FAST. SECURE. GLOBAL.

Digitalisierung und Industrie 4.0 verändern die Anforderungen an IT-Security

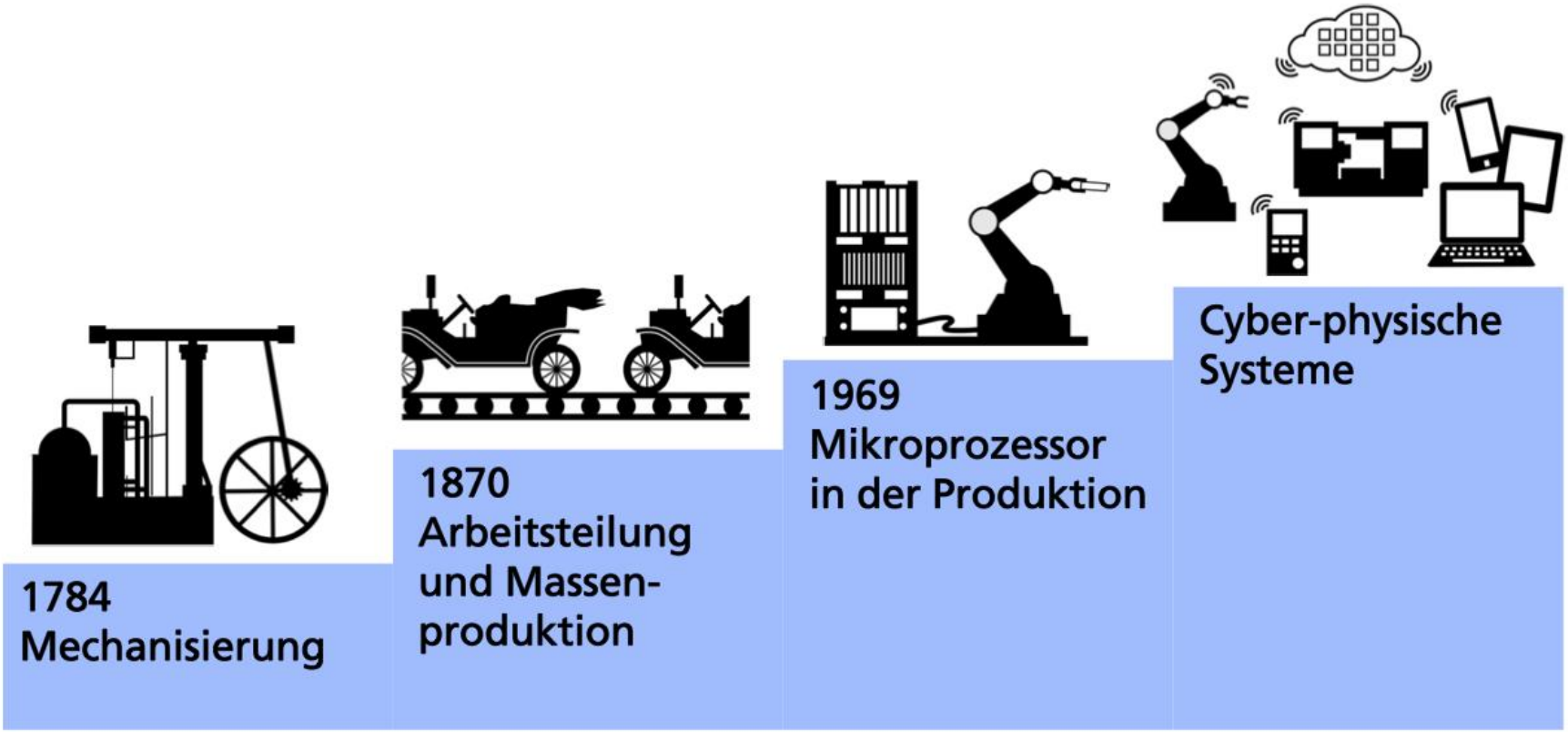
Dirk Wollberg Major Account Manager Utilities

Oberberg Online

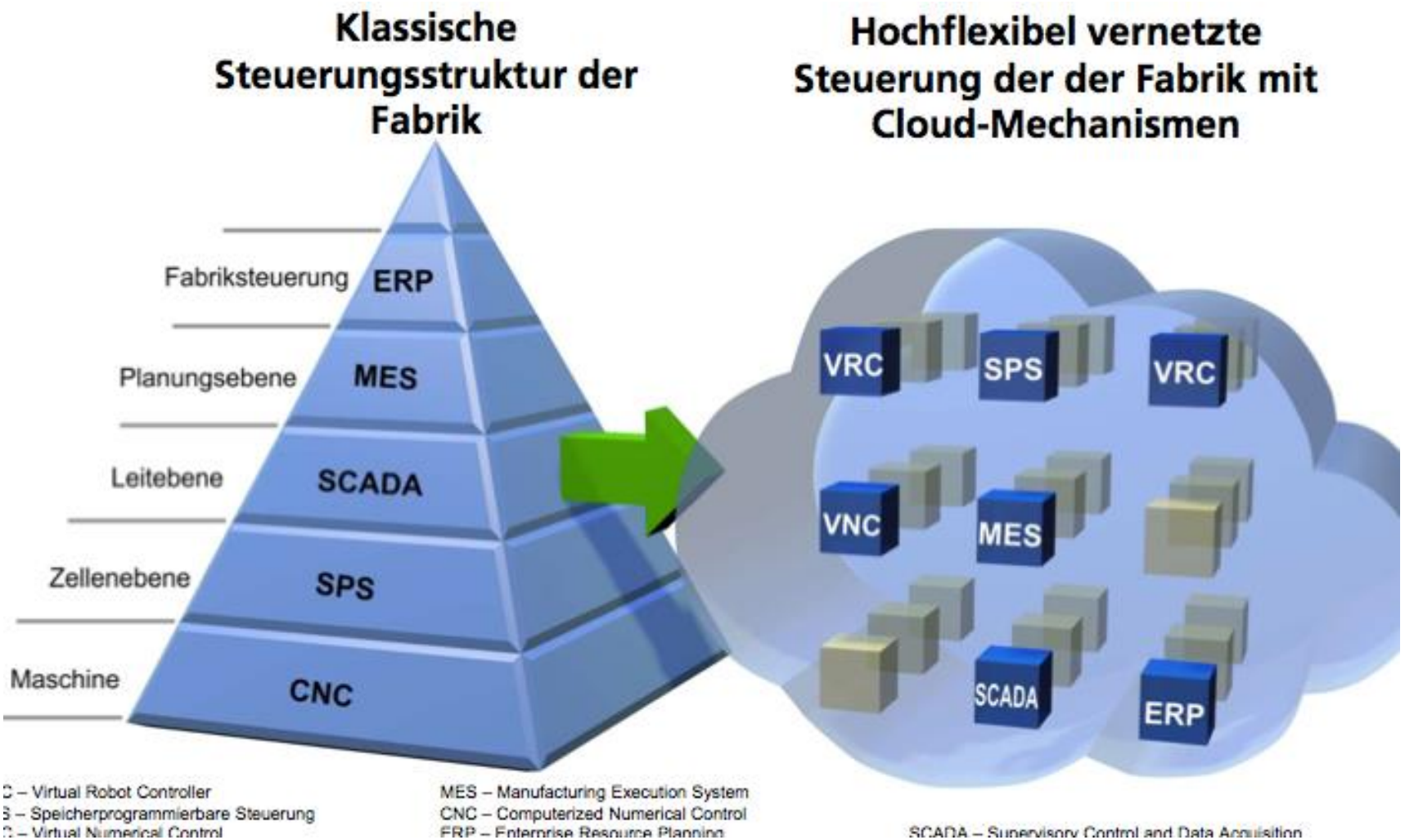
Agenda

- **Industrie 4.0 – Ein Erklärungsversuch**
  - » Der Wandel von 3.0 zu 4.0
- Die Herausforderungen für die Industrie
- Die Änderung der Verwundbarkeit
- Maßnahmen
- Warum Fortinet ?

Industrie 4.0 – Was ist das überhaupt???



Der Wandel von 3.0 zu 4.0

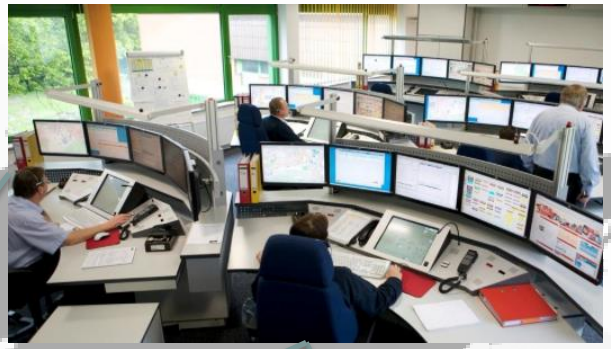


Agenda

- Industrie 4.0 – Ein Erklärungsversuch
  - » Der Wandel von 3.0 zu 4.0
- **Die Herausforderungen für die Industrie**
- Die Änderung der Verwundbarkeit
- Maßnahmen
- Warum Fortinet ?

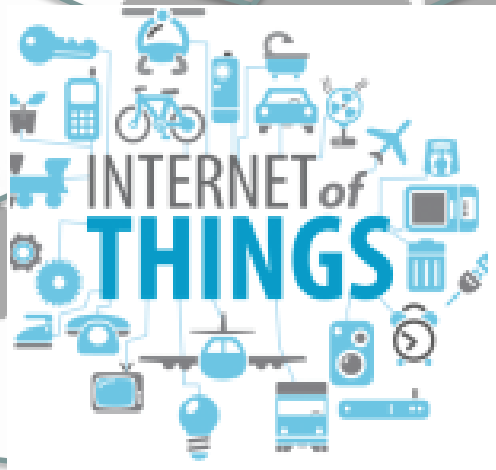
Die Herausforderung:
Globale Vernetzung – globale Standards

Office IT



SCADA

Internet



Feldebene

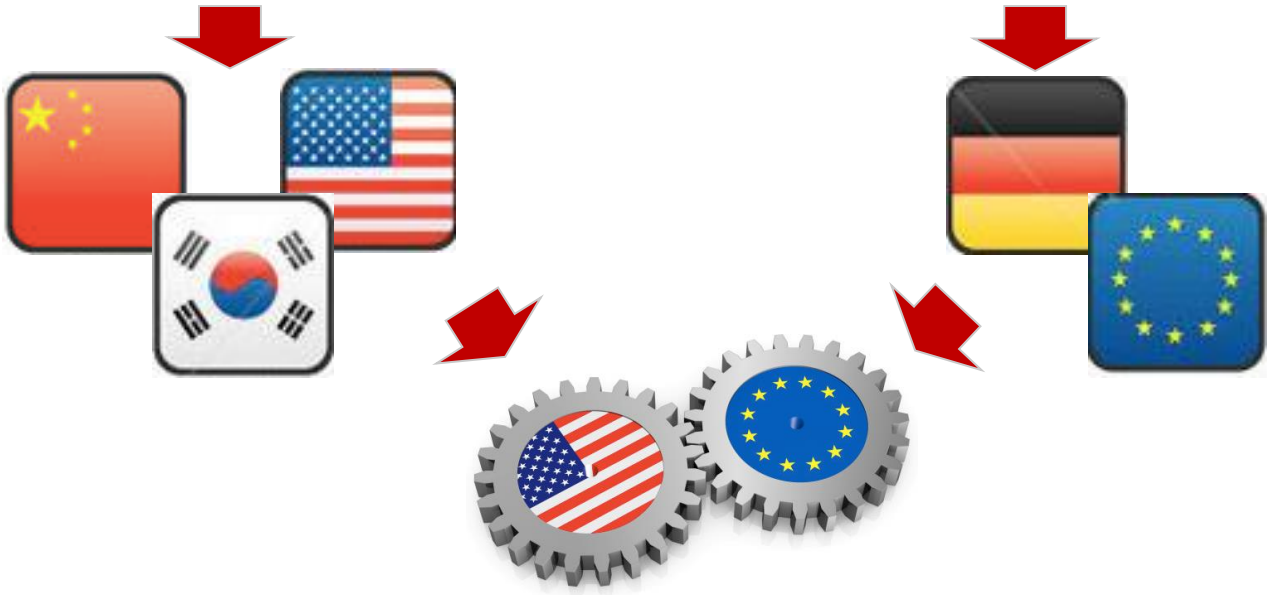
Die Realität!
Turmbau zu Babel der Industrie!

Aufgabe:

Schaffung von weltweiten Standards

Realität: Wettlauf um Normen / Standards / Referenzarchitekturen

Die Macher = **Schnell** (um jeden Preis) vs. Die Denker = **Sicher** / (zu) Langsam



Zwischenfazit

- Schaffung von weltweiten Standards ist schwierig
  - » Persönliche wirtschaftliche Interessen
- Politische Voraussetzungen müssen gegeben sein
  - » z.B. Freihandelsabkommen TTIP – nicht nur Abschaffung der Zölle, sondern auch Wegbereiter für Standardisierung
- Initiativen der Bundesregierung müssen konsequenter werden
  - » USA ist mit der IIC (Industrial Internet Consortium) wesentlich aktiver!!!
- Industrie muss „mitspielen“

Realität von Industrie 4.0 nicht vor 2025 !!! (Analystenmeinung)

ABER:

- **Industrie 3.0 / 3.5 ist JETZT!**

  » Weg von seriellen, proprietären Lösungen - hin zur **Standardisierung** in Industrie-/ Prozessdatennetzen in Form von **Ethernet / IP als Transportmedium**

  » Verwendung von Ethernet-basierenden Industrie-Protokollen wie z.B.

  - IEC 60870-5-104 (Stromnetze, Verkehrsleitsysteme)
  - IEC 61850 (Schutztechnik Strom)
  - Modbus TCP (Industrie / Produktion / Geldautomaten / Kaffeemaschinen usw.)
  - OPC (UA) (Erneuerbare Energien / Heizungssteuerungen usw.)
  - BACnet (Gebäudeautomatisierung / Straßenbeleuchtung)
  - Google, Facebook, Skype, Amazon,....
  - usw...

  » IPv4 <-> IPv6

  » VPN Interconnects / Remote Connects

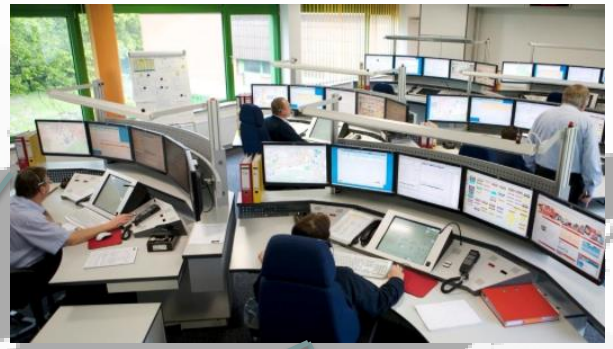
  » Cloud Services (IaaS / PaaS / SaaS / IaaS)

Agenda

- Industrie 4.0 – Ein Erklärungsversuch
  - » Der Wandel von 3.0 zu 4.0
- Die Herausforderungen für die Industrie
- **Die Änderung der Verwundbarkeit**
- Maßnahmen
- Warum Fortinet ?

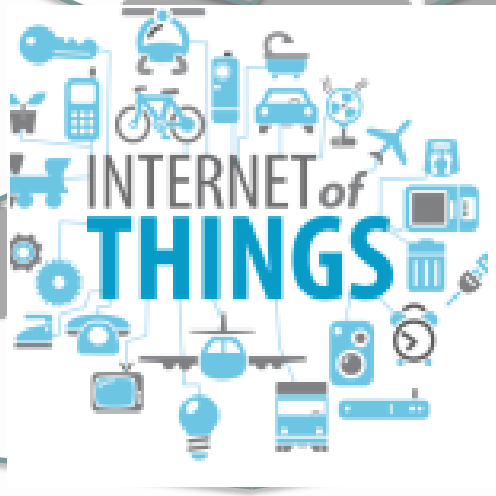
Änderung der Verwundbarkeit

Office IT



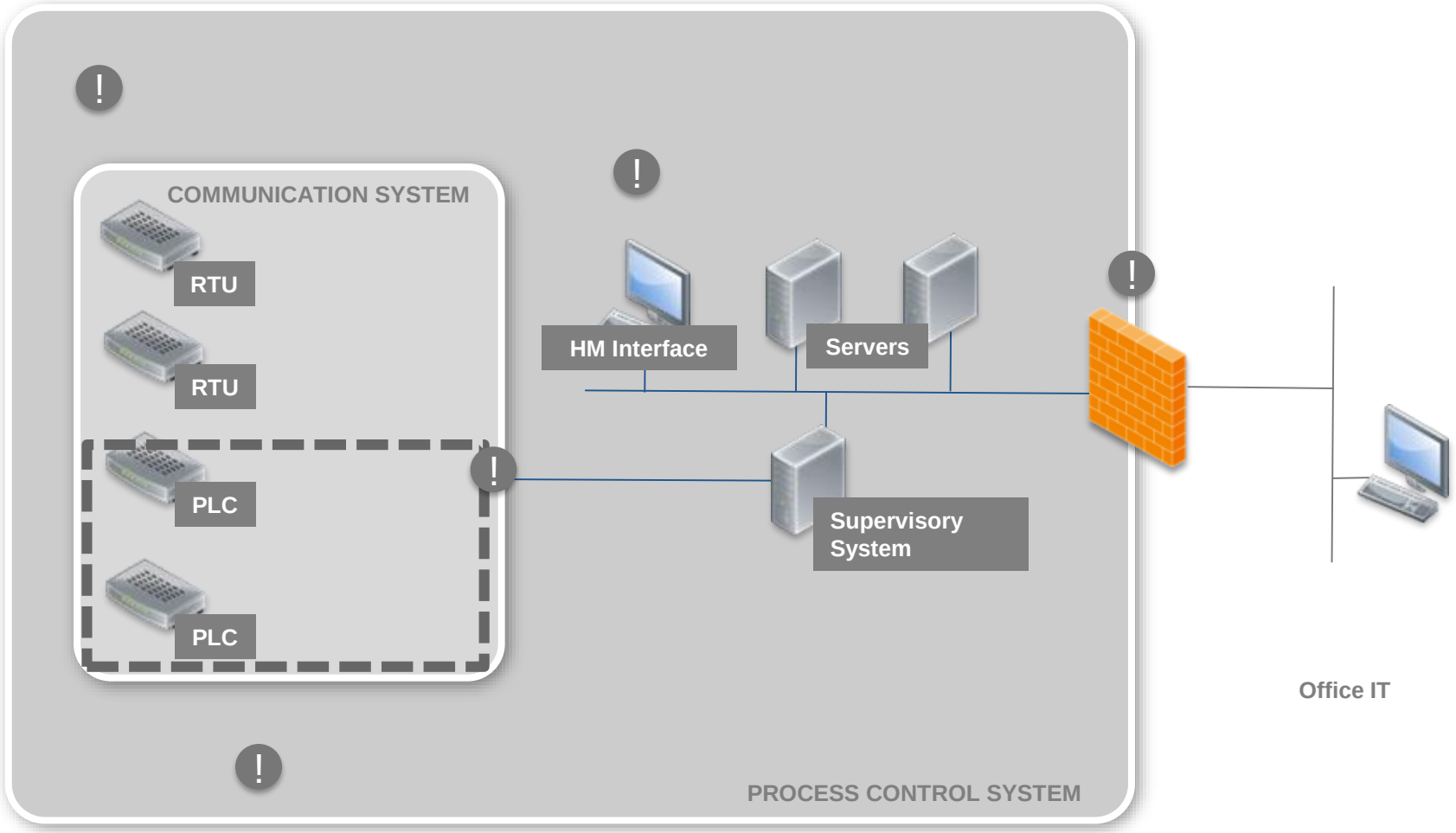
SCADA

Internet



Feldebene

Jeder mit jedem – ohne Kontrolle…!



Sicherheitsbedrohungen sind KEINE Fiktion mehr!!!

Infizierte Geldautomaten spuckten Millionen Euro aus

7 Oct 2014 Alex Savitsky Featured Post, Nachrichten

Was brauchen Sie, um Geld aus einem Geldautomaten zu holen? Zum eine
oder Kreditkarte, die als Schlüssel zu Ihrem Bankkonto fungiert. Dann müsse
ür die Karte wissen und zudem muss etwas Geld auf Ihrem Konto haben. Für
as aber manchmal anders: Sie brauchen keine Karten, PIN-Codes und Bankkc
kommen. Sie brauchen nur einen Geldautomaten, in dem ein bisschen Barge
nz spezielle Software.

TOTAL --> 0 NCR

TOTAL --> 0 NCR

Kritische Sicherheitslücke ermöglicht Fremdzugriff auf Systemregler des Vaillant ecoPOWER 1.0

Publiziert am 15.04.2013

Seit dem vergangenen Freitag erhalten Betreiber einer stromerzeugenden Heizung vom Typ ecoPOWER 1.0 ungewöhnliche Post vom Hersteller des Gerätes. Vaillant informiert seine Kunden mit diesem Schreiben, dass „ein unberechtigter Fremdzugriff via Internet auf den Systemregler des ecoPOWER 1.0 möglich ist" und dass Betreiber einer betroffenen Heizung umgehend „den ecoPOWER 1.0 vo Internet […] trennen [sollen], indem sie den Netzwerkstecker aus dem Systemregler entfernen". Vaillant seinen Kunden in diesem Schreiben nicht mitteilt, ist die Tatsache, dass potentiellen Ang ein umfassender Zugriff auf das Gerät einschließlich der Kundendienst- und Entwicklerebene m dem alle an das Internet angeschlossenen Geräte aufgrund eines unbedarft program auffindbar sind.

info security

STRATEGY /// INSIGHT /// TECHNIQUE

News

Siemens patches security flaws in SCADA systems

25 July 2012

Siemens has patched a number of security holes in its SIMATIC supervisory control and data acquisition (SCADA) systems, according to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

SECURITY WEEK

INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe (Free)

FREE WHITE PAPER

Bit9

Are Your Domain Controllers At Risk?

Malware & Threats Cybercrime Mobile & Wireless Risk & Compliance Security Infrastructure

Cyberwarfare Fraud & Identity Theft Phishing Malware Tracking & Law Enforcement

Saudi Arabia's National Oil Company Kills Network After Cyber Attack

By Mike Lennon on August 16, 2012

Saudi Aramco, Saudi Arabia's national oil company and the largest in the w has confirmed that is has been hit by a cyber attack that resulted in malwar infecting user workstations, but did not affect other parts of its network.

"On Wednesday, Aug. 15, 2012, an official at Saudi Aramco confirmed that company has isolated all its electronic systems from outside access as a precautionary measure that was taken following a sudden disruption that affected some of the sectors of its electronic network," the company wr statement.

"The disruption was suspected to be the result of a virus that had infe personal workstations without affecting the primary components of th

ZEIT ONLINE | DATENSCHUTZ

START POLITIK WIRTSCHAFT GESELLSCHAFT KULTUR WISSEN DIGITAL STUDIUM KARRIERE

Start › DIE ZEIT Archiv › Jahrgang: 2014 › Ausgabe: 16 › Wie ein Hacker ein Stadtwerk angreift

IT-SICHERHEIT

Blackout

Ein Hacker brauchte nur zwei Tage, um die Kontrolle über die Stadtwerke in Ettlingen zu übernehmen. Er zeigt Stromnetze in Deutschland sind nicht sicher. VON GREFE

DIE ZEIT N° 16/2014

17. April 2014 08:37 Uhr | 31 Komme

Es ist Zeit für einen Anruf. "Noch ein paar Klicks, dann ist es dunkel", sagt Lindner. Wenn er jetzt seine Finger bewegt, geht in der süddeutschen Stadt Ettlingen das Licht aus. 40.000 Einwohner haben dann keinen Strom mehr. 200.000 Wasserpumpen könnten jetzt still stehen, weil der Hacker Felix Lindn sein Ziel erreicht hat.

ContingencyToday

Stuxnet cousin can attack SCADA systems

10 August 2012

Analysis on a new cyber espionage weapon, dubbed Gauss, has been released, stating that the tool has capabilities to attack national critical infrastructure and steal financial data

Wie gefährdet sind wir?

ZEIT ONLINE | DATENSCHUTZ

START POLITIK WIRTSCHAFT GESELLSCHAFT KULTUR WISSEN DIGITAL STUDIUM KARRIERE

Start › DIE ZEIT Archiv › Jahrgang: 2014 › Ausgabe: 16 › Wie ein Hacker ein Stadtwerk angreift

IT-SICHERHEIT

Blackout

Ein Hacker brauchte nur zwei Tage, um die Kontrolle über die Stadtwerke in Ettlingen zu übernehmen. Er zeigte: Die Stromnetze in Deutschland sind nicht sicher. VON CHRISTIANE GREFE

DIE ZEIT N° 16/2014 17. April 2014 08:37 Uhr | 31 Kommentare |

Es ist Zeit für einen Anruf. "Noch ein paar Klicks, dann ist es dunkel", sagt Felix Lindner. Wenn er jetzt seine Finger bewegt, geht in der süddeutschen Stadt Ettlingen das Licht aus. 40.000 Einwohner haben dann keinen Strom mehr. 200.000 Wasserpumpen könnten jetzt still stehen, weil der Hacker Felix Lindner sein Ziel erreicht hat.

Hacker „FX“ bei den SW Ettlingen....

Häufige Quellen von Sicherheitsverletzungen

Externe Quellen

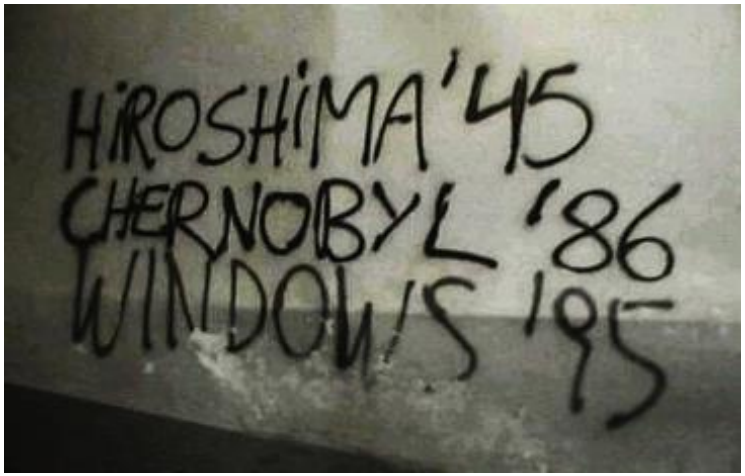
- ✓ Interconnections mit anderen SCADA Systemen
- ✓ RTU's/MGMT Stationen in öffentlichen Netzwerken

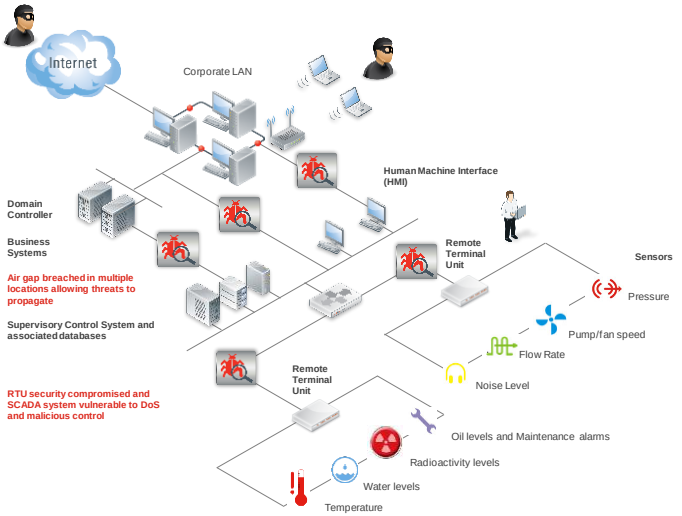
Interne Quellen

- ✓ Viren/Malware/Trojaner auf Laptops, USB-Sticks, Mobile Geräte
- ✓ Industriespionage
- ✓ Third party – Applikationen
- ✓ HMI terminals, offene Ports

Drahtlose Quellen

- ✓ WiFi oder 3G/4G connectivity zu RTU's
- ✓ Rogue AP
- ✓ Encryption exploits
- ✓ Keine Host-basierende Sicherheit auf RTU's





Bedrohungen auf allen Ebenen:

MALICIOUS APPS

MALICIOUS SITES

SPAM BOTNETS

TROJANS

VIRUSES & SPYWARE

INTRUSIONS & WORMS

Layer 5-7: CONTENT & APPLICATION

Layer 3-4: CONNECTION

HARDWARE THEFT

Layer 1-2: PHYSICAL

APPLICATION CONTROL

ANTIVIRUS

IPS

VPN

FIREWALL

LOCK & KEY

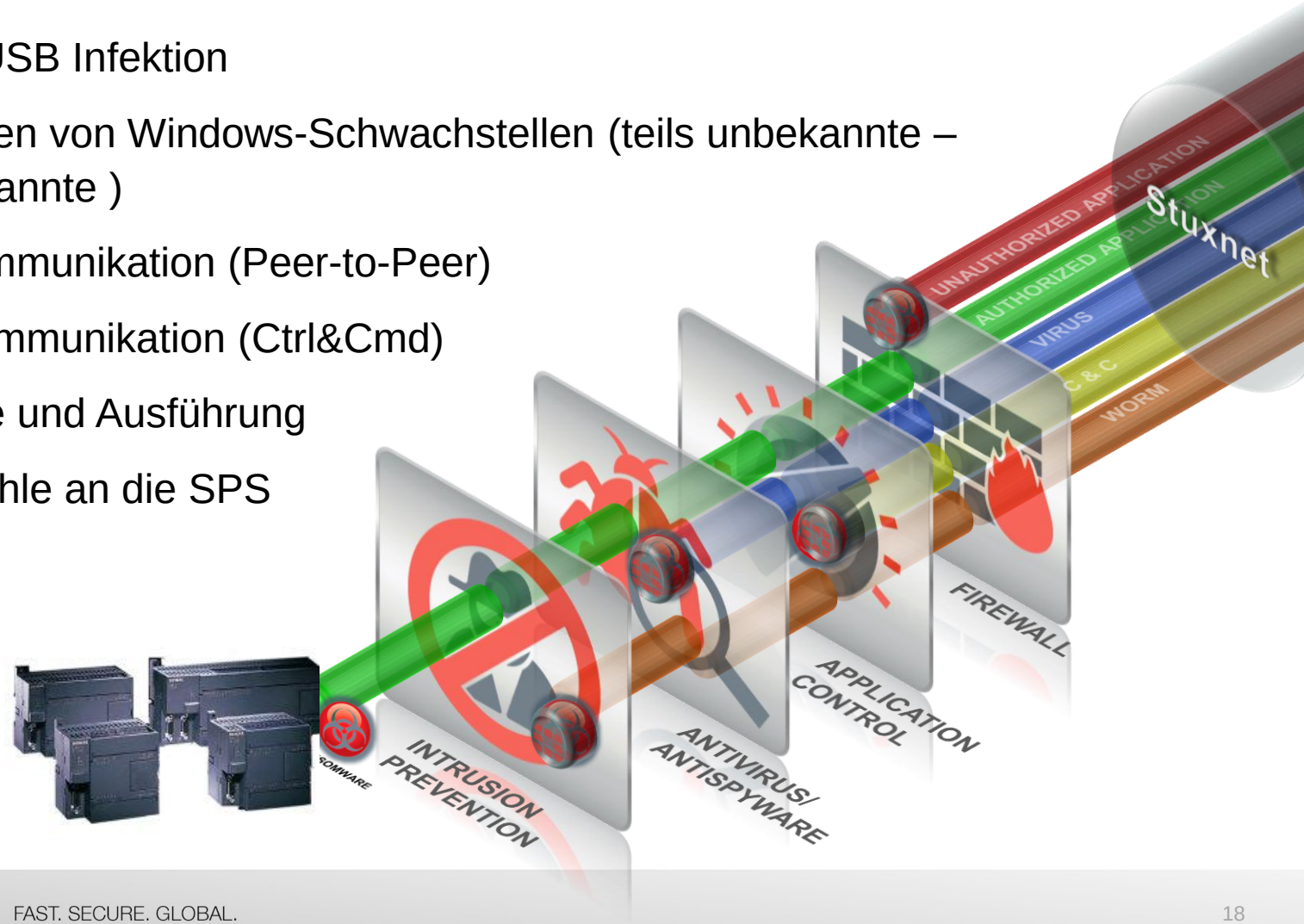
IDENTIFICATION & AUTHENTICATION

Der bekannteste APT: Stuxnet

Einer der raffiniertesten APTs:

1. Lokale USB Infektion
2. Ausnutzen von Windows-Schwachstellen (teils unbekannte – teils bekannte)
3. P2P Kommunikation (Peer-to-Peer)
4. C&C Kommunikation (Ctrl&Cmd)
5. Kontrolle und Ausführung

   der Befehle an die SPS

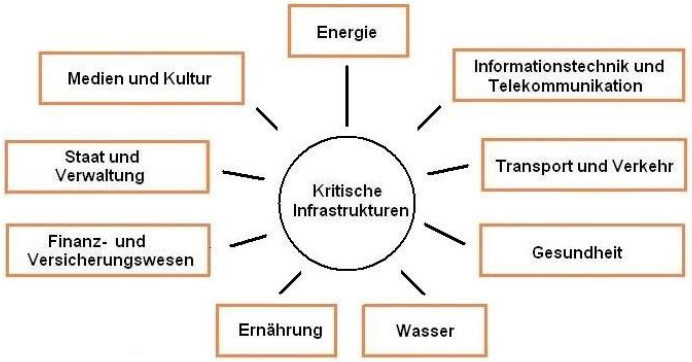


Agenda

- Industrie 4.0 – Ein Erklärungsversuch
  - » Der Wandel von 3.0 zu 4.0
- Die Herausforderungen für die Industrie
- Die Änderung der Verwundbarkeit
- **Maßnahmen**
- Warum Fortinet ?

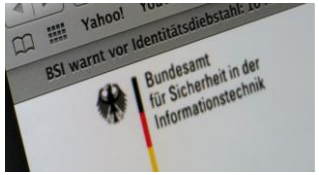
Was bedeutet das alles für Sie?

- **Aktuelles Beispiel: Der „KRITIS-Kreis“:**
  - » Energieversorger, Stadtwerke, Gas-, Wasserversorger
  - » Industrieunternehmen
  - » ISPs, Carrier, Hochschulen usw.....
- **Die Anforderung:**
  - » Re-Design / Ablösung der FW -> NGFW
  - » Absicherung der Netzleitstellen / Office IT
  - » Absicherung-/ Neugestaltung des Prozessdaten- bzw. Fernwirknetzes UND Office IT
  - » Zonenkonzept
  - » **Visability / Logging / Reporting**

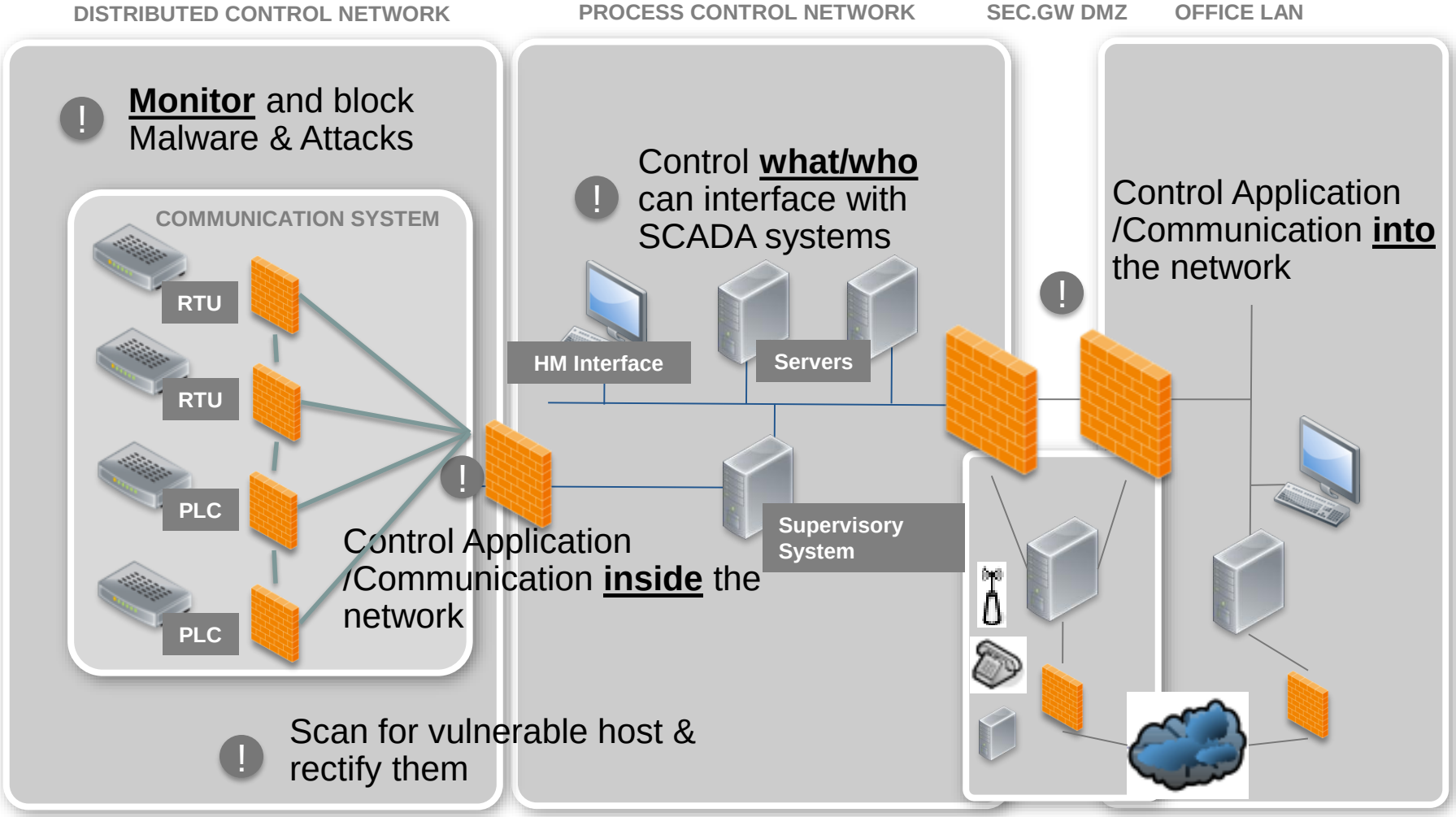


IT Sicherheitsgesetz – Kritische Infrastrukturen

bdew
Energie. Wasser. Leben.

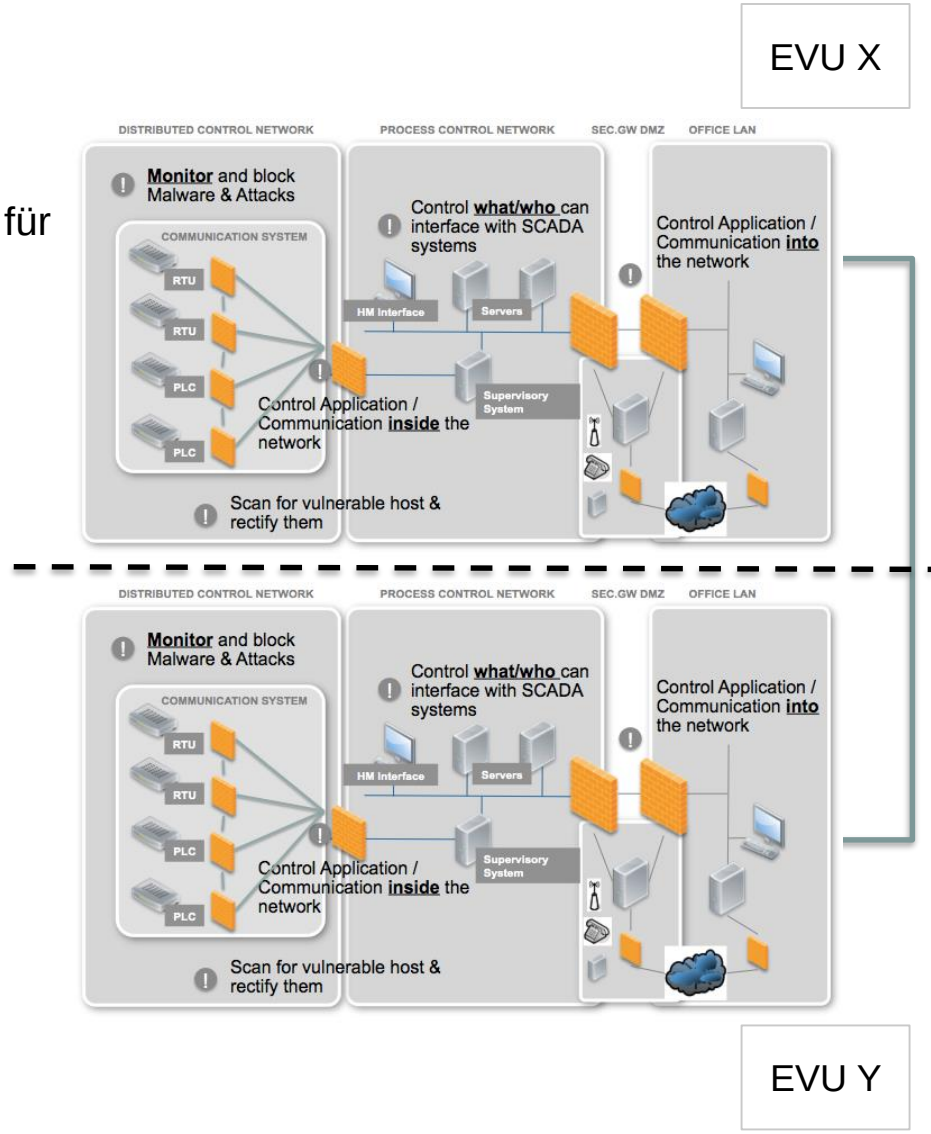


Jeder mit Jedem – maximale Kontrolle !!!



Im Detail

- **Absicherung der Leitstellen**
  - NGFW + ATP, HA-Cluster
    - L3, NGFW insb. Applikationskontrolle für TASE-2 (ICCP)
    - IEC-60870-5-104
    - IEC-61850, Modbus, OPC, usw.
- **Absicherung des Prozessdaten- bzw. Fernwirknetzes**
  - NGFW + ATP (ruggedized)
    - L2 / L3, NGFW insb. Applikationskontrolle für
    - TASE-2 (ICCP)
    - IEC-60870-5-104
    - IEC-61850, Modbus, OPC, usw.
- **Management / Visability / Reporting**

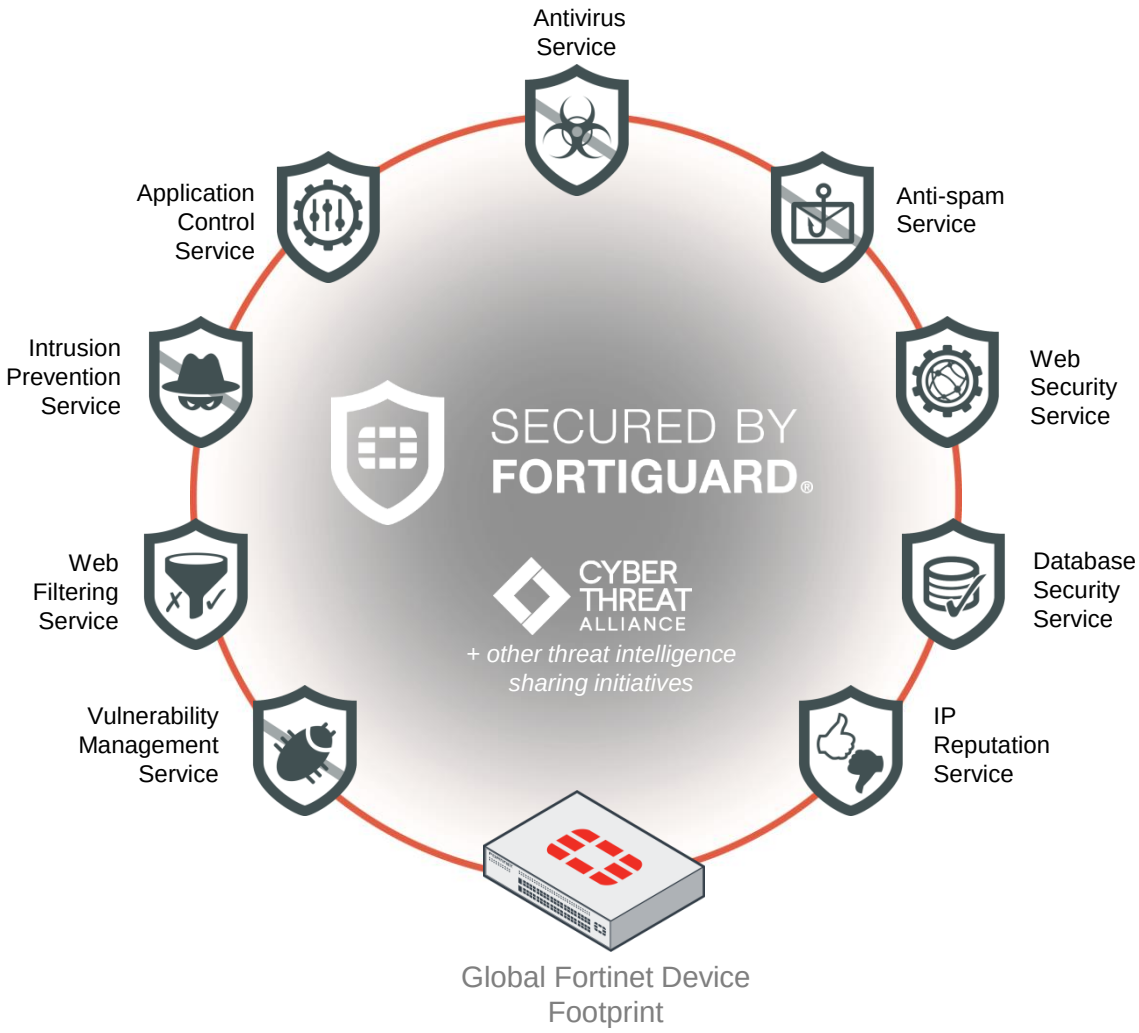


Agenda

- Industrie 4.0 – Ein Erklärungsversuch
  - » Der Wandel von 3.0 zu 4.0
- Die Herausforderungen für die Industrie
- Die Änderung der Verwundbarkeit in 3.0/3.5/4.0
- Maßnahmen
- **Warum Fortinet ?**

Der Fortinet Vorteil: **Kompromisslos SICHER**

- **Globales Threat Research Team**
- **Erkennt** neue Bedrohungen und **stellt zeitnah inhouse-entwickelte** Signatur-Updates und neue Technologien **bereit**
- Updates werden **sofort** geliefert, 24x365
- **Unbhängig getestet** als **hocheffektiv** gegen aktuelle Angriffe



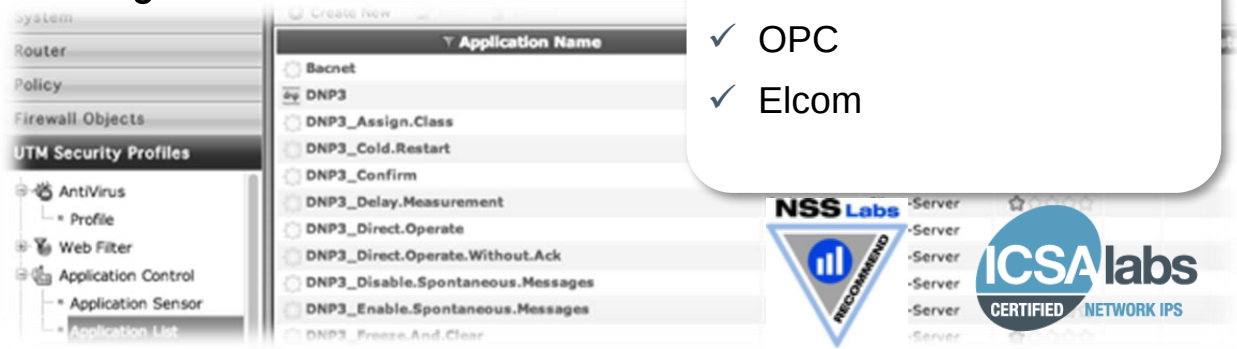
IPS/ Applikationskontrolle für Industrielle Systeme

Superior Coverage & Protection

- Minderung von Netzwerkanomalien und DoS
- Signatur Erkennung
  - Unterstützung von OS, sowie Applikations-Verwundbarkeiten
  - Kommunikations- & Kommandokontrolle
- Wurm & Botnet Protection
- Unterstützung von “Custom signatures”
- User Quarantine
- Packet Logging
- Sniffer Mode

Supported Protocols

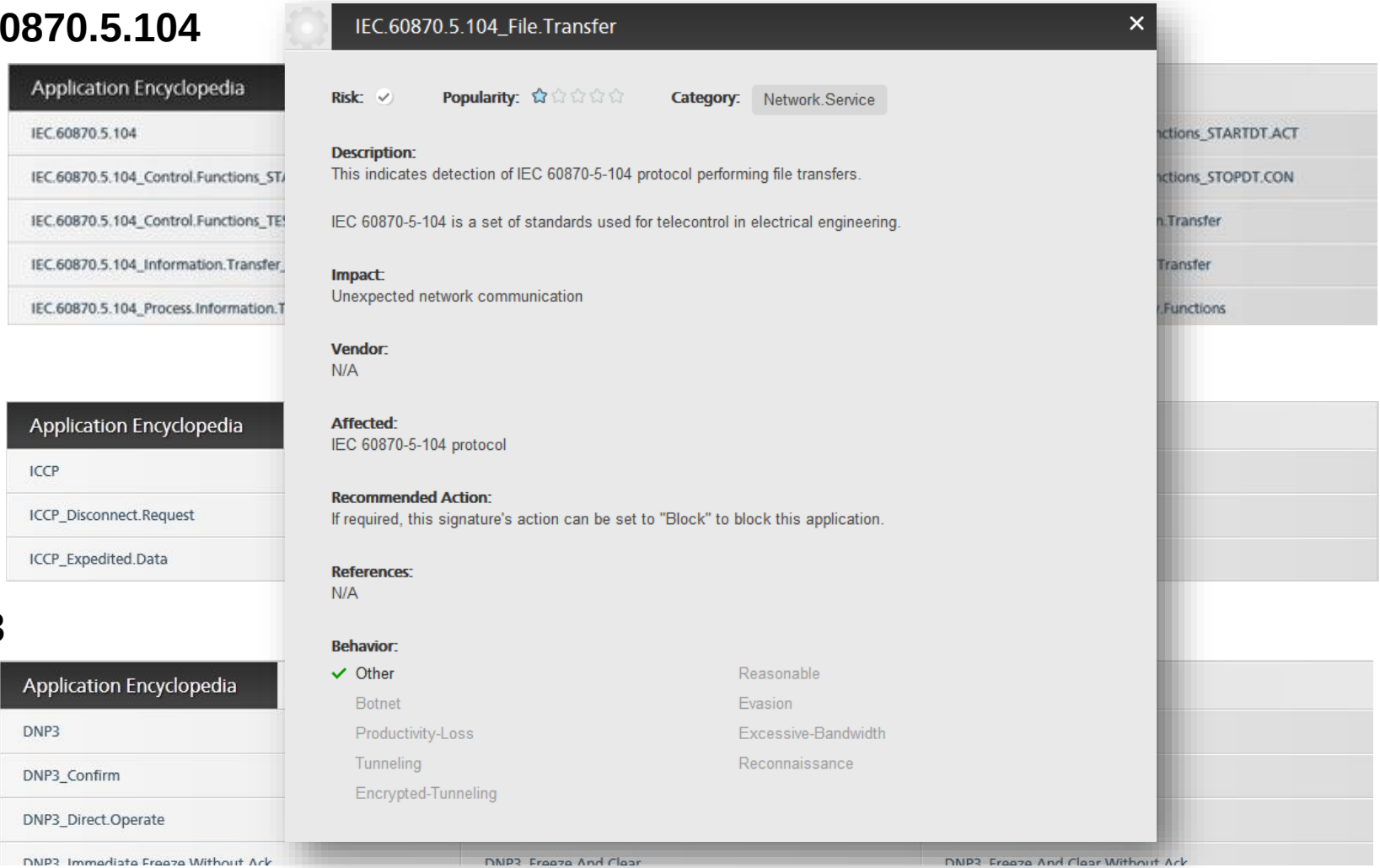
- ✓ BACnet
- ✓ DNP3
- ✓ Modbus
- ✓ EtherNet/IP
- ✓ IEC 60870-6 (TASE 2) / ICCP
- ✓ EtherCAT
- ✓ IEC 60870-5-104
- ✓ IEC 61850
- ✓ OPC
- ✓ Elcom



SCADA Command Control

Application Control

IEC.60870.5.104



ICCP

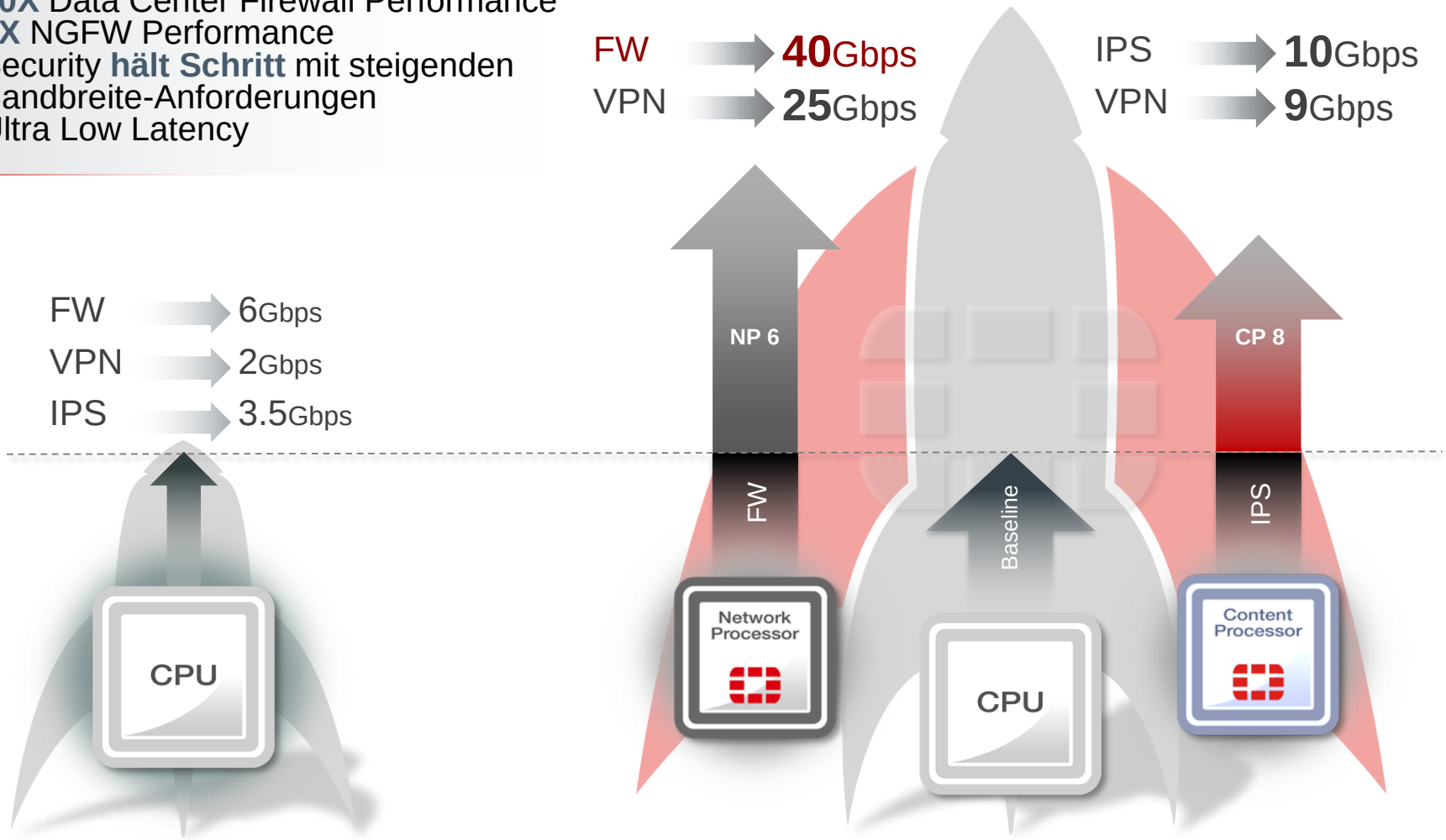
DNP3

Schutz gegen “Advanced Threats”

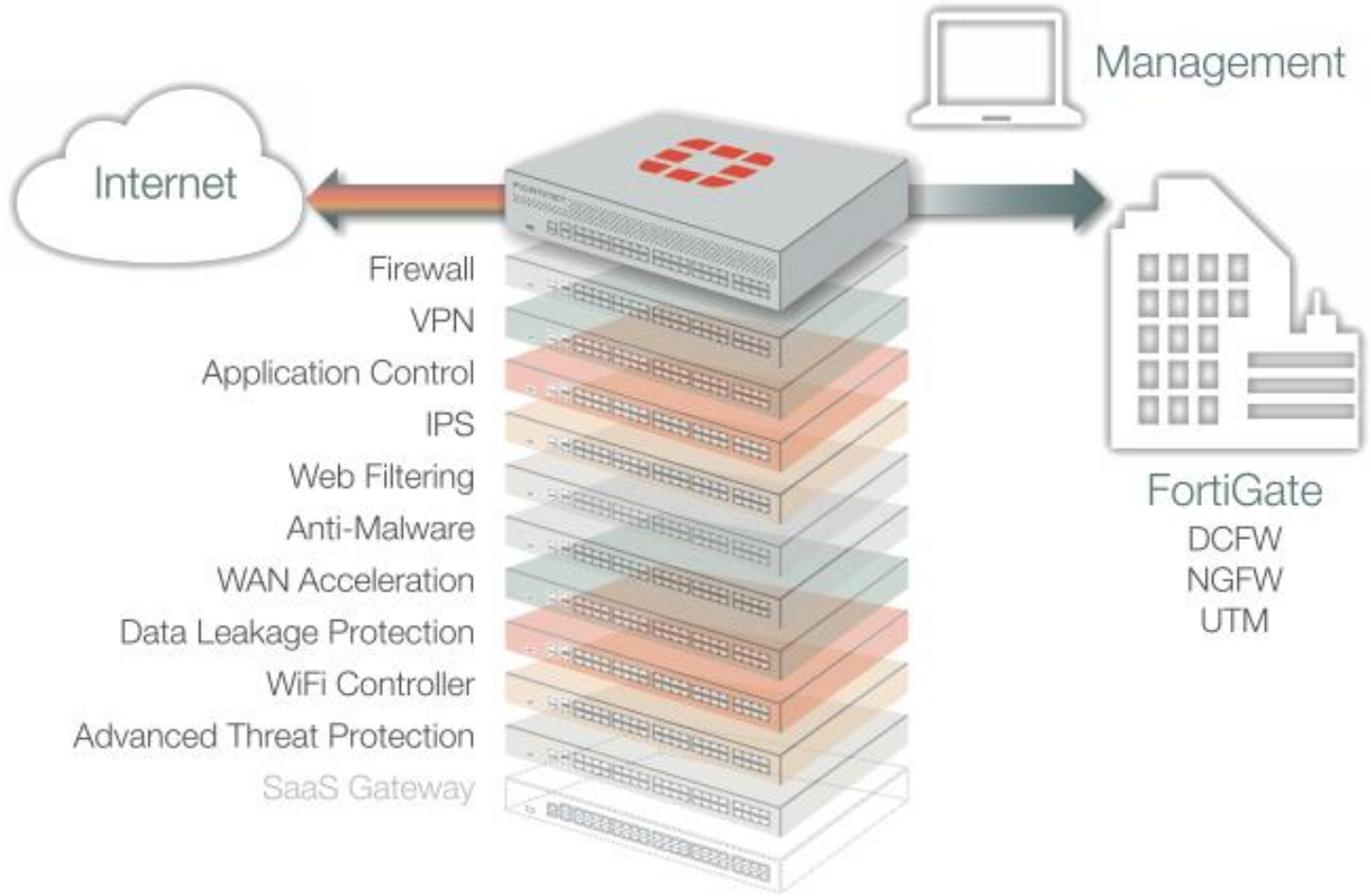
- Hoch effizientes IPS (96%+ effectiveness, “Recommended” by NSS)
  - Mehr als 7000 bekannte malicious Pattern, plus intelligenter Heuristik
  - Vervollständigt durch eine dynamische Botnet-Datenbank und High-Risk Application Kategorien
- Top-bewertete Antimalware (96% RAP according to VB100)
  - Mächtige Kombination aus kompakter Pattern-Erkennung und “Verhaltens-Engine”
  - Entweder im effizienten Stream- oder im aggressiveren Proxy-Modus
- Integrierte Advanced Threat Protection
  - **Code Emulation Engine** für OS-unabhängige Simulation und Einstufung
  - Vollwertige **OS Sandbox** für volle “threat lifecycle” Analyse und Reporting

Der Fortinet Vorteil: **Performance**

- **10X** Data Center Firewall Performance
- **5X** NGFW Performance
- Security **hält Schritt** mit steigenden Bandbreite-Anforderungen
- Ultra Low Latency



Der Fortinet Vorteil: **Konsolidiert Einfach**



Für alles die passende Hardware…

IEC-61850 describes a unified communications system design for use in electrical sub-stations. **IEC-61850-3** provides guidance on the hardware requirements of equipment deployed in this demanding environment.

EMI

Unprotected devices can fail or be destroyed when exposed to high levels of electromagnetic interference

- ✓ A strong electromagnetic compatibility **(EMC) design is required**

Thermal

A wide (-20 to +75C) operating temp can be expected in a hash environment.

- ✓ Requires efficient heat dissipation system and self warming

Vibration

- ✓ Devices must survive being dropped from a cabinet rack mount
- ✓ 50G anti-shock & 5-500 Mhz anti-vibration requirement is present
- ✓ Protective components are used to cushion the device

FortiGate-Rugged-100C

IEC 61850-3 Rugged Form Factor with Complete FortiOS Feature set

FGR-100C **2U**

- **2x GbE Copper Interfaces, 4x FE Copper Interfaces, 4x 100Base-FX Interface (SC)**

Key Highlights:

- ✓ Ruggedized hardware that meets industrial standards
- ✓ Runs on FortiOS – rich networking & UTM feature sets.
- ✓ Integrates with FortiManager and FortiAnalyzer for Centralized management, monitoring and reporting

FortiDINRack

- Einschubgehäuse für FG-60D (OfficeFW)
  - » Dadurch:
    - Hutschienenmontage
    - 24/48 VDC Spannungsversorgung
    - Überspannungsschutz
    - Nach vorne geführte Ports
  - » Aber:
    - Kein erw. Temp. Bereich
    - Keine EMV Störfestigkeit
    - Keine Vibrationsfestigkeit

Computer Rendering

FortiGate-Rugged-60D

Compact & Cost Efficient Rugged Form Factor with Complete FortiOS Feature set

FGR-60D

- **4x GbE Copper, 2x shared media pairs, Serial Interface**
- **DIN rail mountable**

Key Highlights:

- ✓ Ruggedized hardware that meets industrial standards
- ✓ Runs on FortiOS – rich networking & UTM feature sets.
- ✓ Integrates with FortiManager and FortiAnalyzer for Centralized management, monitoring and reporting

FortiGate Rugged 90D

Compact & Cost Efficient Rugged Form Factor with Complete FortiOS Feature set

FortiGate Rugged-90D

- **Interfaces**: 5 x GE RJ45 (1 pair bypass), 2 x SFP Slots
- **Power supplies:** DC + Opt. AC adapter

Highlights:

- ✓ Comprehensive network security protection including IPS, application control and AV
- ✓ Serial Interface for Legacy DNP3 inspection
- ✓ Ruggedized with wide operating temperature of -40 to 75 Deg. Celsius

* SFP transceivers not included

Hardware Übersicht – Rugged Series

	FGR-XADSL	FGR-30D	FGR-35D	FGR-60D	FGR-90D	FGR-100C
Schedule	2016???	Q4/2015	Q4/2015	Now	Now	Now
Ethernet Interfaces	FGR m. integr. ADSL2+ Modem	4x GE RJ45 2x GE SFP	2x GE RJ45 1x GE SFP IP-67	4x GE RJ45 2x shared media pairs	3x GE RJ45 2x GE SFP 1x pair GE Bypass	2x GE RJ45 4x FE 4x 100FX
Power supplies	DC + Opt. AC adapter	DC + Opt. AC adapter	DC + Opt. AC adapter	DC + Opt. AC adapter	DC + Opt. AC adapter	AC Only
Operating Temperature	-40 - 75 deg C	-40 - 75 deg C	-40 - 75 deg C	-20 - 70 deg C	-40 - 75 deg C	-20 to 70 deg C
Certification	IEC 61850-3 (EMC), IEEE 1613 Class 2 Compliant	IEC 61850-3 (EMC), IEEE 1613 Class 2 Compliant	IEC 61850-3 (EMC), IEEE 1613 Class 2 Compliant	IEC 61850-3 (EMC), IEEE 1613 Class 2 Compliant	IEC 61850-3 (EMC), IEEE 1613 Class 2	IEC 61850-3 (EMC), IEEE 1613 Class 2
Firewall Throughput	TBD	TBD	TBD	1.5 Gbps	1 Gbps	2 Gbps
IPS throughput	TBD	TBD	TBD	200 Mbps	400 Mbps	950 Mbps
IPSEC throughput	TBD	TBD	TBD	1 Gbps	60 Mbps	60 Mbps
Others	TBD	TBD	Polemount-Option	DIN Rail Option	DIN Rail Option	-

FortiSwitch Rugged -112D

Ruggedized PoE Switch for Harsh Environments

FortiSwitch Rugged-112D-POE

- **Interfaces**: 8 x GE RJ45 PoE/+, 4 x SFP Slots
- **Power supplies:** External DC Power Input

Highlights:

✓ High PoE/PoE+ Port Density in compact form

✓ Ruggedized with wide operating temperature of -40 to 75 Deg. Celsius

* SFP transceivers not included

FortiExtender-20B

Qualified Modem Supplied by Customer

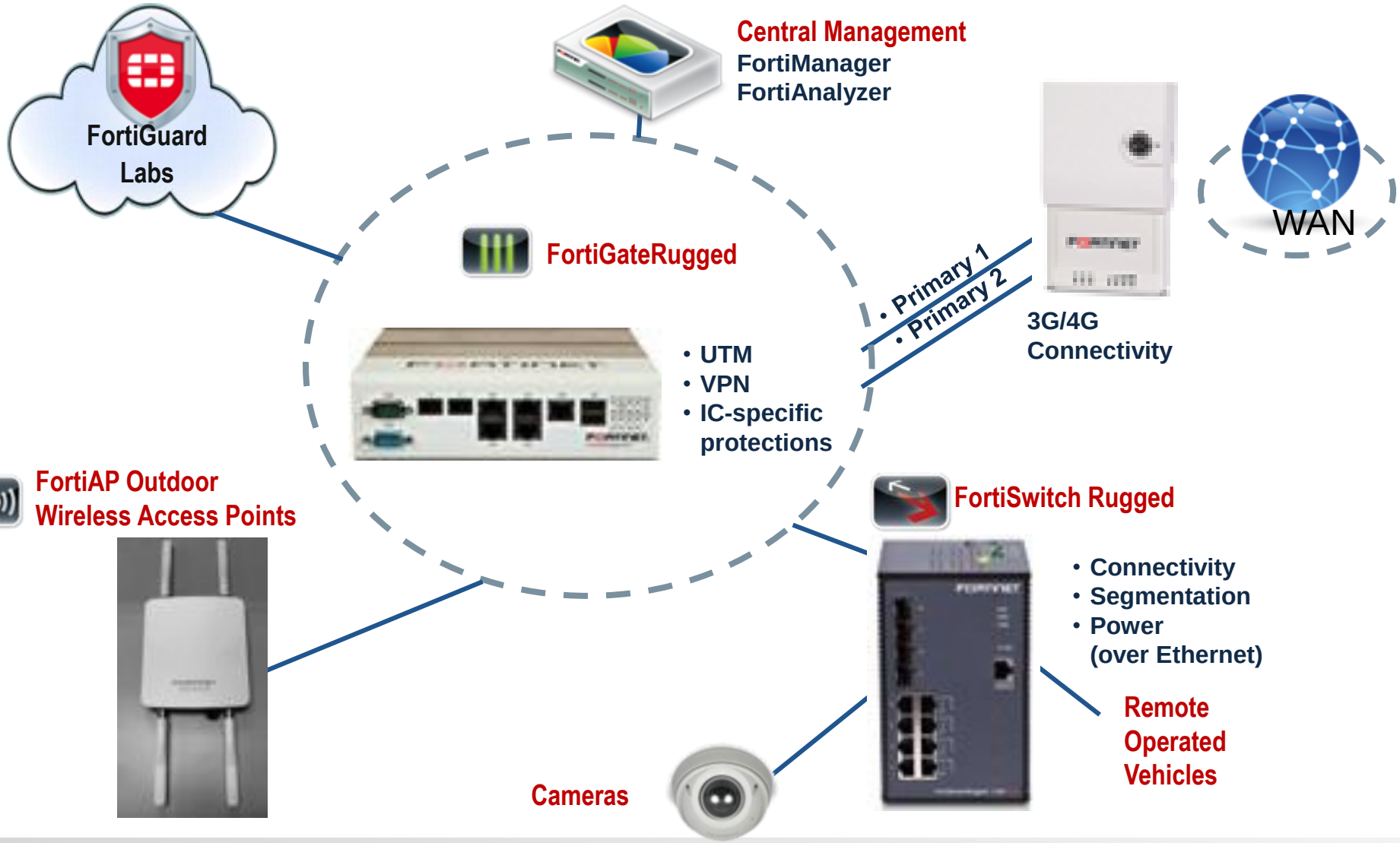
- Wall Mount, indoor
- PoE powered
- USB modem to be supplied by user
- USB security cover with lock
- Kensington security slot
- Operating Temp: 0-40 ºC

FortiExtender-100B

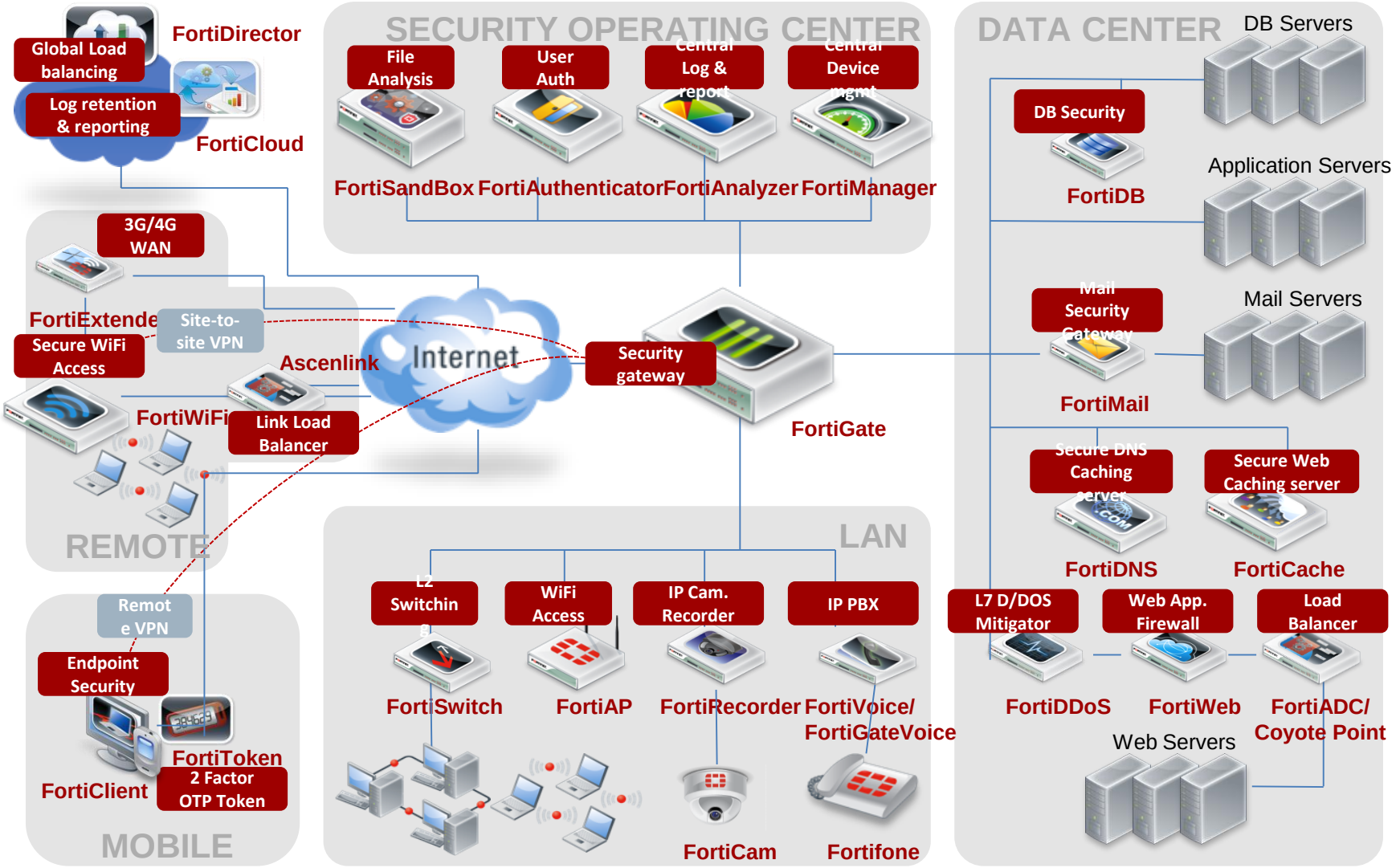
Qualified Modem & Antennas Supplied by Customer

- IP55 rated enclosure
- Ruggedized for use in outdoor and harsh environments
- PoE powered (injector included)
- USB modem and antenna to be supplied by user

Der Fortinet Vorteil: **Besonders gehärtet**



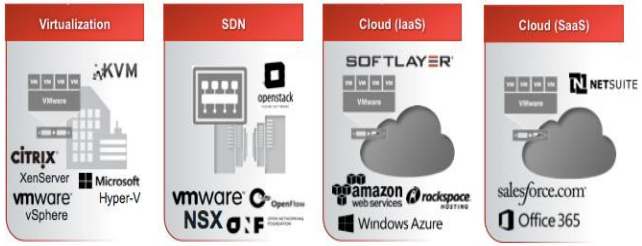
Kompromisslos. Komplett. Unabhängig. Besonders.



Die SCADA / IoT - “Ende-zu-Ende” - Lösung

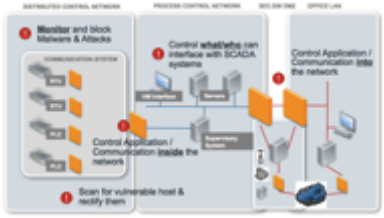
SCADA/IoT - Feldebene

- **>80.000 Ortsnetzstationen, >300.000 EEG Anlagen, Kaffeeautomaten, Geldautomaten, Ampelsteuerungen, Verkehrsleitsysteme, usw...**
- Ruggedized NGFW, L2/L3
  - » IPsec / SSL VPN
  - » 2-Faktor-Authentifizierung
  - » AV, ATP



SCADA - Leitstelle

- **Perimeter / Internal NGFW**



- **Zentrale VPN-Cluster**
  - » n x GW-t-GW IPsec-Tunnel
  - » X.509 Zertifikatsverwaltung
- **Remote-Connects**
  - » 2-Faktor Authentifizierung
  - » Token / Authenticator
  - » SSL-Portal

Office IT

- **Perimeter / Internal NGFW**
- **ATP**
  - » AV, Sandboxing
- **App.Control**
  - » Facebook, Skype -> SCADA
- **E-Mail Security**
- **Web Applications**
  - » WAF
- **DB Security**
  - » Vulnerability Scanning
- **DDoS**
  - » Layer 7 DDos
- **secureWLAN**

Fazit

- Auf 4.0 warten bedeutet: Geduld haben – aber auch im entscheidenden Moment vorbereitet zu sein!
- 3.0 / 3.5 ist JETZT und birgt eine Menge Potenzial (-> 4.0 “ready”)
- Ziel ist es, Risiken auf ALLEN Ebenen zu minimieren.
- -> **Full Mesh Security**
- Ein guter Beginn wäre: Einführung von Richtlinien / Standards (BDEW, BSI, NERC, ISA99, CPNI, TSA, etc.)
- Fortinet ist **DER** Marktführer in der **GESAMTHEITLICHEN** Absicherung von **Industrienetzen** in Kombination mit der **Office IT**:
  - » Pionier im Feld der Security Consolidation
  - » High-performance / low-latency / “gehärtete” Hardware
  - » Permanente Security Updates -> FortiGuard

Vielen Dank!

Dirk Wollberg
Major Account Manager Energy & Utilities FORTINET GmbH |
Feldbergstrasse 35 | 60323 Frankfurt am Main |
Mobil +49 151 2 91 94 90 6 | Fax +49 69 310 19 222 |
Email dwollberg@fortinet.com

FORTINET Geschäftsstellen
Deutschland
60323 Frankfurt, Feldbergstrasse 35
80539 München, Maximilianstrasse 13
20354 Hamburg, Neuer Wall 50