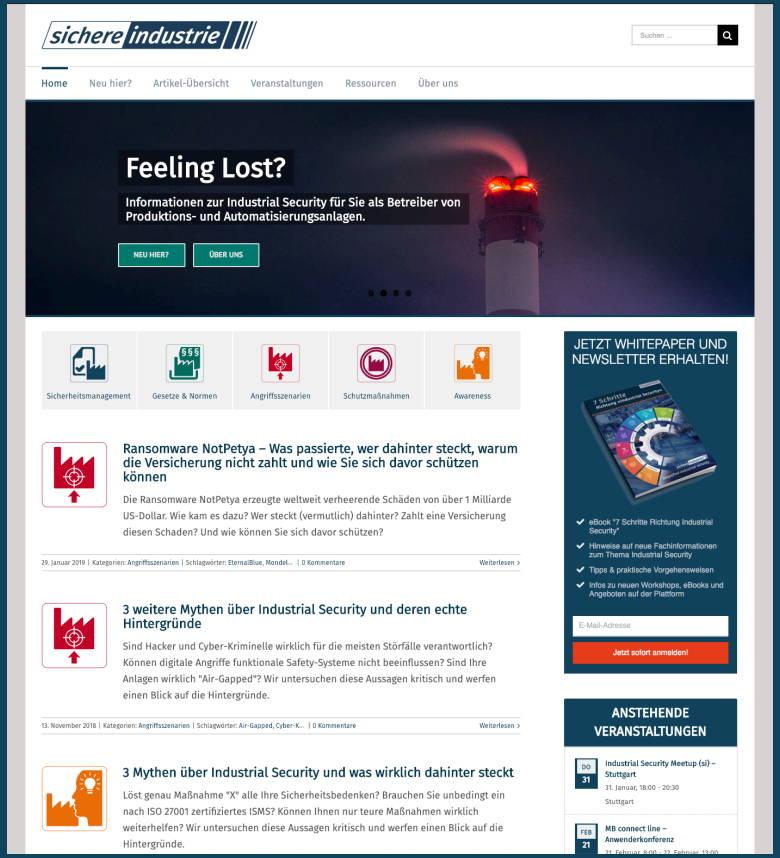

Ist schon blöd...
ohne Strom
§§§
sichere industrie

Industrial **Security 4.0**

Angriffe auf **Produktion, Fertigung** und das **IoT**

by Max Weidele

sichere-industrie.de



Industrie 4.0


CLOUD-SCIENCE.DE
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

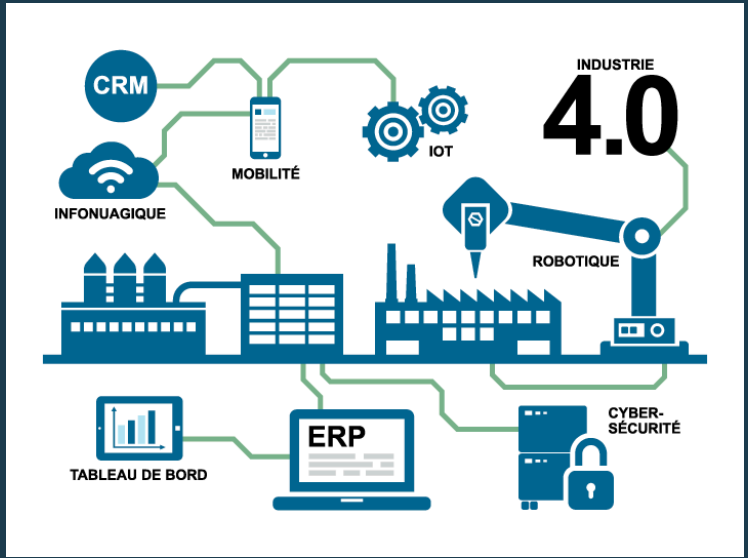
Cloud

Autonomous driving

Datenbrille

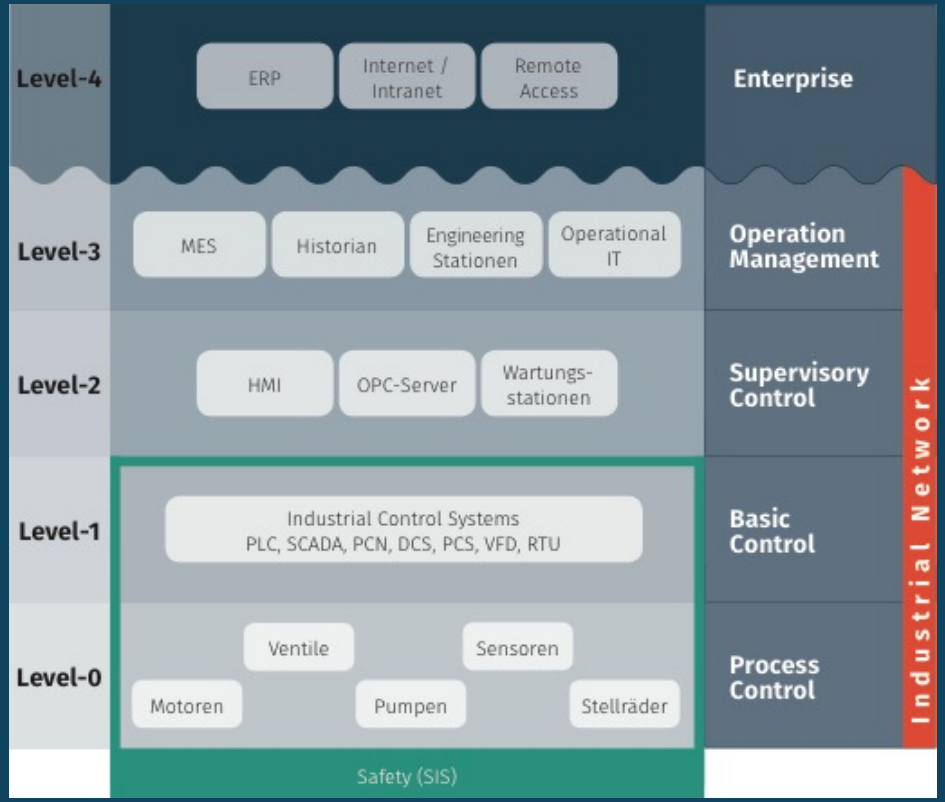
Big Data

4.0 – What?



Quelle:
http://productique.quebec/communiques/feuille-de-route-industrie-4-0-mesi/

ICS Purdue Reference Model



ICS Glossar: Basic Control

Quelle: siemens.com

ICS Glossar: Supervisory Control

Quelle: edson.com

Angriffe auf die Industrie

Norsk Hydro


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

Deutsche Bahn

Bild Martin Wiesner über www.heise.de

Maersk & FedEx

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 Hafenbetreiber 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.

Bilder über www.heise.de

Hafen Barcelona

- 20.09.2018
  Hafen Barcelona
- Nochmal Glück gehabt

Bild: Screenshot von www.sichere-industrie.de

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

Öfraffinerie (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.

Bildquelle: heise.de

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**)

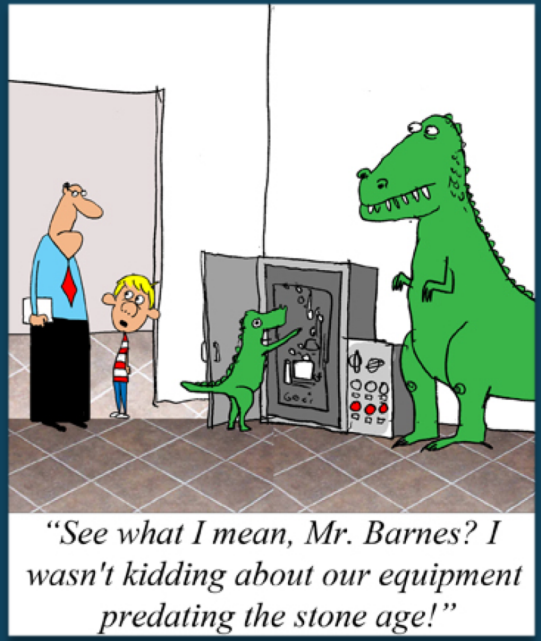
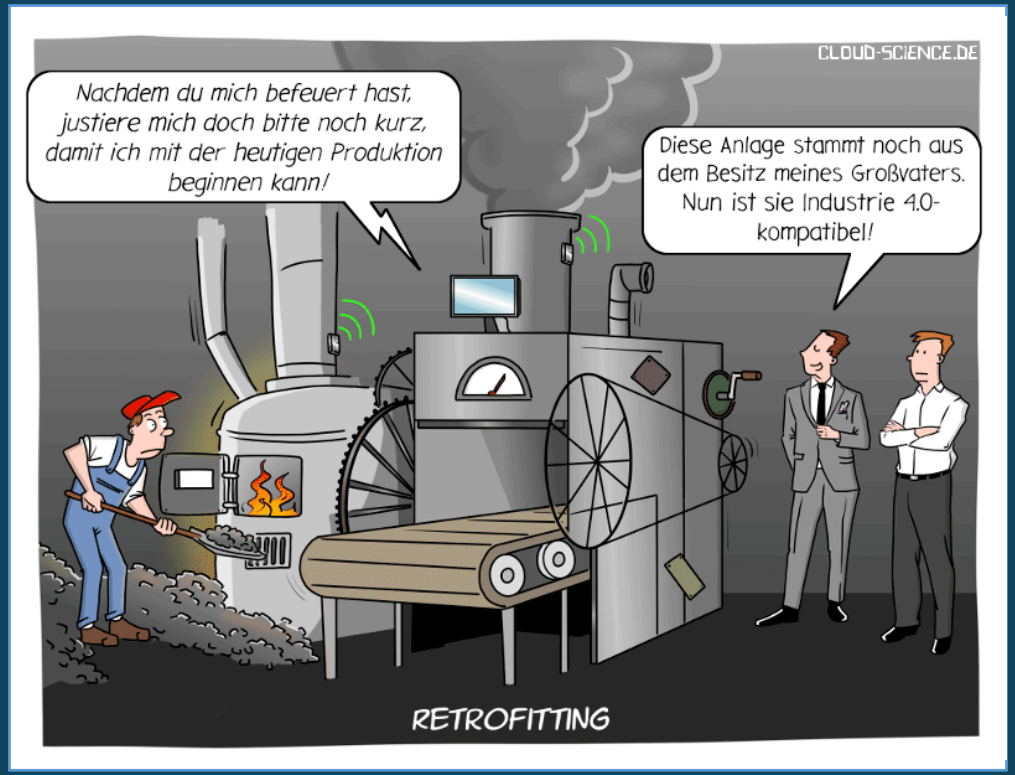


Bild: automation.com


CLOUD-SCIENCE.DE
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?

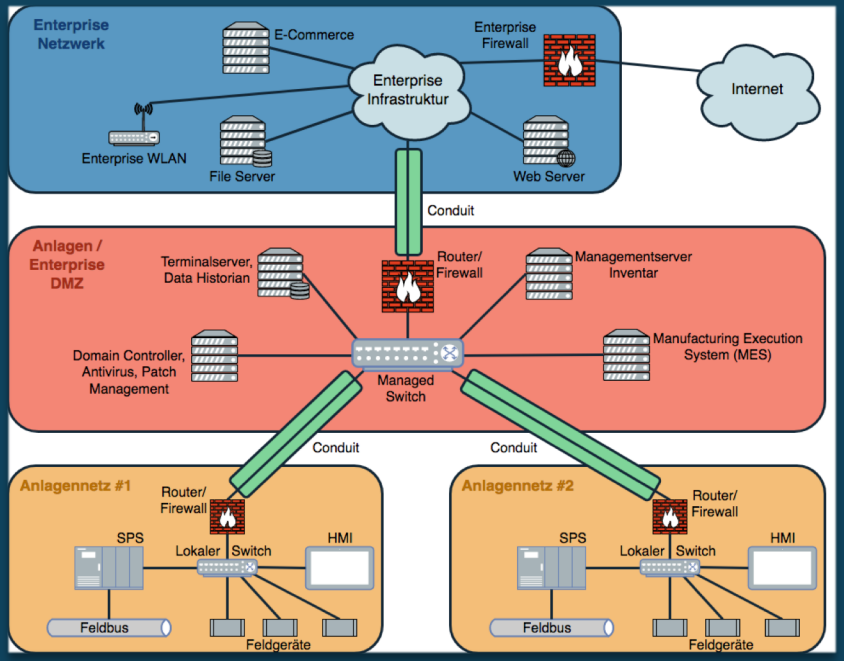
Defense in Depth – Analogie

Quelle: Castle Cornet, Photo by Enrapture Media on Unsplash

Zones & Conduits

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

Zones & Conduits



Dateitransfer

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

Lieferanten

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

Management

- Risikobasierter Ansatz
- Dokumentation
- Awareness des Personals

Zusammenfassung

Keine
IT-Sicherheit zum Selbstzweck!

Weitere Informationen

- OWASP - Open Web Application Security Project
- IEC 62443
- BSI-Grundschutz
- VDI/VDE 2182
- Schwellwerte aus IT-SiG beachten
- CERT abonnieren
- B3S des BSI
- **… 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

sichere industrie

max.weidele@sichere-industrie.de