IT/ OT Solution Day 2024

Die Zukunft der Fertigung:
OT Automation Blueprint für die Smart Factory

Driving Digitalization for Industrial Automation

Unrestricted | © Siemens 2024 Jörg Menzner | April 2023

SIEMENS

IT/OT

Herausforderungen der Digitalen Transformation

Den Stecker ziehen können !	**3** Wochen Prod. Ausfall
Unsere OT ist ein Komponenten Zoo !	OT Asset Standard
Den Knopf drücken können !	OT Asset Mngt. (FCAPS)
Das Brownfield greift an !	Standard Schnittstellen zw. IT/OT
Backdoors hinter der Hutschiene !	Intranet & Remote Access
Cloud First ! Private vs. Public !	Vom Sensor in die Cloud
Weg vom Papier !	Sichere Integration von MES & MOM
Mein LAN geht in die Cloud ! Safety ?	LAN Management in der Cloud
OEM Vorgaben & Standardisierung !	

= **IEC 62443** + **ISA 95**

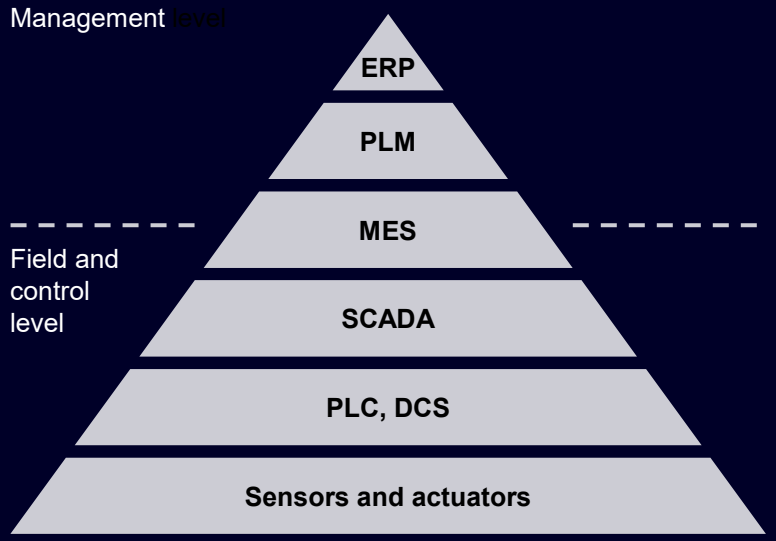
And the right **communication network** is the key

Unrestricted | © Siemens 2024

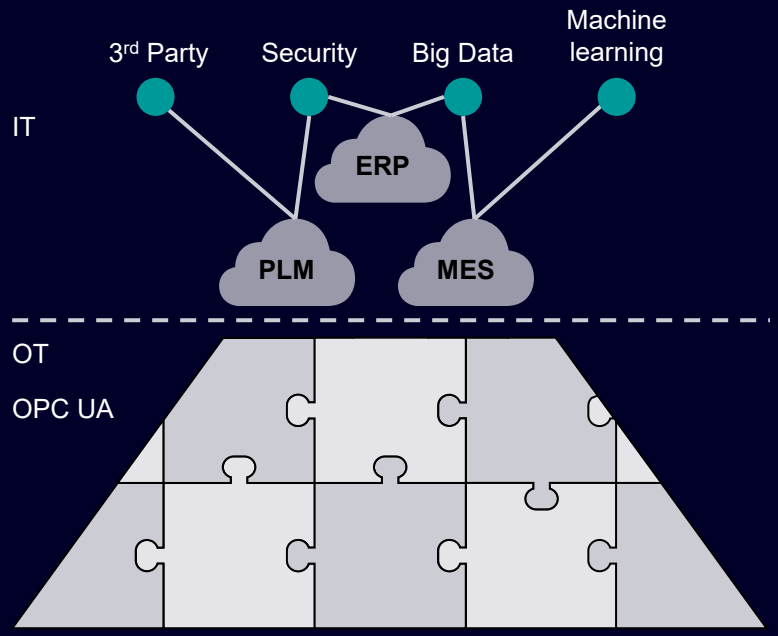
SIEMENS

Weg vom Papier / Cloud First

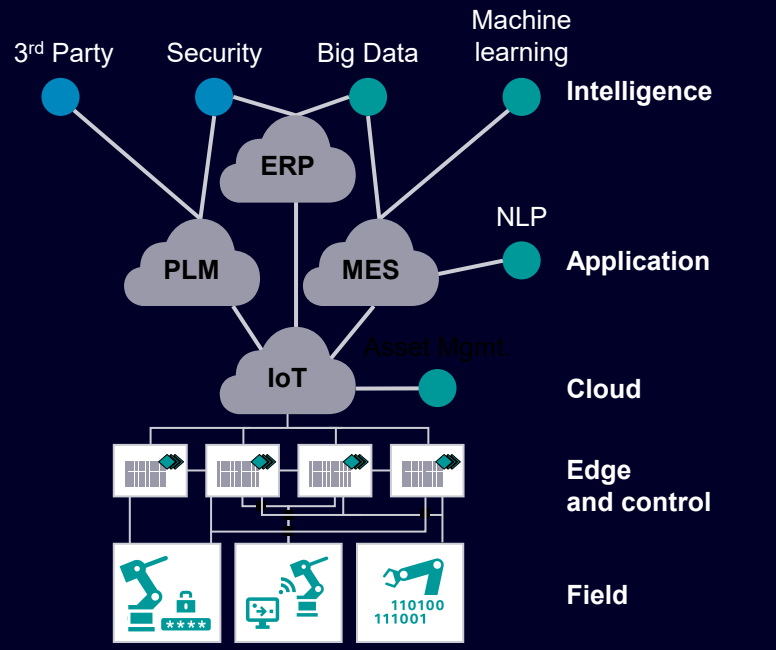
Yesterday



Today



Near Future



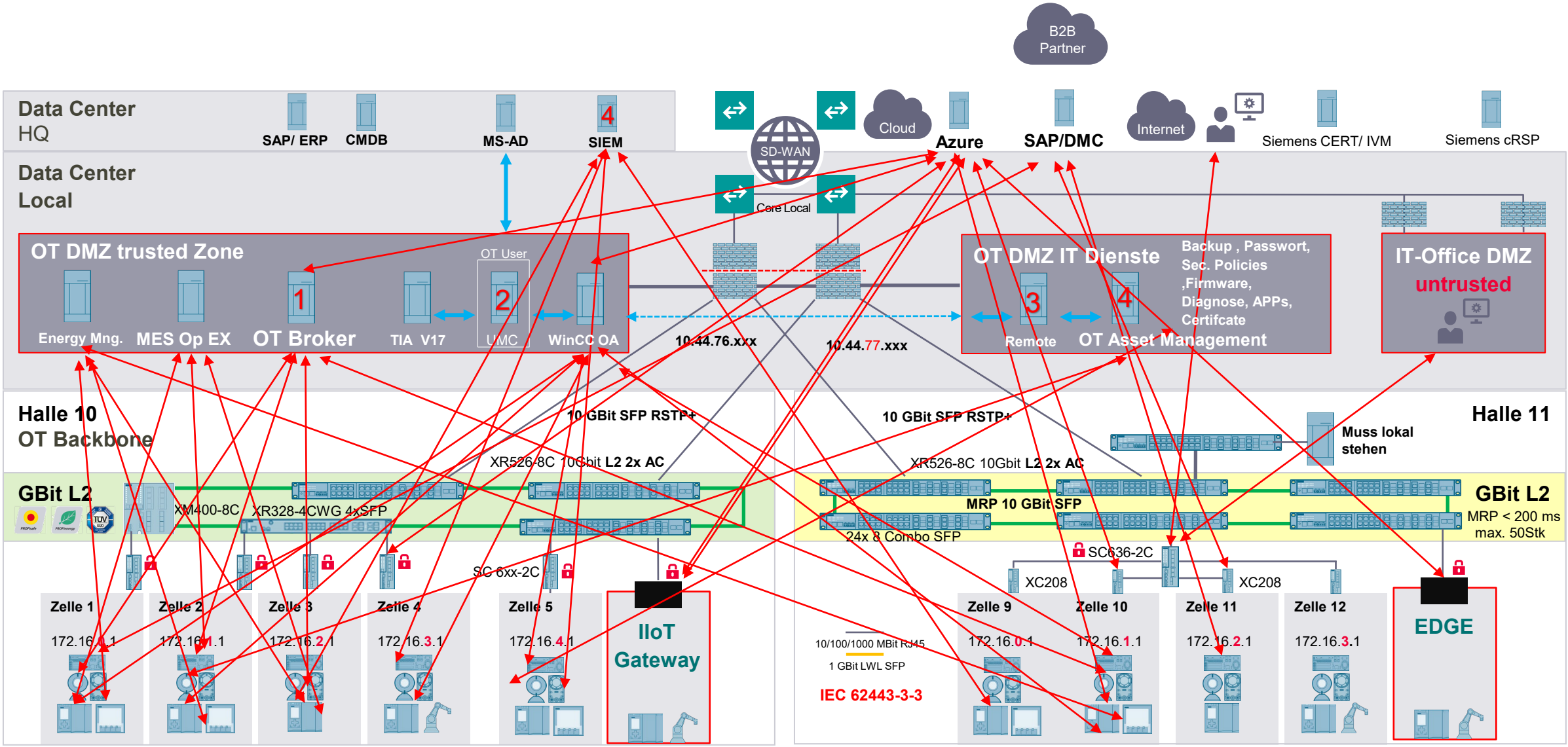
Monolithic Pyramid → The two worlds of IT and OT → End-2-End service oriented

Unrestricted | © Siemens 2024

Slide by Boston Consulting
Copyr ight © 2020 by Boston Consulting Group. All r ights reserved

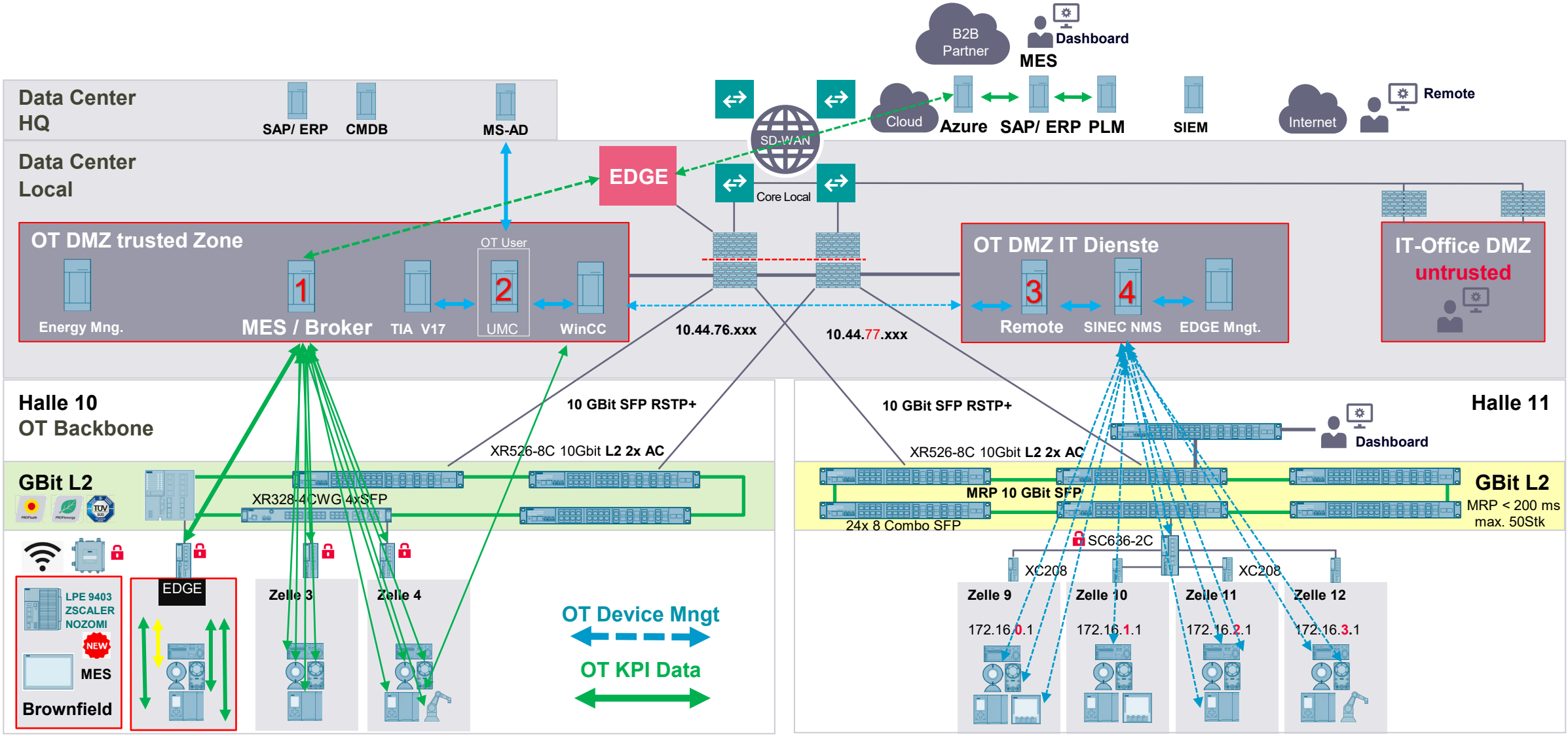
SIEMENS

Verboten ! Hohes Angriffspotential = Ist Zustand !



Unrestricted | © Siemens 2024
SIEMENS

Erlaubt ! Geringes Angriffspotential



Unrestricted | © Siemens 2024

SIEMENS

IIH / EDGE / App & Connector Suite

Easy, open & flexible App & Connector Suite

Totally Integrated Apps

Apps

Easy to start & scale

- Productivity increase
- Improve Resource Efficiency
- Improve machine interaction
- Maintenance optimization
- Reduce operational costs

Integ. layer

Open integration for OT & IT systems

OPC™ MQTT { REST:API } GraphQL 10 01

OT ⟷ IT

Connectors

Flexible OT Connectivity

PROFINET IO · Modbus-TCP · MQTT · Beckhoff ADS · SLMP · OPC UA

Sensor — Device — PLC — Machines — Lines

Unrestricted | © Siemens 2024

SIEMENS

Projektablauf

IST ANALYSE	EMPFEHLUNGEN	DESIGN	BUILD & TRANSITION

Quality Gates

Funktionsbeschreibung ISA 95, Safety, Security	**Technische** Maßnahmen	**IT/ OT Blueprint** HW, SW, Sizing	**Cloud/ IT/ OT PoCs**
Prozessbeschreibung Maschinen / Anlagen	**Organisatorische** Maßnahmen	**Service Design** Cloud/ IT/ OT	**ROLLOUT**
IT/ OT Netzanalyse OT Assets,Traffic, Zonen	**IT/ OT Betrieb** 24x7, Partner ?	**OEM Leitfaden** Maschinen Konzept	**BETRIEB**
Masch. Assessment IEC 62443	**Management Summary** **Preisschilder !**	**SIMULATION** Cloud/ IT /OT	
Branchen GMP, KRITIS		**OT Data Modelling** umati,EUROMAP,PackML	

Unrestricted | © Siemens 2024

IST Analyse/ ISA 95: Prozessbeschreibung/ Funktionsbeschreibung/ Maßnahmen

Level X
Cloud

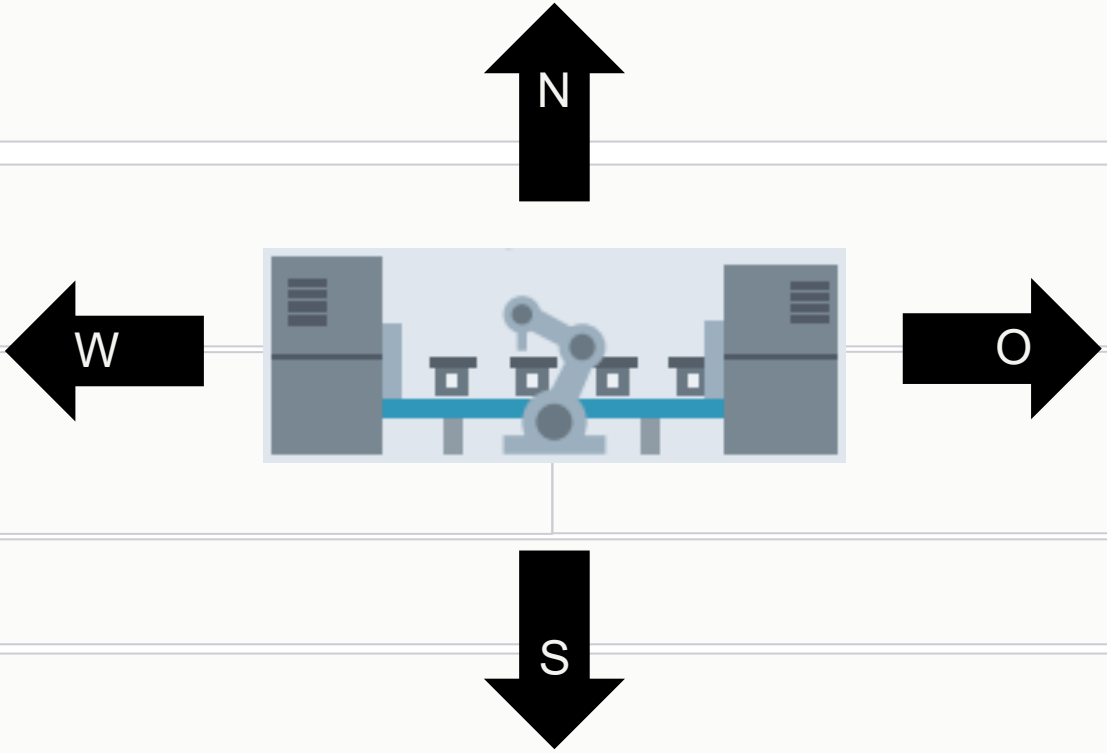
Level 4
ERP/ PLM
Local ?

Level 3
MES
Local/ Cloud ?

Level 2
ICS/ SCADA

Level 1
S7 CPU/ PLCs

Level 0
Aktoren/ Sensoren



Unrestricted | © Siemens 2024
SIEMENS

ISA 95: IST Aufnahme/ Security Zonen / Den Stecker ziehen können !

Level X
Cloud

SAP S4 HANA/ ERP / MES /MOM | Azure AD | IT/ OT/ Remote | ZSCALER

AWS / AZURE / EDGE Mngt | OT- Data Lake | ServiceNow

EDGE /Cloud

Level 4
ERP/ PLM
Local ?

SAP R&D / Engineering
PLM Teamcenter
SIMIT, D-Twin,Virt. -IB
CAD Siemens NX
M Center/ MC

SAP ERP
SAP Manufacturing

• SAP Asset Management
• SAP Service
• SAP Supply Chain

SAP Human Ressources
Zeitwirtschaft
Ideenmanagement
Compliance
Rechte/ Rollenmanagement
Personalmanagement

• SAP Financial/ Banking
• SAP Sales

IT Mngt. Systeme
Netzwerk / Security / Microsoft…
ISMS
Druckmanagement

Level 3
MES
Local or Cloud

Qualitätsmanagement | Werkerführung | Materialmanagement | Energiemanagement | QR Codes | Werkzeugmngt.

Auftragsmanagement | Zeiterfassung | Instandhaltung | Betriebsmittel Verwaltung | Messdaten | Ind. Bildverarbeitung

Datenerfassung
OT- Broker

Level 2
ICS/ SCADA

TRUSTED
MCenter | TIA Server
WinCC | File / SMB !
GMP | SQL / Database

UNTRUSTED/ OT Dienste
OT AD | Viren Pattern | White Listing | Passw, Ceriticate, Firmware Mngt.
NTP | **OT VLANs ?** | WSUS
OT Backup | IPC Backup

Remote Access
„n“ Lösungen ?

Gateway / EDGE

Level 1
S7 CPU/ PLCs

HMI
PLC

Maschinen

Scanner | Reader
Messdaten | Bilddaten

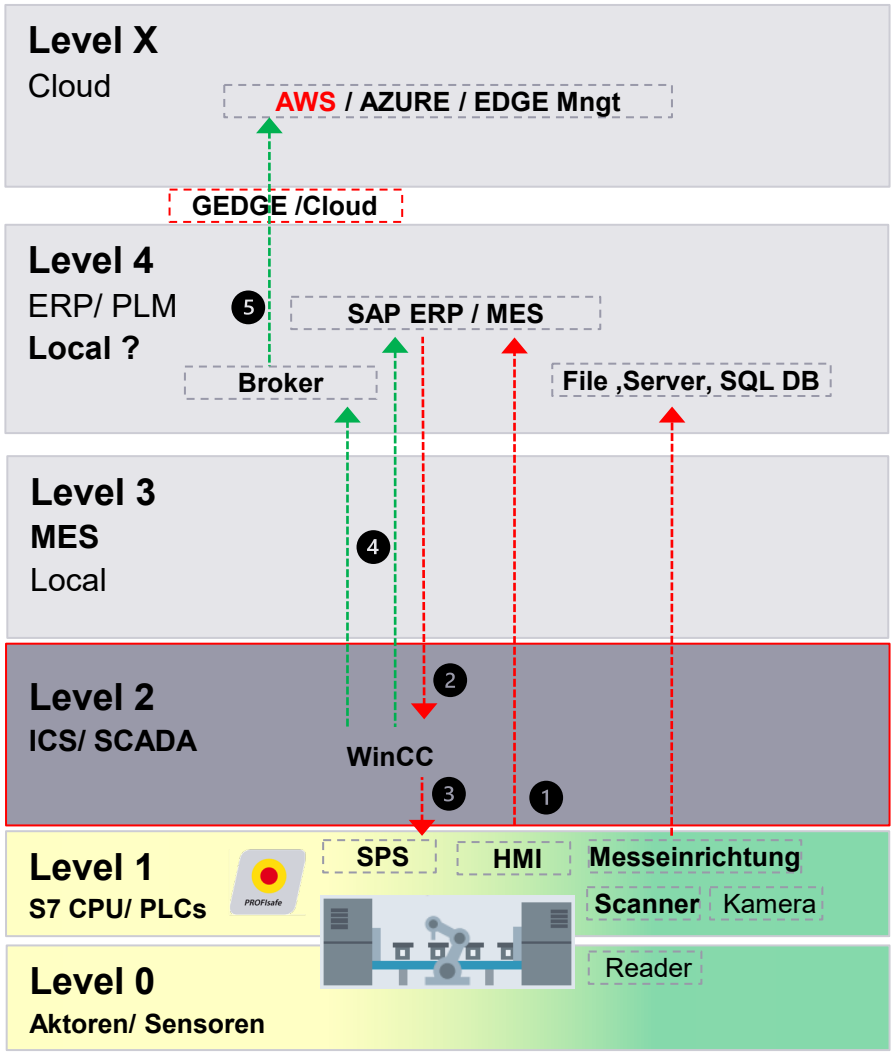
Level 0
Aktoren/ Sensoren

Unrestricted | © Siemens 2024

SIEMENS

IST Analyse, Security Zonen ?

ISA 95 Netzschichten



Funktionsbeschreibung

Maschinetyp Klasse 1
(400 Stk.)

Bidirektional:
- ERP + SQL Anbindung !
- File Server - HMI
- WinCC – SPS optimierung

SPS:
- S7 300 Step7 od. OPC UA

Bildverarbeitung:
- separater IPC (Win 7)

Messeinrichtung:
- separtater IPC (Win 3.11)

Prozessbeschreibung

Fertigungsauftrag wird derzeit noch von Maschinen Führer gescannt

Job wird an ERP gesendet (HMI + Scanner)

ERP sendet Daten QR/ QS an WinCC zurück

WinCC steuert über Variablen SPS + HMI

WinCC sendet Auftragsdaten zurück an Broker + ERP

Messeinrichtung sendet Daten an File FTP

Maßnahmen

Keine IT/OT Trennung mit L7 Firewall

Zu viele „Altlasten IPCs“ gefährnden Level 4

Maschine Remote über Backdoor !

Empfehlung:
Firewall Gateway zw. Level 1 +2
inkl. Remote
Keine Daten über SMB mit Zelle. 400 Maschinen in einem VLAN = hohes Risiko

Unrestricted | © Siemens 2024

IST Analyse, Maschinen NORD – SÜD Kommunikation

SÜD	System	BS	Applikation	TCP/	Ports	IP	L2/L3	Protokolle Dienste	Parametrierung Remote	Backup	Verschlüsselt	NORD	NORD Zonen	Ziel Systeme	Ziel IP	User AAA	Zero Downtime IEC 62443/ SL
Siemens Gateway	SC 626/ Remote +FW	--	Firewall + Remote + Segmentierung	TCP/ OpenVPN	80, 102,48.5 443,119 4	172.30.1.1	**NAT**	Https, Opc UA, OpenVPN SMB	Nur mit NMS	VersionDog/ P4Data	Nein	⇄	L1- L2	SINEMA RC	10.10.10.1	Ja	SC 626 Ja SINEMA RC Nein
SINUMERIK	840d	--	--	TCP	443, 123	172.30.1.10	NAT/ NTP		SRC	Auvesy/ P4Data	Nein	⇢⇠	L1- L2	WinCC /	10.10.100.x	Ja	Ja / SL 2
SINUMERIK	TCU	Win NT				192.168.214.241			Verboten	SSD	Nein						
Mcenter	IPC	Win10	Mcenter Tool Mngt.	TCP		172.30.1.20	NAT+NTP	Https, Opc UA	Verboten	Acronis	Ja	⇢⇠	L1- **L4**	Mcenter+PLM +ERP	10.10.200.x	Ja	Ja / SL 2
Siemens Sentron	PAC 4000		Netzlast Messung			172.30.1.30		NTP	Verboten			⇢⇠	L1- L2	SIMATIC Energy Suite			
Siemens Sentron	Schaltgerät		Netzlast Schalten			172.30.1.31			Verboten			⇢⇠	L1- L2	SIMATIC E Manager			
Siemens EDGE	**IIH**	Linux	Beckhoff/NodeRed	TCP		172.30.1.40	NAT	Https, NTP, OPC UA	Ja / SRC			⇢⇠	L1-LX	Ind EDGE Mngt Cloud	AWS		Nein
Siemens PLC	S7 1500 F	--			80, 102	172.30.1.50	--		Verboten								Ja/ 2
Siemens PLC	S7 1500	--			80, 102..	172.30.1.60	NAT	NTP	SRC	VersionDog		⇢⇠	L1- **L3**	WinCC + MES		Ja	Ja/ 2

Unrestricted | © Siemens 2024
SIEMENS

OT Dschungel ! Security Zonen / IDMZ/ OT Dienste

Cloud

zscaler | aws Azure | servicenow | BeyondTrust Remote TeamViewer | TIA V18 .....

EDGE

OT Data / Trusted (kritisch)

- SAP ERP
- Opcenter APS
- softing OT Broker Cybus
- Echtzeit-Lokalisierung mit RTLS
- **BDE** Betriebsdaten
- GMP
- Data Lakes SQL/ FTP/ SMB
- SENTRON
- WinCC OA
- WINCC

IT/OT

- aruba ClearPass
- FORTINET paloalto
- **ZERO TRUST**
- **Radius**

OT Dienste

- BeyondTrust
- Engineering Tools
- SIEMENS SIENMA RC
- TIA V18 TIA V17 TIA V16
- **TDM** Werkzeugverwaltung
- UMC SERVER
- Mcenter
- OT AD, **NTP**, DHCP…
- Passw. ,Certif. ,F-Ware Mngt
- Industrial Edge Hub
- Whitelist
- RA Server (CA)
- Viren Pattern
- PLUS4DATA OT Backup versiondog
- Acronis

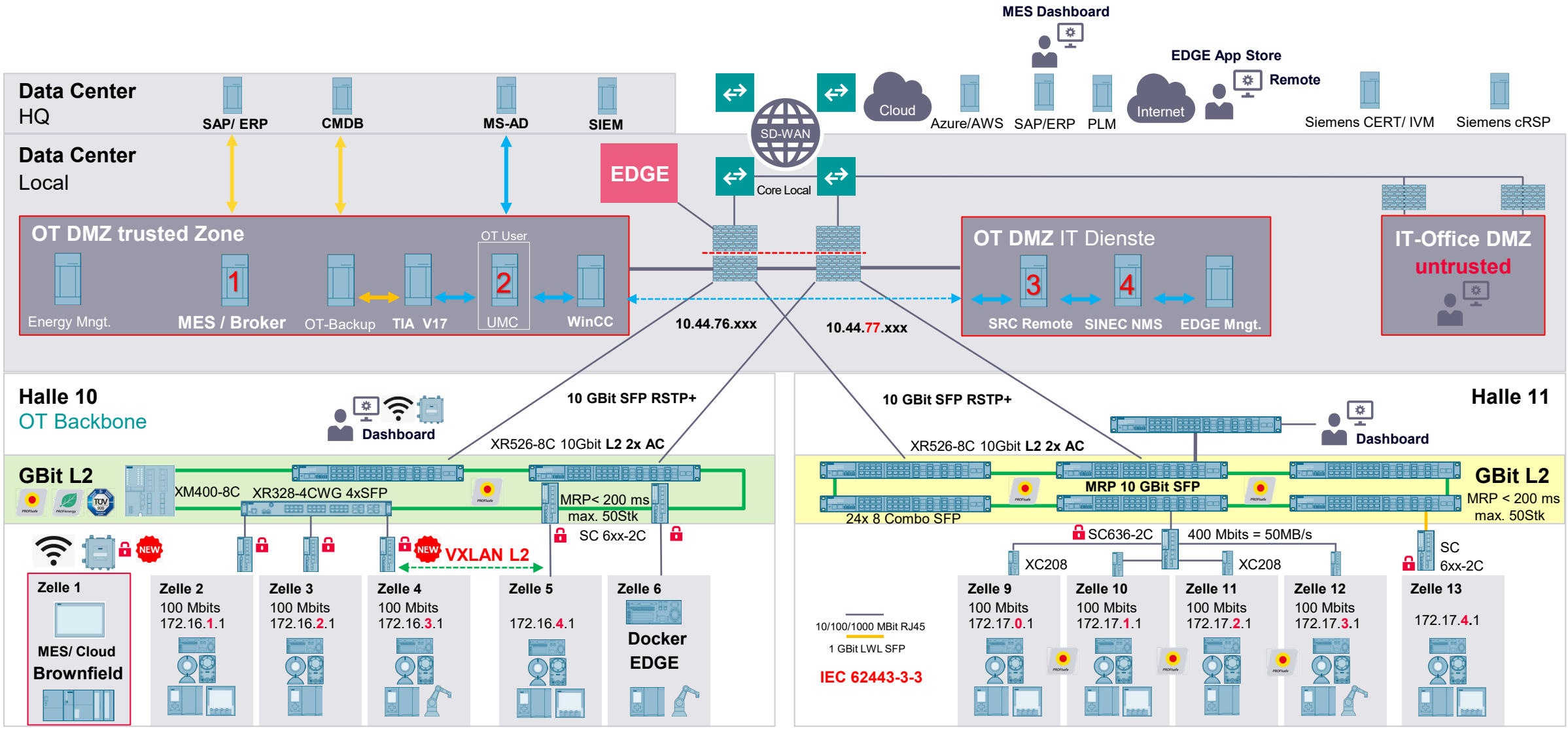
Maschinen

STEMMER IMAGING | BALLUFF | COGNEX

Firewall

EDGE/IIH | softing Cybus | zscaler Node-RED | Beckhoff ADS | FANUC

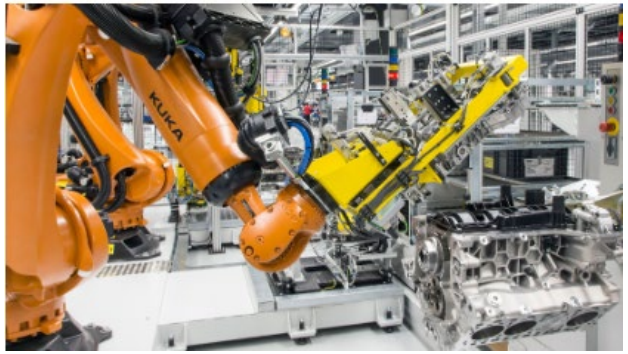
IEC 62443-3-3 „Bau einer sicheren Anlage“



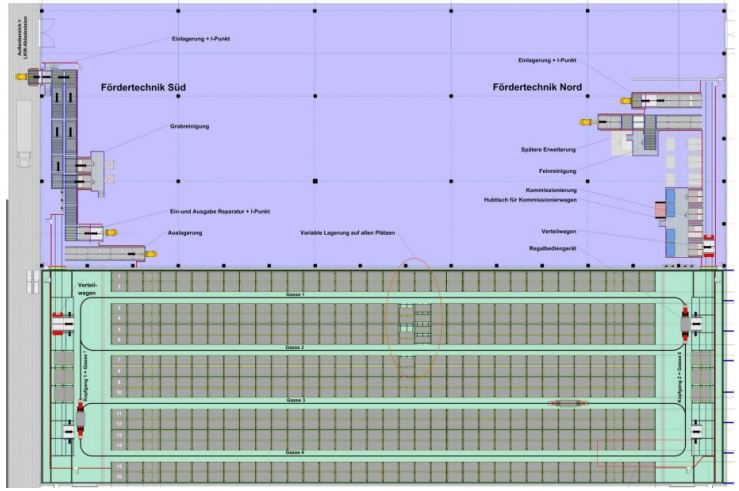
Unrestricted | © Siemens 2024

SIEMENS

Safety & Security



PROFIsafe



Unrestricted | © Siemens 2024

INTER-OPERABILITY

Die Welten wachsen zusammen

Unrestricted | © Siemens 2024

SCALANCE Firewalls
Industrial Security Appliance

SC632-2C **SC636-2C** **S615** **SC642-2C** **SC646-2C** **SC 622/626** **M804PB***

Ohne IPsecVPN

Mit IPsecVPN

Brownfield

PROFIsafe

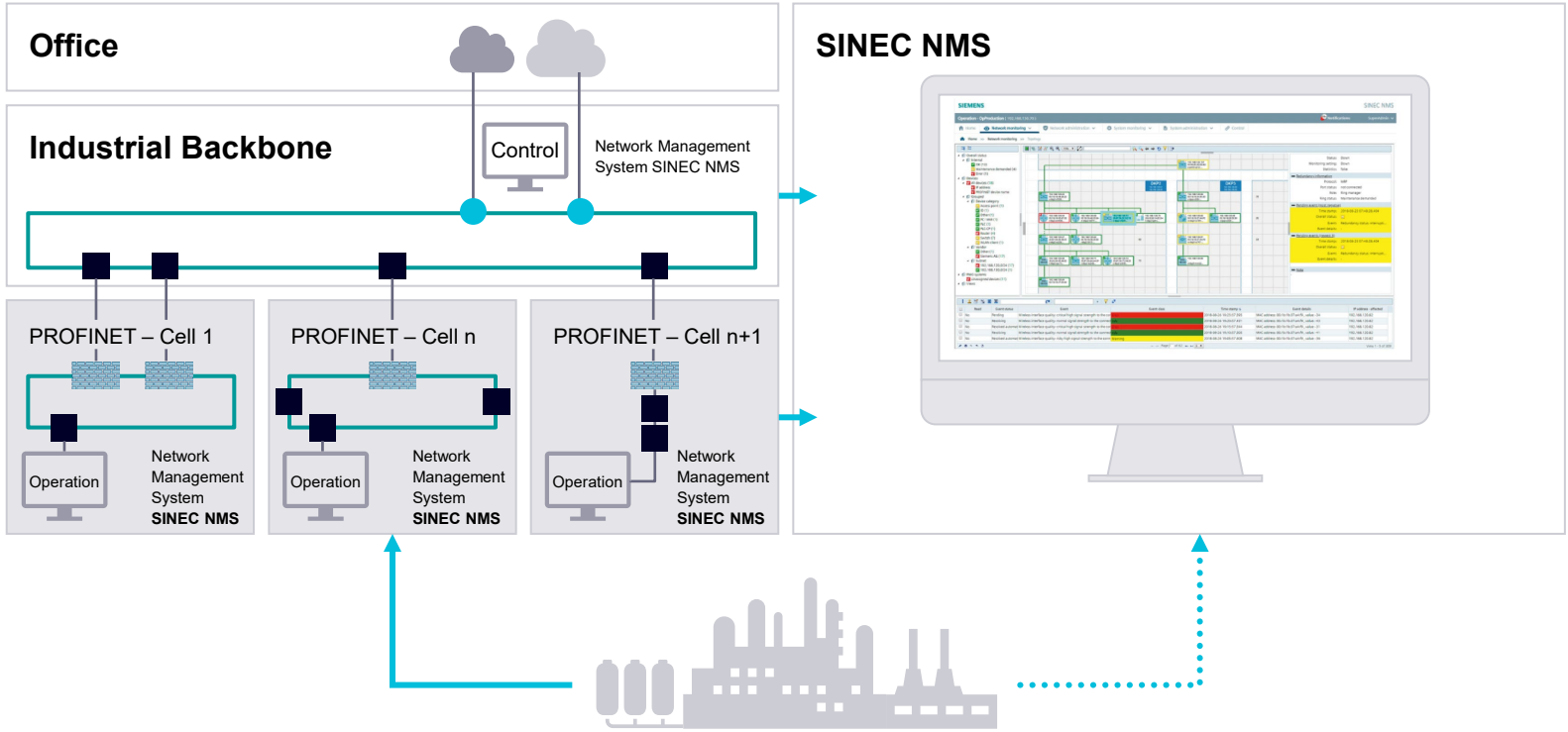
Unrestricted | © Siemens 2024

OT-NETWORK MANAGEMENT

- All-around Network Management System for industrial networks

  Policy-based network management

  Maximum transparency

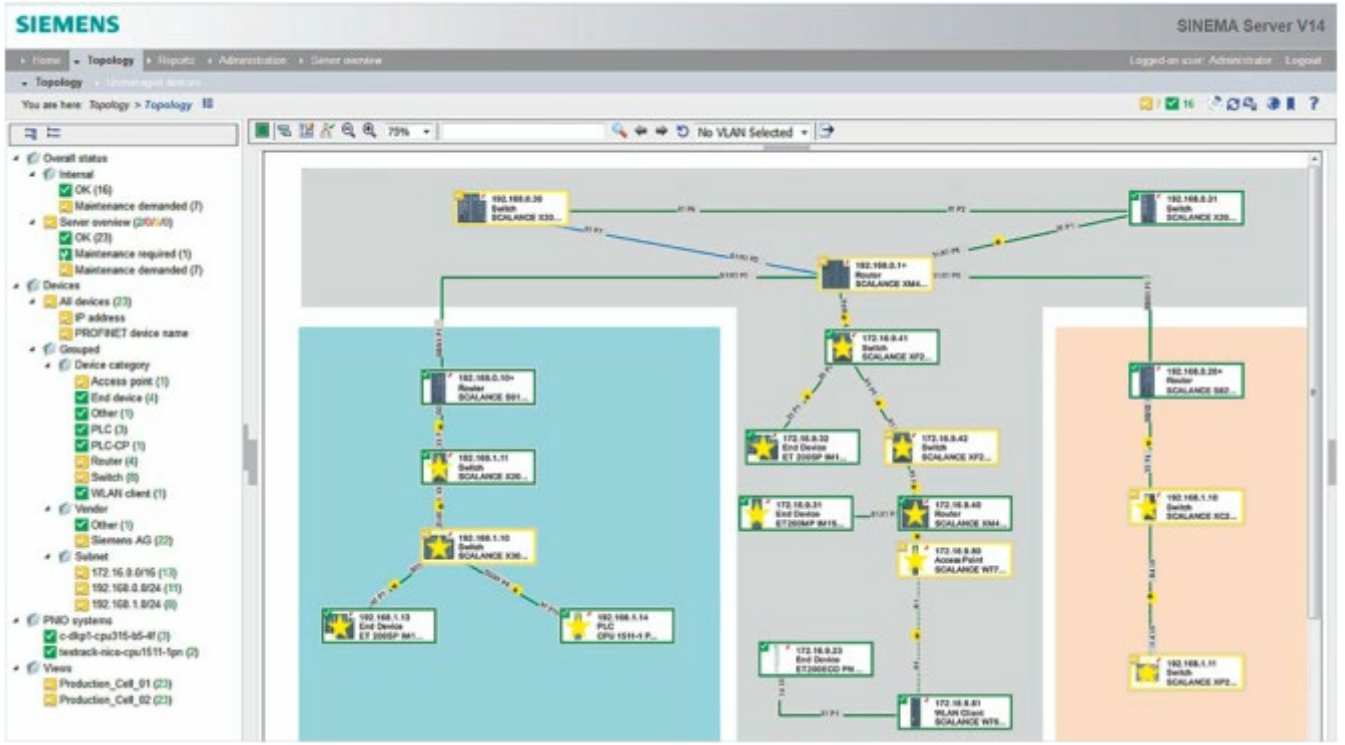


Fault Management incl. S7 CPU	Graphic representation
Validation and documentation	
Security Management	Transparent diagnostics
Openness and flexibility	

Unrestricted | © Siemens 2024

SIEMENS

SINEC NMS: Netzwerk-, PLCs-, Security- Management in der Produktion



Unrestricted | © Siemens 2024

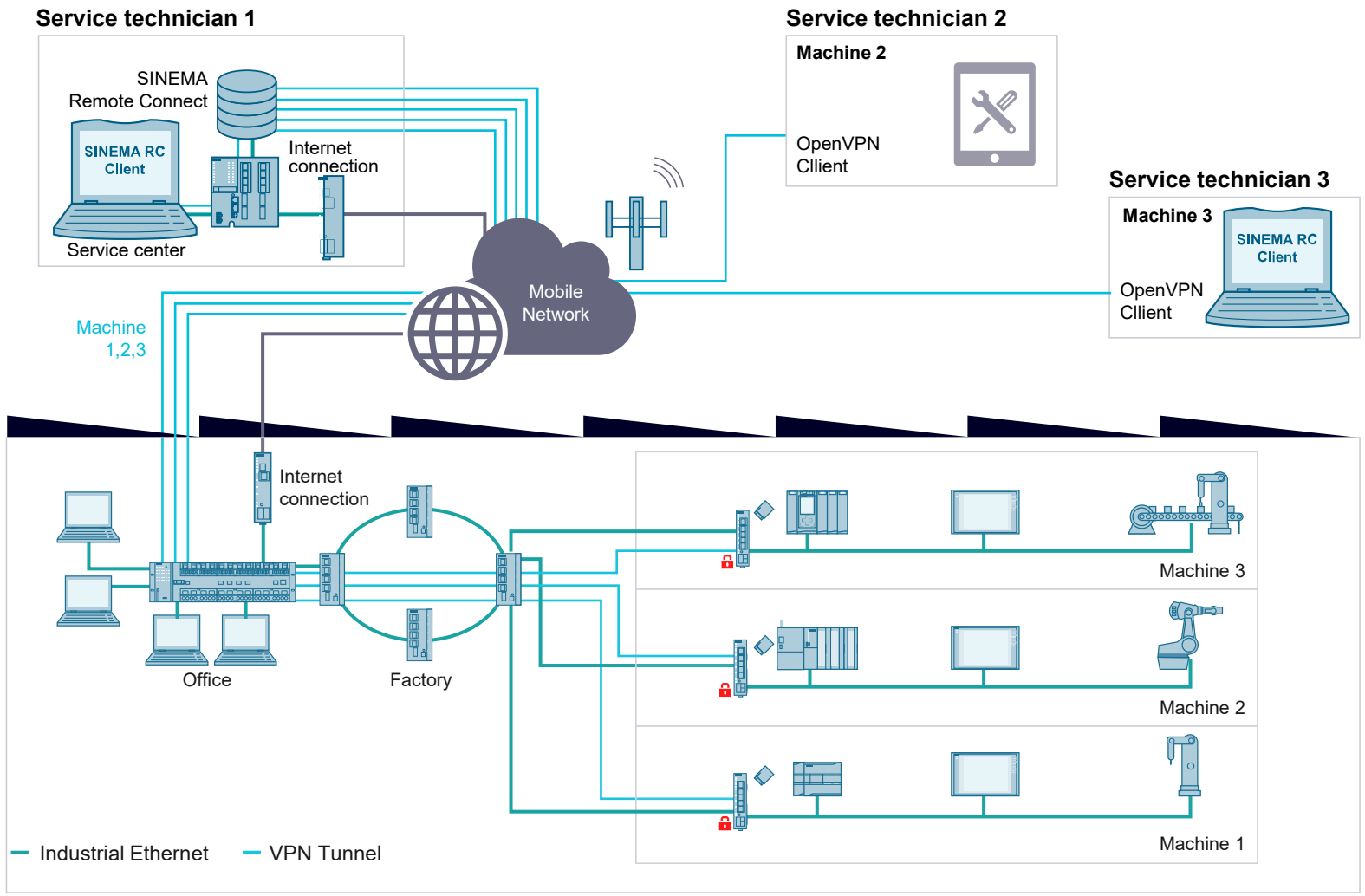
INTERNET &

Intranet Remote Communication

- High security (VPN) remote access to “things” for maintenance and troubleshooting

- Easy integration in existing plant networks and auto-configuration

- Standard user interface and flexible administration



Unrestricted | © Siemens 2024

SIEMENS

IEC 62443

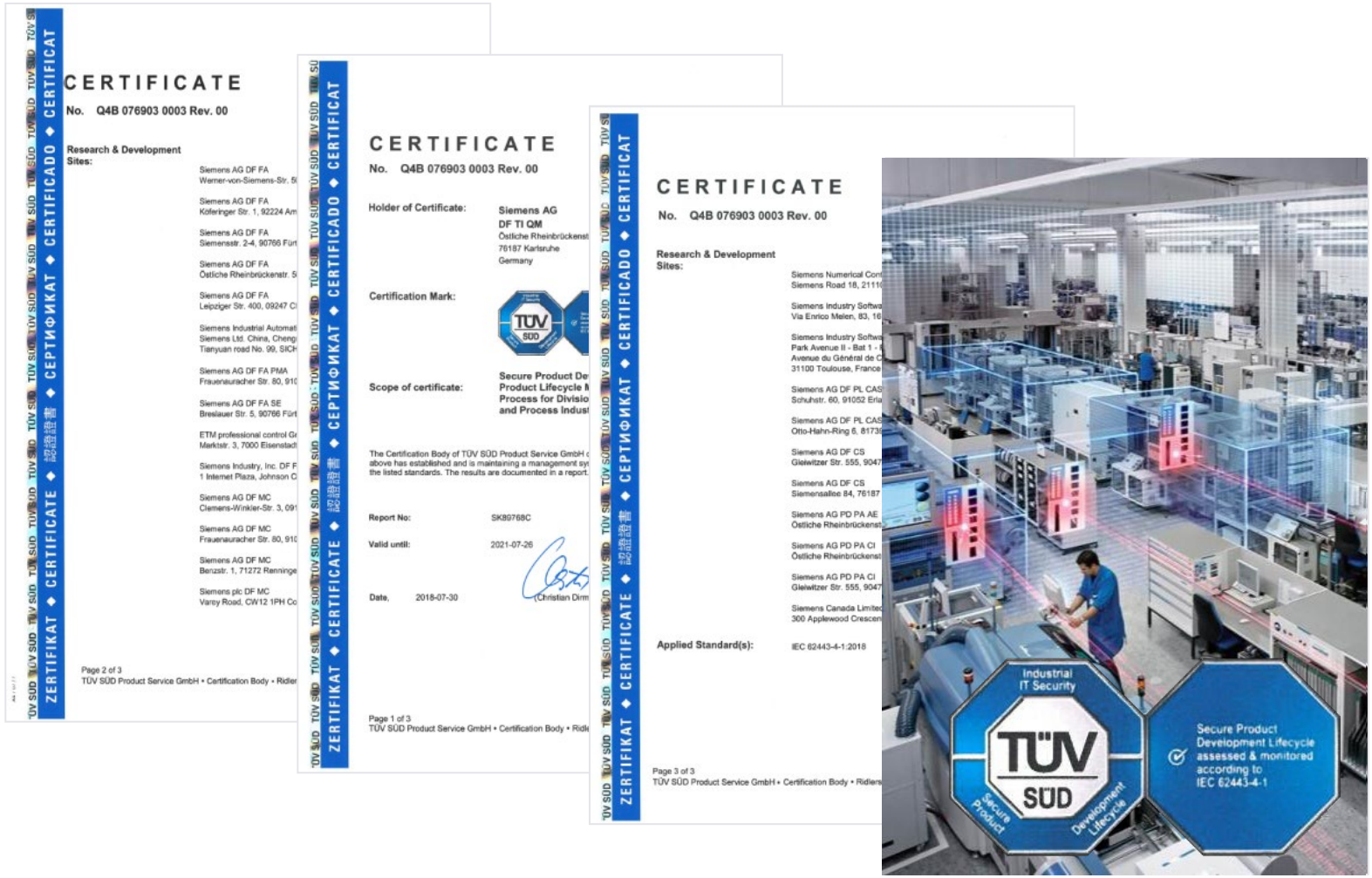
CERTIFICATES

Already starts in R&D

- IEC 62443-4-1
- IEC 62443-4-2

Read more

[Practical standards for Industrial Security]



Unrestricted | © Siemens 2024

SIEMENS

Industrial Security
Security-Hinweise

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen.

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen einen Bestandteil eines solchen Konzepts.

Die Kunden sind dafür verantwortlich, unbefugten Zugriff auf ihre Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Diese Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und nur wenn entsprechende Schutzmaßnahmen (z.B. Firewalls und/oder Netzwerksegmentierung) ergriffen wurden.

Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Security finden Sie unter https://www.siemens.com/industrialsecurity

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Produkt-Updates anzuwenden, sobald sie zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter https://www.siemens.com/industrialsecurity

Unrestricted | © Siemens 2024

Contact

Published by Siemens AG
Process Industries and Drives
RC-DE PD PA /PT 5

Jörg Menzner
Promotion Industrielle Kommunikation
Net Consulting

E-Mail: joerg.menzner@siemens.com

 Unrestricted | © Siemens 2021 | January 2021

SIEMENS