Fraunhofer Institut für Sichere Informationstechnologie

Industrieelle Revolution 4.0

Dr. Thorsten Henkel

CASED

Fraunhofer SIT

Industrieelle Revolution 4.0

Agenda

- Fraunhofer & SIT
- Die vierte Industrielle Revolution – Industrie 4.0
- Wirtschaftlicher Paradigmenwechsel – Serie 0 Produkt
- IT-Security – Enabling Factor für I4.0
- Status Quo & Forschungsfragen
- Lösungsansätze

Industrieelle Revolution 4.0

Fraunhofer Institut
für Sichere Informationstechnologie

Methoden

- Secure Engineering
- Security Testlab
- IT Security Management
- IT Forensics

Systems & Services

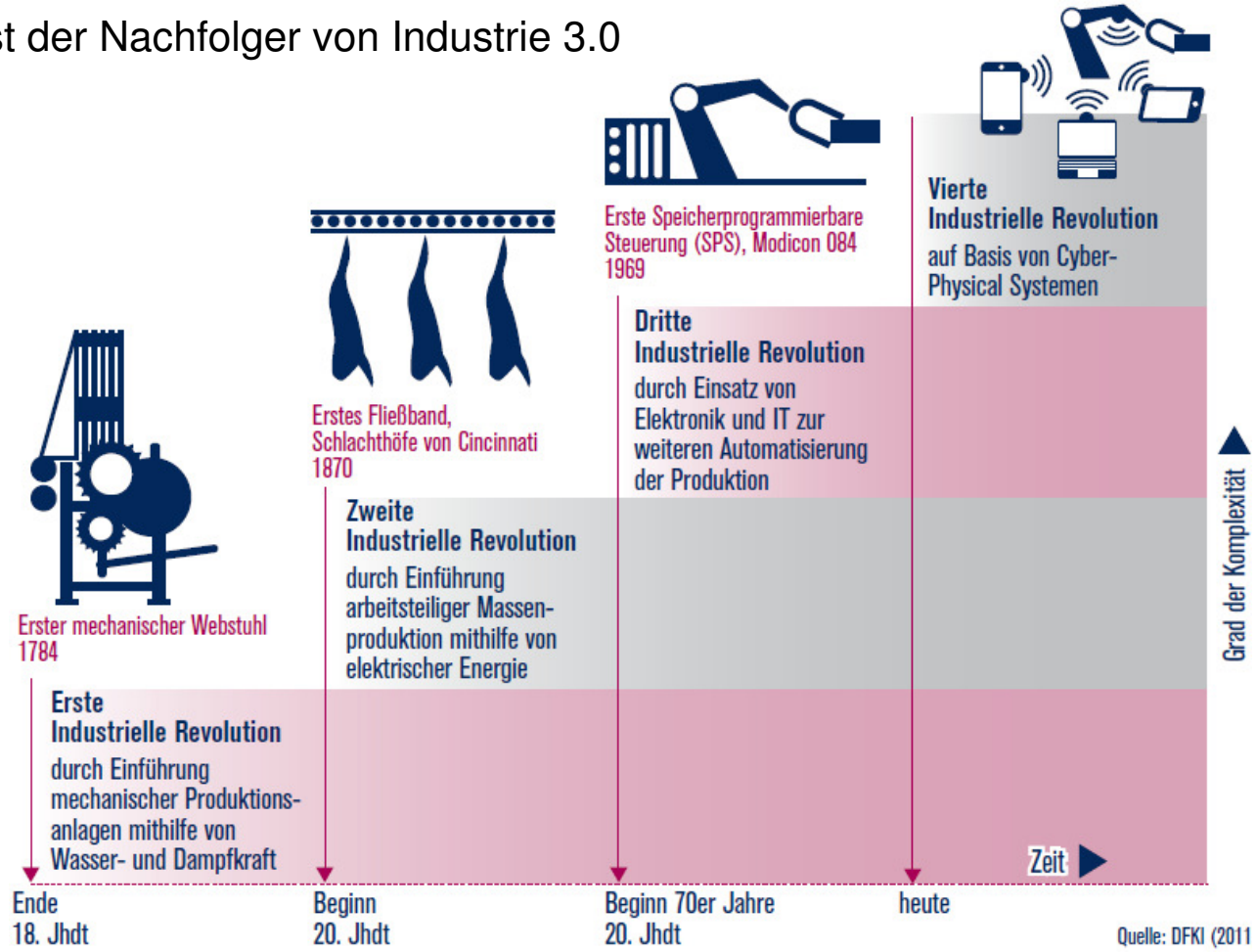
- Mobile Systems
- Cyber Physical Systems
- Cloud Systems & Services

Mechanisms

- Identity & Privacy
- Multimedia Security

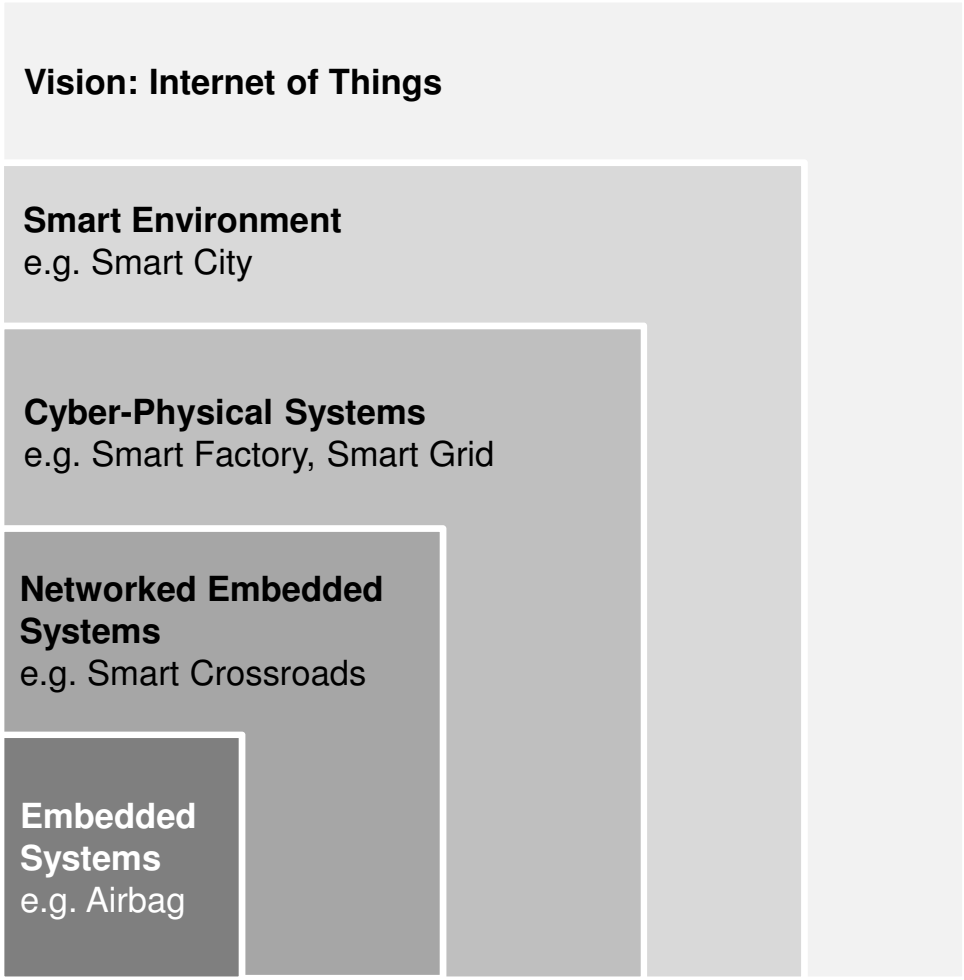
Industrieelle Revolution 4.0

Industrie 4.0 ist der Nachfolger von Industrie 3.0



Industrieelle Revolution 4.0

Industrie 4.0 ist der Nachfolger von Industrie 3.0



CASED

Quelle: Kagermann, H.; Wahlster, W.; Held, J.; (Hrsg.) : Bericht der Promotorengruppe Kommunikation. Im Fokus: Das Zukunftsprojekt Industrie 4.0. Forschungsunion, 2012

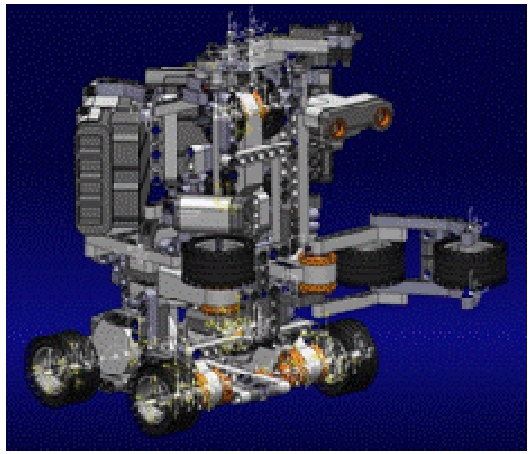
Fraunhofer SIT

Industrieelle Revolution 4.0

Cyber Physical Systems adressieren zwei Sichten

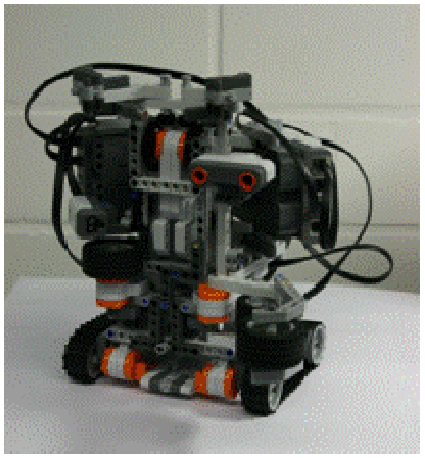
Cyberizing the physical

Planung & Spezifizierung der physikalischen Systeme



Physicalizing the cyber

Zur Beschreibung von Software & Netzwerk-Komponenten



Industrieelle Revolution 4.0

Serie 0 Produkt

Wettbewerbsfähige Kosten

On Customer Demand

Optimierter Co2 Footprint

Agiler Markt-Respond

Ergonomische Bedienung

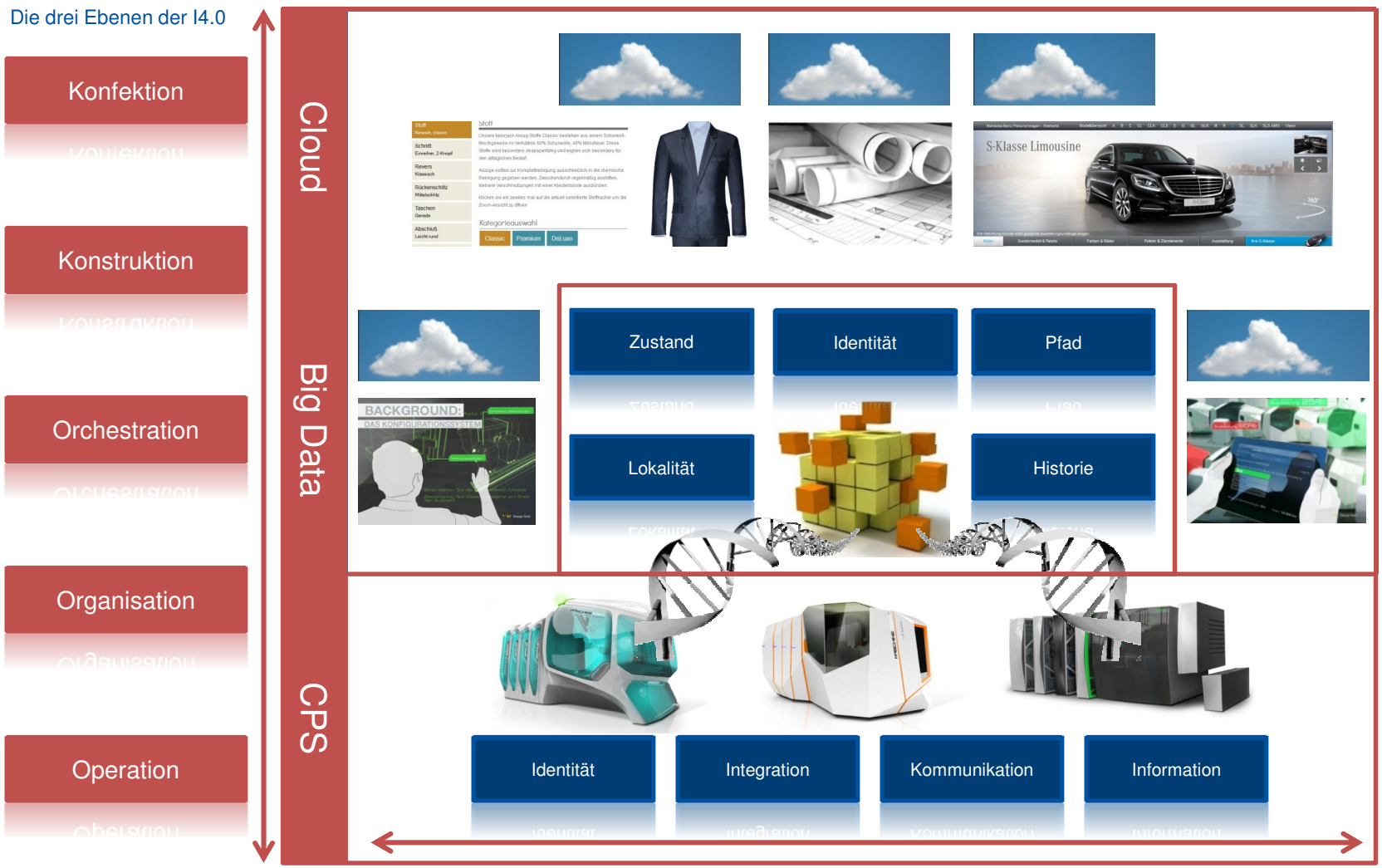
hochtechnologisiert

Personalisiertes Produkt

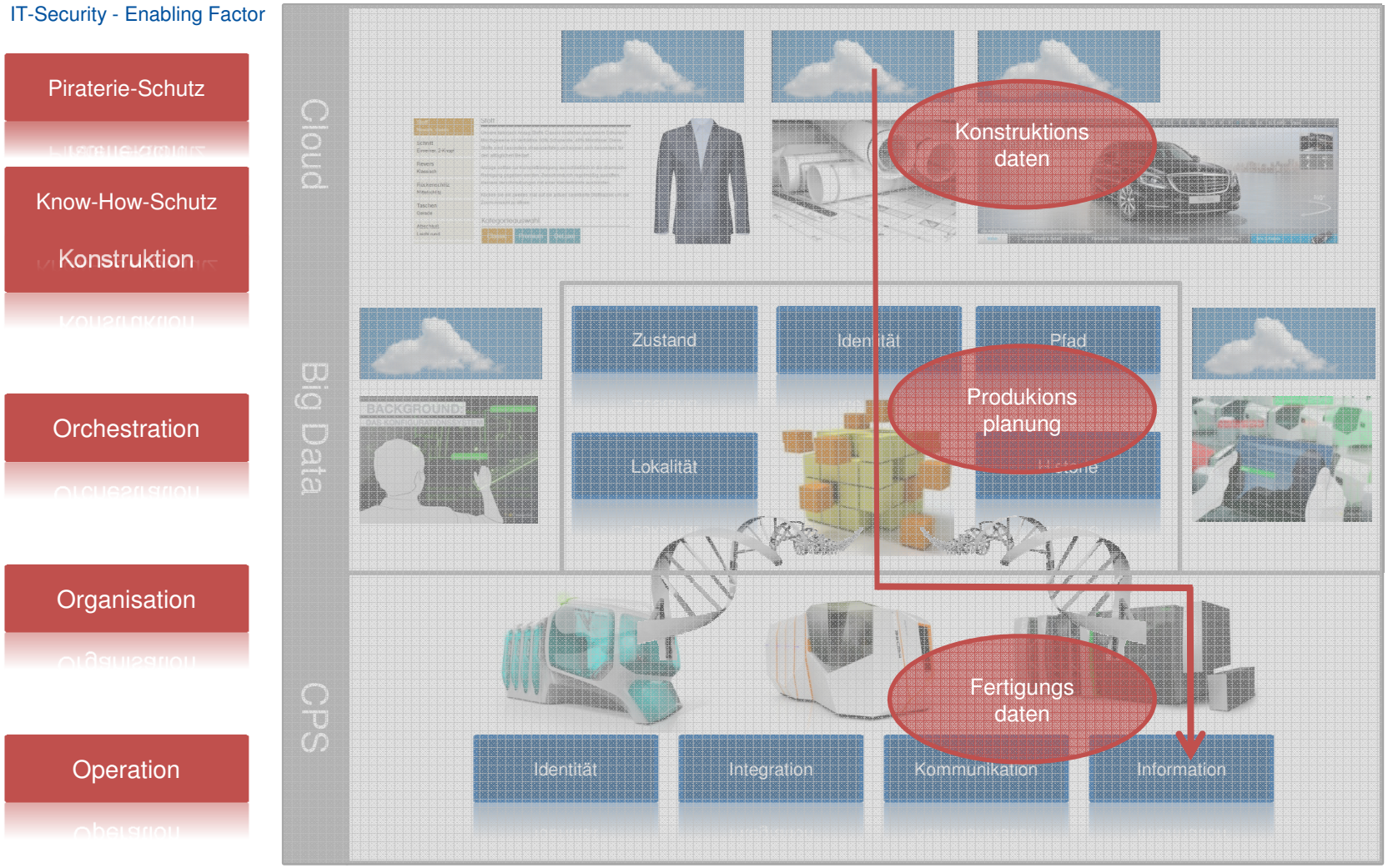
Industrieelle Revolution 4.0

Paradigmenwechsel I.40

Industrieelle Revolution 4.0



Industrieelle Revolution 4.0

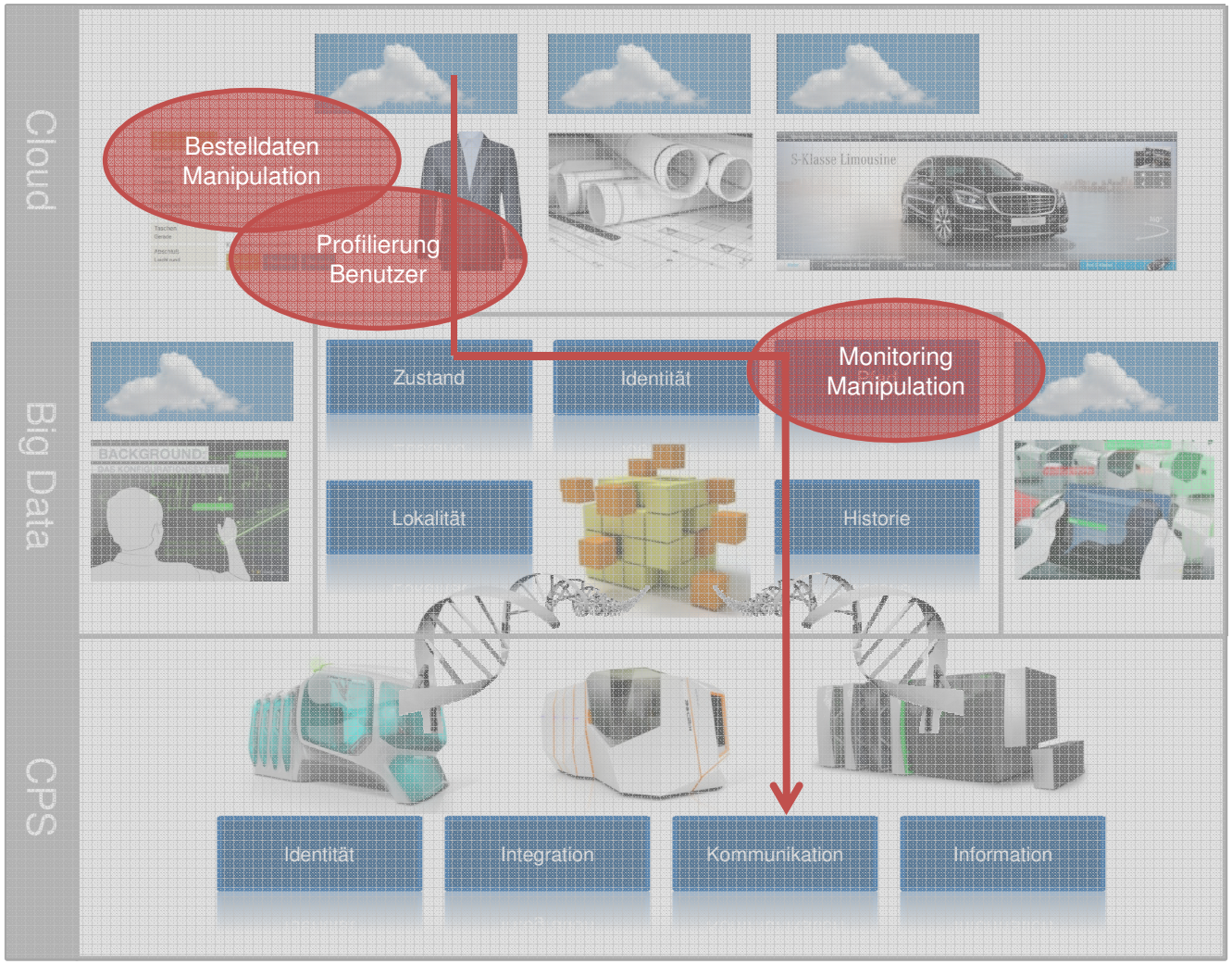


Industrieelle Revolution 4.0

IT-Security - Enabling Factor

Daten-Schutz

Kundenwerte

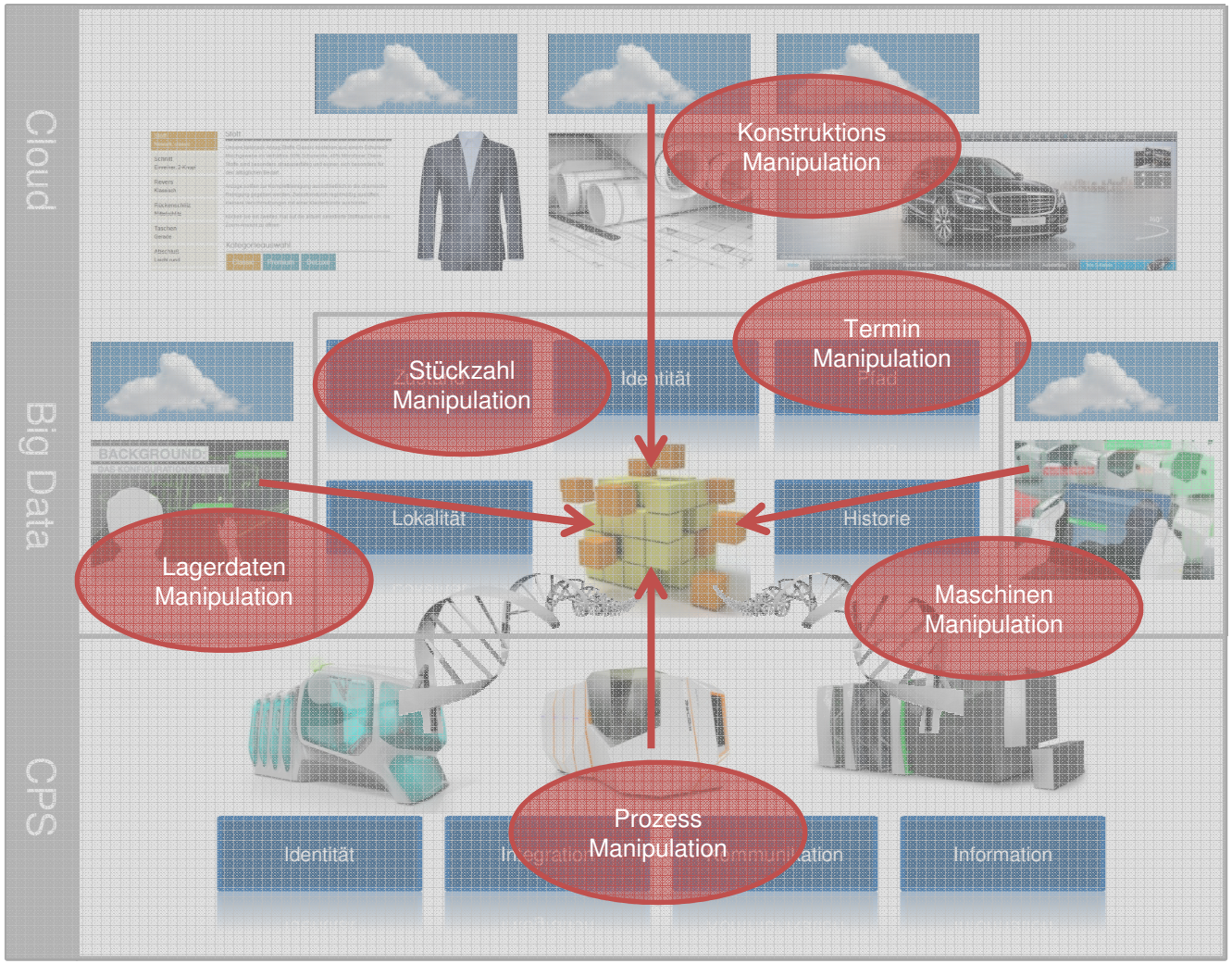


Industrieelle Revolution 4.0

IT-Security - Enabling Factor

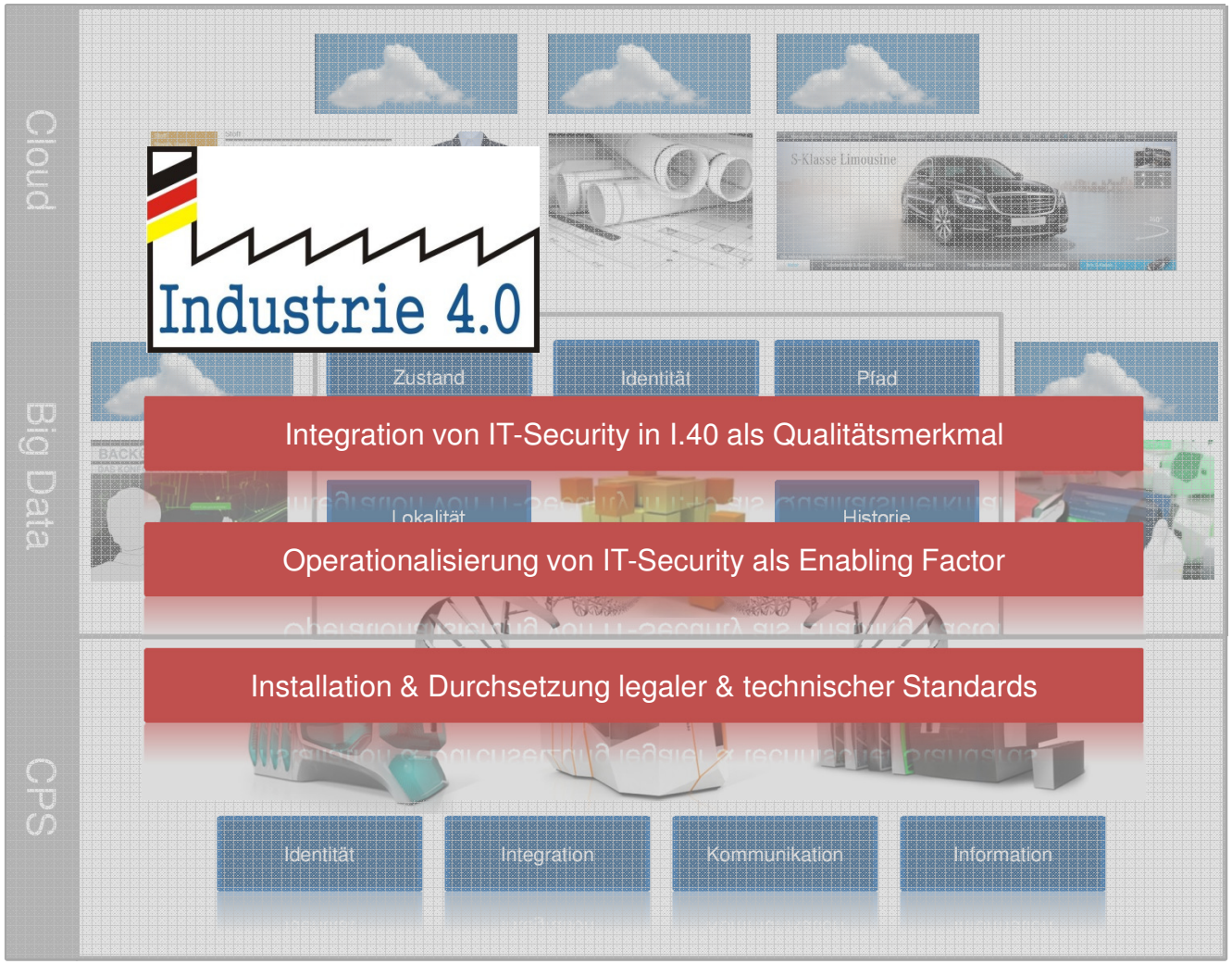
Sabotage-Schutz

Terror-Schutz



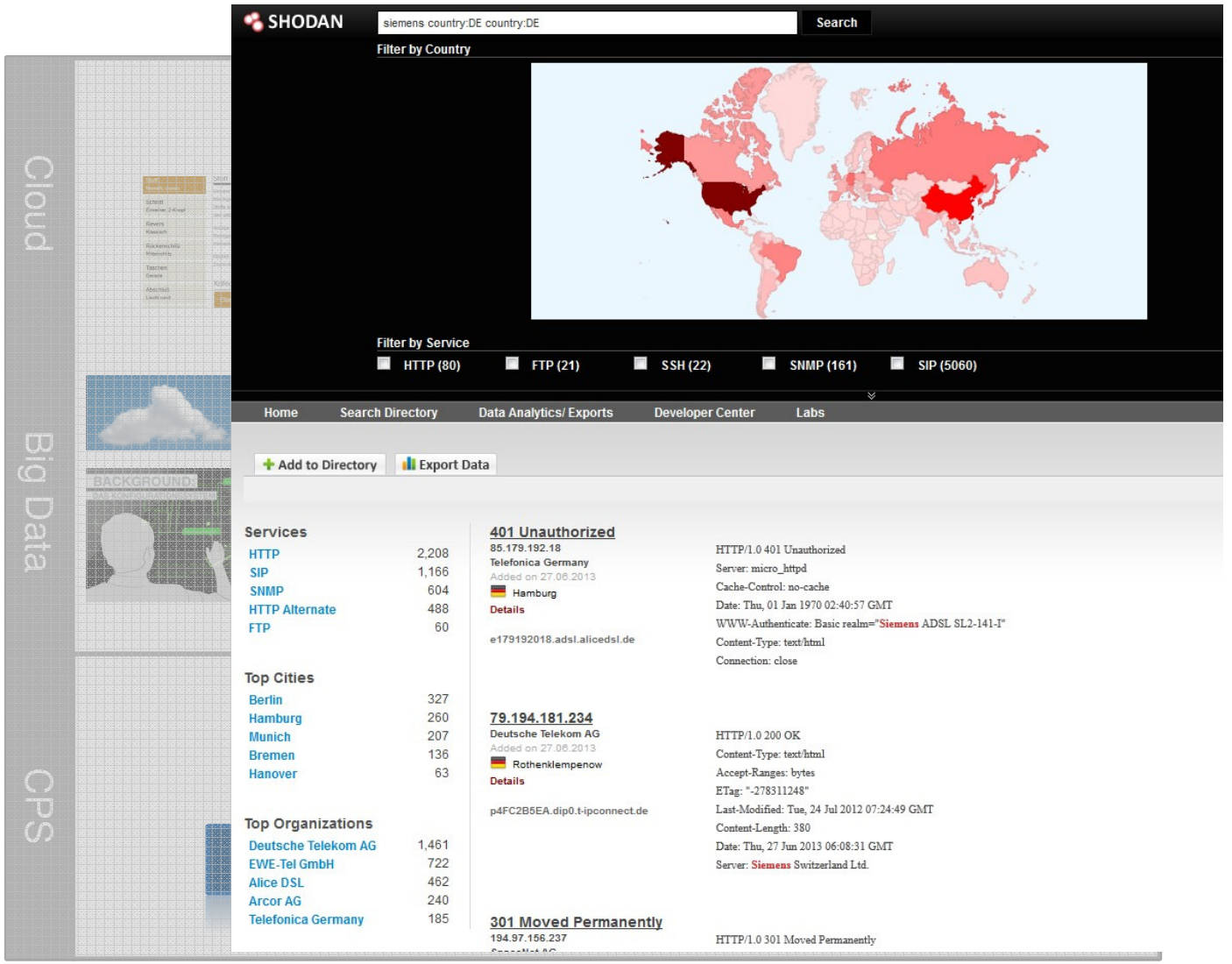
Industrieelle Revolution 4.0

IT-Security - Enabling Factor



Industrieelle Revolution 4.0

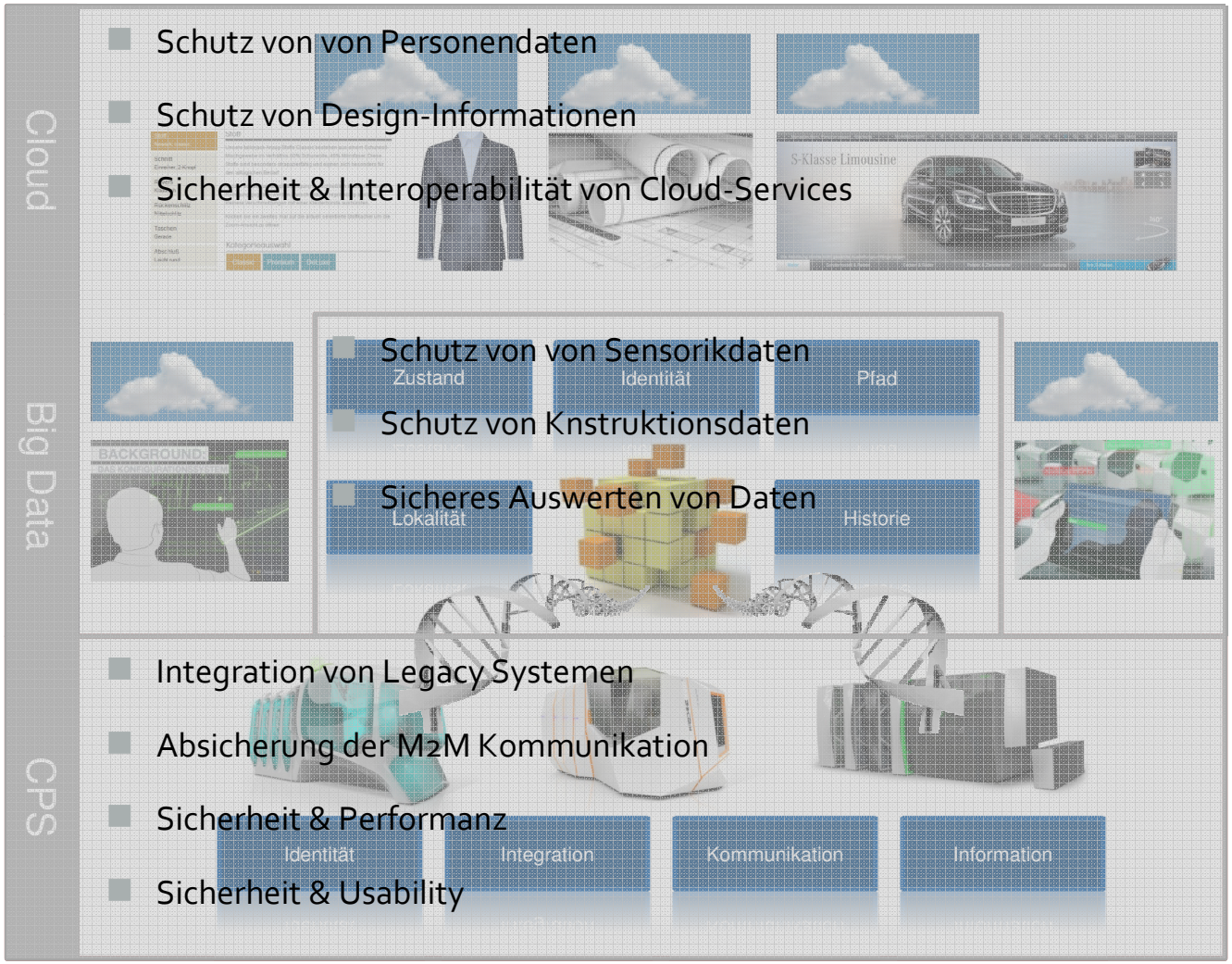
IT-Security – Status Quo



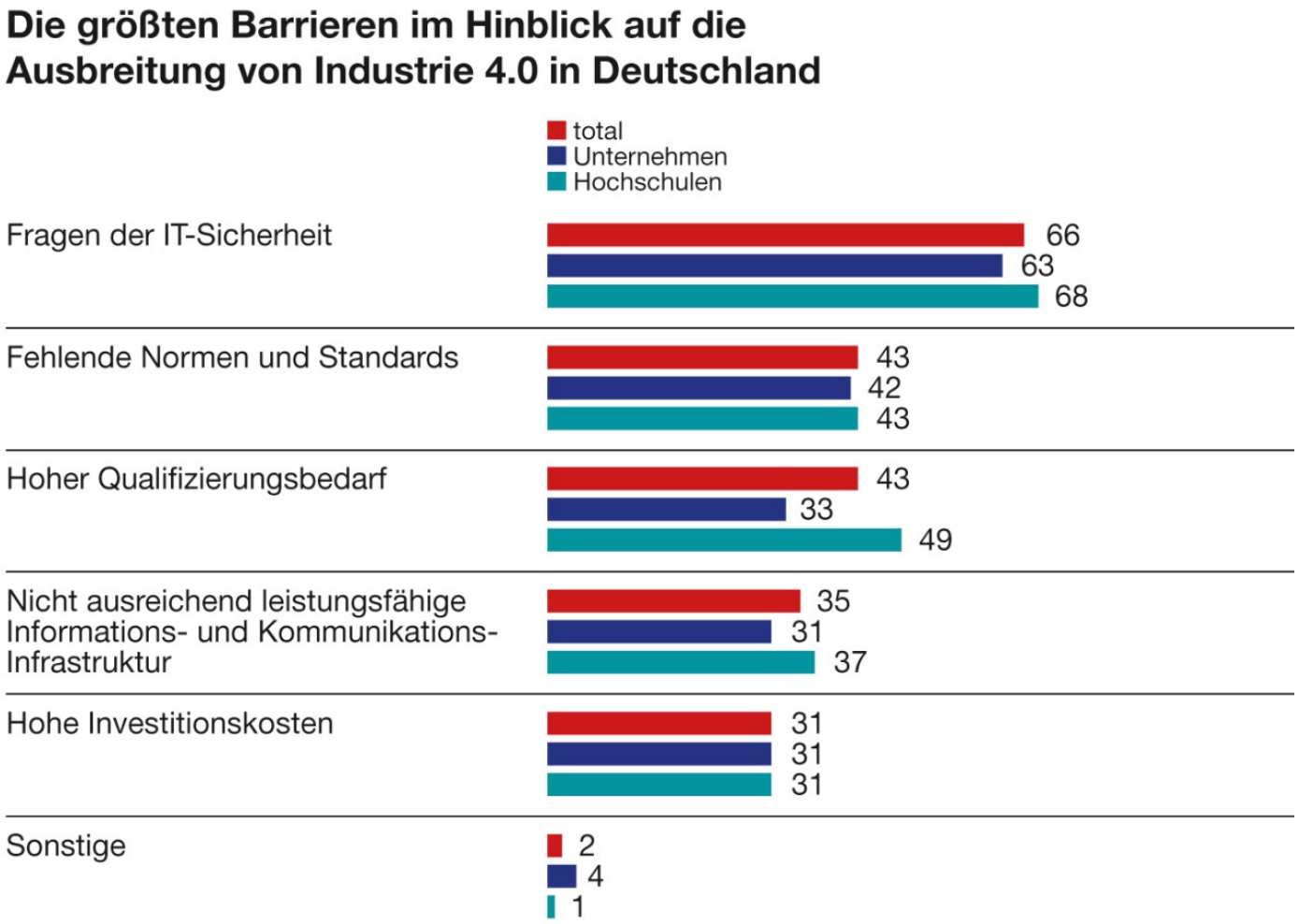
Industrieelle Revolution 4.0

Forschungsfragen

- Konfektion
- Konstruktion
- Orchestration
- Organisation
- Operation



Industrieelle Revolution 4.0



Quelle: VDE-Trendreport 2013, Befragung Unternehmen und Hochschulen

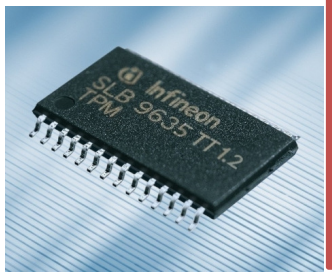
Industrieelle Revolution 4.0

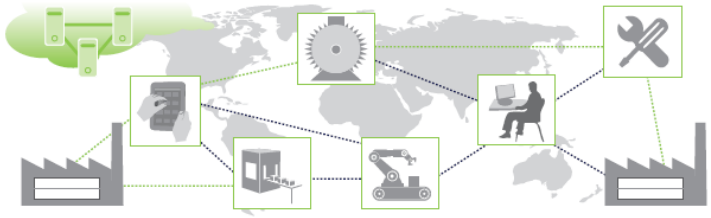
IT-Security - Enabling Factor

Cloud

Big Data

CPS



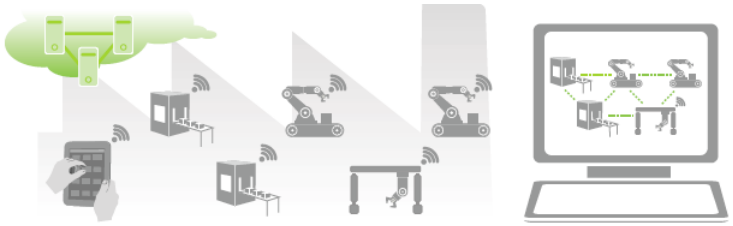


Horizontale Integration

- Neue Wertschöpfungsnetze und Geschäftsmodelle auf Basis von vernetzten CPS

Durchgängigkeit des Engineering

- Verschmelzung der digitalen und realen Welt über die Wertschöpfungskette eines Produkts über Firmengrenzen hinweg



Vertikale Integration

- Flexibilität, Rekonfigurierbarkeit und digitale Durchgängigkeit durch vernetzte Produktionssysteme

Zunehmende Vernetzung kontra Daten-Sicherheit.

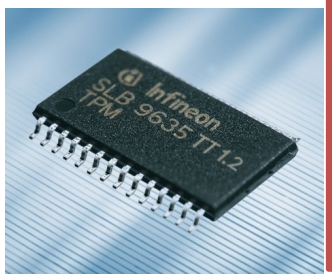
Industrieelle Revolution 4.0

IT-Security - Enabling Factor

Cloud

Big Data

CPS



Handlungsempfehlungen des Arbeitskreises Industrie 4.0

1 **Eindeutige und sichere Identitätsnachweise für Produkte, Prozesse und Maschinen**

Sicherer Informationsaustausch entlang des gesamten Produktionsprozesses

2 **Sicherer Schutz vor Produktpiraterie**

Verhinderung des Abgreifens von Unternehmens- und Produkt-Know-how, insbesondere vor dem Hintergrund globaler Wertschöpfungsketten

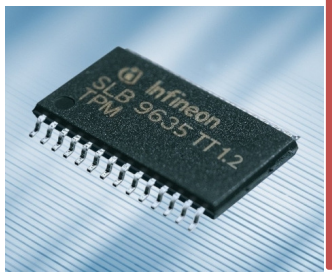
Industrieelle Revolution 4.0

IT-Security - Enabling Factor

Cloud

Big Data

CPS



Szenario: CAD/CAM-Gestützte Produktentwicklung


Produkt-Idee

= Geistiges Eigentum

= Know-how


CAD-Workstation → **Produktionsdaten**


CAM-Workstation → **Farbrikationsdaten**


Werkzeugmaschine (z.B. CNC) → Produkt

Aktuelle und künftige Produktionsumgebungen weisen ein hohes Potential für ungewollten Datenabfluss auf.

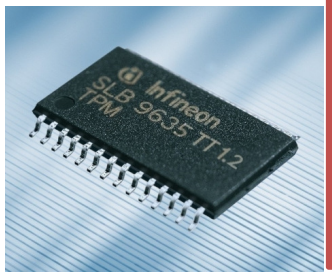
Industrieelle Revolution 4.0

IT-Security - Enabling Factor

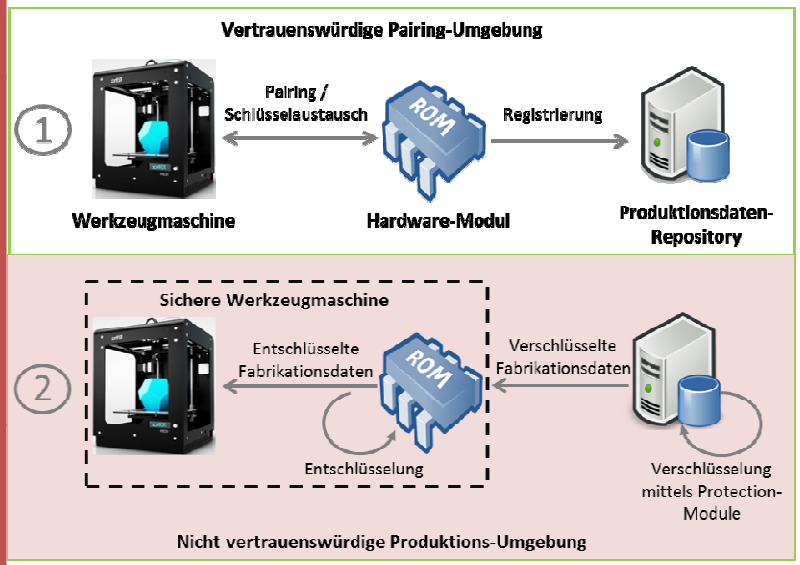
Cloud

Big Data

CPS



Erweiterung der CAD-CAM-gestützen Produktionsumgebung um transparente Sicherheitsfeatures und Kontrollmöglichkeiten



Erweiterung der Werkzeug-maschine um:

- Sichere und eindeutige Identifizierbarkeit
- Kryptographische Funktionen
- Stückzahlkontrolle

Erweiterung der CAD/CAM-Umgebung um SW-Protection Module:

- Festlegung von erlaubten Werkzeugmaschinen-IDs
- Verschlüsselung von Fabrikationsdaten
- Festlegung von erlaubten Stückzahlen

Industrieelle Revolution 4.0

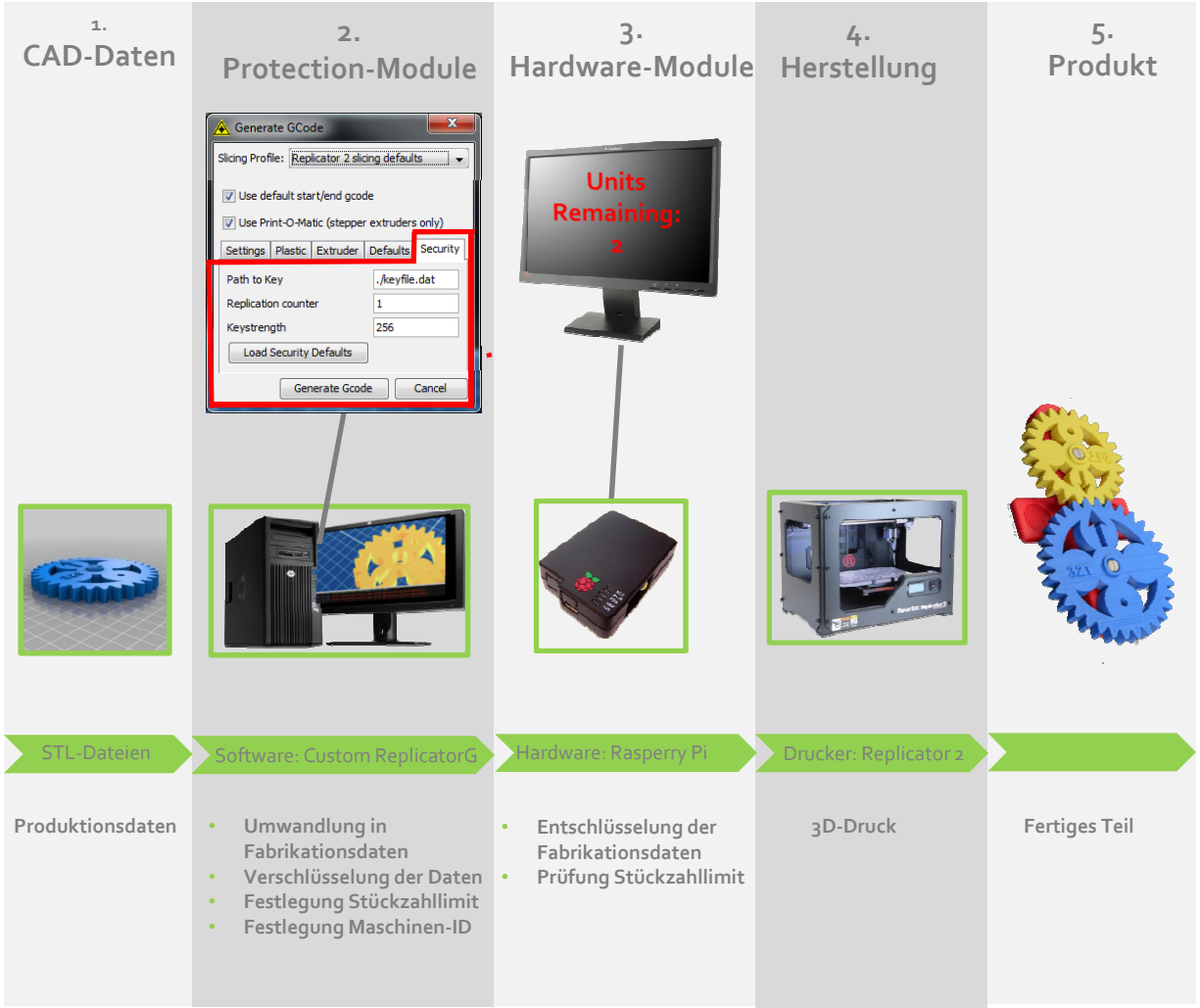
IT-Security - Enabling Factor

Cloud

Big Data

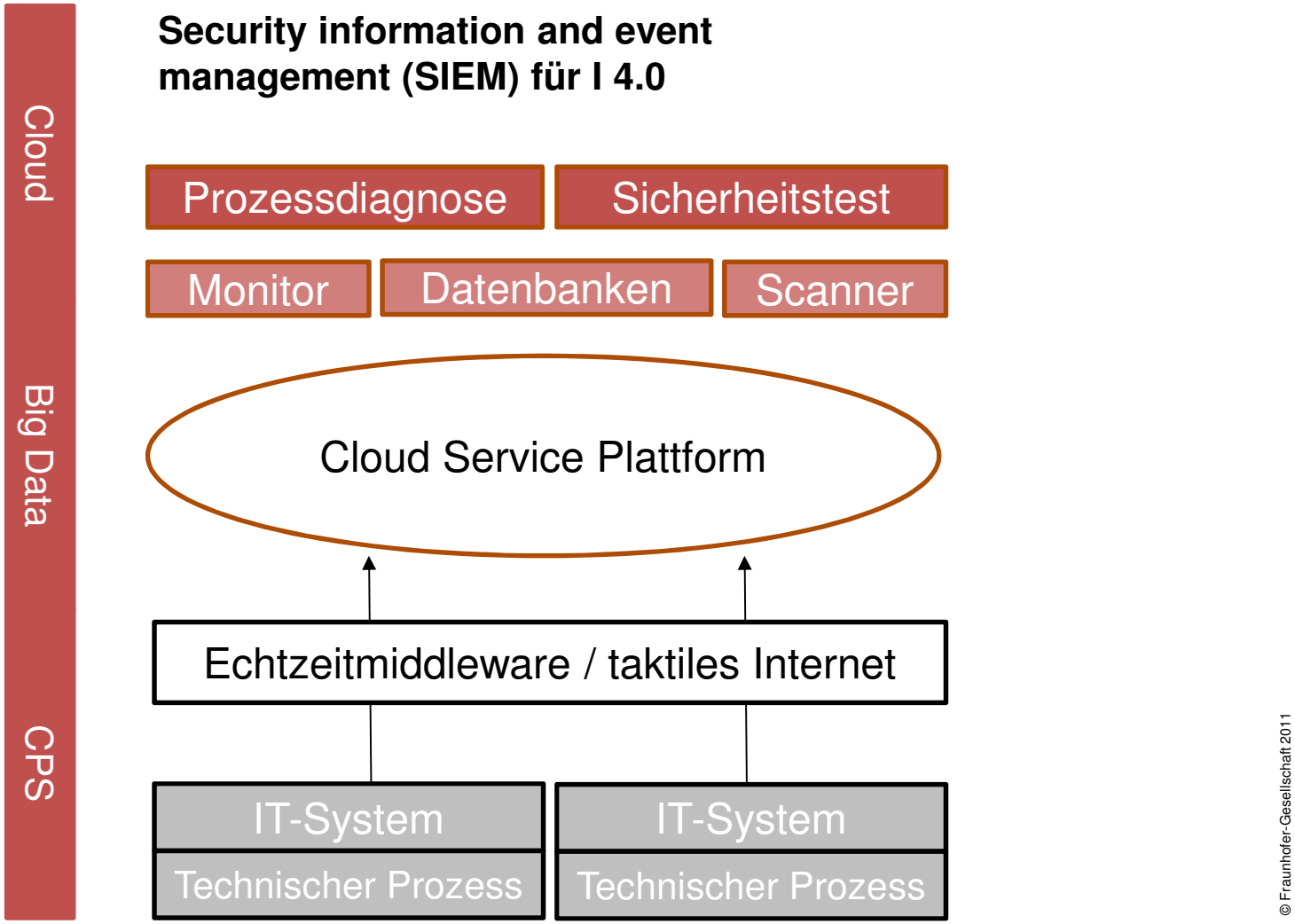
CPS

Prototyp am Beispiel 3D-Druck



Industrieelle Revolution 4.0

IT-Security - Enabling Factor



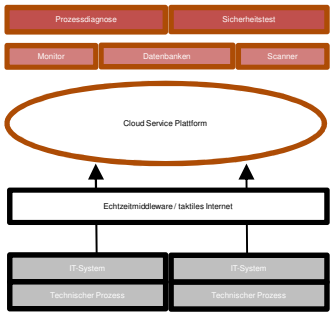
Industrieelle Revolution 4.0

IT-Security - Enabling Factor

Cloud

Big Data

CPS



Security information and event management (SIEM) für I 4.0

- Automatische Analyseverfahren, intelligente Allgorithmen, maschinelles Lernen, etc. ist state-of-the-art, findet aber „on premise" statt
- Vision ist Anlagen cloud-gestützt zu analysieren und zu optimieren
- Öffnung der Anlagen zum Internet ist erforderlich und bringt neben Skalierungseffekten auch Sicherheitsprobleme
- Gleichzeitig bieten die vorhandenen Analyseverfahren aber auch die Option ggf. Sicherheitsaspekte damit zu erkennen
- Projekt KOSIPRO zielt auf die Realisierung cloud-gestützer Analyseverfahren für Optimierung und IT-Sicherherheit

Industrieelle Revolution 4.0

IT-Security - Enabling Factor

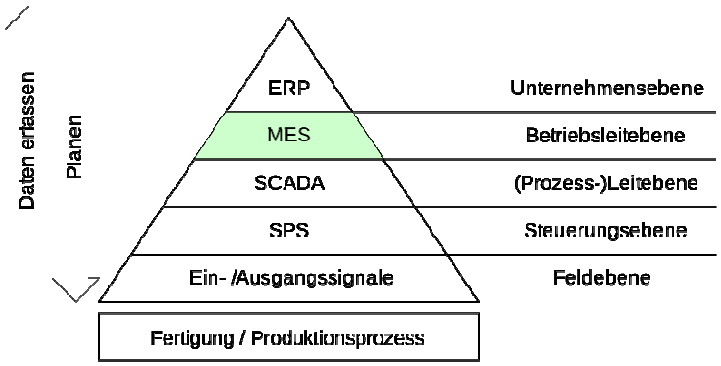
Cloud

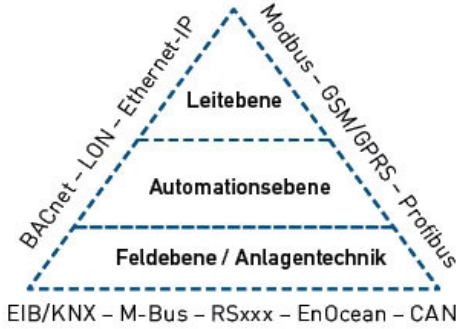
Big Data

CPS

Safety & Security

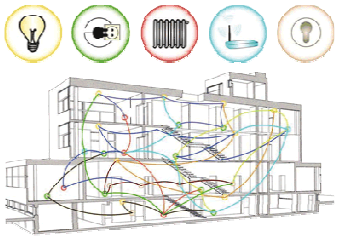
- Die Technologiebasis von Gebäudeautomation und industrieller Produktion bilden Feldbussysteme mit ähnlichen bis identischen Layern
- Gebäudeautomation und Produktion wachsen zusammen, Infrastruktur könnte geteilt werden, gemeinsame Brandmeldeanlagen, etc.
- Safety als integraler Bestandteil der Produktion bekommt über die Integration der Anlagen zentrale Bedeutung im Kontext der IT-Security.

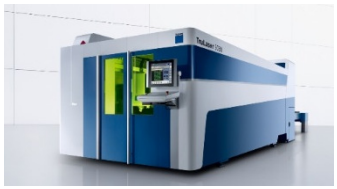


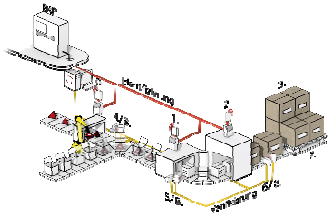


Industrieelle Revolution 4.0

IT-Security - Enabling Factor







Cloud

Big Data

CPS

Safety & Security

- Integration aller Feldbus-Systeme auf eine Technologieebene
- Integrierte Steuerung der Gebäude- und Produktionsautomation
- Durchsetzen eines einheitliches Sicherheitsniveaus auf allen Prozessebenen
- Skalierung von Safety-Qualiäten in Abhängigkeit von Anlagen und Gebäudenutzung (maximale Produktion wenn Personen abwesend sind)

Industrieelle Revolution 4.0

IT-Security - Enabling Factor

Sichere Ad-hoc Netze

- Verteilte/redundante Kontrolle (peer-to-peer)
- Ausbreitung von Malware unterbinden
- Monitoring mit schnellen Warnungen
- Schutz vertraulicher Daten
- Sichere und effiziente Managementprozesse

Industrieelle Revolution 4.0

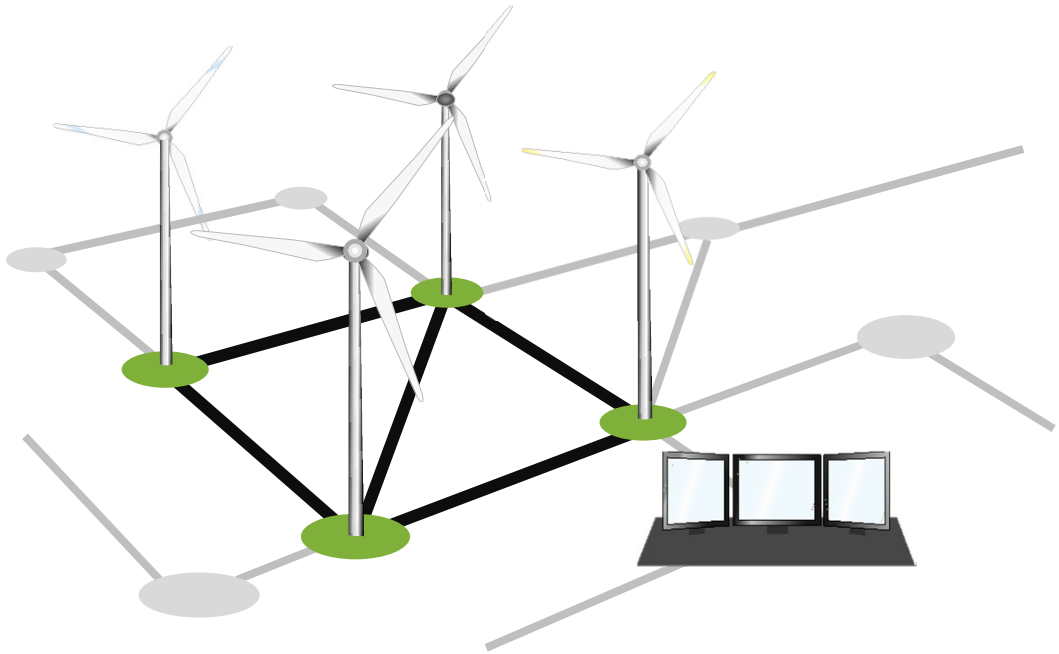
IT-Security - Enabling Factor

Cloud

Big Data

CPS

TrustMANET verbindet Geräte direkt und dynamisch.



Industrieelle Revolution 4.0

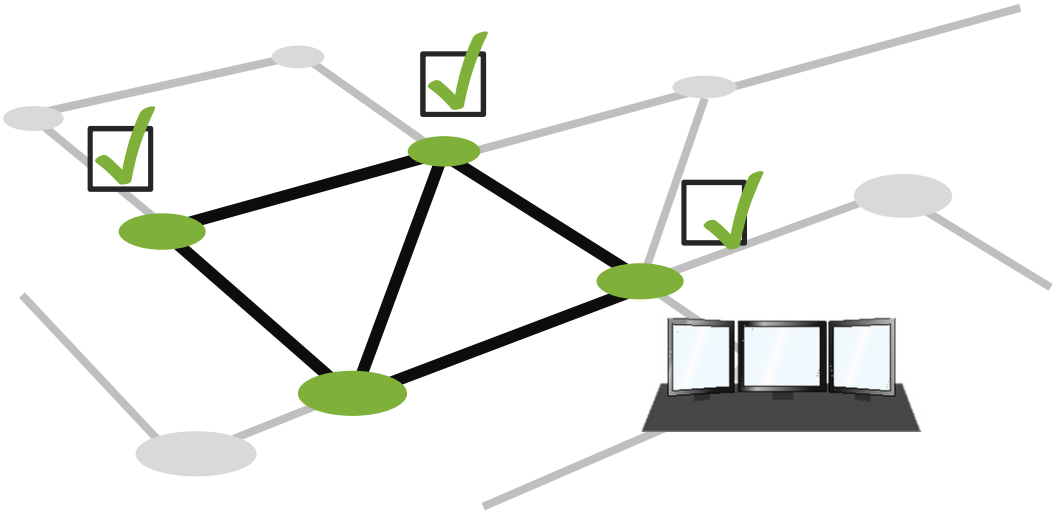
IT-Security - Enabling Factor

Cloud

Big Data

CPS

Jeder Knoten prüft den Zustand anderer Knoten und erkennt Änderungen.



Industrieelle Revolution 4.0

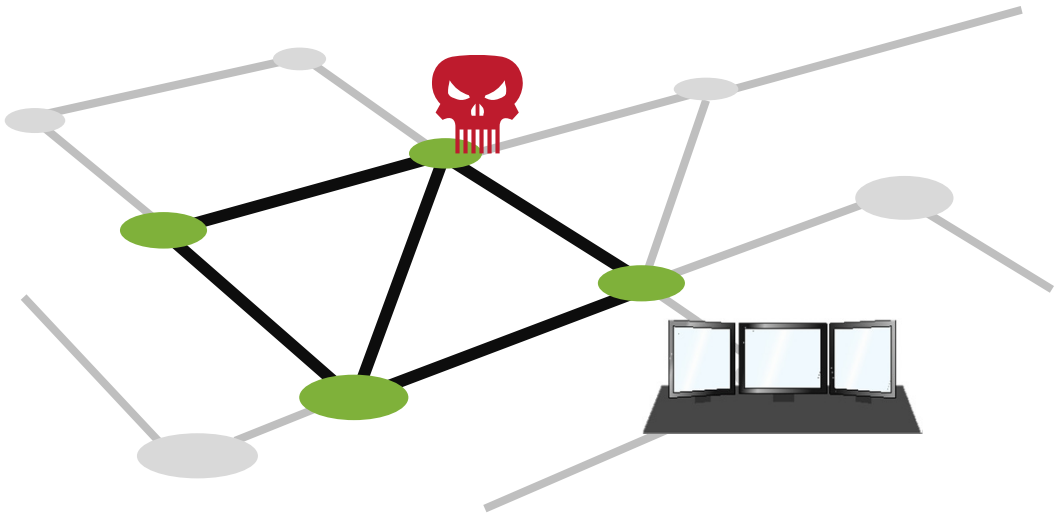
IT-Security - Enabling Factor

Cloud

Big Data

CPS

…wenn auf einem Knoten die Konfiguration geändert oder andere Software installiert wird...



Industrieelle Revolution 4.0

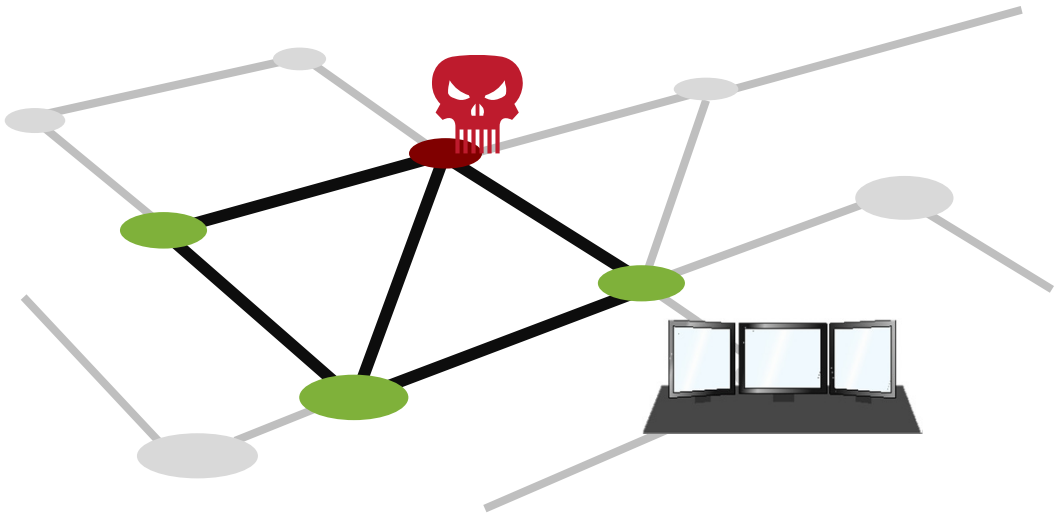
IT-Security - Enabling Factor

Cloud

Big Data

CPS

... wird der Knoten im Netz isoliert (Quarantäne, eventuell Beibehaltung wichtiger Funktionen)...



Industrieelle Revolution 4.0

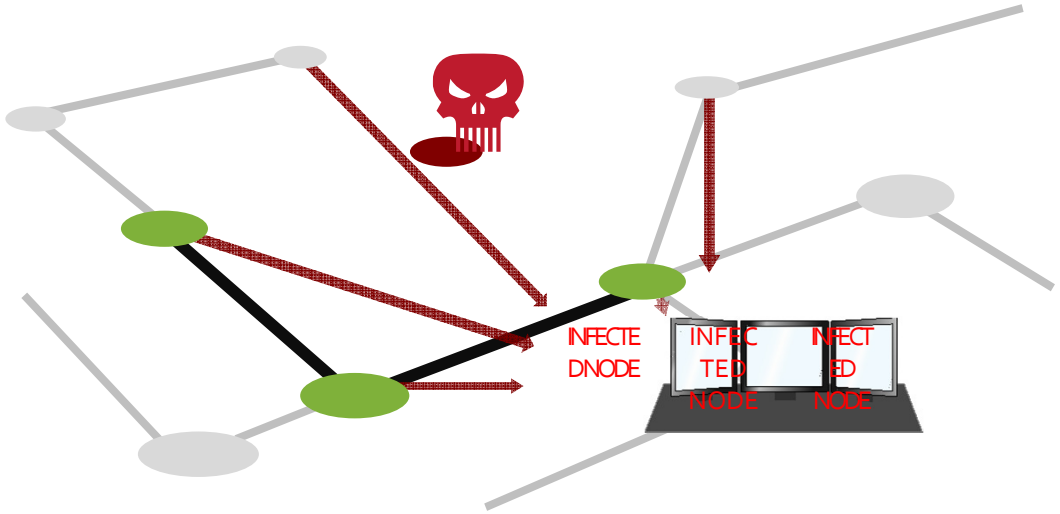
IT-Security - Enabling Factor

Cloud

Big Data

CPS

... und es wird eine Warnung produziert.



Industrieelle Revolution 4.0

IT-Security - Enabling Factor

Cloud

Big Data

CPS

Vertrauenswürdiges Mobiles Ad-Hoc Netzwerk entwickelt von Fraunhofer SIT:

- Verschlüsselte links zwischen allen benachbarten Geräten
- Hardware-basierte Authentisierung der Geräte und Schutz der Routing Information
- Manipulierte Geräte/Knoten werden über gegenseitige Prüfung des Gerätszustandes identifiziert und damit Angriffe über manipulierte Knoten verhindert.
- Jeder Knoten entdeckt selbständig benachbarte infizierte Knoten.
  Reaktion: Infizierte Knoten können direkt isoliert werden.

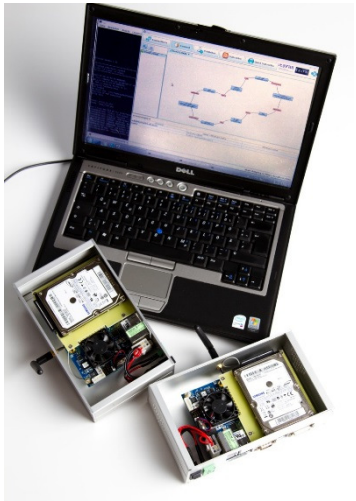
Industrieelle Revolution 4.0

IT-Security - Enabling Factor

Cloud

Big Data

CPS



Prototyp SetUp mit Visualisierung

- Mehrere Knoten bilden automatisch ein MANET unter Verwendung von Trusted BATMAN.
- Auch ein Laptop bildet einen MANET Knoten und zeigt per IF-MAP gesammelte Information zum Status des Netzes als Graph.
- Wird ein Knoten manipuliert, wird er automatisch aus dem Netz ausgeschlossen.
- Visualisierung zeigt, dass der Knoten nicht mehr akzeptiert wird.

Industrieelle Revolution 4.0

IT-Security - Enabling Factor

Cloud

Big Data

CPS

Allgemeiner: Trust establishment

- Vertrauen zwischen zwei Geräten benötigt:
  - Sichere Identität der Geräte (nicht nur MAC)
  - Sicherstellen, dass Software und Konfiguration der Geräte in Ordnung sind
  - Mechanismen, um Informationen zu Identität und Gerätesttus effizient und sicher auszutauschen
- Außerdem müssen effiziente Prozesse existieren
  - Registrierung und Verwaltung der Geräte
  - Schlüsselmanagement
  - Installation, Konfiguration, Update, Wartung

Industrieelle Revolution 4.0

IT-Security - Enabling Factor

Cloud

Big Data

CPS

Effizientes Set-Up: Zero Touch Configuration

- Registrierung der Geräte benötigt lediglich eine eindeutige Gerätenummer (z.B. fingerprint eines krypt. Schlüssels), der das Gerät identifiziert.
- Das Gerät kommt direkt von der Produktion zur Installation. Je nach Protokoll muss keinerlei kundenspezifische Information eingebracht werden.
- Der Techniker schließt das Gerät an (eventuell erst an einen speziellen Konfigurationsport). Die Konfiguration, Registrierung, usw. ist vollautomatisch.
- Keine USB-Sticks, kein Laptop zur Konfiguration, kein Nutzerinterface am Gerät. Leuchtdioden zeigen die erfolgreiche Konfiguration an. Interaktion nur im Fehlerfall nötig.

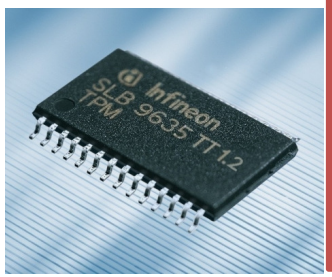
Industrieelle Revolution 4.0

IT-Security - Enabling Factor

Cloud

Big Data

CPS



Trusted Platform Module - TPM

- Eine verfügbare Möglichkeit für hardware-basierte Sicherheit bietet das Trusted Platform Module (TPMs) integriert in das Gerät.
- Das TPM bietet
  - Vereinfachte Verwendung von Kryptographie und sicheres Schlüsselmanagement
  - *Eingebaute* PKI entweder mit Herstellerzertifikaten oder durch von Kunden eingebrachte (bzw. im TPM generierte) Schlüssel.
  - Zertifizierte Sicherheit (security). Common criteria EAL-5 für chip design und EAL-4+ für gesamten TPM.

Industrieelle Revolution 4.0

Fraunhofer SIT – Leistungsportfolio im Industrie 4.0 Umfeld

- Analysieren & Bewerten von Sicherheitskonzepten von Industriesteuerungen
- Testen von Steuerungsanlagen
- Entwickeln von Konzepten zur Informationssicherheit in Industrieanlagen, ggf. Zertifizierungen nach Standards mit Partnern
- Entwickeln von Technologien für Produkt- und Pirateriesschutz
- Entwicklung von Technologien für die sichere Identifikation von Geräten und effizientes Schlüsselmanagement
- Entwicklung von Technologien für Verteiltes Security-Monitoring von Geräten
- Entwicklung und Validierung von Apps

Industrieelle Revolution 4.0

Fraunhofer SIT – Leistungsportfolio im Industrie 4.0 Umfeld

- Analysieren & Bewerten von Sicherheitskonzepten von Clouddiensten im I.40 Umfeld
- Aufstellen von Kriterien für die Auswahl sicherer Clouddienste & -diensteanbieter
- Secure Engineering Methoden für Steuerungsanlagen Software Entwicklung
- Entwicklung von Secure Engineering Test-tools

Dr. Thorsten Henkel

Thorsten.henkel@sit.fraunhofer.de

Fraunhofer-Institut für
Sichere Informationstechnologie

Rheinstrasse 75
64295 Darmstadt, Germany

www.fraunhofer.de
www.sit.fraunhofer.de