

IT-Security-Konzepte in der Produktion

Wolfgang Kerschbaumer

wolfgang.kerschbaumer@stiwa.com

STIWA Automation GmbH

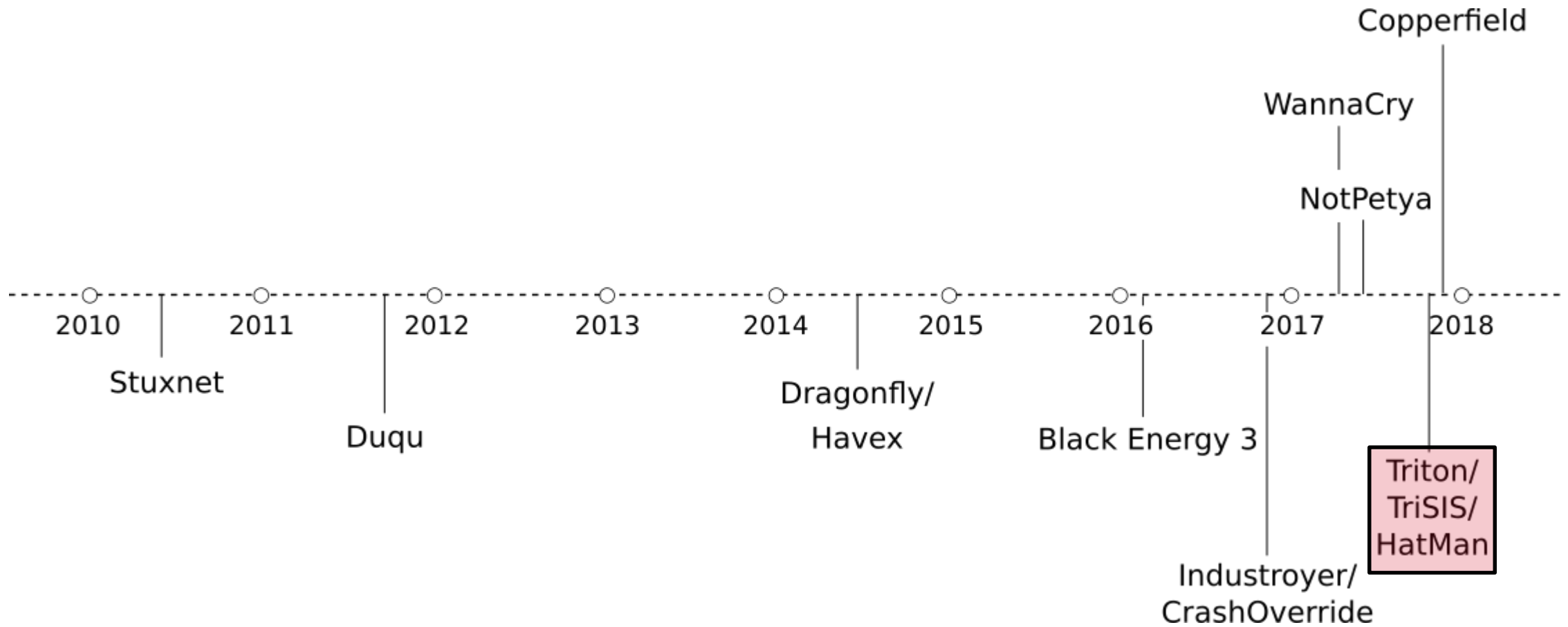




I. Gefährdungslage

»We only have two modes – complacency and panic«
James R. Schlesinger

Beispiel ICS-Angriffe



The New York Times

A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.

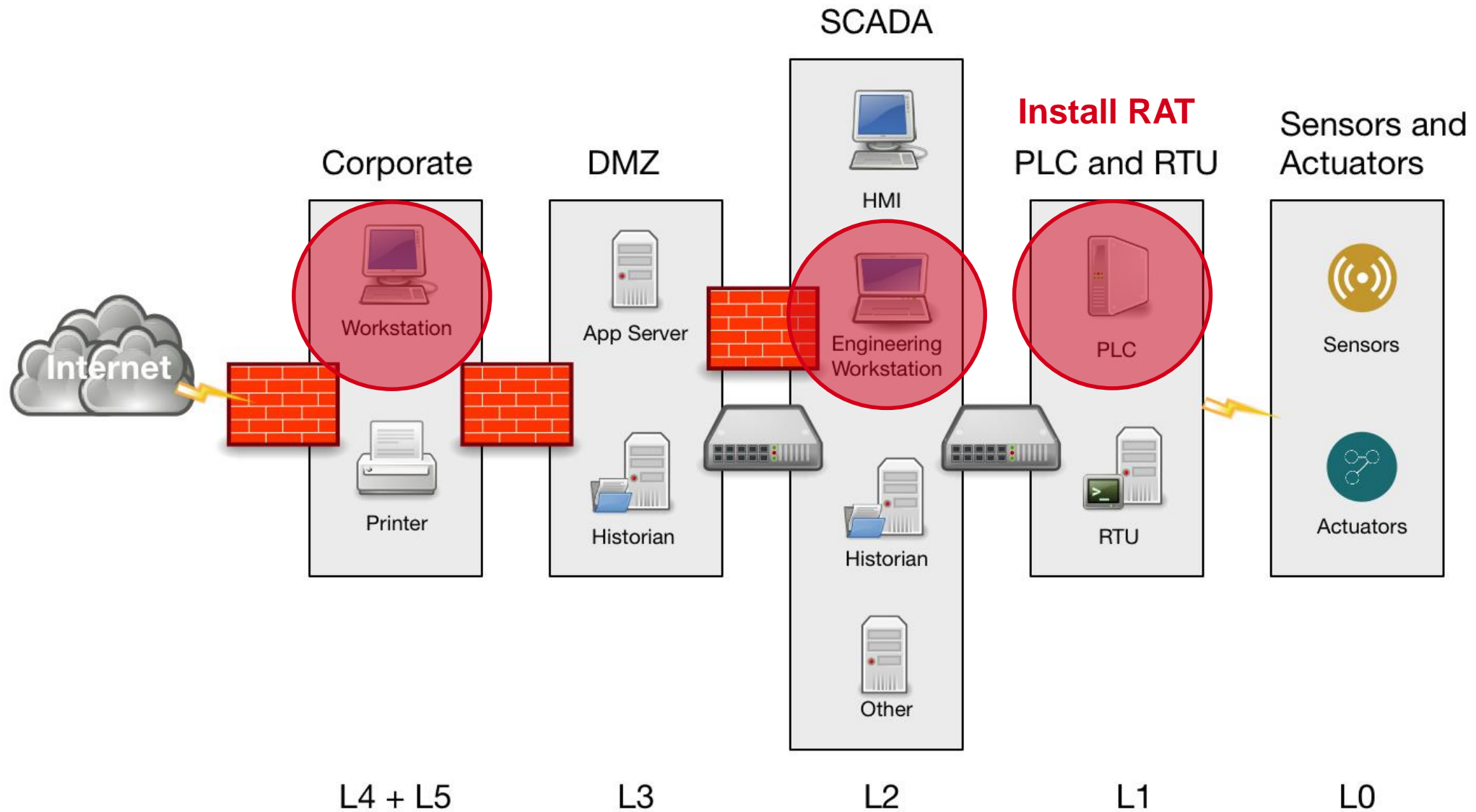


Quelle: <https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html>

Triton – Überblick

- **Triton** aka **TriSIS** aka **HatMan**
- SIS Schneider Electric Triconex Tricon Model 3008
- Schadsoftware mit zwei Bestandteilen
 - PC-Komponente
 - Binärcode-Komponente

Triton – Ablauf des Angriffs



Triton – Vulnerability

- **Unsicherer Systemcall**
- Speicheradressen im Userspace werden ungeprüft gelesen
- Pointer können während des System-Call-Aufrufs verändert werden
- Es wird nicht überprüft, auf welchen Bereich Pointer zeigen

Advisory (ICSA-18-107-02)

Schneider Electric Triconex Tricon (Update A)

Original release date: April 17, 2018 | Last revised: May 03, 2018

Legal Notice

1. EXECUTIVE SUMMARY

- **CVSS v3 9.0**
- **ATTENTION:** Exploitable remotely/HatMan malware specifically targets these vulnerabilities.
- **Vendor:** Schneider Electric
- **Equipment:** Triconex Tricon, Model 3008
- **Vulnerabilities:** Improper Restriction of Operations within the Bounds of a Memory Buffer

Triton – Schneider Electric Triconex Tricon



»To date, the information gathered indicates that if the Tricon key switch had been left in the correct position per our recommended guidelines, the injection of malware would not have been successful«

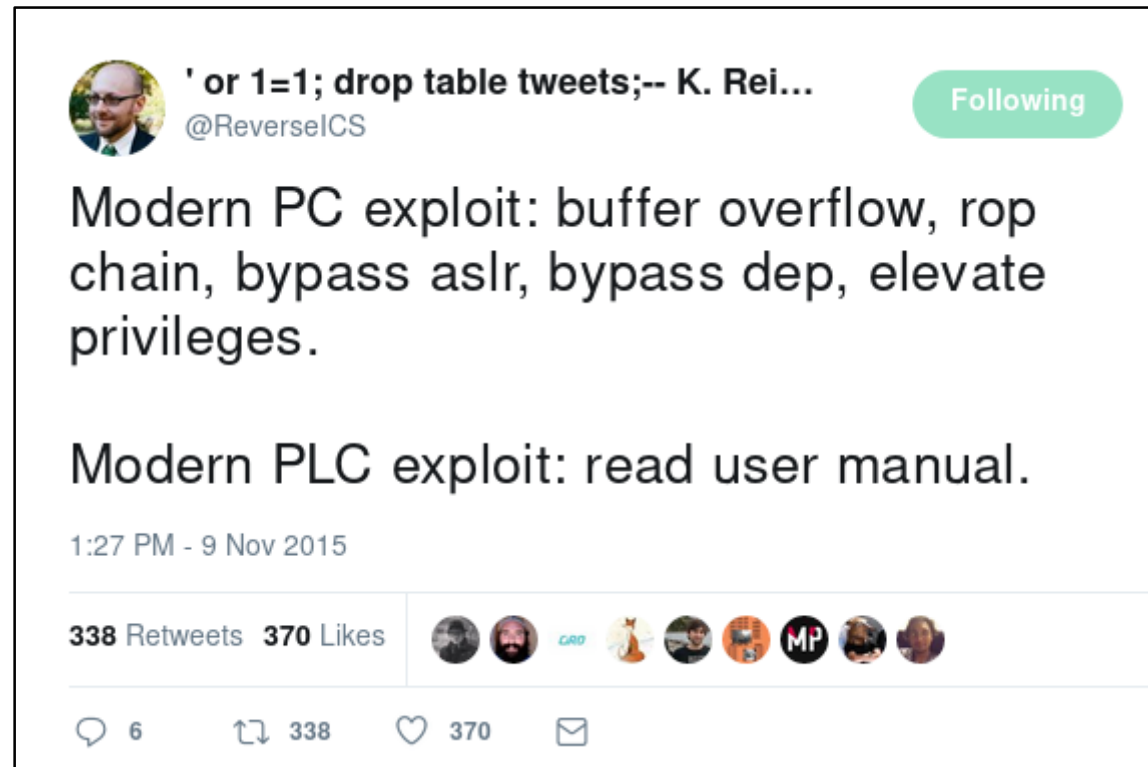
Quelle: https://download.schneider-electric.com/files?p_enDocType=Technical+leaflet&p_File_Name=SEVD-2017-347-01+Triconex+V2.pdf

Quelle Abb.: <https://images-na.ssl-images-amazon.com/images/I/41jr93jKzML. SX466 .jpg>



II. Besonderheiten der Produktions-IT

»It's not a vulnerability, it's a feature«



' or 1=1; drop table tweets;-- K. Rei...
@ReverseICS Following

Modern PC exploit: buffer overflow, rop chain, bypass aslr, bypass dep, elevate privileges.

Modern PLC exploit: read user manual.

1:27 PM - 9 Nov 2015

338 Retweets 370 Likes

6 338 370

	IT	OT
Prioritäten	<ol style="list-style-type: none">1. Security2. Integrität3. Verfügbarkeit	<ol style="list-style-type: none">1. Safety2. Verfügbarkeit3. Integrität
Verfügbarkeit	mittel bis hoch	extrem hoch
Einspielen von Security-Patches	häufig	selten
Faktor Zeit	meist Verzögerung erlaubt	oft Echtzeitverhalten erforderlich
Lebenszyklus	3 bis 5 Jahre	10 bis 30+ Jahre
Security-Awareness	mittel bis hoch	gering



III. ICS-Security-Konzepte

»Security is a process, not a product«

Bruce Schneier

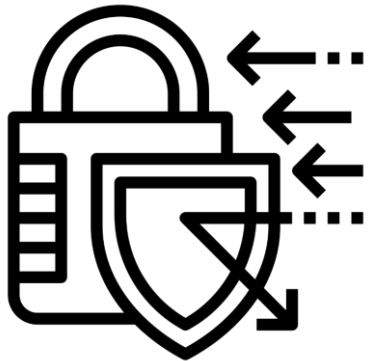


- IACS Sicherheits-Management-System
 - Anlagenbauer und Integratoren
- Risiko-Management und Bedrohungsanalyse
- Wiederherstellungsplan
- Security by design
- Finale Zuständigkeit: Management

Unzureichende Absicherung

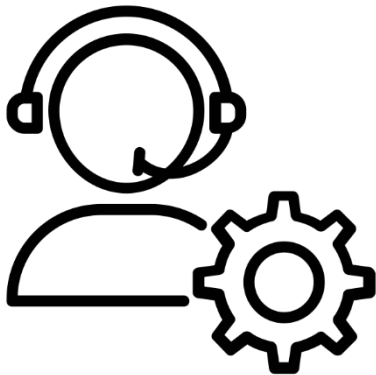


- Physikalische Netzwerksegmentierung
- Physikalischer Zugangsschutz
- Security-Monitoring und -Logging
- Passwörter
- Schutz vor Schadcode
- M2M-Kommunikation
- Public-Key-Infrastruktur (PKI)
- Application Whitelisting
- Zero Trust and Micro-Segmentation

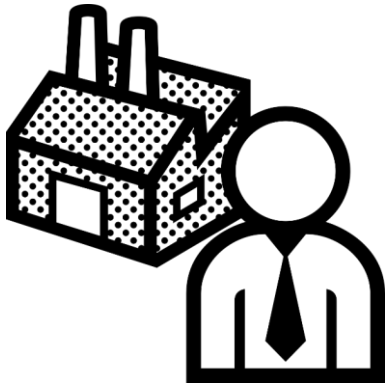


- Lifecycle-Management
- Patch-Management
- Moderne AAA-Methoden
- Verschlüsselung
- Minimalitätskonzept
- Security through obscurity

Fernwarten und Fernwirken



- Verbindungsaufbau von innen
- Vier-Augen-Prinzip
- Monitoring der Fernwartungs-Aktivitäten
- Beschränkung auf betroffene Anlagenteile



- Innentäter
- »Innentäter«
 - Shadow-IT
 - BYOD
- IT-Automatisierung
- Off-Boarding
- **Awareness**

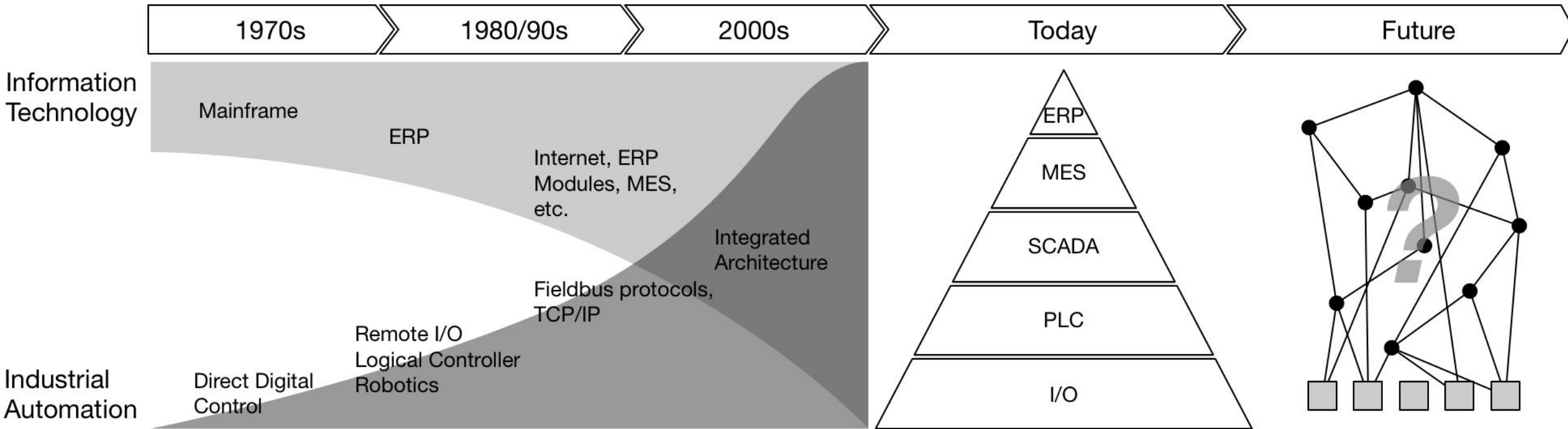
»You can teach somebody the technical bits and pieces till you're blue in the face, but unless you can get them **to care about the why**, you'll never see a change in their behavior« *Laura Bell, SafeStack*

IV. Ausblick und Fazit

»May you live in interesting times«

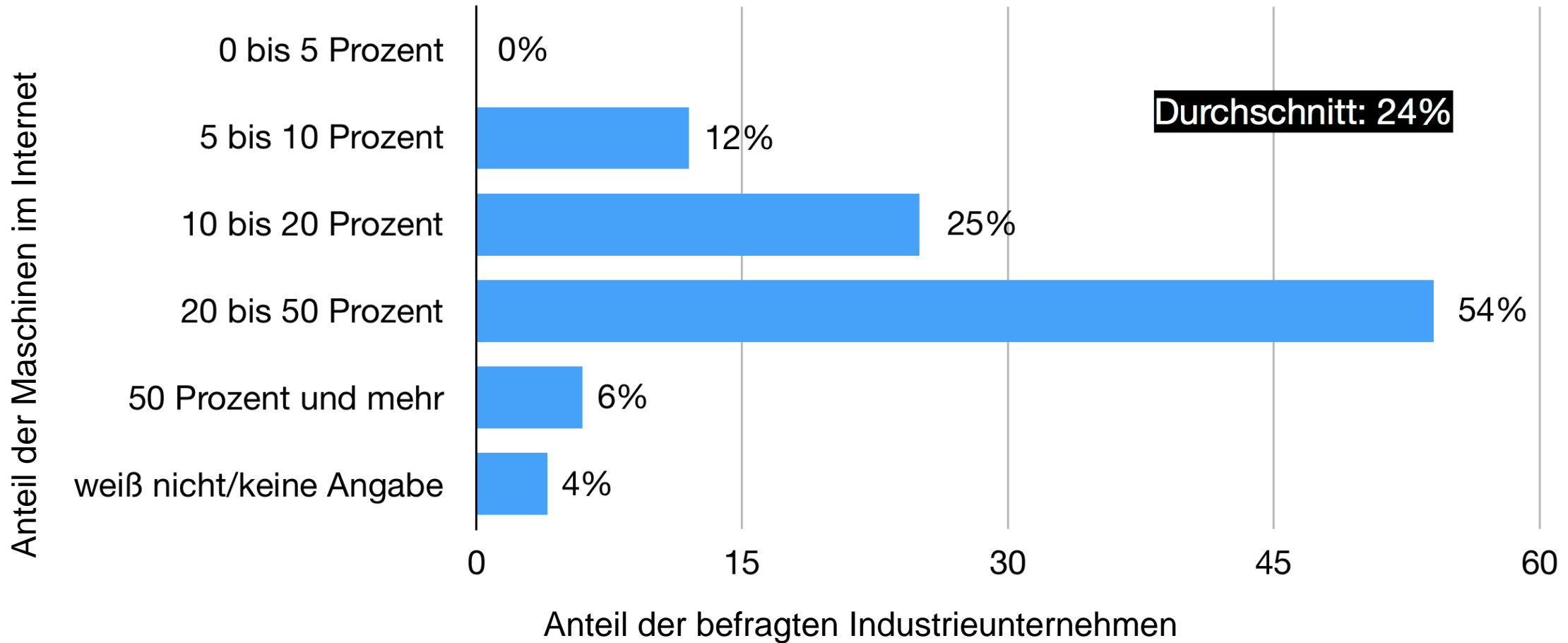


Entwicklung Produktion und IT



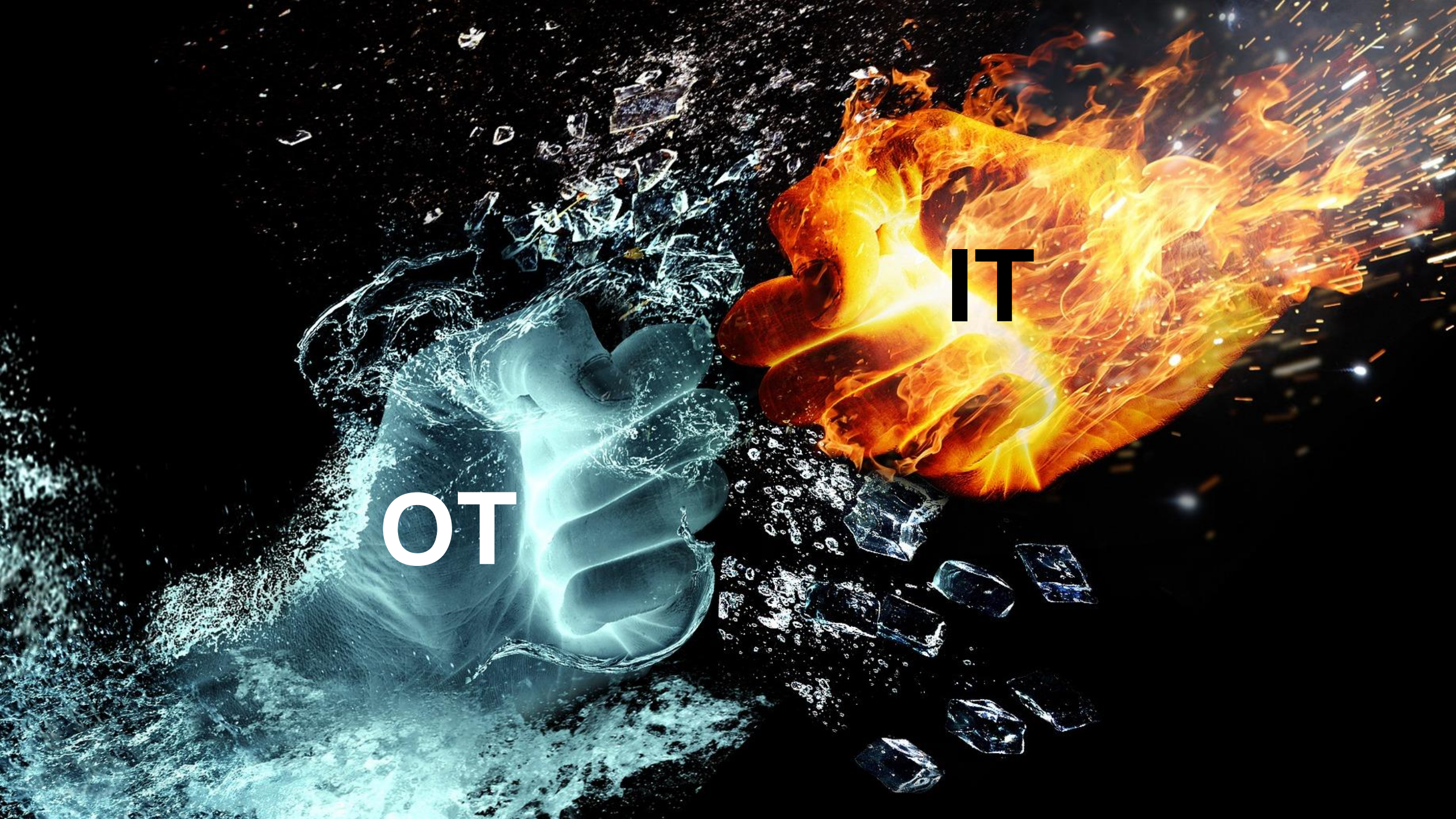
Industrial Edge Analytics Virtual Power Plants Embedded Business Intelligence
Bayesian Networks AI-powered Manufacturing
Industrial Internet of Things
Knowledge Discovery NoSQL Preventive Maintenance
Industrial Internet of Everything LoRa Hybrid Cloud GoAP IT/OT-Convergence
Hyper-converged Storage M2M Wearables
Cloud-based MES Intelligent Transportation Data Swamp Smart Automation Self-Service Analytics
Data Science Smart Contracts Augmented Reality
Cyber Manufacturing Dark Data Smart Architecture
Just in sequence. Microservice Architecture
Predictive Analytics OPC UA Multi-Cloud Strategy
Smart Factory IPv6
Deep Learning TSN MapReduce Fast Data Intelligent Maintenance Systems
Serverless Architecture Continuous Delivery
Software-Define Everything
Infrastructure as Code
Integrated Industry
Mobile First
Cybermanufacturing
PLC4X
Smart Manufacturing Continuous Deployment
HTAP Linux Edge Computing E2EE
Data Lake
Data Memory Database
NewSQL Smart City
Blockchain ROSIN IOTA 5G
AIOps Fog Computing Mesh Networking MQTT DevOps
AMQP Data Mining
Predictive Maintenance
Artificial Intelligence
Factory 4.0
Autonomous Databases In-Memory Database
Industrial Big Data
pICASSO
Decision Support Systems
Cyber-physical Systems
Data Quality Management
Ambient Intelligence Continuous Integration
Machine Learning
Smart Grid
Lean Production SCADA-as-a-service Artificial Neural Networks Data Governance
Open-Source Software Virtual Reality
Design Thinking
Multi-agent Systems
Hyperledger
Complex Systems
Containerization
Complex Systems
Machine Learning
Smart Grid
Data Governance

Jede vierte Maschine mit dem Internet verbunden



Basis: 553 Industrieunternehmen ab 100 Mitarbeitern in Deutschland

Quelle: <https://www.bitkom.org/Presse/Presseinformation/Industrie-40-Jede-vierte-Maschine-ist-smart.html>



IT

OT

	IT	OT
Prioritäten	<ol style="list-style-type: none">1. Security2. Integrität3. Verfügbarkeit	<ol style="list-style-type: none">1. Safety2. Verfügbarkeit3. Integrität
Verfügbarkeit	mittel bis hoch	extrem hoch
Einspielen von Security-Patches	häufig	selten
Faktor Zeit	meist Verzögerung erlaubt	oft Echtzeitverhalten erforderlich
Lebenszyklus	3 bis 5 Jahre	10 bis 30+ Jahre
Security-Awareness	mittel bis hoch	gering

	IT	OT	OT 4.0
Prioritäten	<ol style="list-style-type: none"> 1. Security 2. Integrität 3. Verfügbarkeit 	<ol style="list-style-type: none"> 1. Safety 2. Verfügbarkeit 3. Integrität 	<ol style="list-style-type: none"> 1. Security for Safety 2. Verfügbarkeit 3. Integrität
Verfügbarkeit	mittel bis hoch	extrem hoch	extrem hoch
Einspielen von Security-Patches	häufig	selten	häufig
Faktor Zeit	meist Verzögerung erlaubt	oft Echtzeitverhalten erforderlich	oft Echtzeitverhalten erforderlich
Lebenszyklus	3 bis 5 Jahre	10 bis 30+ Jahre	3 bis 30+ Jahre
Security-Awareness	mittel bis hoch	gering	hoch

- **die Gefahr ist real**
- **die Gefahr nimmt zu**
- **die meisten Angriffe sind nicht zielgerichtet**
- **»Be liberal in learning new tech,
be conservative in using it«**



Danke für Ihre Aufmerksamkeit.

STIWA Group – Führend in Hochleistungsautomation