

Digitalisierung – mit Sicherheit



Mittelstand 4.0 – Agentur Prozesse
c/o tti Technologietransfer und
Innovationsförderung Magdeburg GmbH

Förderinitiative Mittelstand 4.0 –
Digitale Produktions- und Arbeitsprozesse

Mike Wäsche

Würzburg, 07.06.2018

Relevanz des Themas Sicherheit

- Einbindung aller industriellen Steuerungen und vernetzten Geräte in das Internet
- Systeme sind direkt oder indirekt sichtbar für Suchmaschinen

Shodan

- <https://shodan.io>

Censys

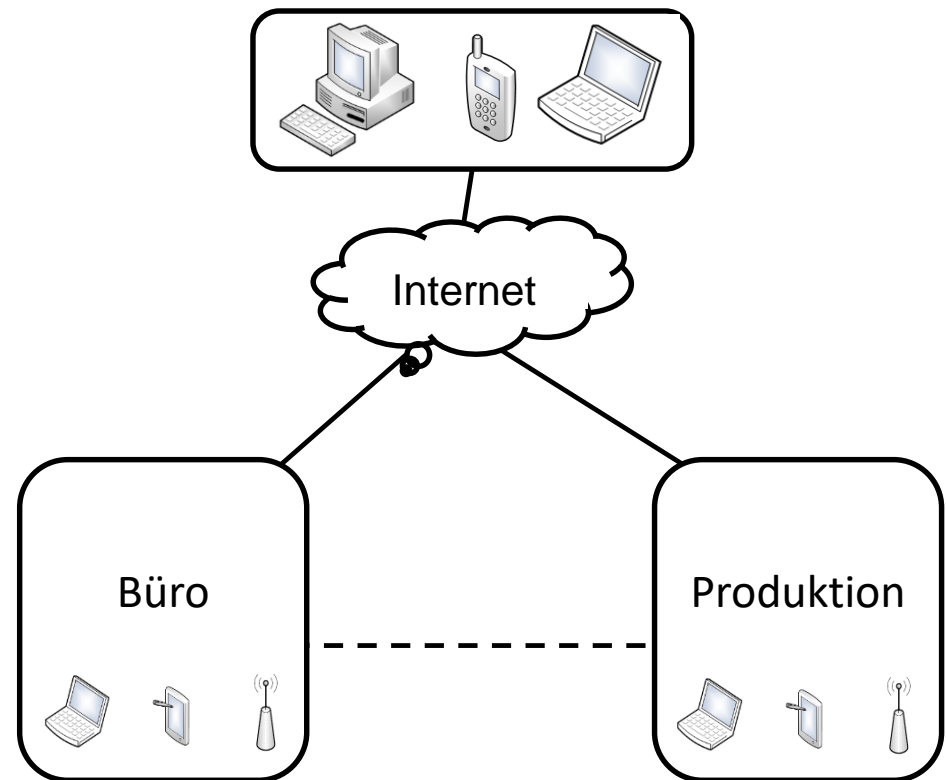
- <https://censys.io>

Google

- <https://www.google.de>

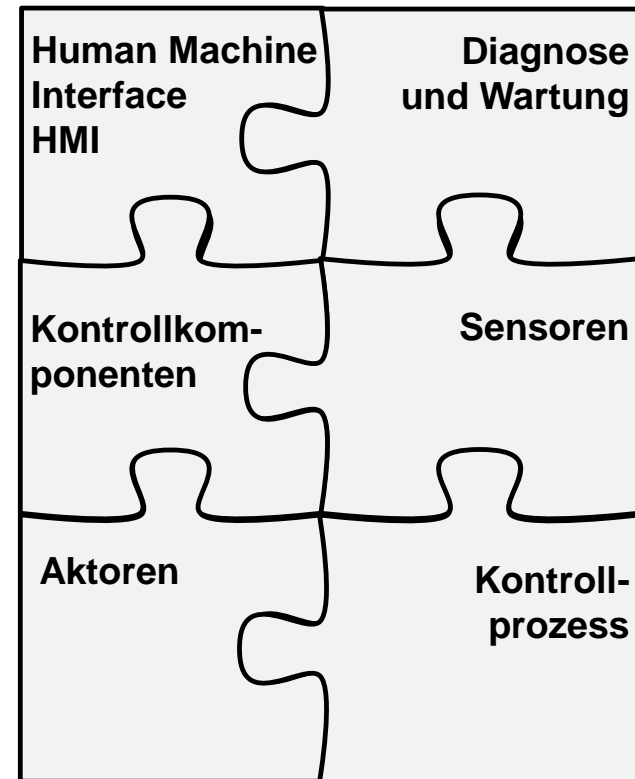
Angriffspotenziale und technische Bedrohungen in Unternehmen

- Malware
- Fernzugriff
- Technische Störungen
- Softwarefehler
- Wechseldatenträger

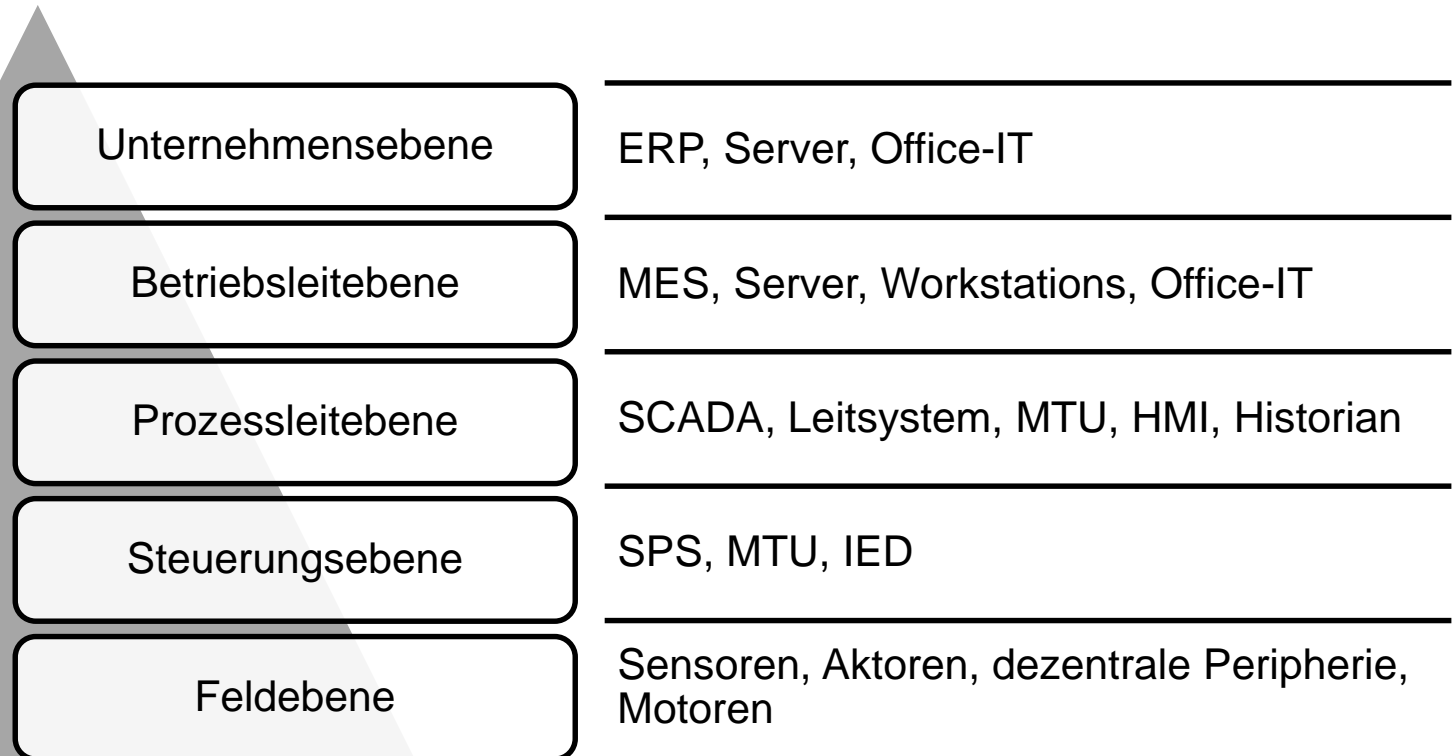


Industrielle Steuerungen

- Industrielle Steuerung = Industrial Control System ICS
- Überbegriff für industrielle Steuerungen
- ICS verarbeiten Informationen und steuern regelbasiert

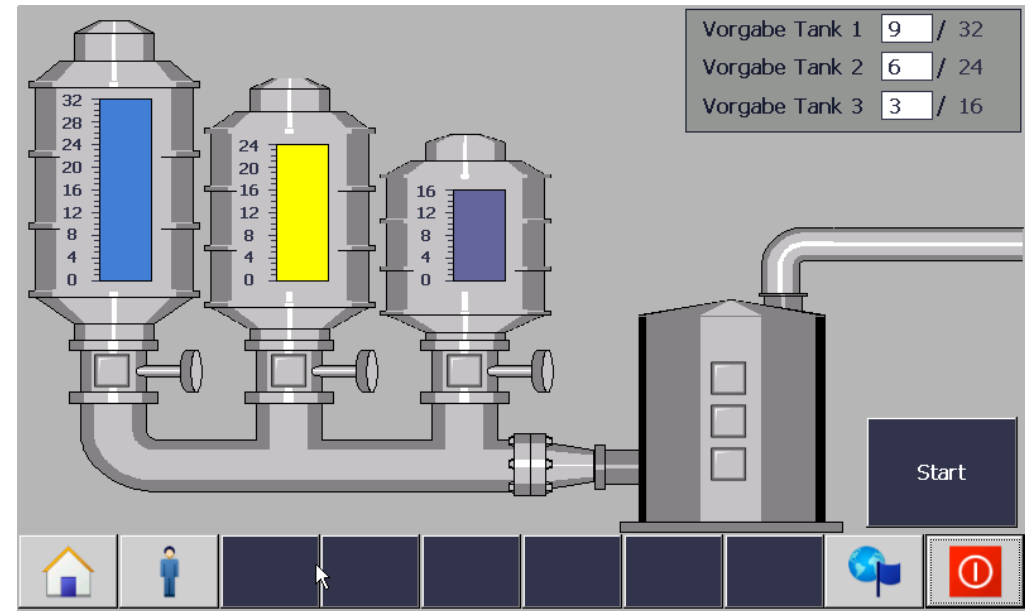


Industrielle Steuerungen und die Automatisierungspyramide



Industrielle Steuerungen – Human Machine Interface HMI

- Mensch-Maschine-Schnittstelle
- Visualisiert den Prozess (Darstellung von Istwerten)
- Dient oft zur Eingabe von Sollwerten
- Panel-PC mit Touchscreen



Industrielle Steuerungen – Top 10 Bedrohungen nach BSI

Nr. (Nr. alt)	Top 10 2016	Top 10 2014
1 (3)	Social Engineering und Phishing ⁺	Infektion mit Schadsoftware über Internet und Intranet
2 (2)	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3 (1)	Infektion mit Schadsoftware über Internet und Intranet	Social Engineering
4 (5)	Einbruch über Fernwartungszugänge	Menschliches Fehlverhalten und Sabotage
5 (4)	Menschliches Fehlverhalten und Sabotage	Einbruch über Fernwartungszugänge
6 (6)	Internet-verbundene Steuerungskomponenten	Internet-verbundene Steuerungskomponenten
7 (7)	Technisches Fehlverhalten und höhere Gewalt	Technisches Fehlverhalten und höhere Gewalt
8 (9)	Kompromittierung von Extranet und Cloud-Komponenten	Kompromittierung von Smartphones im Produktionsumfeld
9 (10)	(D)DoS Angriffe	Kompromittierung von Extranet und Cloud-Komponenten
10 (8)	Kompromittierung von Smartphones im Produktionsumfeld	(D)DoS Angriffe

Quelle: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf%3bjbjsessionid=31D99F123864924D07605528E1B40837.2_cid369?_blob=publicationFile&v=4

Industrielle Steuerungen – woher kommen die Angriffe?

Innentäter Terroristen
Kriminelle

Spammer Angreifer
Bot-Netzwerke

Geheimdienste Spione

Phisher Schadsoftware

IT-Sicherheit in der Produktion – Beispiele von Vorfällen

Maroochy Water Services

- Australien 2000
- Ex-Mitarbeiter
- Manipulation der Wasseraufbereitungsanlage
- Zugangsdaten wurden nicht gelöscht

Störfall im AKW Davis Besse

- USA 2003
- Wurm SQL-Slammer
- unsichere Datenleitung
- Ausfall des Sicherheitssystems für ca. 5 Stunden

Computerwurm Stuxnet

- Iran 2010
- Störungen der Leittechnik der Urananreicherungsanlage in Natanz

Angriff auf ein Stahlwerk

- Deutschland 2013
- Zugriff auf das Büro-Netzwerk durch Social Engineering
- Störfälle von Komponenten
- Beschädigungen der Anlage

Kontakt

- Mittelstand 4.0-Agentur Prozesse
c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH
Bruno-Wille-Straße 9
39108 Magdeburg

Roland Hallau
0391 7443524
rhallau@tti-md.de

Wilfried Müller
0391 7443537
wmueller@tti-md.de

Andreas Neuenfels
0391 7443523
aneuenfels@tti-md.de

Mike Wäsche
0391 7443534
mwaesche@tti-md.de



<http://www.prozesse-mittelstand.digital>