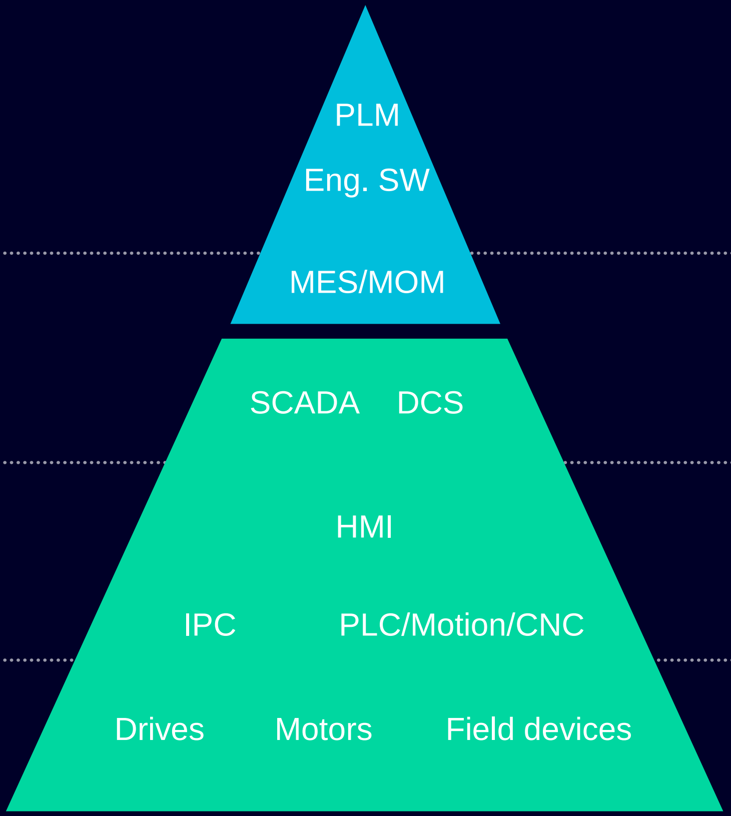
From …

Enterprise IT, Engineering software, …

Operations

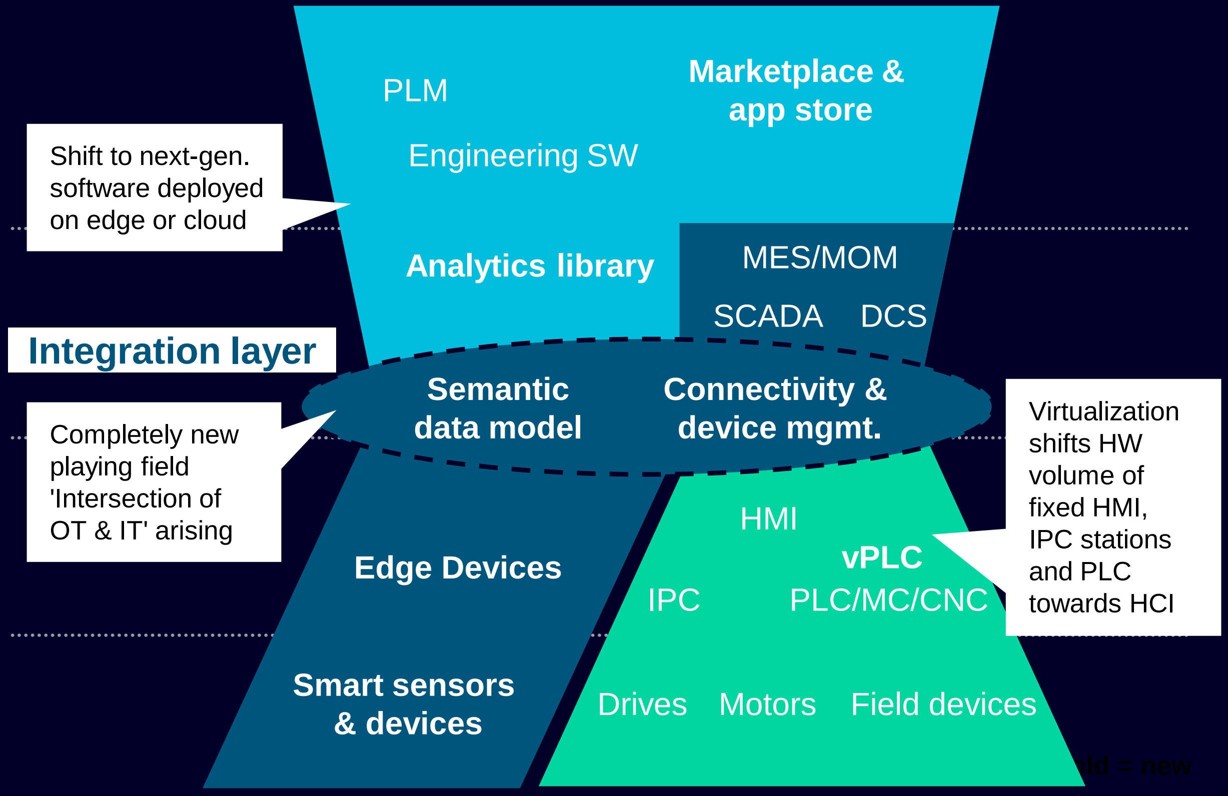
Control

Sense & Act



… to

Not exhaustive, schematic



Shift to next-gen. software deployed on edge or cloud

Completely new playing field 'Intersection of OT & IT' arising

Virtualization shifts HW volume of fixed HMI, IPC stations and PLC towards HCI

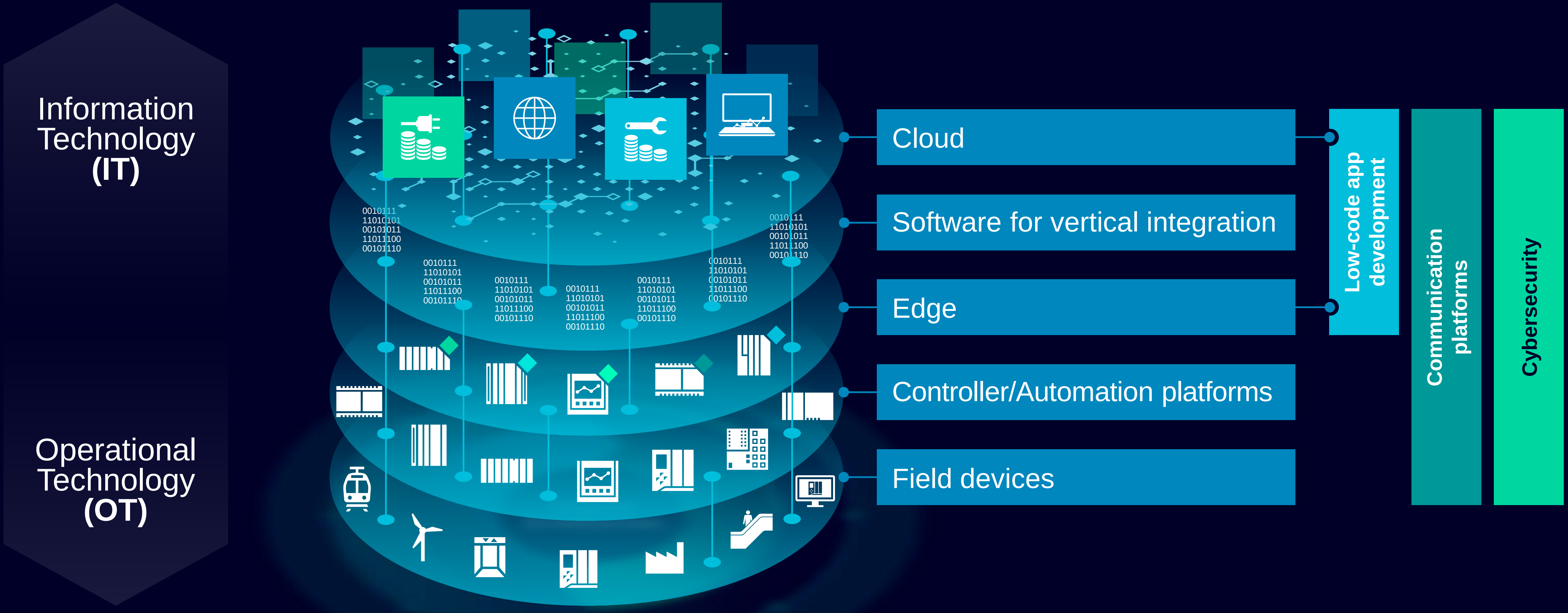
Note: HCI = Hyperconverged Infrastructure

🟩 OT 🟦 IT ▨ Intersection of OT & IT

SIEMENS

IT/OT integration across all areas and layers

Cybersecurity is a must have in IT **and** OT!



Information Technology (IT)

Operational Technology (OT)

Cloud

Software for vertical integration

Edge

Controller/Automation platforms

Field devices

Low-code app development

Communication platforms

Cybersecurity

Office (IT) and Industrial (OT) Communications are Fundamentally Different

IT Network		OT Network
Confidentiality Integrity Availability		**Availability** Integrity Confidentiality
Data transfer	**Purpose**	Production, control
IT / Network experts	**Responsibility**	Electro technical qualified personel
Controlled environment (Datacenter, office)	**Location**	Production, close to machines
~10ms (VoIP)	**Real-time**	128us (motion control, IRT)
Hierarchical, vertical communication	**Topology**	Flat, horizontal communication
Business hours	**Availability**	24/7 production
2-5 years, patching and upgrades	**Lifecycle**	10+ years, limited patching or updates

The security needs of industrial control systems differ greatly from those of office IT

IT Security

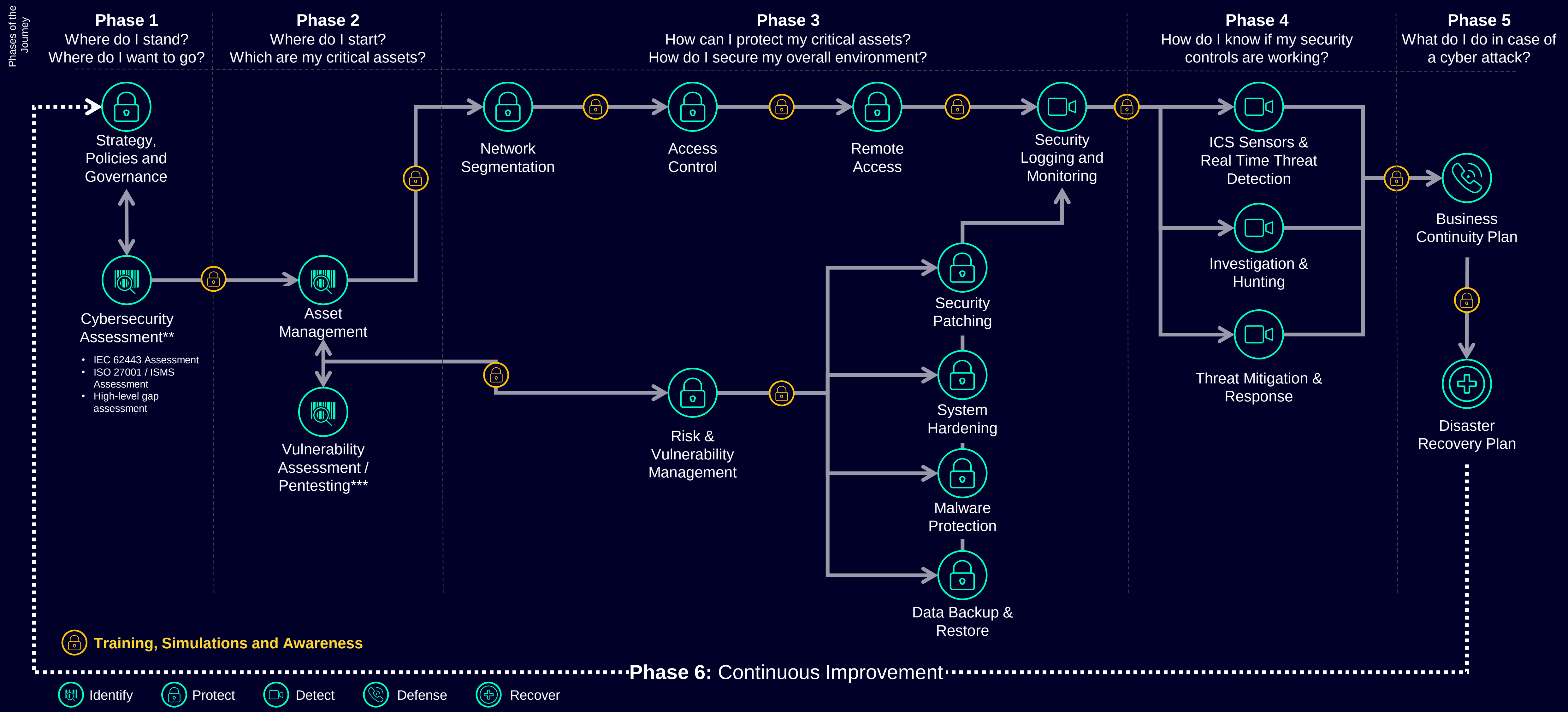
Confidentiality

Industrial Security

Availability and Safety

3-5 years	**Asset lifecycle**	20-40 years
Forced migration (e.g. PCs, smart phone)	**Software lifecycle**	Usage as long as spare parts available
High (> 10 “agents” on office PCs)	**Options to add security SW**	Low (old systems w/o “free” performance)
Low (mainly Windows 10)	**Heterogeneity**	High (from Windows 95 up to 10)
Standards based (agents & forced patching)	**Main protection concept**	Case and risk based

Cybersecurity step by step



Phases of the Journey

Phase 1
Where do I stand?
Where do I want to go?

Phase 2
Where do I start?
Which are my critical assets?

Phase 3
How can I protect my critical assets?
How do I secure my overall environment?

Phase 4
How do I know if my security controls are working?

Phase 5
What do I do in case of a cyber attack?

Strategy, Policies and Governance

Cybersecurity Assessment**

- IEC 62443 Assessment
- ISO 27001 / ISMS Assessment
- High-level gap assessment

Asset Management

Vulnerability Assessment / Pentesting***

Network Segmentation

Access Control

Remote Access

Security Logging and Monitoring

Risk & Vulnerability Management

Security Patching

System Hardening

Malware Protection

Data Backup & Restore

ICS Sensors & Real Time Threat Detection

Investigation & Hunting

Threat Mitigation & Response

Business Continuity Plan

Disaster Recovery Plan

Training, Simulations and Awareness

Phase 6: Continuous Improvement

Identify · Protect · Detect · Defense · Recover

© Siemens 2023 | Matjaž Demšar | Digital Enterprise Services | 4. 4. 2023

SIEMENS

> The highest priority within automation is to maintain the control of process and production.
>
> Any measurement to avoid the spread of any security threat may not interfere with this goal.

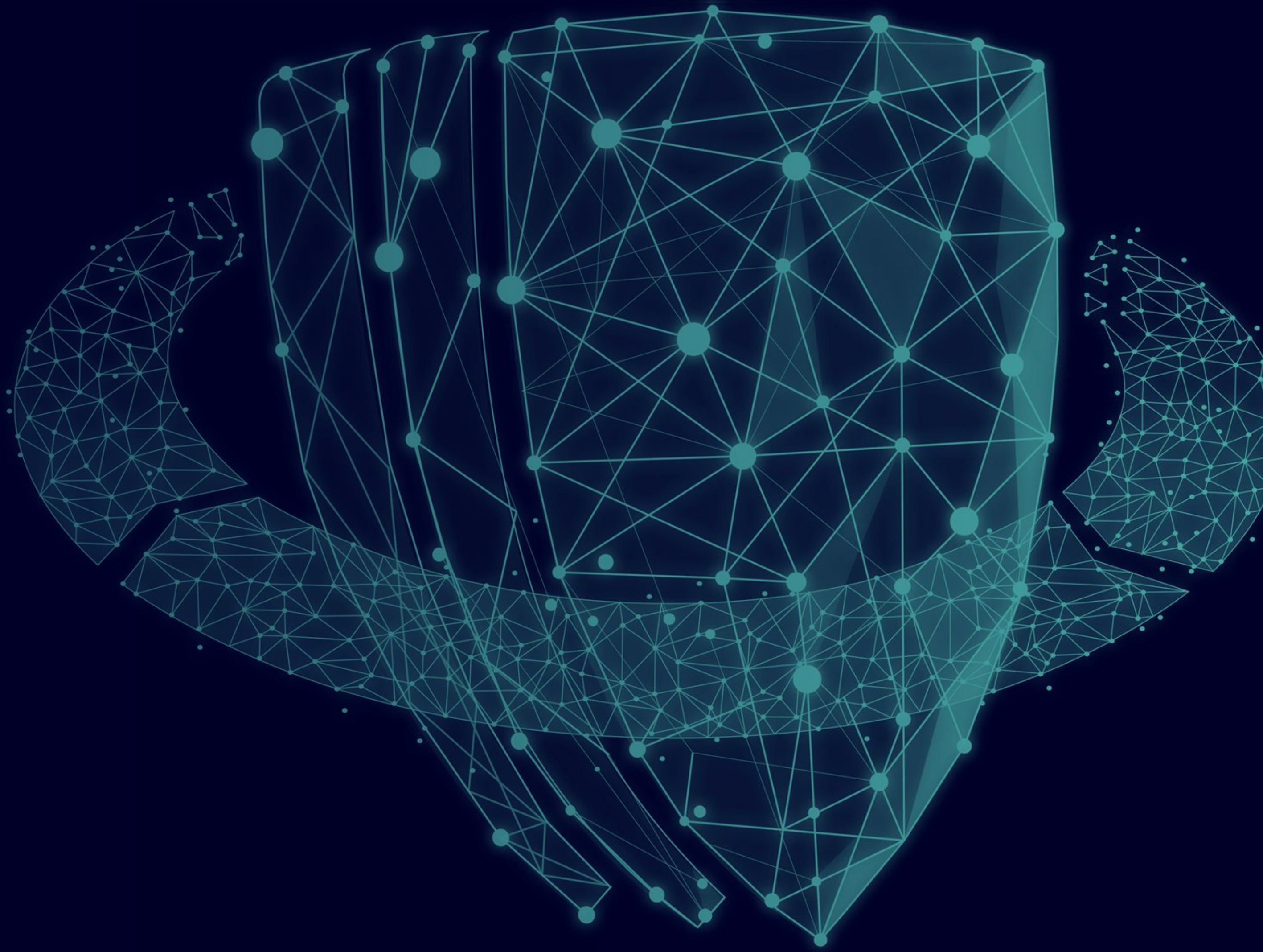
Thank You!

Published by Siemens Slovenia

Matjaž Demšar
Digital Enterprise Services Engineer
RC-SI DI S-REG
Letališka cesta 29c
1000 Ljubljana
Slovenia

Mobile +386 31 684 810

E-mail matjaz.demsar@siemens.com



Disclaimer

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations, product names, etc. may contain trademarks or other rights of Siemens, its affiliated companies or third parties. Their unauthorized use may infringe the rights of the respective owner.

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under https://www.siemens.com/industrialsecurity