

Ist schon blöd...

ohne Strom



sichere industrie // // //

Industrial Security 4.0

Angriffe auf Produktion, Fertigung und das IoT



by Max Weidele

sichere-industrie.de

sichere industrie

Suchen ...

[Home](#) [Neu hier?](#) [Artikel-Übersicht](#) [Veranstaltungen](#) [Ressourcen](#) [Über uns](#)

Feeling Lost?

Informationen zur Industrial Security für Sie als Betreiber von Produktions- und Automatisierungsanlagen.

[NEU HIER?](#) [ÜBER UNS](#)

Sicherheitsmanagement

Gesetze & Normen

Angriffsszenarien

Schutzmaßnahmen

Awareness

Ransomware NotPetya – Was passierte, wer dahinter steckt, warum die Versicherung nicht zahlt und wie Sie sich davor schützen können

Die Ransomware NotPetya erzeugte weltweit verheerende Schäden von über 1 Milliarde US-Dollar. Wie kam es dazu? Wer steckt (vermutlich) dahinter? Zahlt eine Versicherung diesen Schaden? Und wie können Sie sich davor schützen?

26. Januar 2019 | Kategorien: Angriffsszenarien | Schlagwörter: EternalBlue, Nordl... | 0 Kommentare [weiterlesen >](#)

3 weitere Mythen über Industrial Security und deren echte Hintergründe

Sind Hacker und Cyber-Kriminelle wirklich für die meisten Störfälle verantwortlich? Können digitale Angriffe funktionale Safety-Systeme nicht beeinflussen? Sind Ihre Anlagen wirklich "Air-Gapped"? Wir untersuchen diese Aussagen kritisch und werfen einen Blick auf die Hintergründe.

13. November 2018 | Kategorien: Angriffsszenarien | Schlagwörter: Air-Gapped, Cyber-K... | 0 Kommentare [weiterlesen >](#)

3 Mythen über Industrial Security und was wirklich dahinter steckt

Löst genau Maßnahme "X" alle Ihre Sicherheitsbedenken? Brauchen Sie unbedingt ein nach ISO 27001 zertifiziertes ISMS? Können Ihnen nur teure Maßnahmen wirklich weiterhelfen? Wir untersuchen diese Aussagen kritisch und werfen einen Blick auf die Hintergründe.

JETZT WHITEPAPER UND NEWSLETTER ERHALTEN!

- ✓ eBook "7 Schritte Fichtung Industrial Security"
- ✓ Hinweise auf neue Fachinformationen zum Thema Industrial Security
- ✓ Tipps & praktische Vorgehensweisen
- ✓ Infos zu neuen Workshops, eBooks und Angeboten auf der Plattform

[Jetzt sofort anemelden!](#)

ANSTEHENDE VERANSTALTUNGEN

	Industrial Security Meetup (s3) – Stuttgart 31. Januar, 18:00 - 20:30 Stuttgart
	MB connect line – Anwenderkonferenz 28. Februar 2019 - 29. Februar 2019

Industrie 4.0

thingbook



Roboterarm
2001:db8::8d3:0:0:0



secure_cam_03bx
hat ein Video
veröffentlicht



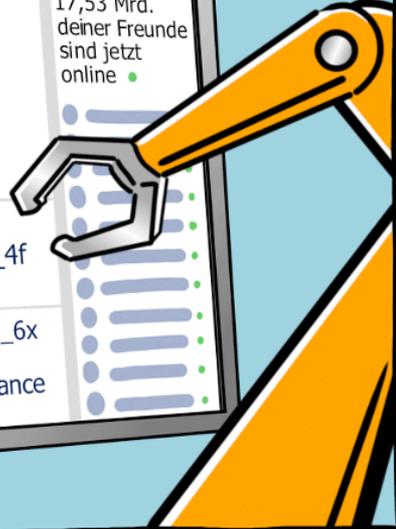
17,53 Mrd.
deiner Freunde
sind jetzt
online ●



Glühbirnchen_23x
ist jetzt mit Lampe_4f
befreundet



Schraubenschlüssel_6x
ist der Gruppe
Predictive Maintenance
beigetreten



Eindrücke Industrie 4.0



FTS



Smart City



KI



Sensoren/ IIoT



Predictive Maintenance



Cloud



Autonomous driving



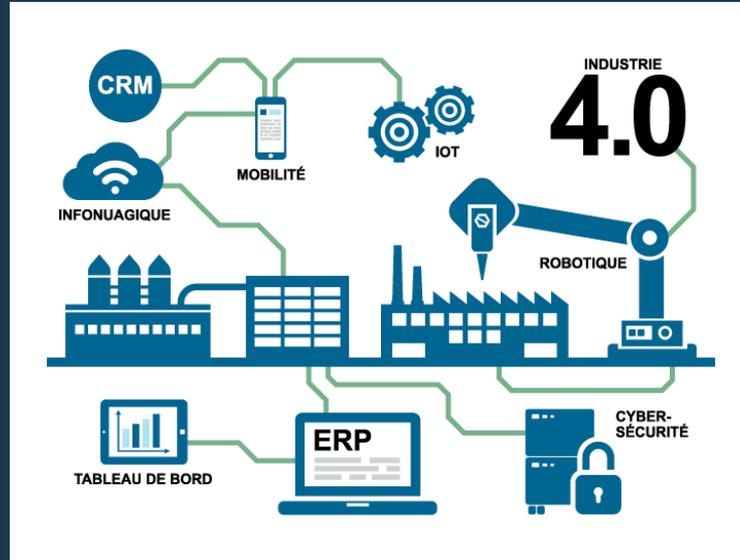
Datenbrille



Big Data



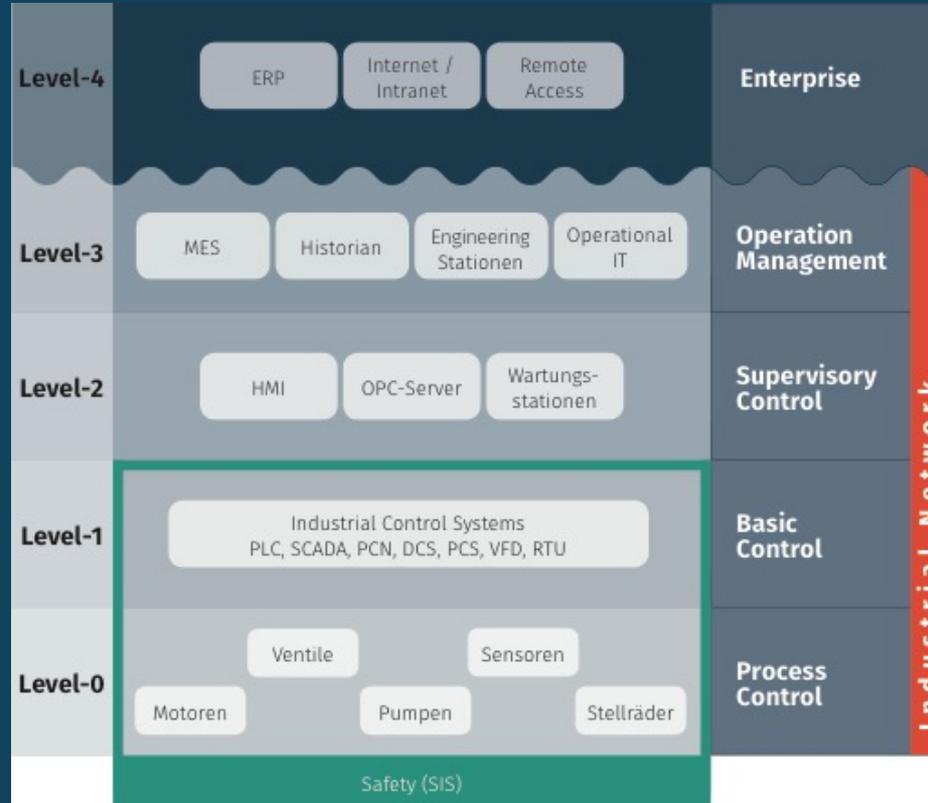
4.0 – What?



Quelle:

<http://productique.quebec/communiqués/feuille-de-route-industrie-4-0-mesi/>

ICS Purdue Reference Model



ICS Glossar: Basic Control



Quelle: siemens.com

ICS Glossar: Supervisory Control



Angriffe auf die Industrie

Norsk Hydro

The Magnor extrusion plant in Norway was one of 160 Hydro sites hit by the cyberattack



Deutsche Bahn

Zeit	Über	22:10	DB	Nach	Gleis
22:15 RB61	Dresden Mitte			Dresden Hbf	8
22:20 S1	Dresden Hbf				2
22:25 S2	Dresden-K				1
22:25 RE50	Coswig (b.)			Hbf	6
22:25 RE50	Dresden M			Hbf	3
22:29 IC 2045				Hbf	7
22:32 S2	Dresden Mitte			Dresden Hbf	2
22:37 S1	Radebeul Ost - Coswig (b. Dre)			Meißen Trieb	1

Oops, your files have been encrypted!

It is possible that someone has encrypted your files. If you are not the owner of this computer, please contact your system administrator immediately.

Files will be lost on:
0:00:00 00:00:00
Time Left: 02:23:50:46

Files will be lost on:
0:00:00 00:00:00
Time Left: 05:23:50:46

Wie löse ich?

Send 1000 worth of Bitcoin to this address:
12WYDFpnce8Hghgqf8y7ANhup85Me

Send Bitcoin

Bild Martin Wiesner über www.heise.de

NotPetya: Maersk erwartet bis zu 300 Millionen Dollar Verlust

16.08.2017 18:08 Uhr - Fabian A. Scherschel

vorlesen



Die Gunvor Mærsk der Maersk Line mit Kurs auf den Hamburger Hafen. (Bild: Bernhard Fuchs, CC BY 2.0)

Containerterminals standen still, Schiffe konnten weder gelöscht noch beladen werden: Mehrere Wochen hielt der Trojaner den dänischen Mega-Konzern Maersk in Atem. Die Reederei Maersk Line und der Hafentreiber APM Terminals wurden schwer getroffen.

NotPetya: Auch FedEx kostet die Cyber-Attacke 300 Millionen US-Dollar

22.09.2017 09:57 Uhr - Martin Holland

vorlesen



Nach Maersk hat nun auch FedEx eingestanden, wie teuer es war, die Schäden durch die Malware NotPetya zu beheben. Insgesamt beziffert das US-Unternehmen die Kosten bei der niederländischen Tochter TNT Express mit 300 Millionen US-Dollar.

Hafen Barcelona



- ▲ 20.09.2018
Hafen Barcelona
- ▲ Nochmal Glück gehabt

TRISIS – Angriff auf Safety

- ▲ Zielt auf Safety-Systeme
- ▲ Keine finanzielle Motivation
- ▲ Komplexität des Angriffs
- ▲ => vermutlich staatlicher Angreifer

Saudi-Arabien: Cyberangriff hätte Explosion auslösen können – Ermittler sind alarmiert

15.03.2018 15:42 Uhr – Martin Holland

vorlesen



Öraffinerie (Bild: anekoho/Shutterstock.com)

Vor wenigen Monaten hat es in Saudi-Arabien angeblich einen Hackerangriff gegeben, der Menschen ihr Leben hätte kosten können. Dass es die angepeilte Explosion in einem Kraftwerk nicht gegeben hat, war einem Bericht zufolge nur glückliche Fügung.

Eine Fabrik eines petrochemischen Unternehmens in Saudi-Arabien ist vergangenen August angeblich Ziel eines Cyberangriffs geworden, der unter anderem eine Explosion auslösen sollte, bei der Menschen hätten sterben können. Das [berichtet die New York Times](#) und ergänzt, dass diese Explosion nur deshalb ausgeblieben sei, weil der Code der Angreifer einen Bug enthalten habe. Der Zeitung zufolge haben Ermittler weder das betroffene Unternehmen, noch deren Heimatland genannt beziehungsweise erklärt, wen sie für verantwortlich halten. Der Angriff werde aber als eine weitere Eskalation eines sich zuspitzenden Cyber-Wars zwischen Saudi-Arabien und dem Iran aufgefasst, der immer gefährlichere reale Konsequenzen nach sich zieht.

Weitere Angriffe

- ▲ Stuxnet
- ▲ Industroyer
- ▲ BlackEnergy
- ▲ WannaCry
- ▲ Havex
- ▲ ...

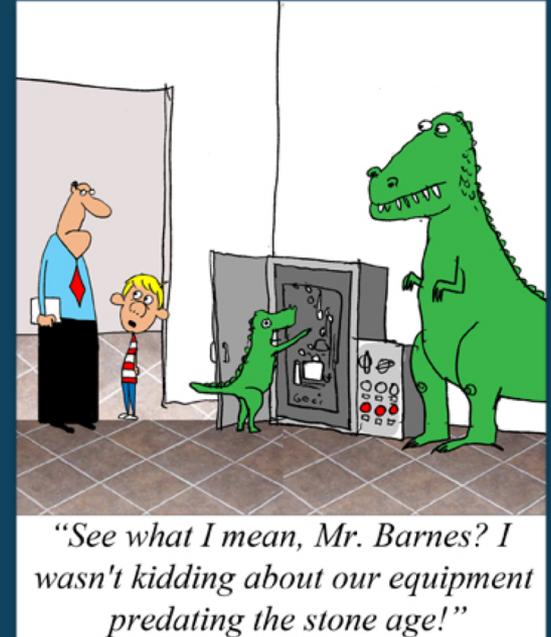
Wie kommt es dazu?

Wie kommt es dazu?

- ▲ Internet & seine unsicheren Technologien
- ▲ „Air gap“ Gedanke hält an
- ▲ Schleichender Anstieg der Vernetzung („historisch gewachsen“)
- ▲ IT-Sicherheit zum Selbstzweck erzeugt kein ROI

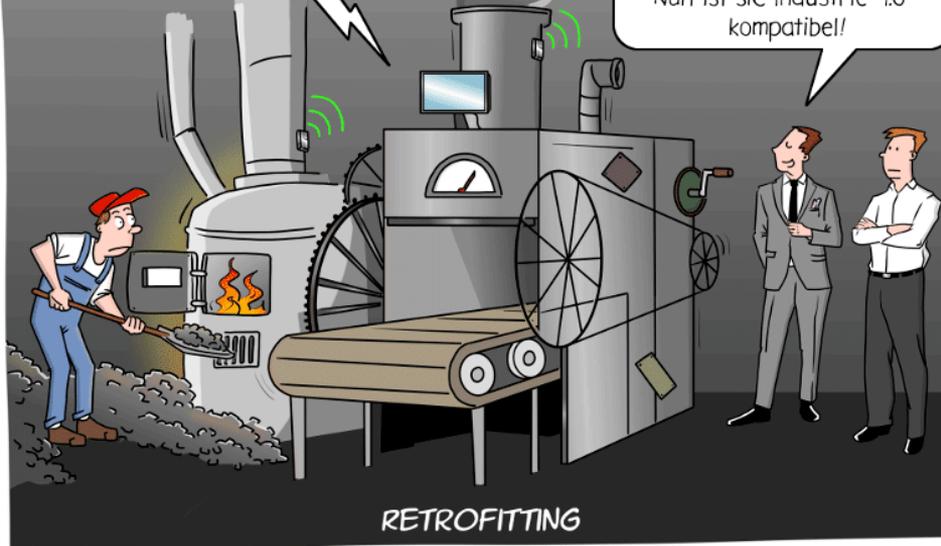
Wie kommt es dazu? Pt.2

- ▲ IIoT / Industrie 4.0-Produkte: „Ship it first“ / „feature driven“
- ▲ Vielzahl proprietärer Protokolle
- ▲ Lebensdauer 15 bis 30 (!) Jahre
- ▲ „hard coded passwords“
- ▲ Grundlegende Unterschiede Information Technology (IT) / Operational Technology (OT)



*Nachdem du mich befeuert hast,
justiere mich doch bitte noch kurz,
damit ich mit der heutigen Produktion
beginnen kann!*

Diese Anlage stammt noch aus
dem Besitz meines Großvaters.
Nun ist sie Industrie 4.0-
kompatibel!



RETROFITTING

Lösungsansätze?

Defense in Depth – Analogie



Quelle: Castle Cornet, Photo by Enrapture Media on Unsplash

Zones & Conduits

- ▲ Teil von „Defense in depth“
- ▲ Segmentierung in Sicherheitszonen
- ▲ Definition der Zonenübergänge

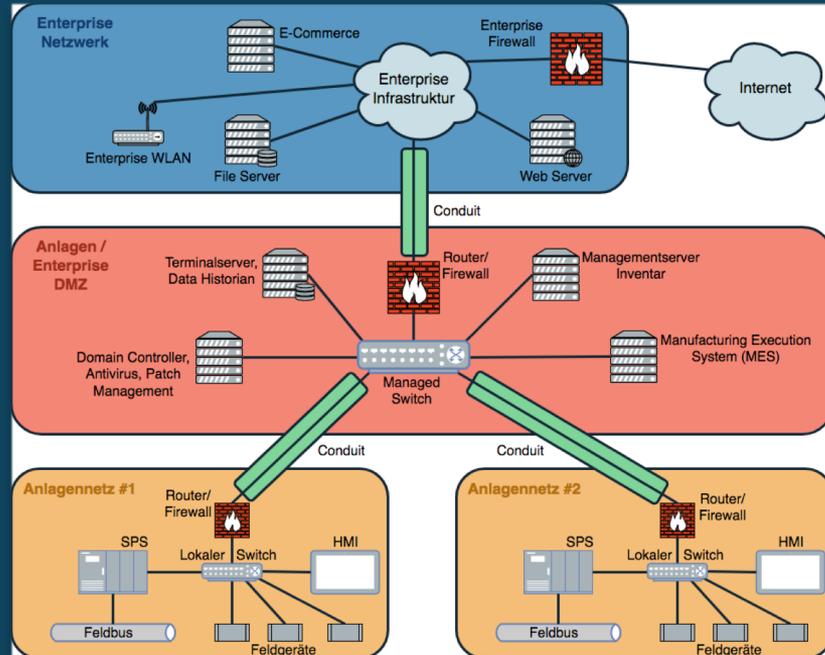
Netzwerk

Dateitransfer

Lieferanten

Management

Zones & Conduits



Netzwerk

Dateitransfer

Lieferanten

Management

Dateitransfer

- ▲ USB-Sticks
- ▲ E-Mail Anhänge
- ▲ Updates für Systeme



Netzwerk

Dateitransfer

Lieferanten

Management

Lieferanten

- ▲ Standardisierte Fernwartung
- ▲ Konzept für externe Geräte
- ▲ Einkaufsbestimmungen
- ▲ Speicherort Projektierungsdaten



Netzwerk

Dateitransfer

Lieferanten

Management

Management

- ▲ Risikobasierter Ansatz
- ▲ Dokumentation
- ▲ Awareness des Personals



Netzwerk

Dateitransfer

Lieferanten

Management

Zusammenfassung

***Keine
IT-Sicherheit zum Selbstzweck!***

Weitere Informationen

- ▲ OWASP - Open Web Application Security Project
- ▲ IEC 62443
- ▲ BSI-Grundschatz
- ▲ VDI/VDE 2182
- ▲ Schwellwerte aus IT-SiG beachten
- ▲ CERT abonnieren
- ▲ B3S des BSI
- ▲ ... [sichere-industrie.de](https://www.sichere-industrie.de)

Partner & Kooperationen



Digital Hub Logistic
- Hamburg



VdS –
Schadenverhütung



Freies Institut für
IT-Sicherheit e.V.



Zentralverband
Elektrotechnik- u.
Elektronikindustrie
e.V.



CERT@VDE



Mitmachen erwünscht!

- ▲ *Ausrichten von Veranstaltungen*
- ▲ *Verfassen von Artikeln & Praxisberichten*
- ▲ *Teilnehmen an lokalen Gesprächsrunden*

Mit gutem Beispiel vorangehen!

Nächste Termine!

- ▲ 15.05.: Industrial Security meets Leipzig
- ▲ *Hamburg, Düsseldorf, Augsburg und Stuttgart wieder in Kürze*

Kontakt - Max Weidele



Industrial & IIoT Security

Security in Produktion

Industrielle Fernwartung

