Herzlich willkommen zur Veranstaltung

IT-Sicherheit in der Produktion

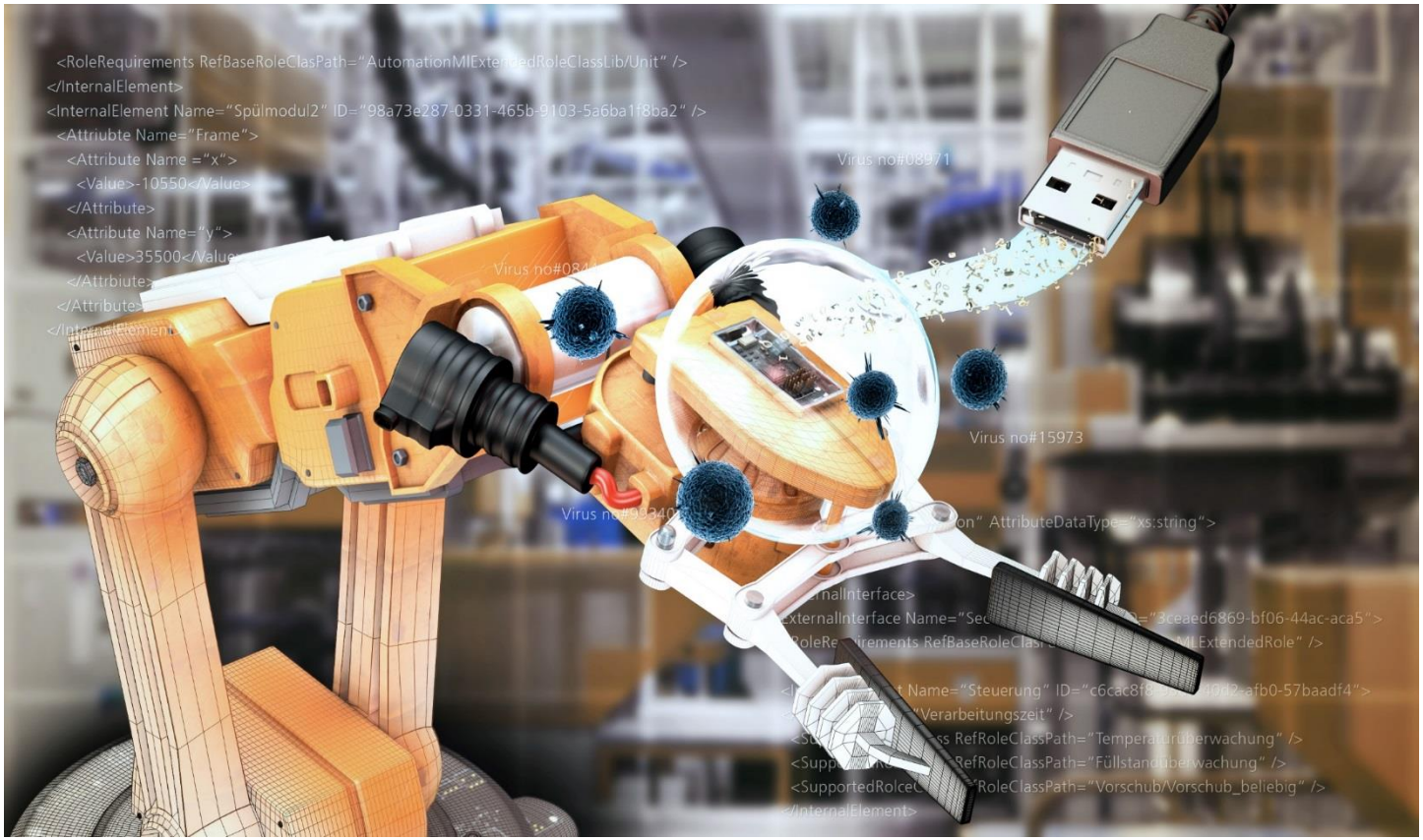
Gerhard Sutschet

Fraunhofer IOSB

DGQ

Deutsche Gesellschaft für Qualität

IT-Sicherheit in der **Produktion**



Stefan Riel © Fraunhofer IOSB 2014

DGQ

Fraunhofer IOSB

IT-Sicherheit in der Produktion

- Ist IT-Sicherheit in der Produktion wichtig?
- Industrie 4.0 und die Konsequenzen
- IT-Sicherheit auch in den Produktionshallen!
  - Was muss mein Unternehmen schützen?
  - Wer greift mein Unternehmen an?
  - Wer ist für was verantwortlich?
- Weiterbildung – Warum?

Umfrage des VDMA

Risiken:

- 92% der Mittelständler wurden bereits attackiert.
- 38% melden sogar mehrfach wöchentlich attackiert zu werden.
- 76% sagen, dass der Fachkräftemangel zu messbaren Beeinträchtigungen ihrer Unternehmensnetzwerke geführt habe.
- 83% der Entscheider verweisen auf einen Sicherheits-Fachkräfte-Mangel

Umfrage des VDMA

Chancen:

- Mehr als 56% sehen in IT-Security den maßgebliche Technologietreiber
- 57% der Betriebe sehen IT-Sicherheit als unabdingbare Voraussetzung für die Digitalisierung in ihrem Unternehmen

Stuxnet

Angriff auf Irans Atomprogramm

Stuxnet-Virus könnte tausend Uran-Zentrifugen zerstört haben

Neue Erkenntnisse über den hinterhältigen Stuxnet-Wurm: Möglicherweise hat die Schad-Software in der iranischen Anreicherungsanlage Natans größere Schäden angerichtet, als das Regime in Teheran eingestehen will. Bis zu tausend Uran-Zentrifugen hat der Virus womöglich auf dem Gewissen.

Von Christian Stöcker

Quelle: SPIEGEL ONLINE 2010

Ist IT-Sicherheit in der Produktion wichtig?

Cyber-Attacke auf deutsches Stahlwerk

heise Security News Hintergrund Foren Events

Security > News > 7-Tage-News > 2014 > KW 51 > BSI-Sicherheitsbericht: Erfolgreiche Cyber-Attacke auf deu

« Vorige | Nächste »

BSI-Sicherheitsbericht: Erfolgreiche Cyber-Attacke auf deutsches Stahlwerk

17.12.2014 15:58 Uhr – Fabian A. Scherschel vorlesen

Bei einem bislang unbekannten Angriff beschädigten die Angreifer einen Hochofen schwer. Doch neben den gezielten Angriffen auf Industrieanlagen bilanziert das BSI auch eine steigende Gefahr für Endanwender.

Quelle: Heise Security 2014

Cyber-Attacke auf deutsches Stahlwerk

- Methode:
  - Spear-Phishing und Social Engineering
  - Eindringen über das Büronetz in das Produktionsnetz
- Schadenswirkung:
  - Ausfälle einzelner Steuerungskomponenten oder ganzer Anlagen
  - Ein Hochofen konnte nicht geregelt heruntergefahren werden
  - In Folge massive Beschädigungen der Anlage
- Quelle: BSI – Die Lage der IT-Sicherheit in Deutschland 2014

DGQ

Fraunhofer IOSB

Top 10 Bedrohungen nach BSI

# (# alt)	2016	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 Smartphones im Produktionsumfeld
10 (8)	Kompromittierung von Smartphones im Produktionsumfeld	(D)DoS Angriffe

DGQ

Fraunhofer IOSB

Industrie 4.0

Cloud- und Cyber-Physische-Systeme, Smart Factory

Vernetzte Produktion
Vernetzte der Produktions-abläufe durch **Cloud-** und **Cyber-Physische-Systeme** (CPS)

Industrie 4.0

1. programmierbare Steuerung (SPS), Modicon 084, 1969

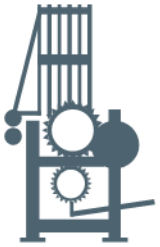
Automatisierung
Weitere Automatisierung der Produktionsprozesse durch **Elektronik** und **IT**

Industrie 3.0

1. Fließband, Schlachthöfe von Cincinnati, 1870

Massenproduktion
Arbeitsteilige Massenproduktion mithilfe **elektrischer Energie**

Industrie 2.0



1. Mechanischer Webstuhl, 1784

Mechanisierung
Mechanischen Produktions-anlagen, betrieben mit **Wasser-** und **Dampfkraft**

Industrie 1.0

Grad der Komplexität

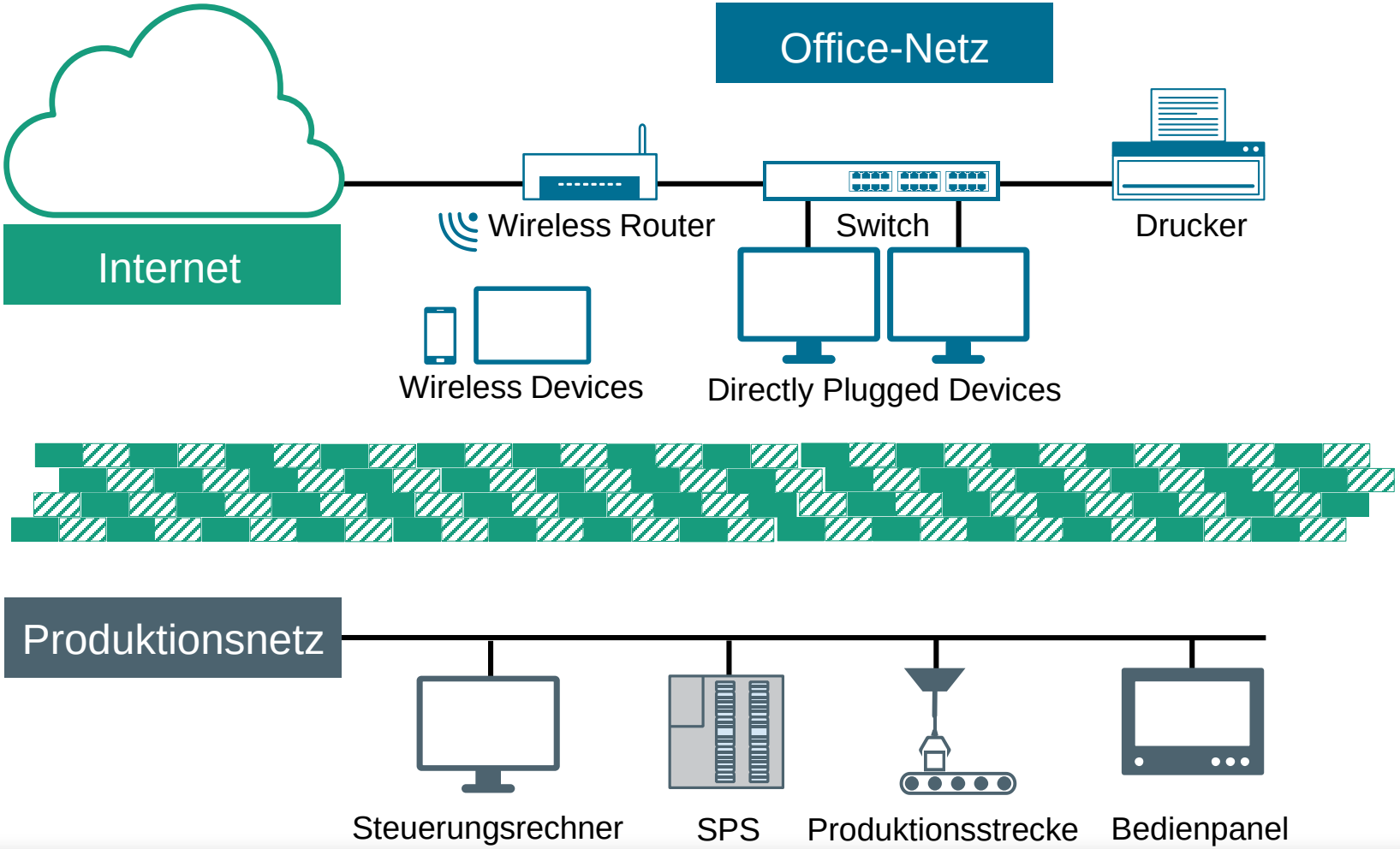
Ende 18. Jh. | Beginn 20. Jh. | Beginn 70er Jahre, 20. Jh. | heute

Industrie 4.0

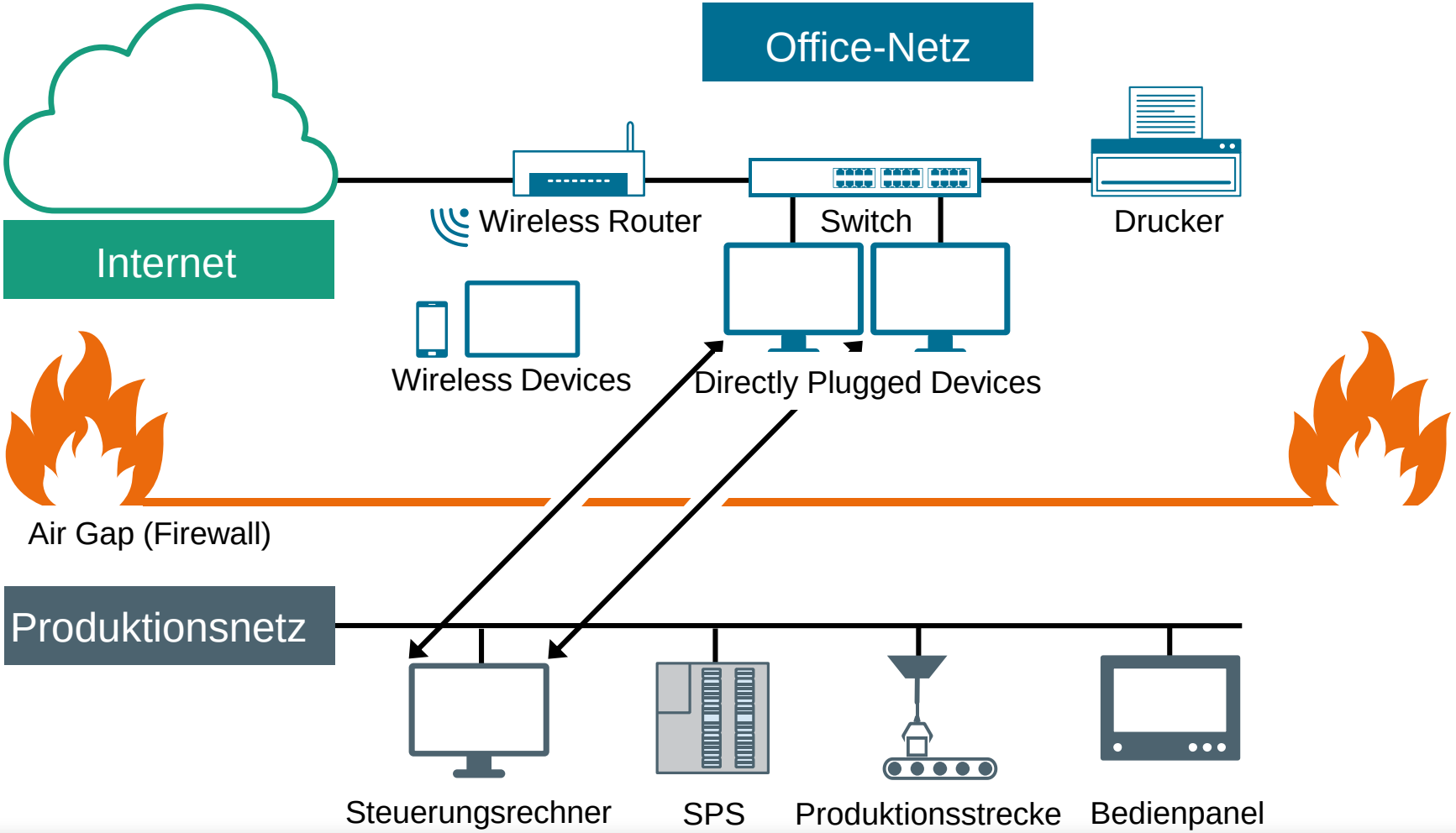
- Höhere Effizienz durch intelligente Vernetzung von Produktentwicklung, Produktion, Logistik und Kunden
- Mehr Flexibilität → Resiliente Fabrik
- Neue Geschäftsmodelle durch Service-Orientierung:

  „Everything as a service“

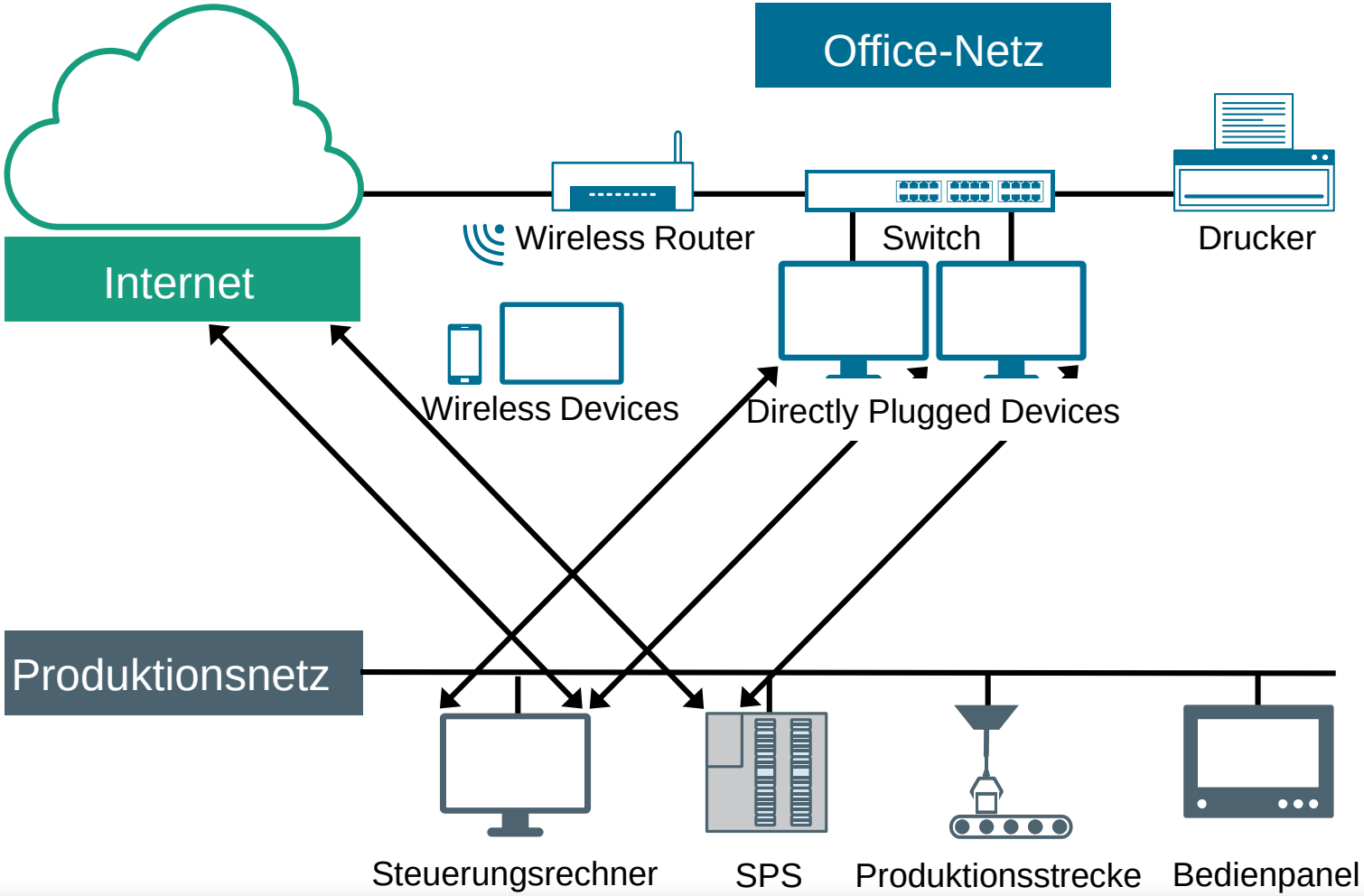
Produktionsnetze in der Vergangenheit



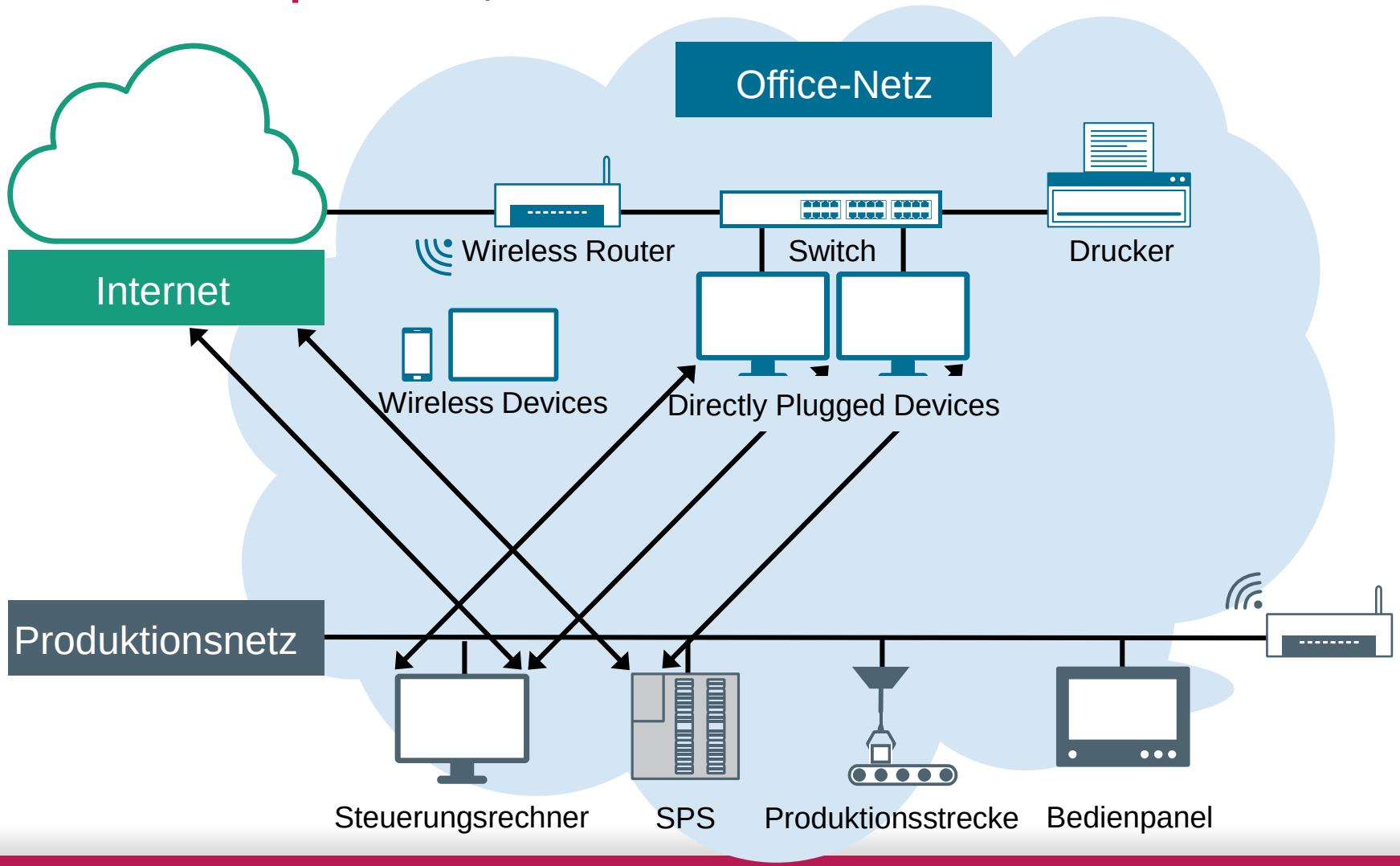
Produktionsnetze in der Gegenwart



Produktionsnetze in der Zukunft



Drahtlose Komponenten, Daten- und Service-Clouds



Alles, was für das Unternehmen von Wert ist (Assets)!

- Hardware: PCs, Laptops, Server, Produktionsanlagen, …
- Software: gekaufte, selbst erstellte, SPS-Programme, …
- Daten: nicht nur auf elektronischen Medien, sondern auch in Papier- und anderer Form
- Infrastruktur: Gebäude, Elektrizität, Klimatisierung, IT, OT, …
- Personen: Know-How, Erfahrungswissen, …
- Ausgelagerte: Online-Services, Rechtsdienstleistungen Rechnungswesen, …

Wer greift mein Unternehmen an?

- Rolle / Position:
  - Außenstehender
  - Benutzer
  - Betreiber
  - Wartungsdienst
  - Produzent

Wer greift mein Unternehmen an?

- Verbreitung:
  - Stellen im System, an denen der Angreifer Informationen gewinnen oder Systemzustände verändern kann
- Verhalten:
  - passiv / aktiv
  - beobachtend / verändernd

Wer greift mein Unternehmen an?

- Ressourcen:
  - Rechenzeit
  - Geld
  - Personal
- Motivation:
  - Spieltrieb / Geltungsbedürfnis
  - Geld
  - Vandalismus

DGQ

Fraunhofer IOSB

Wer ist für was verantwortlich?

Verantwortung Beteiligung

Schritt \ Rolle	Entscheider	Experte Security	Experte System	Experte Anwendung	Koordinator	Auditor
Assets identifizieren	V	B	B	B	B	
Bedrohungen analysieren		V+B	B	B	B	
Schutzziele ermitteln		B	B	V+B	B	
Risiken analysieren und bewerten	V	B	B	B	B	
Schutzmaßnahmen (SM) aufzeigen		B	V+B	B	B	
SM auswählen	V	B	B	B	B	
SM umsetzen			V+B		B	
Prozessaudit durchführen					B	V+B

Quelle: VDI/VDE: Richtlinie 2182

Weiterbildung – warum?

- Fachkräftemangel in der IT-Sicherheit
- IT-Sicherheitsexperten sind nicht in der Produktion „zu Hause“
- Automatisierungsexperten haben wenig IT-Sicherheits-Know-How
- Zwingend erforderlich:
  Interaktion von Unternehmens-IT und Automatisierungsexperten
- IT-Sicherheit ist ein fortlaufender Prozess

Wie sehen die Herausforderungen der Zukunft aus?

**„Prediction is very difficult –
especially if it's
about the future“**

Nils Bohr

Vielen Dank für Ihre Teilnahme und kommen Sie gut nach Hause.

Gerhard Sutschet

Fraunhofer IOSB

DGQ
Deutsche Gesellschaft
für Qualität