(I)OT Security *Auf dem Weg zur "Smart Factory"*

Cyber Security am Scheideweg

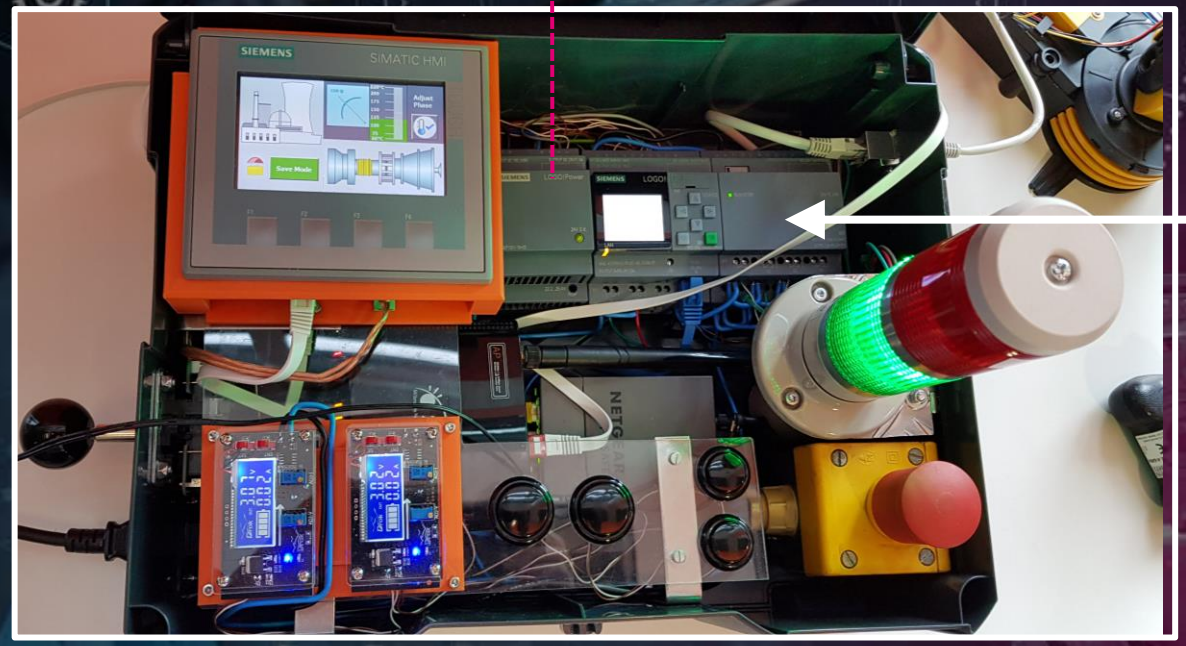
Bernd Jäger
Bernd.jaeger@t-systems.com
GRID, GCFA, GCIA, GREM, GWASP, CISSP
Practice Lead ICS/IoT Security

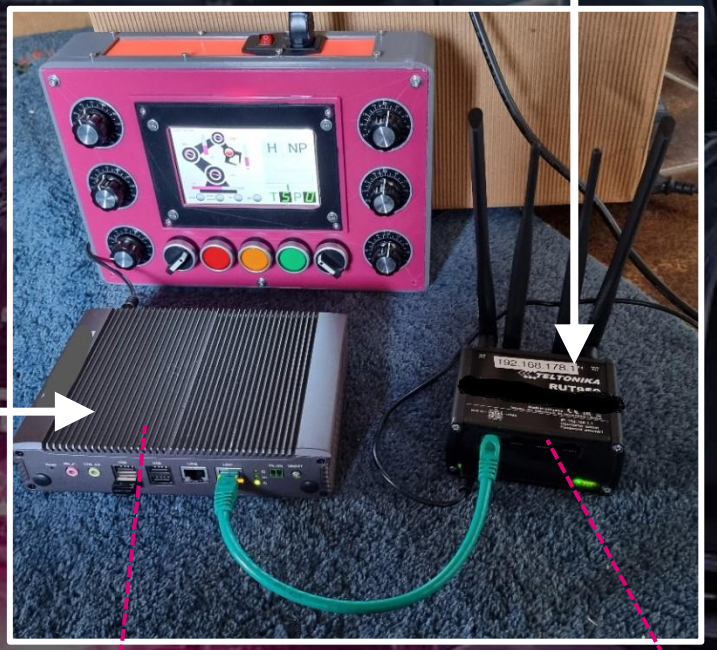
Telekom Industrial Security

INDUSTRIAL HONEYPOT DEMO

Internet

Hardware Honeypots



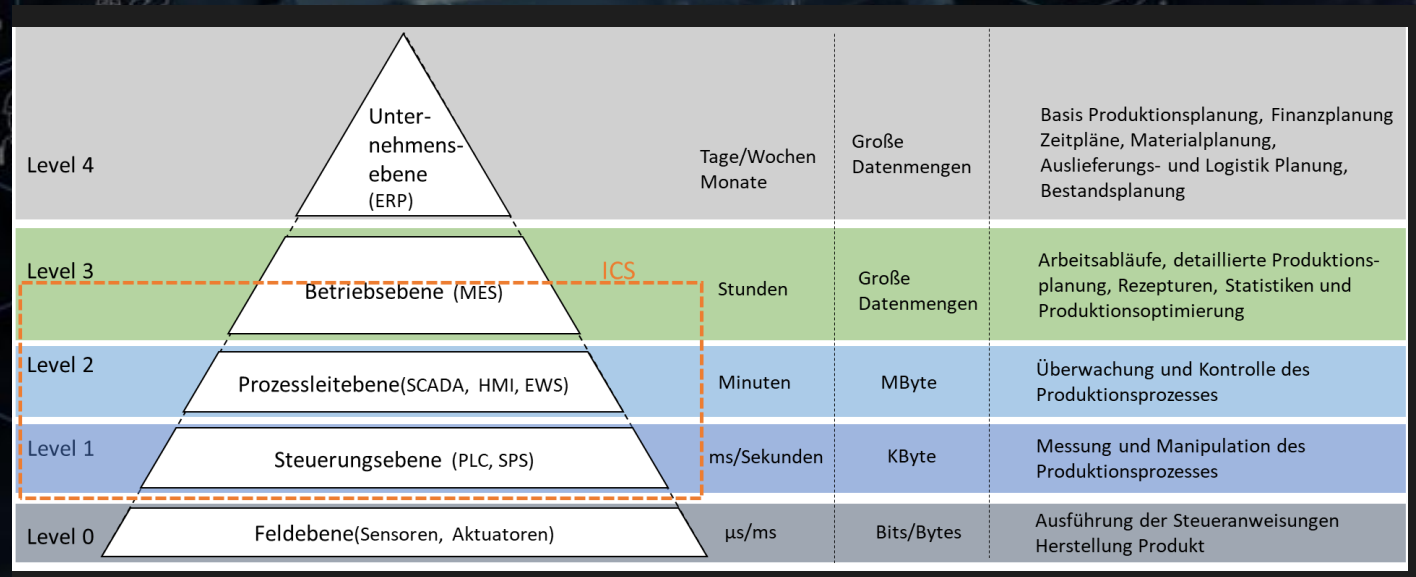


FW und Software Honeypot(s)

LTE Access Point


Industrie <=3.0
Die Alte Welt
Monolithisch, hierarchisch

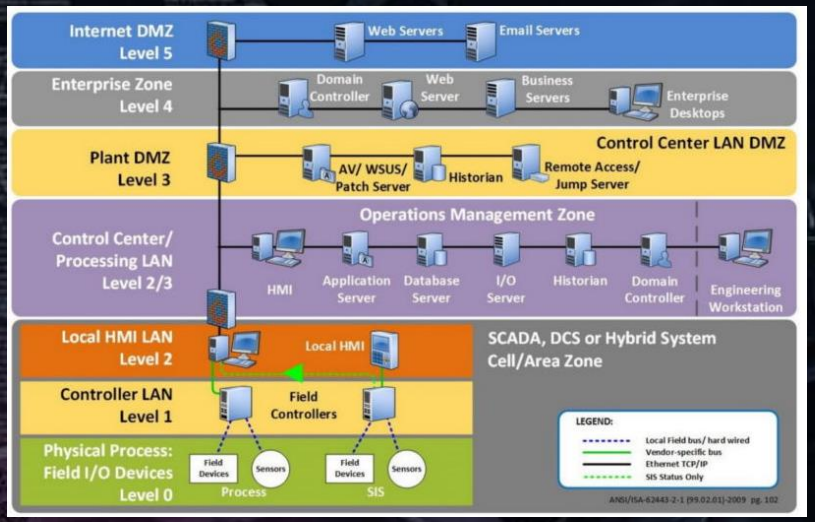
Die Alte Welt – Teil I: Hierarchien

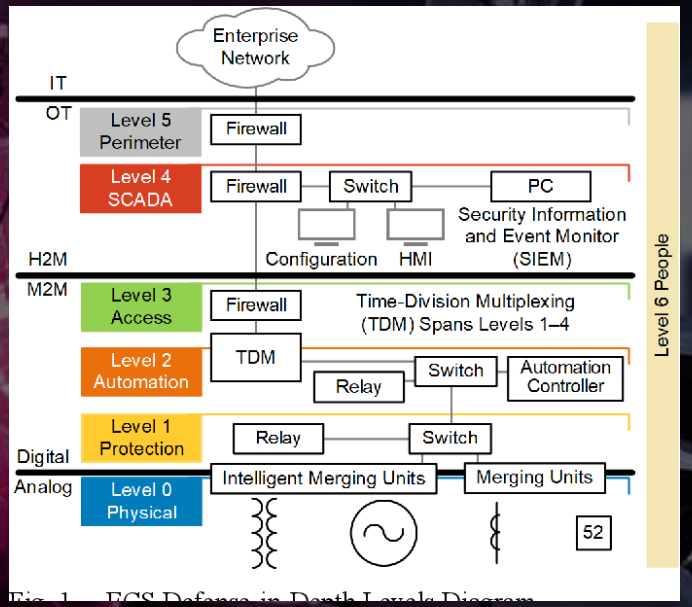


Hierarchische Strukturen

In der "alten Welt"

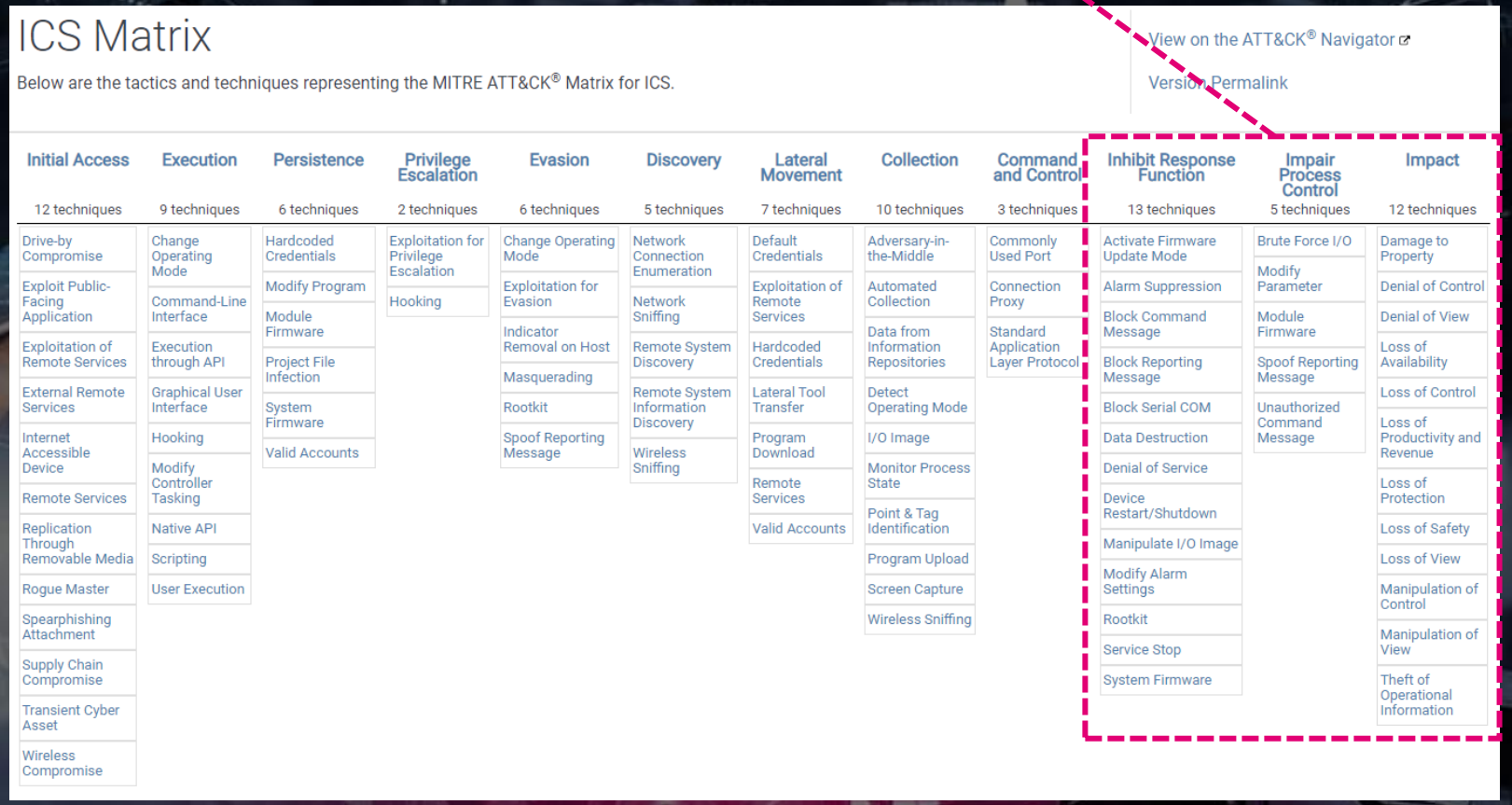
Klassische Pyramide,
Isolierte Maschinen Inseln
Diskrete Fertigung: SAP und SCADA





Die Alte Welt – Part II: Risikoprofile

- Cyber Risiko Profil (Disruption)
- Remote Zugänge
- Malware Infection
- Downtime
- ICS lastig
- seltener Daten Diebstahl
- ...
- Supplier Chain



ICS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for ICS.

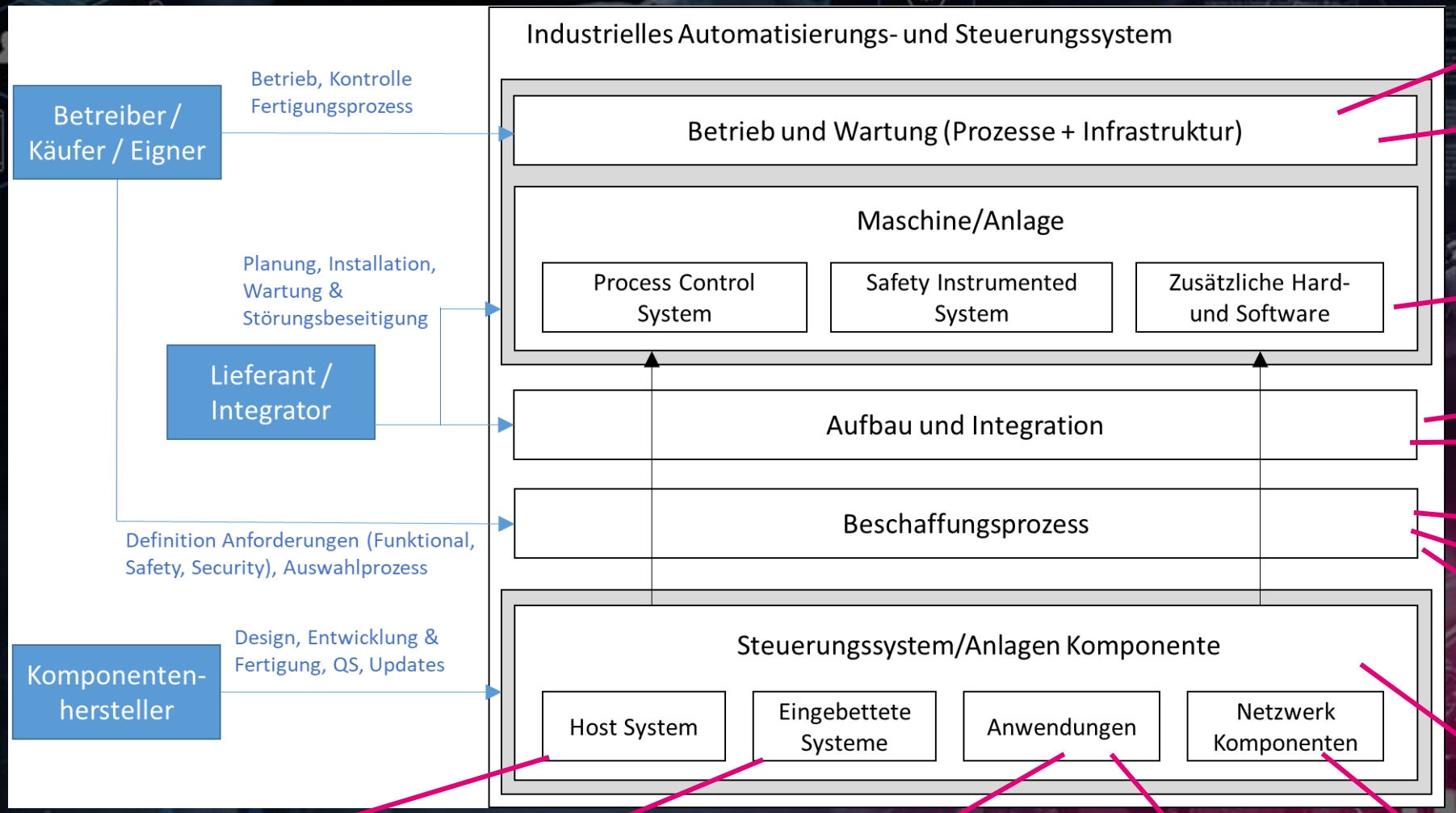
View on the ATT&CK® Navigator

Version Permalink

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	10 techniques	3 techniques	13 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Detect Operating Mode		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	I/O Image		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

Was wir in der Vergangenheit gelernt haben. Unser kollektives Gedächtnis

Talking Supplier Chain ...



Infected Notebooks, USB, ...

Unsecure and/or unknown Remote Access

Vulnerable Software, **APIs, E2E View**

Admin Backdoors

Unsecure Configuration

No or limited supplier assessment

No Cyber Requirements

Lack of Know-how

Trojaned Compiler/Linker

Vulnerable Libraries

0-Days

Default Passwords

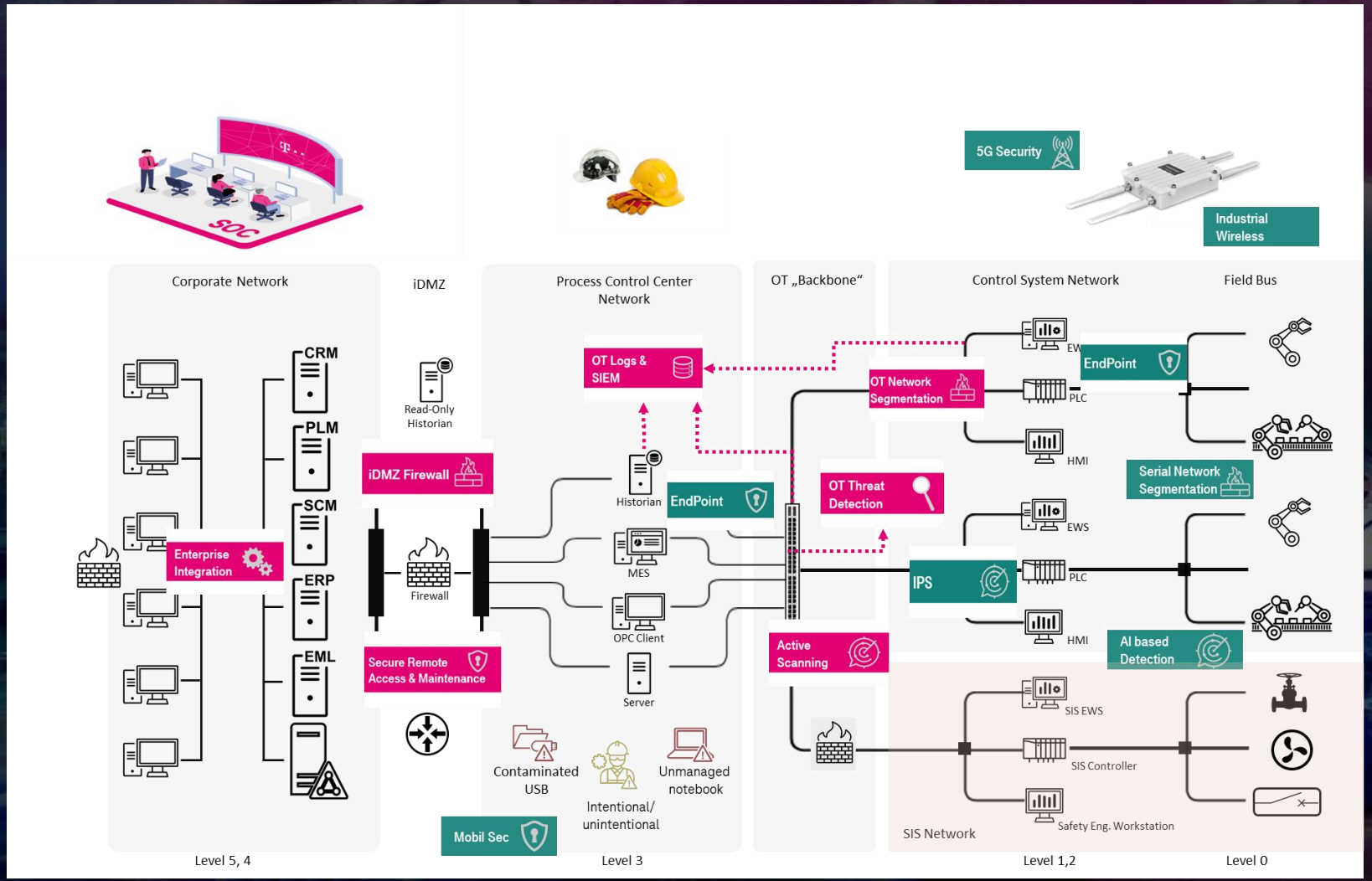
Weak Crypto Keys

Hardware Backdoor

Die Alte Welt – Part III: Schutzmaßnahmen

Derzeitige Verteidigungsmodelle und “Leitplanken”

- IEC 62443
- MITRE ATTACK ICS
- NIST
- ISO 27xxx
- SANS Sliding Scale for ICS
- KRITIS, R155/156
- Security „Good Practice“



Die Alte Welt – Part III: Schutzmaßnahmen

„Fünf Cyber-Security Maßnahmen zusammen, schaffen ein effizientes und effektives OT-Sicherheitsprogramm.“ [1]

Incident Response Plan

Netzwerk Architektur die man schützen kann

Netzwerk Sichtbarkeit Transparenz und Monitoring

Sichere Fernwartung

Risiko basiertes Vulnerability Management

[1]SANS Institut

Schutzmaßnahmen umsetzen

OT Security is a Journey

OT Threat Intelligence

Angriffserkennung

Network Segmentation

SOAR Automation

Assessments

- Assets,
- Network Topo/Flows,
- Behaviour Baseline
- Vulnerabilies & Risks

Remote & Cloud Access

X-Domain Playbooks

OT Endpoints

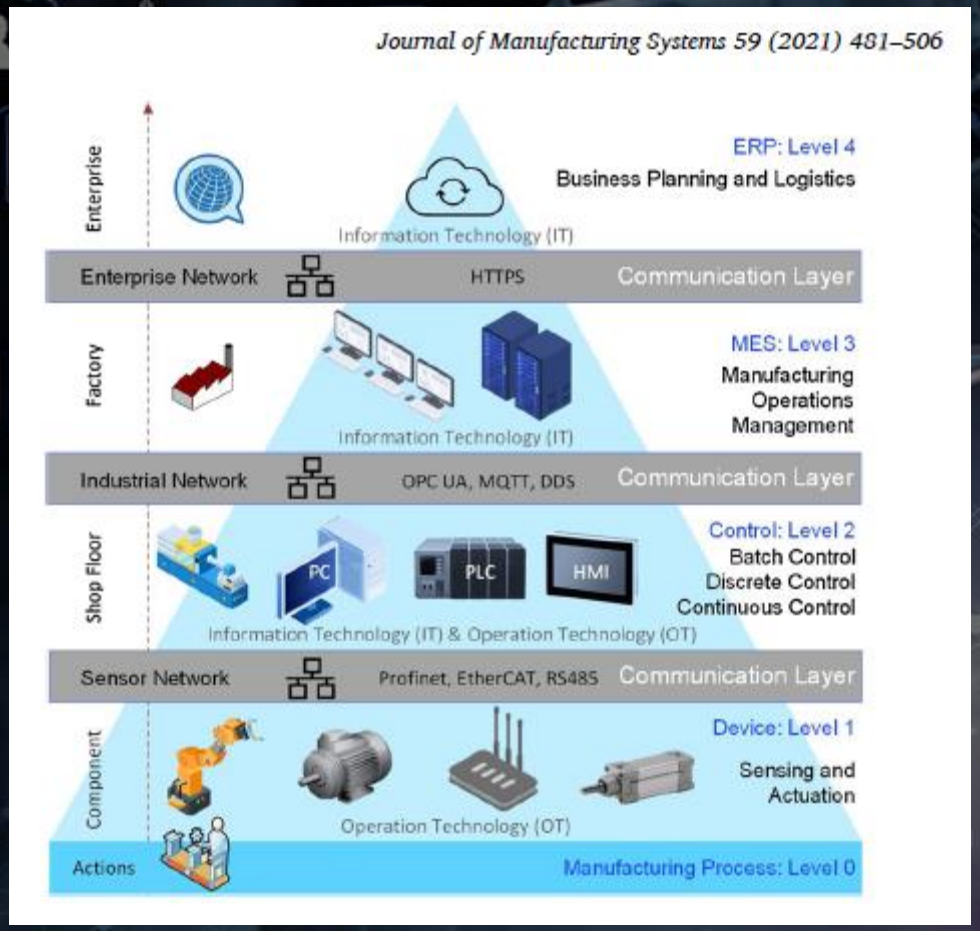
Align your Organisation/ Mindset

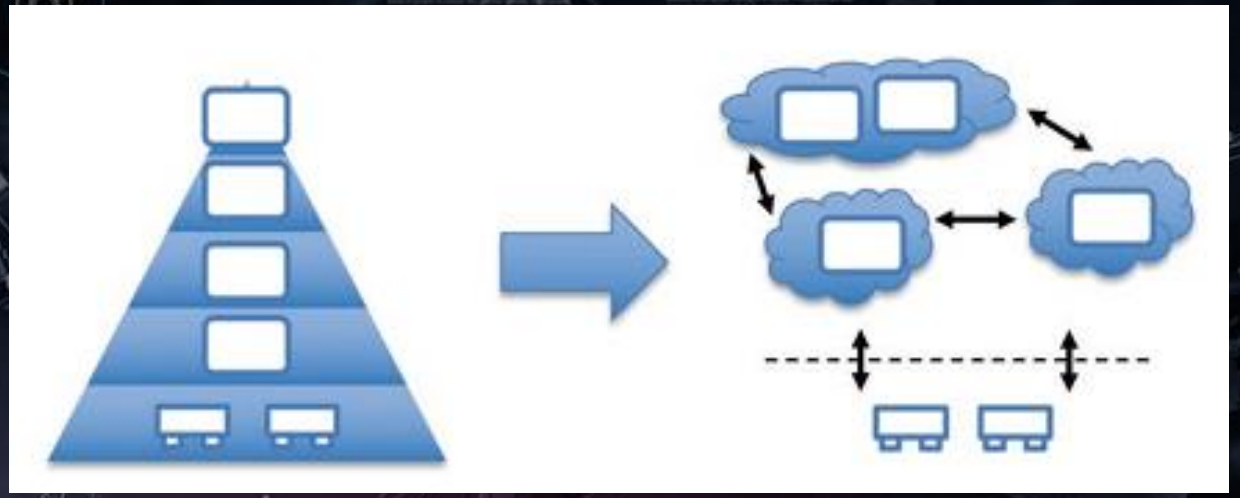
Start here

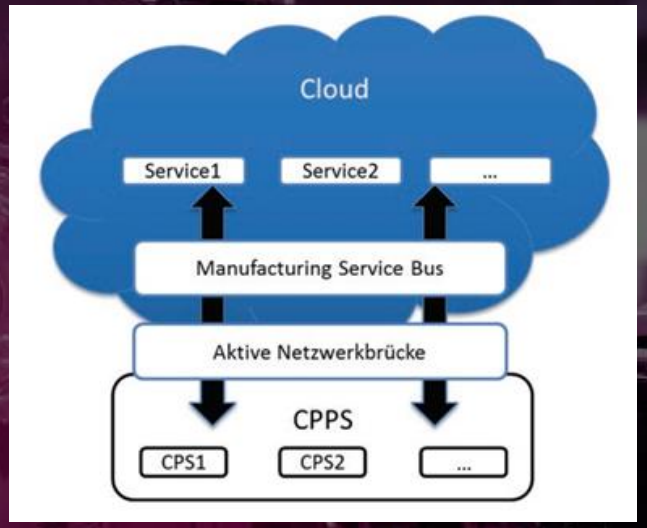
Die neue Welt

Service Orientiert und Cloud Connected

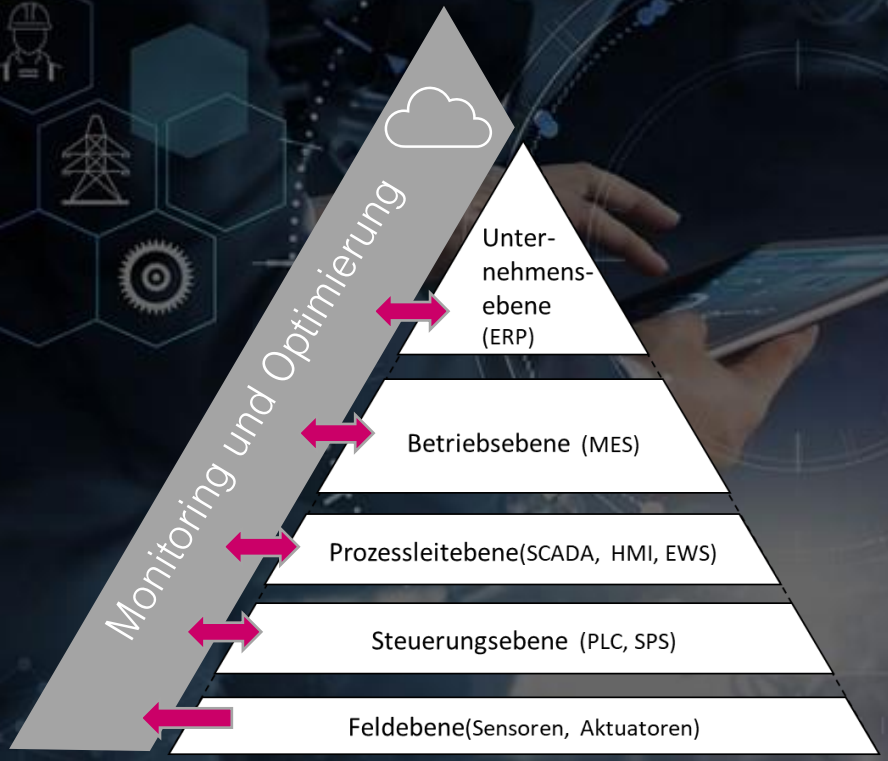
Die Neue Welt – Part I: Verteilt und Bewölkt

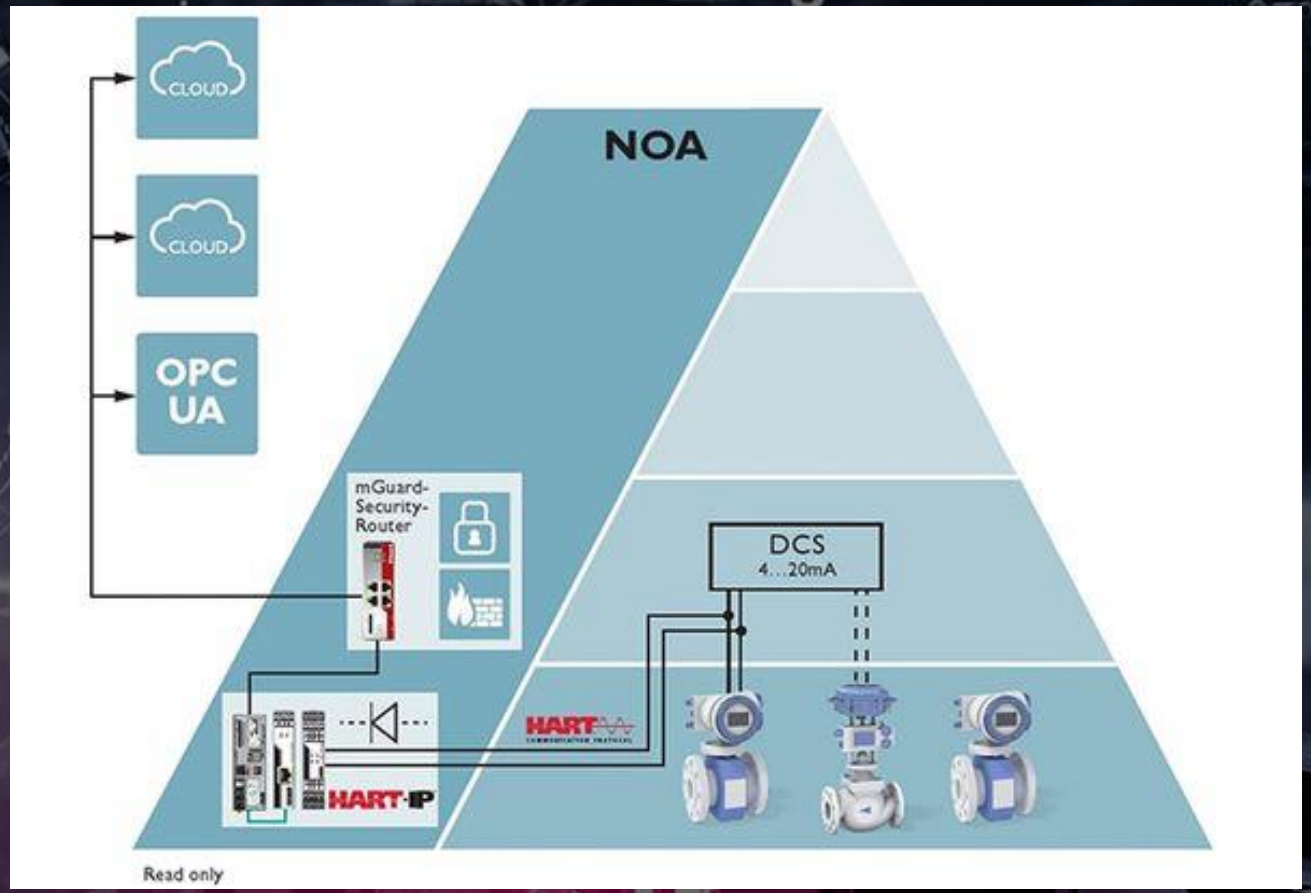






„Smarte“ Modelle …



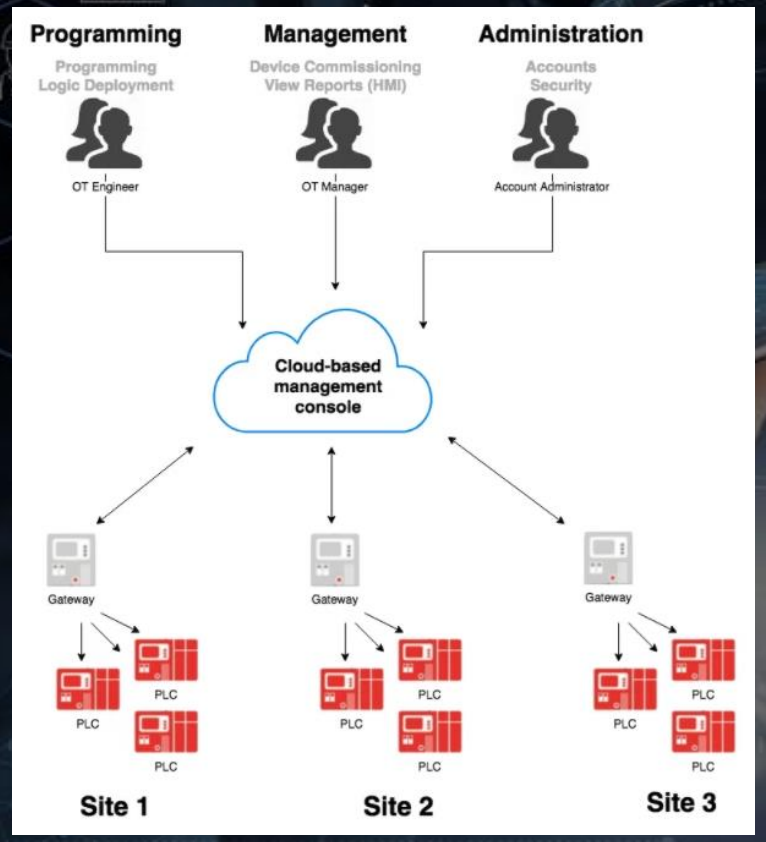


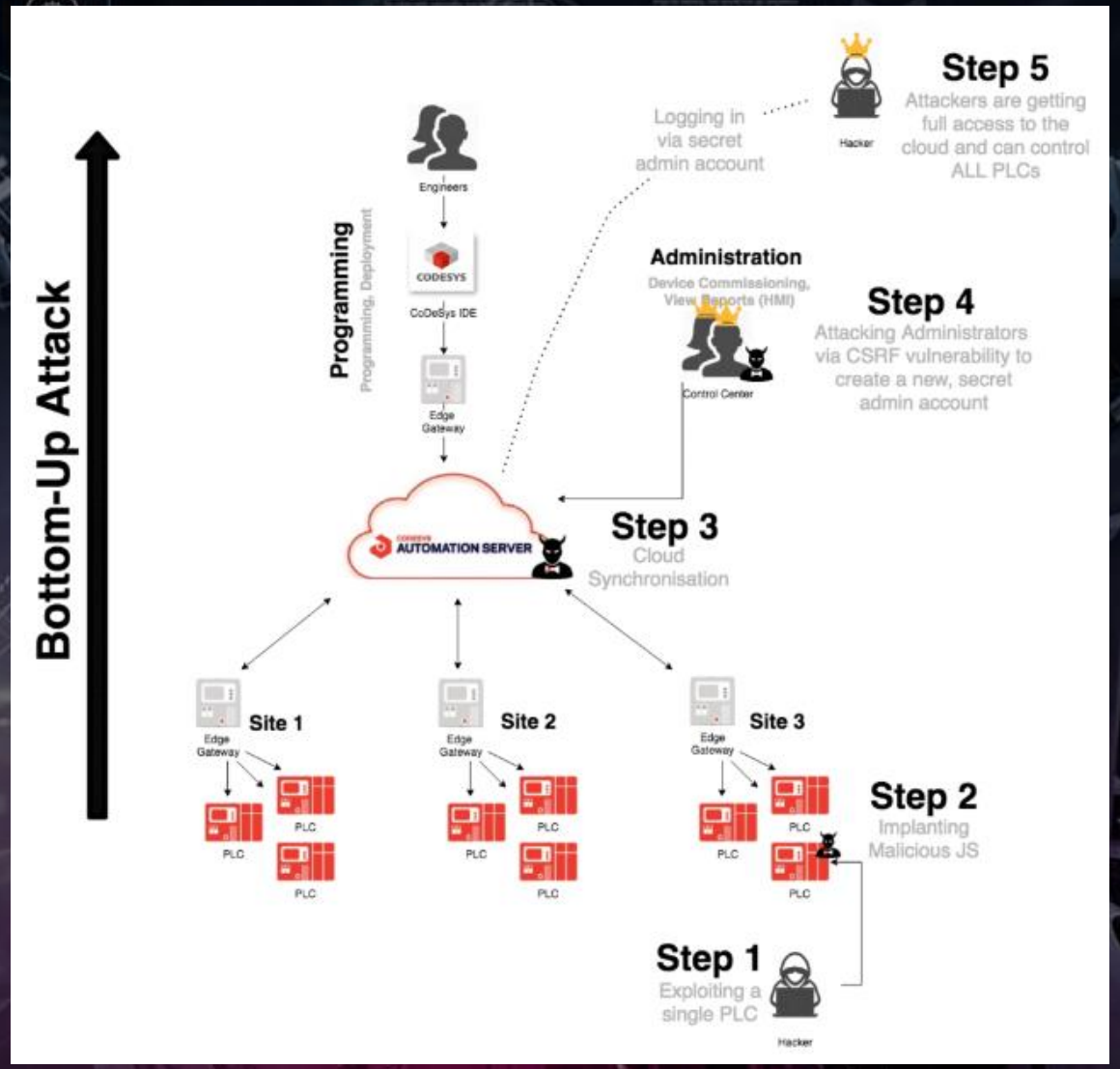
Die Neue Welt – Part II: Risikoprofile

Cyber Risiko Profil (Loss of Data & Control)

- Verlust vertraulicher Daten
- Verlust des Zugangs zu produktionskritischen Daten
- Kontrollverlust durch z.B. Cloud Steuerung
- mehr IT-, IoT lastig
- breitere Angriffsfläche (Cloud, Virtualisierung, Mobile Geräte, ...)
- ...
- Beispiel: Evil PLC

Es ist nicht immer die Cloud schuld



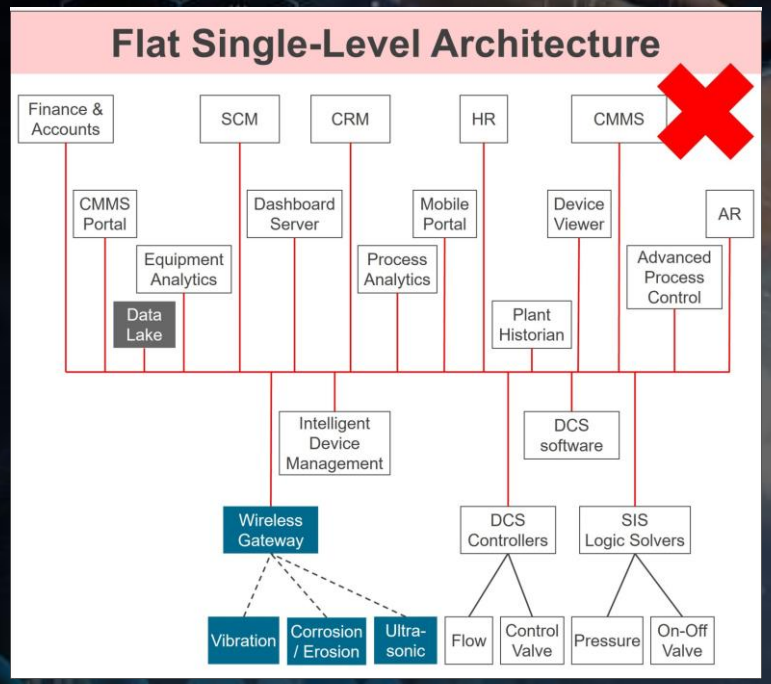


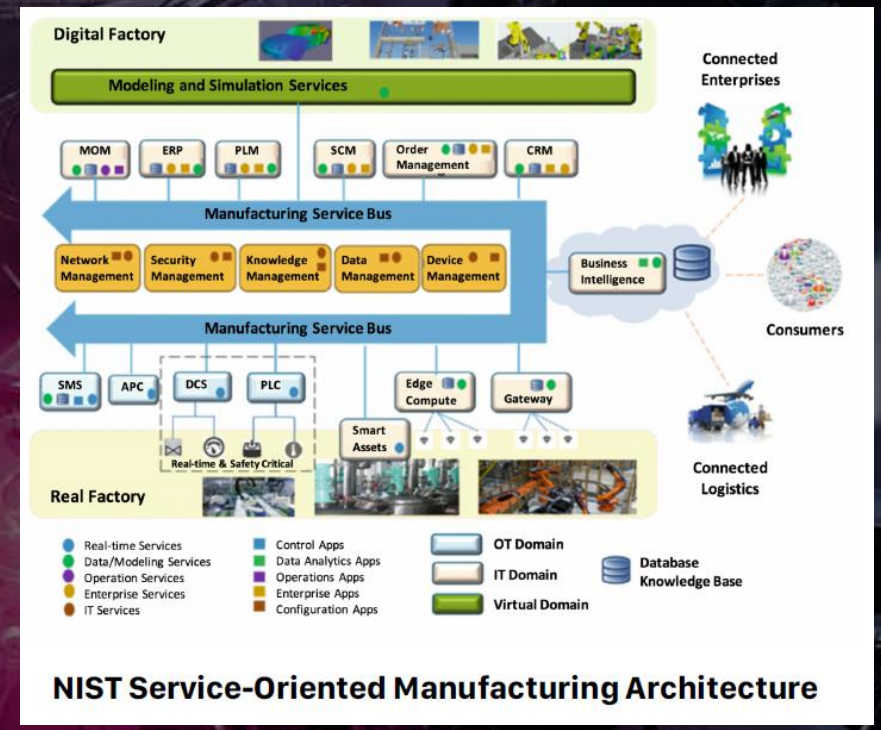
https://claroty.com/team82/research/exploiting-vulnerabilities-in-the-ot-cloud-era


Der Weg dahin ...

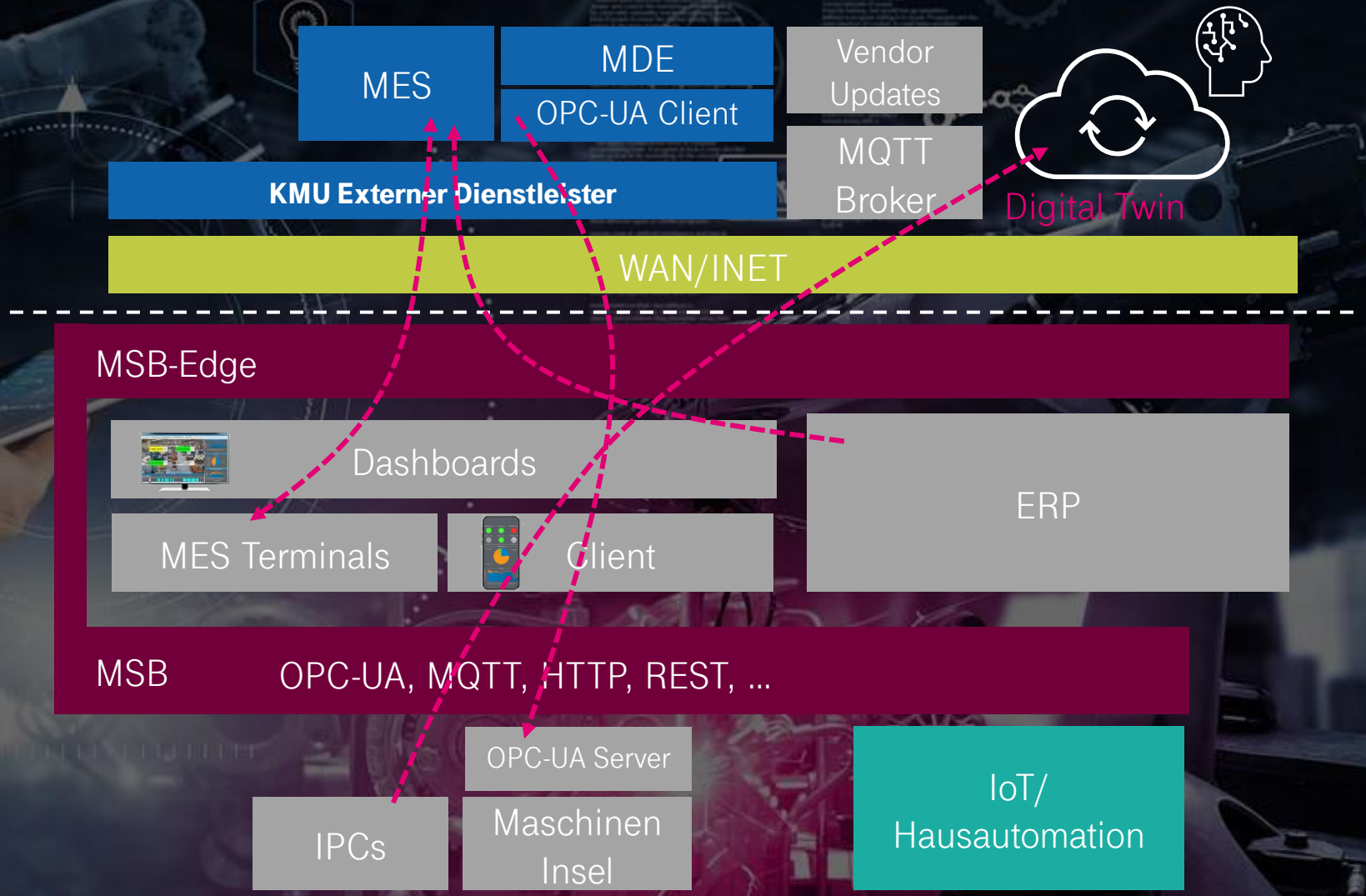
Die richtige Architektur ist nur ein Aspekt auf dem Weg zur sicheren Smart Factory…

Wir können das Werk nicht zumachen, umbauen und dann weiter produzieren ...

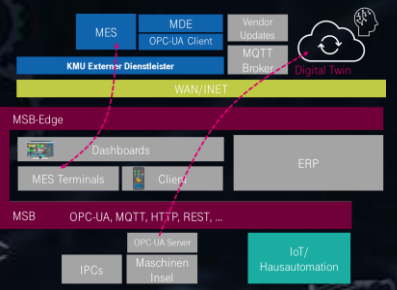




Transition: Architektur Beispiele

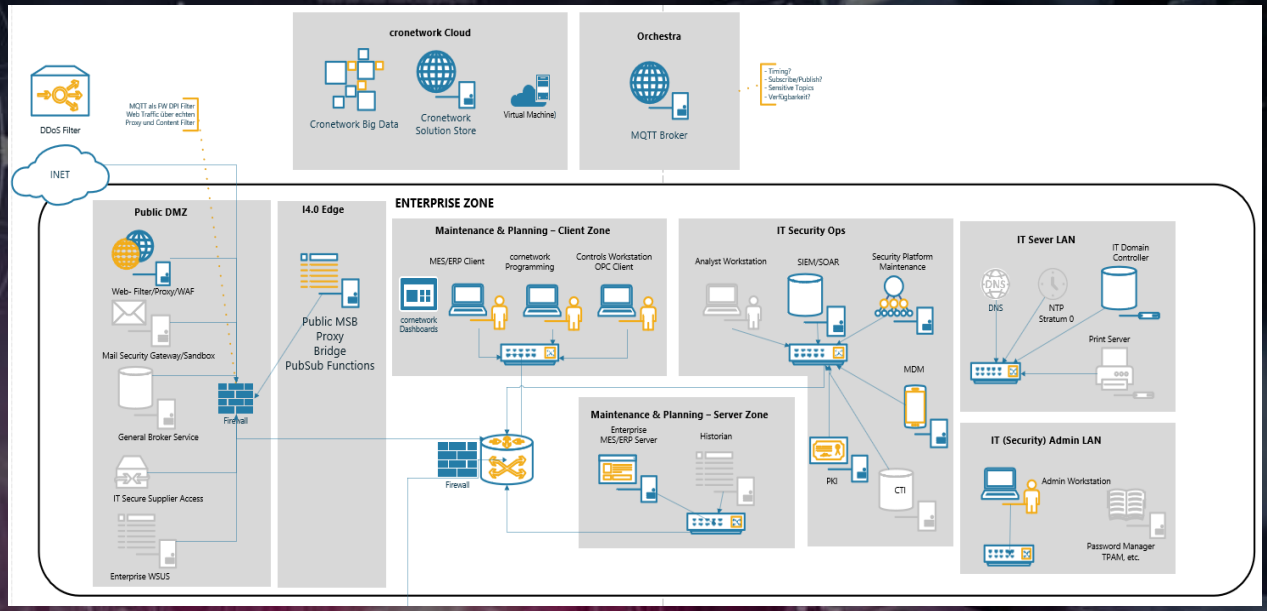


Transition: Architektur Beispiele



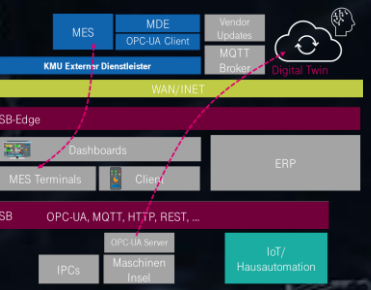
- „Edge“ Netzwerksegment in der Enterprise Zone für Smart Factory Funktionen
- Es sollte getrennte (VLAN an FW) Netzsegmente für:
  - MES/ERP Clients und Server
  - Security Administration
  - Office Clients und Server (AD!)

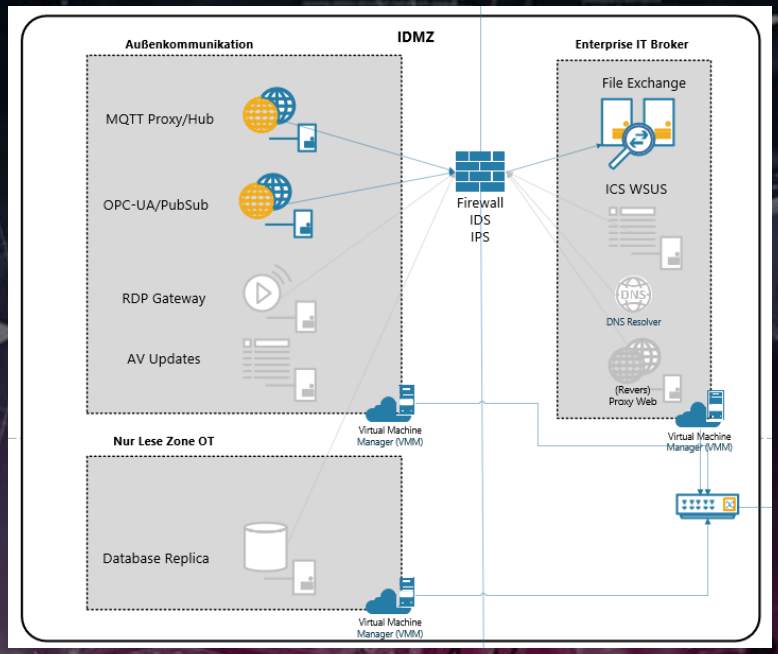
  geben
- Um die Verfügbarkeit aller externen (Cloud) Anwendungen zu gewährleisten, sollten alle notwendigen Systeme (Internet Zugang, DNS, Webservices, Cloud-APIs, etc.) gegen DoS Angriffe oder techn. Störungen gesichert werden

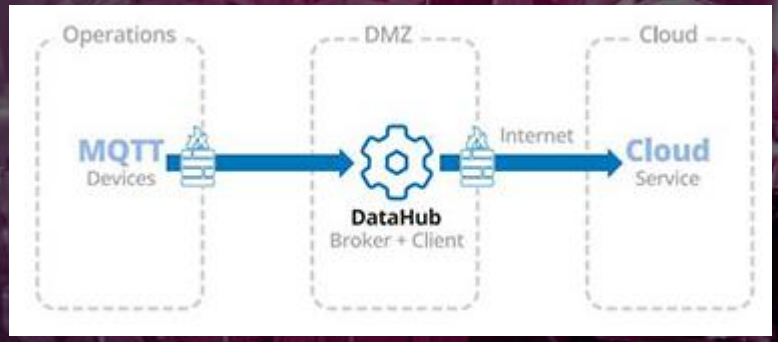


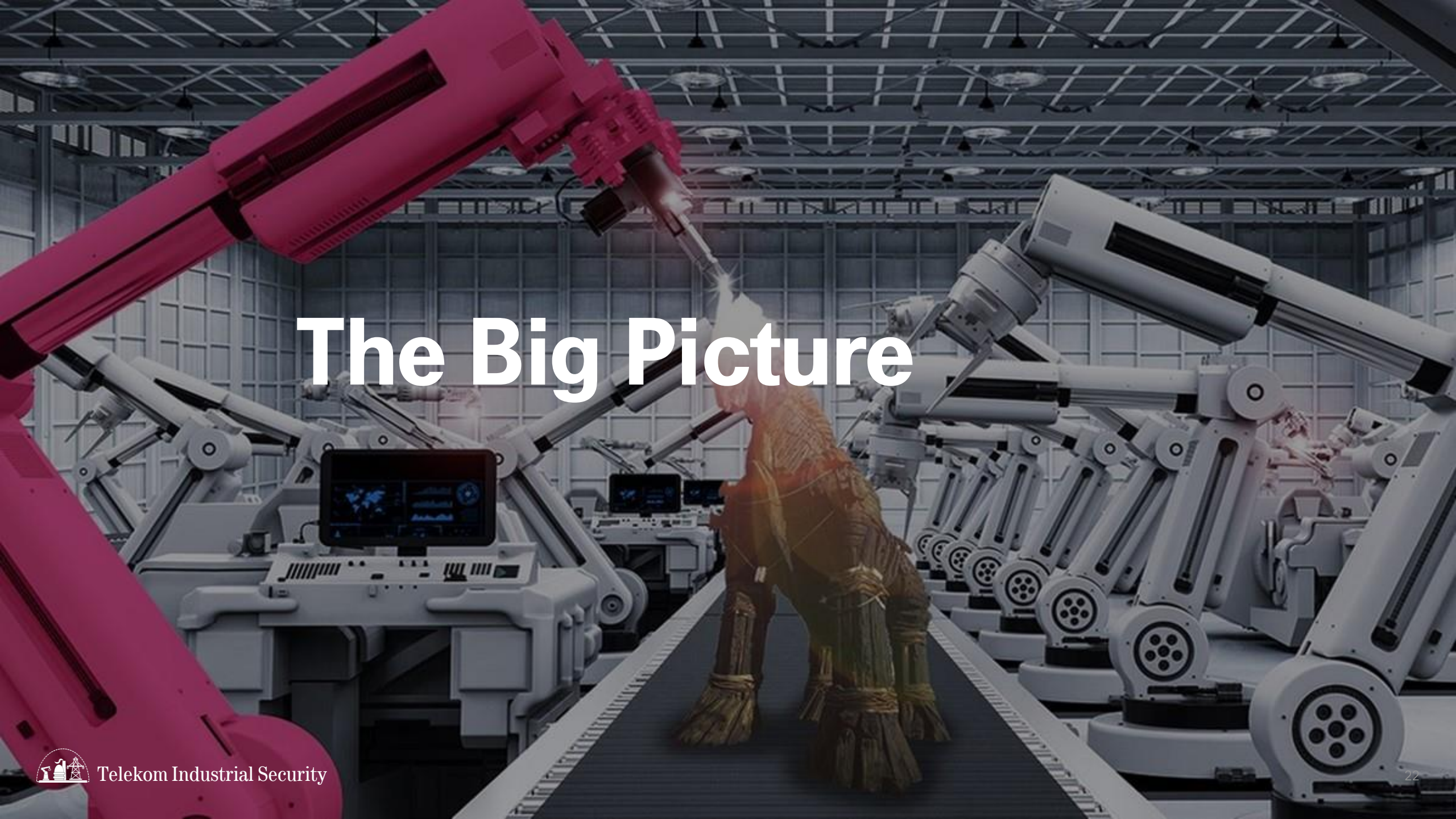
Transition: Architektur Beispiele

- „Industrial DMZ“ (iDMZ) mit
- Getrennte DMZ Segmente für Außenkommunikation
- Broker Services

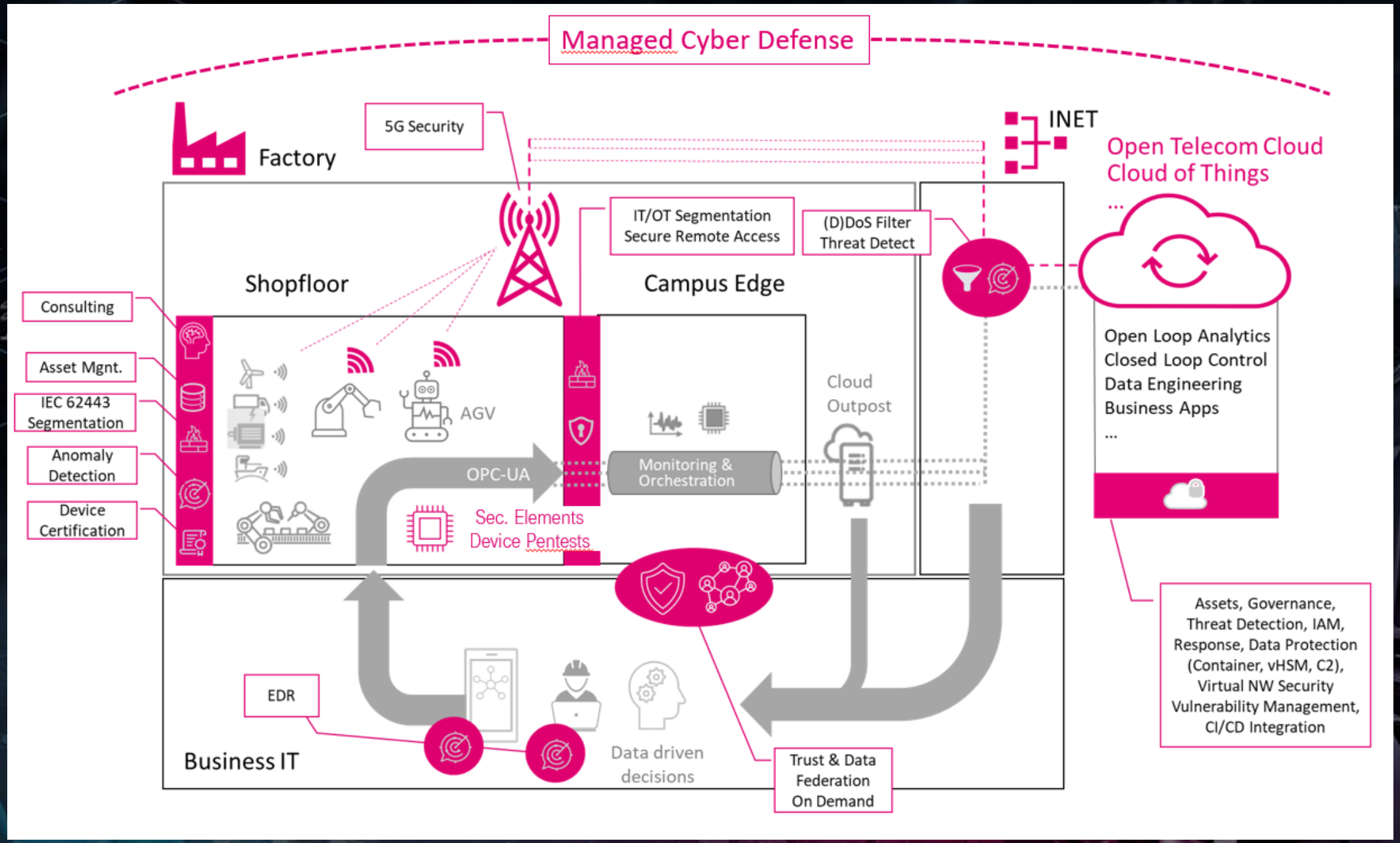




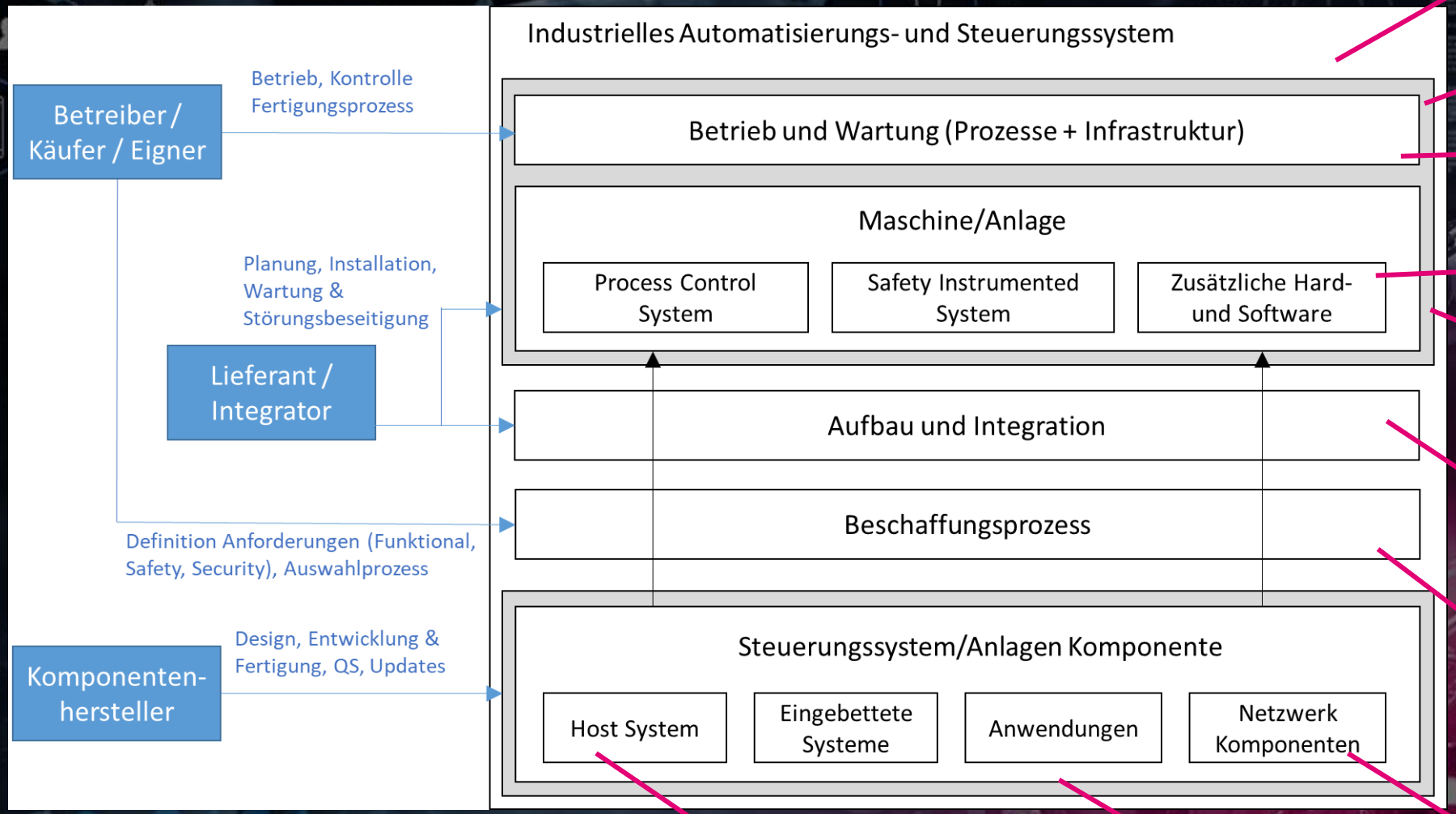




The Big Picture


Managed Cyber Defense
Factory
5G Security
INET
Open Telecom Cloud
Cloud of Things
...
IT/OT Segmentation
Secure Remote Access
(D)DoS Filter
Threat Detect
Shopfloor
Campus Edge
Consulting
Asset Mgnt.
IEC 62443
Segmentation
Anomaly
Detection
Device
Certification
AGV
OPC-UA
Monitoring &
Orchestration
Cloud
Outpost
Sec. Elements
Device Pentests
Open Loop Analytics
Closed Loop Control
Data Engineering
Business Apps
...
EDR
Business IT
Data driven
decisions
Trust & Data
Federation
On Demand
Assets, Governance,
Threat Detection, IAM,
Response, Data Protection
(Container, vHSM, C2),
Virtual NW Security
Vulnerability Management,
CI/CD Integration

The Smart Supplier Chain



Incident Response / SOC

Threat Detection

Segmentierung, Fernwartung

E2E-Systeme Pen-Tests

Vulnerability Assesments

Schlüsselfertige Lösungen, Schulung, etc.

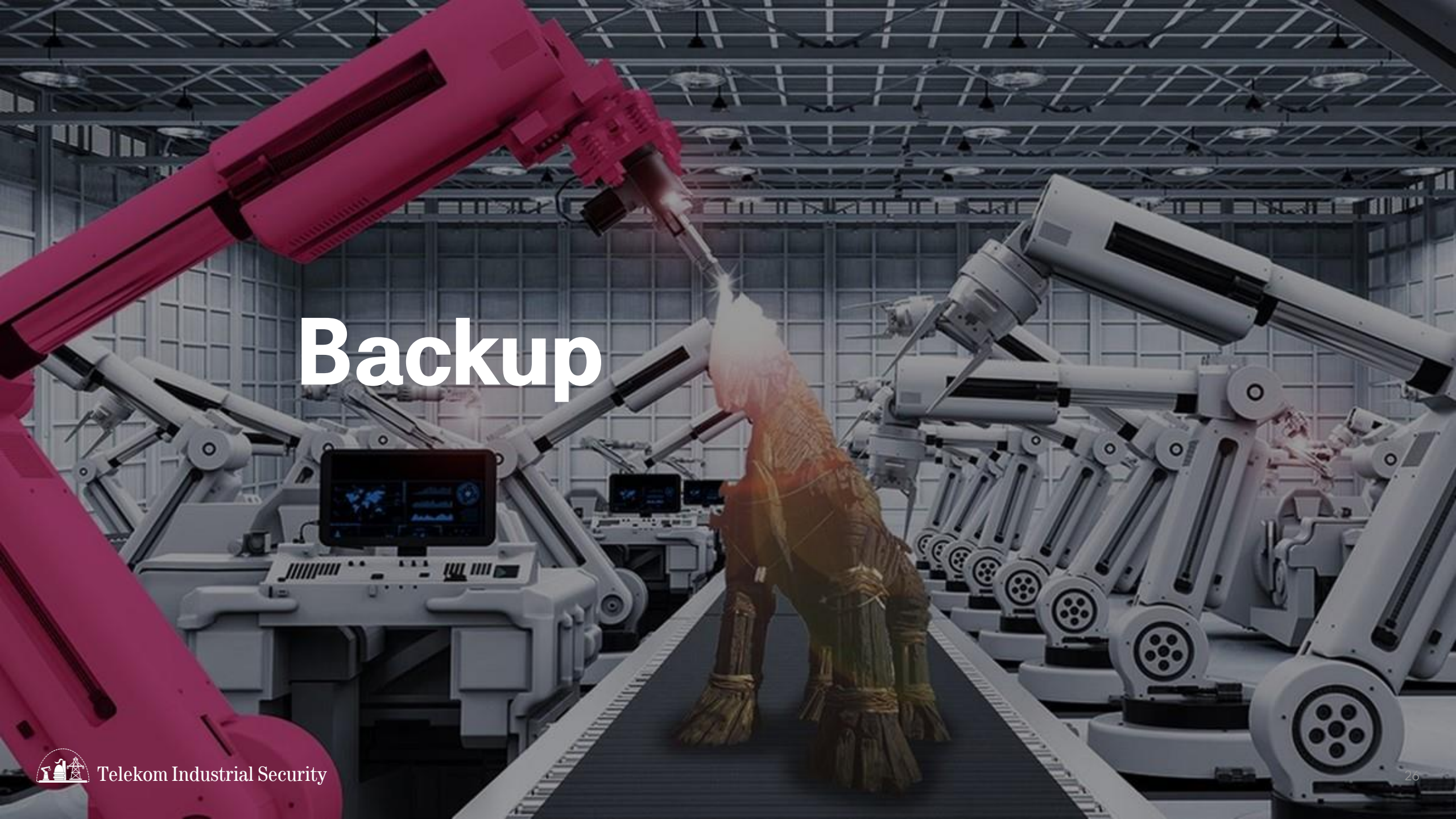
Beratung bei Ausschreibungen

Secure Elements

Pentesting

Code Signing & PKI


Honeypot,
Still alive?



Backup