Security in Industry 4.0
Industrial IoT

@TEMET 2018

André Clerc | Security Engineer | TEMET AG
Marcel Suter | Director Solutions | libC SA

11.06.2018

Agenda

- Introduction in Industry 4.0, Industrial IoT (IIoT)
- IT Security versus IIoT Security
- Solution Approaches
- Security and the IIoT
- Secure Key Management

Speaker Information

André Clerc

Dipl. Inf.-Ing. FH , CISSP,
CAS Project Management

Expert IT Security Consultant
Works in Information Security since 2000

Core Competencies
PKI incl. Hardware Security Modules
Strong Authentication
Network and Perimeter Security
FATCA, AIA and MiFIR Reporting

Engagements
Founder of About and Beyond PKI Event
Author PKI Education @ SwissSign

Speaker Information

Marcel Suter

M.Sc. Computer Science, Dartmouth
Economiste d'entreprise, Lausanne

Security SW Engineer & Consultant
Works in Information Security since 1993

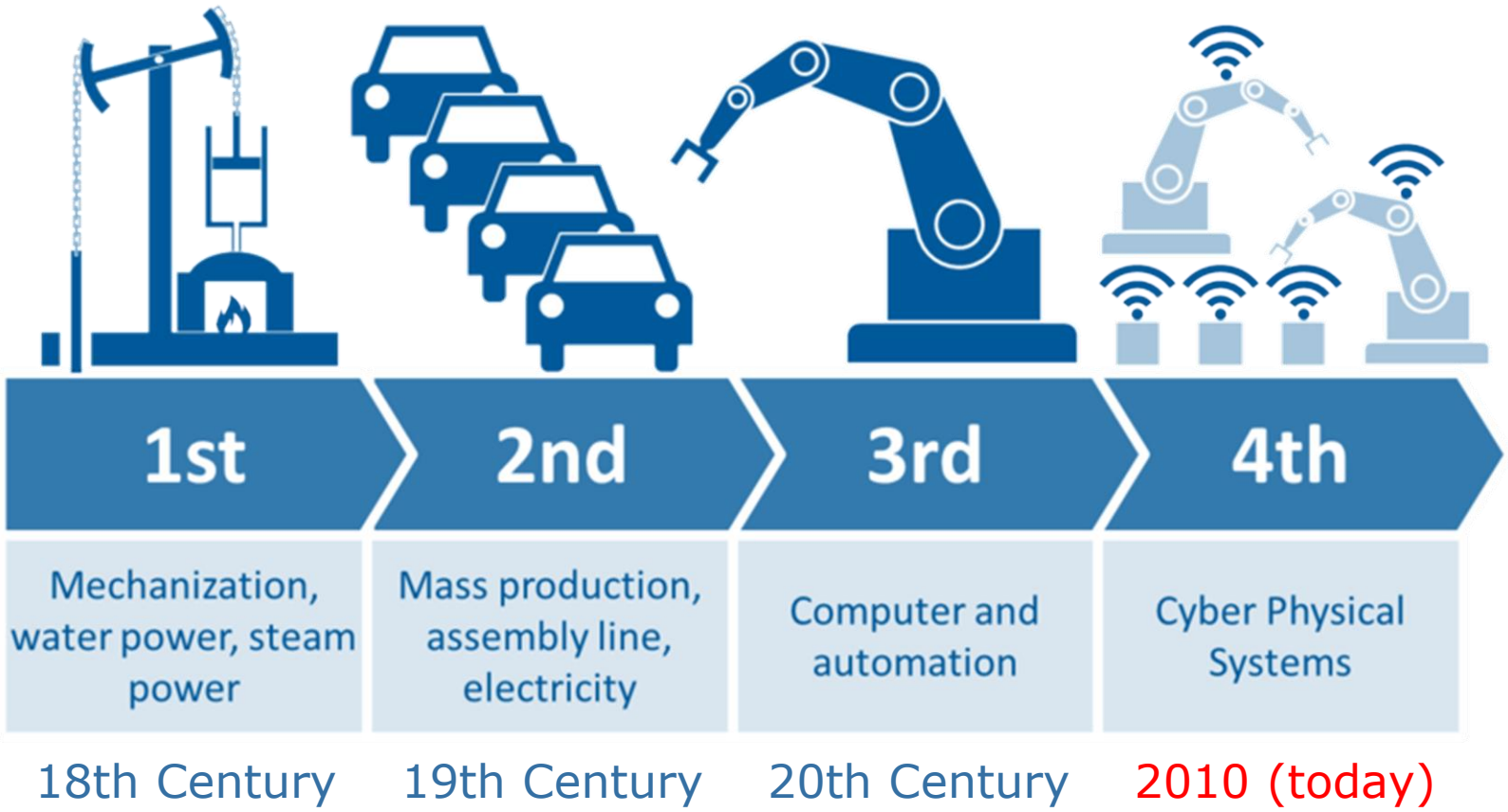
Core Competencies
PKI incl. Hardware Security Modules
Full life-cycle software/product development
Provide customers with best practices in IT Security

Engagements
Chargé de cours à l'Ecole d'Ingénieurs VD

INTRODUCTION IN INDUSTRY 4.0 (IIOT)

Introduction in Industry 4.0 (IIoT)

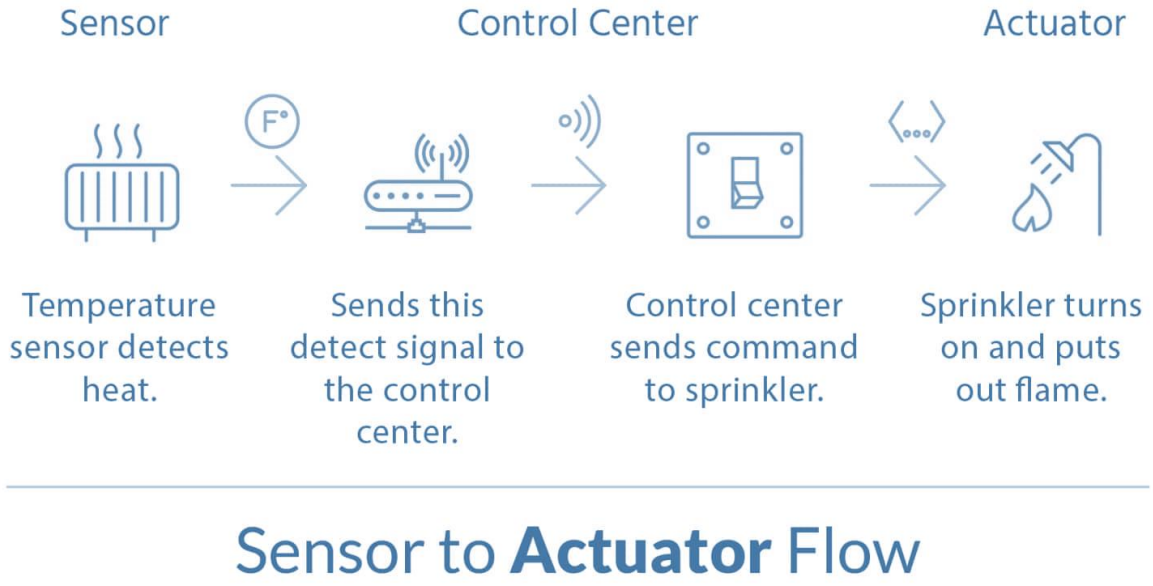
Industry 4.0



Introduction in Industry 4.0 (IIoT)

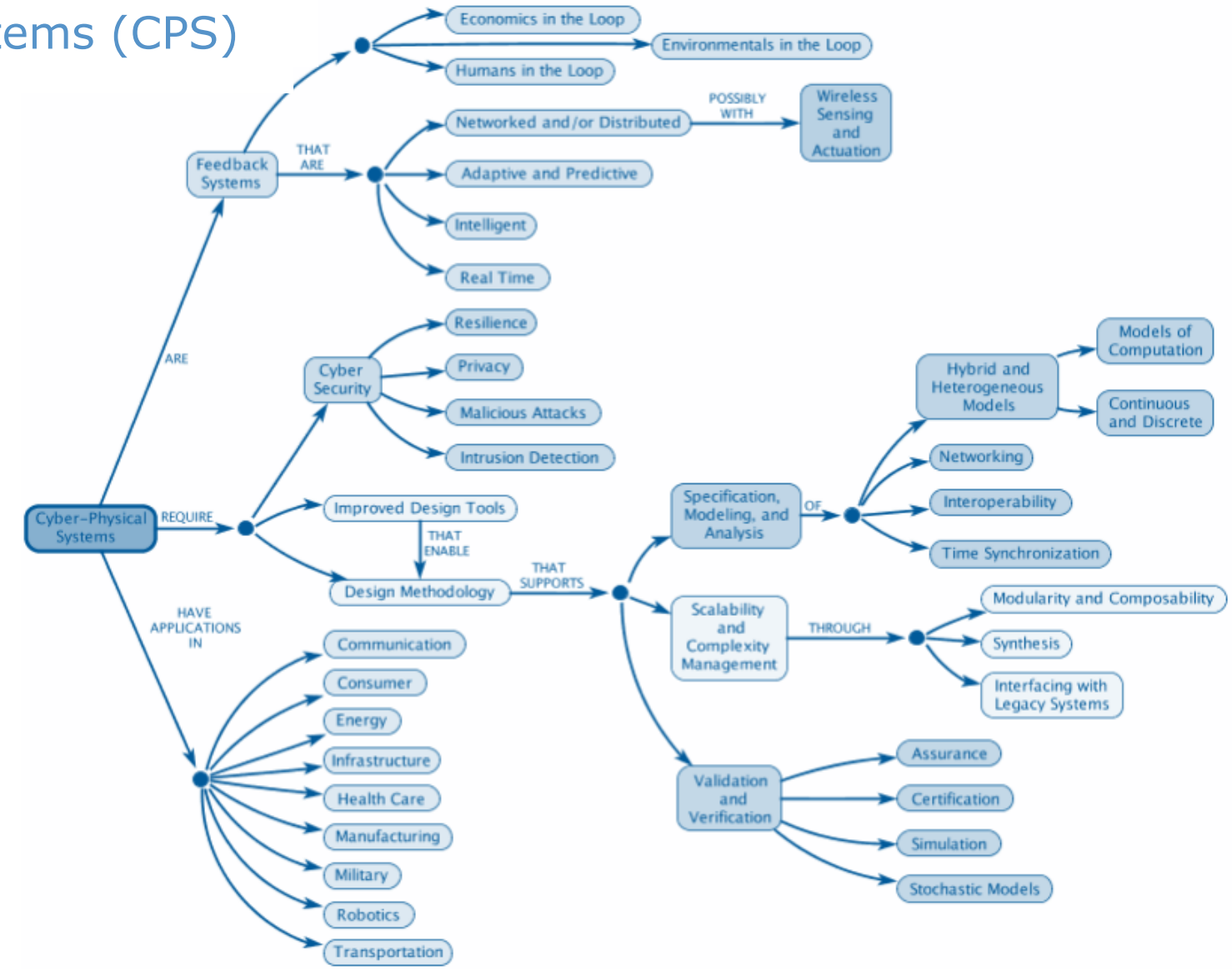
IIoT – Sensors and Actuators

- Everything is connected
- Use sensors and actuators in an industrial environment
- Typically systems that interact with the physical world where uncontrolled change can lead to hazardous conditions



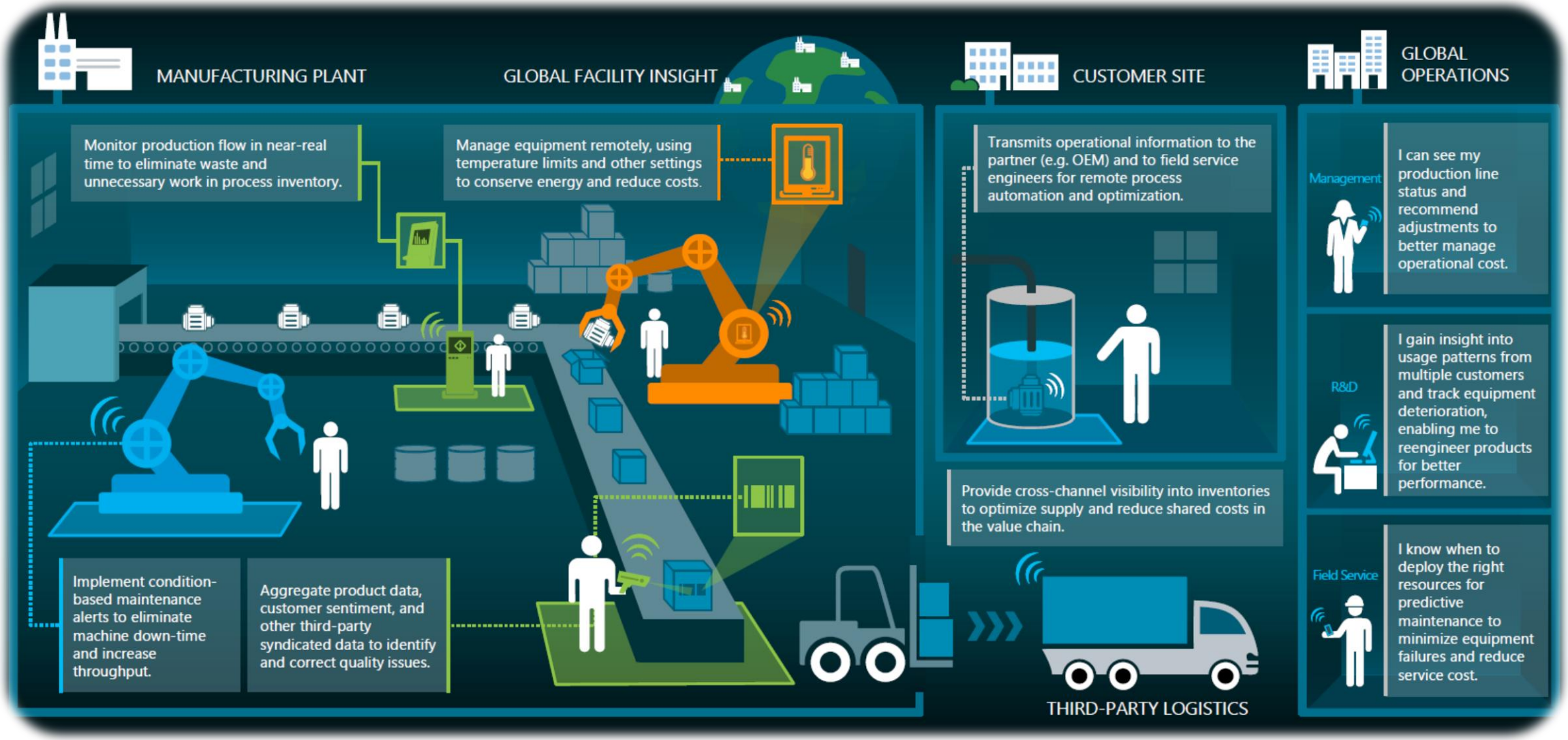
Introduction in Industry 4.0 (IIoT)

Cyber-Physical Systems (CPS)



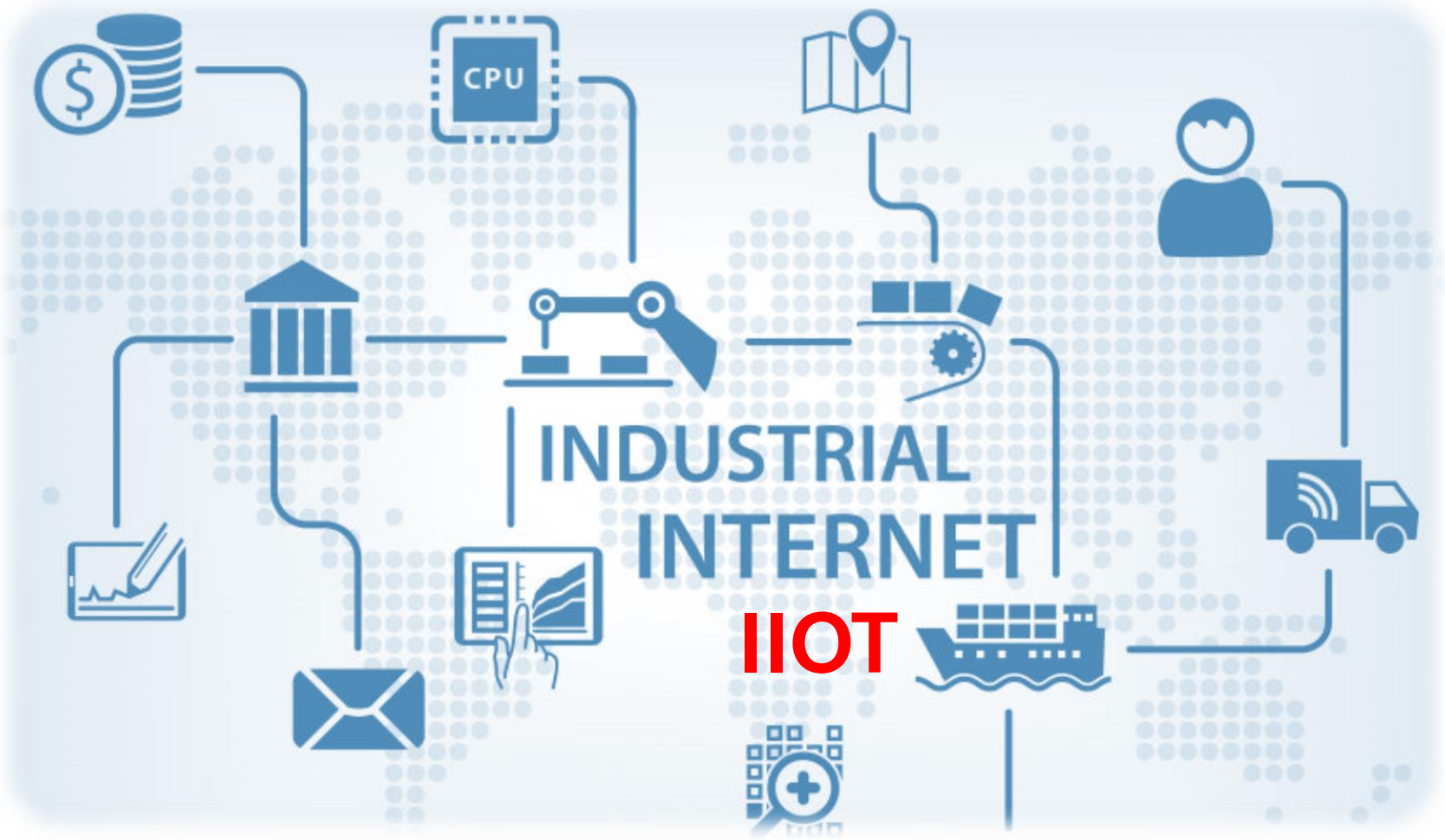
Introduction in Industry 4.0 (IIoT)

IoT (Sensors) as a Base



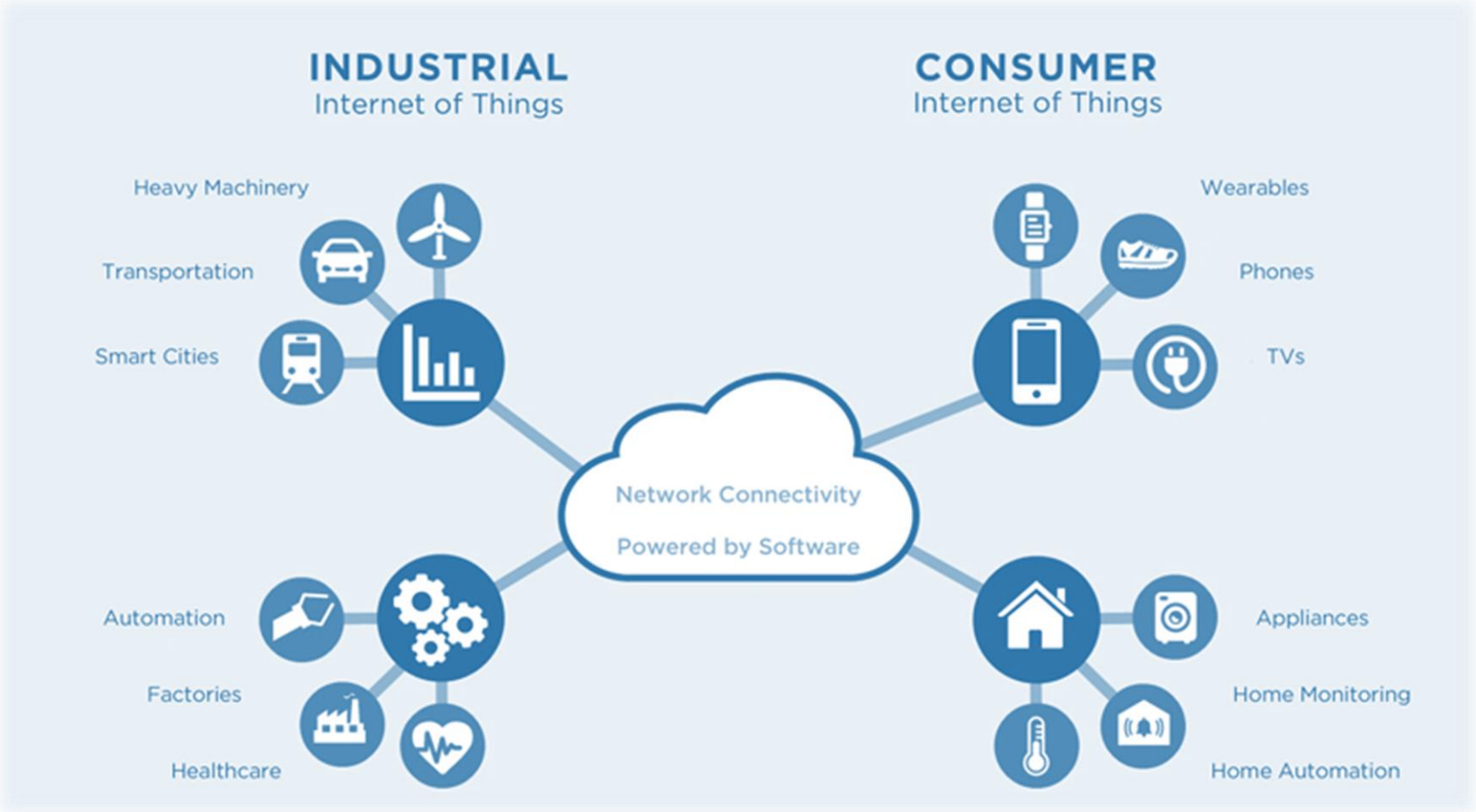
Introduction in Industry 4.0 (IIoT)

IoT vs. IIoT



Introduction in Industry 4.0 (IIoT)

IoT vs. IIoT



SECURITY IN IIOT
IT/OT

Security in IIoT (IT/OT)

Security of Traditional IT Systems

- Cybersecurity and information assurance in IT systems revolve around three traditional pillars:
  - Confidentiality
  - Integrity
  - Availability

  } CIA
- Stresses on Core Services
- Less Attention on Peripheral Devices
- Often not in Focus (see IAM):
  - Authentication
  - Authorization
  - Access Control
- Layered Defense and Zoning

IT Security versus IIoT Seccurity

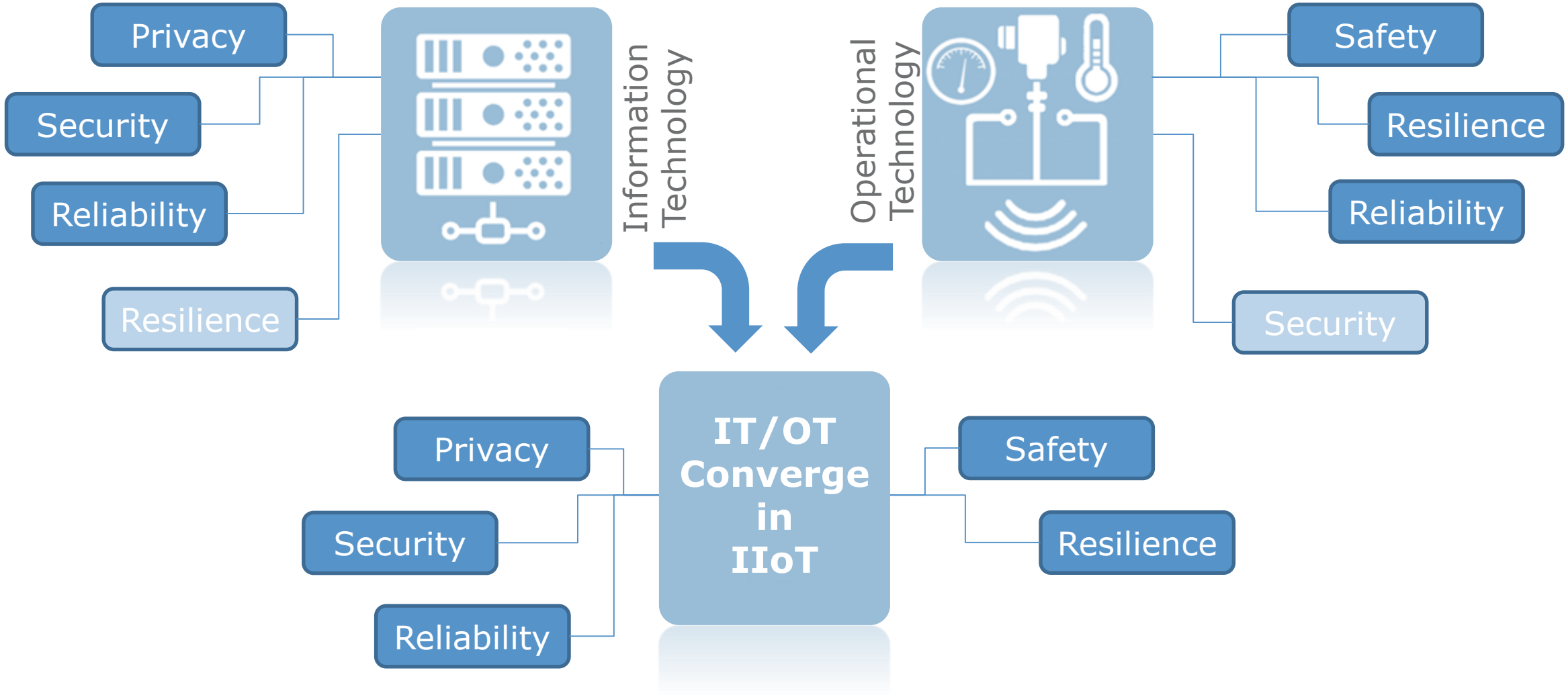
IIoT Ecosystem Security

- The whole ecosystem moves into focus
  - Core Services
  - Peripheral Devices
  - Communication Channels
- To focus traditional (Cyber)-Security pillars is not enough **confidentiality**, **integrity** and **availability**
- Priority order moves: 1) availability, 2) integrity, 3) confidentiality
- To stress on authentication, authorization, access control is mandatory

- Countless attack vectors spread over the production chain
  → one weakness/vulnerability might break down the production or result in producing faulty products

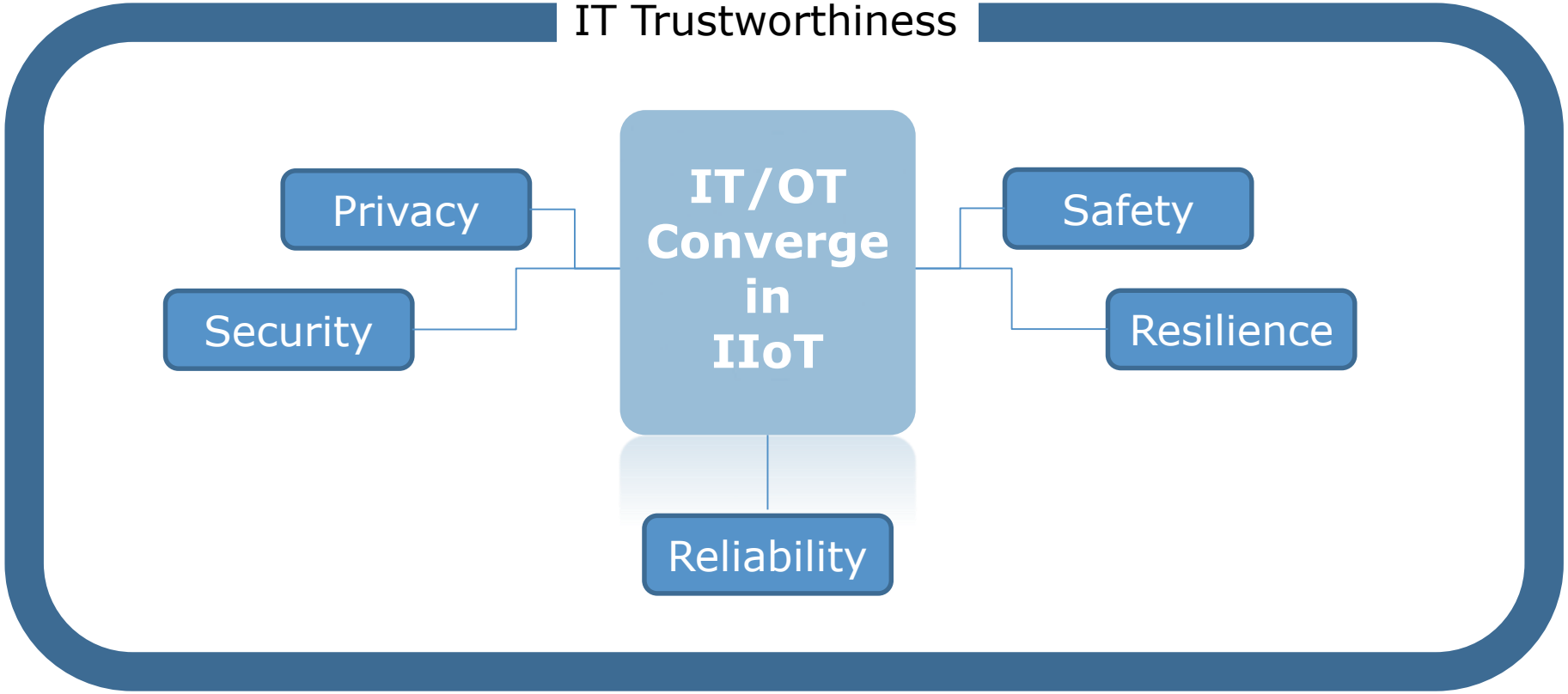
Security in IIoT (IT/OT)

IT/OT Convergence



Security in IIoT (IT/OT)

Trustworthiness on Key System Characteristics



Trustworthiness [Schneider1998], [NIST-CPS] is the **degree of confidence** one has that the **system performs as expected** in respect to all the key system characteristics in the face of environmental disruptions, human errors, system faults and attacks. The needs of IT and OT must both be met.

Security in IIoT (IT/OT)

Assurance

control or influence information usage — **Privacy**

access, change or destruction — **Security**

physical injury or damage to the health of people — **Safety**

avoid, absorb and manage dynamic adversarial conditions — **Resilience**

ability to perform its required functions under stated conditions for a specified period of time. — **Reliability**

Risk Analysis

Design Reviews

Testing

What has been done to address specific attacks and weaknesses?

Security in IIoT (IT/OT)

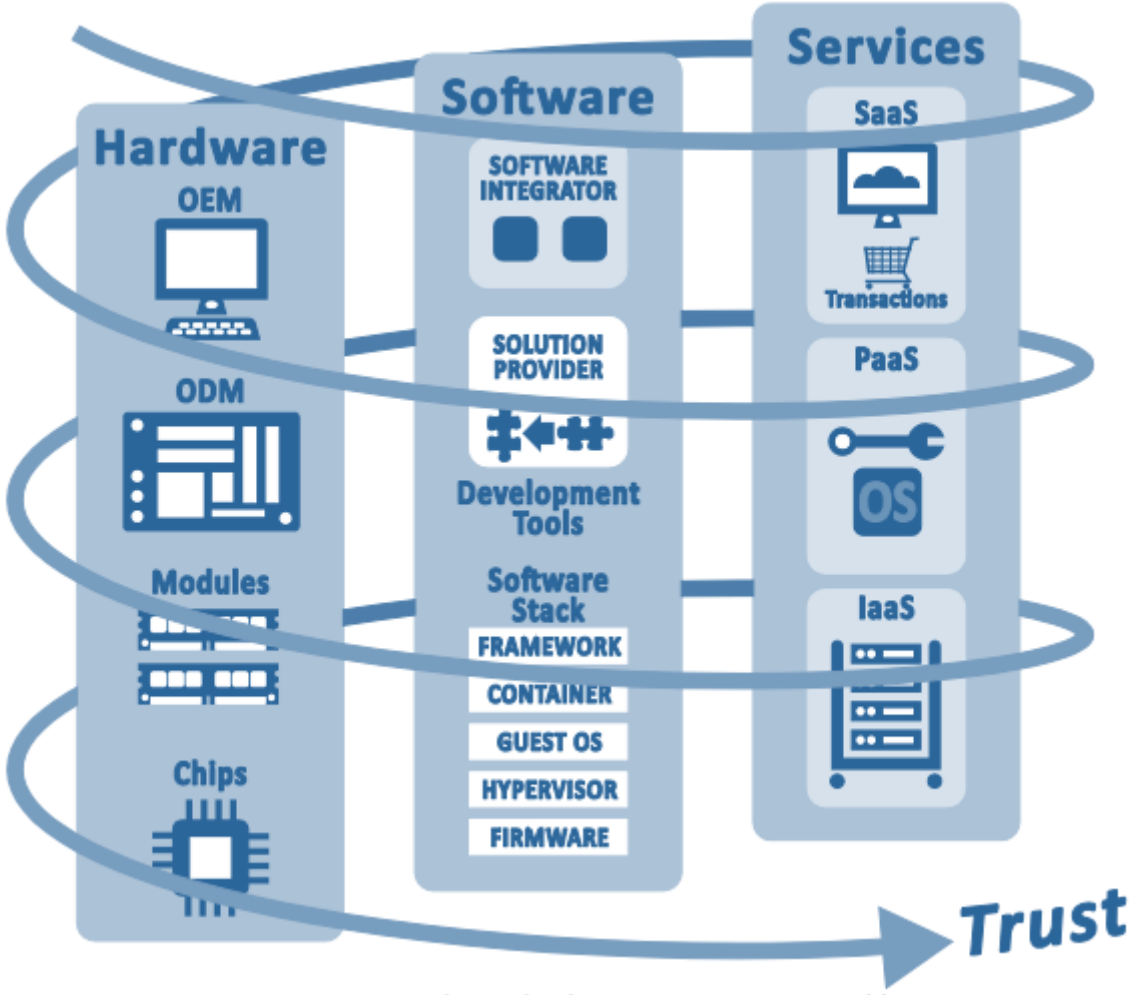
Rist Management

- Security Programm
- Risk Assessment
- Communicate Risks to the Management
- Ongoing Business Attention - Updates to Security-related Technologies
- Metrics and Key Performance Indicators

- *Managing risk balances the threats against the IIoT system with the security responses that counteract those threats and the risk they represent.*

Security in IIoT (IT/OT)

Trust Relationship



Security in IIoT (IT/OT)

Framework

- Security Programm
- Risk Assessment
- Communicate Risks to the Management
- Ongoing Business Attention - Updates to Security-related Technologies
- Metrics and Key Performance Indicators

- *Managing risk balances the threats against the IIoT system with the security responses that counteract those threats and the risk they represent.*

TEMET
end-to-end IT security

Framework

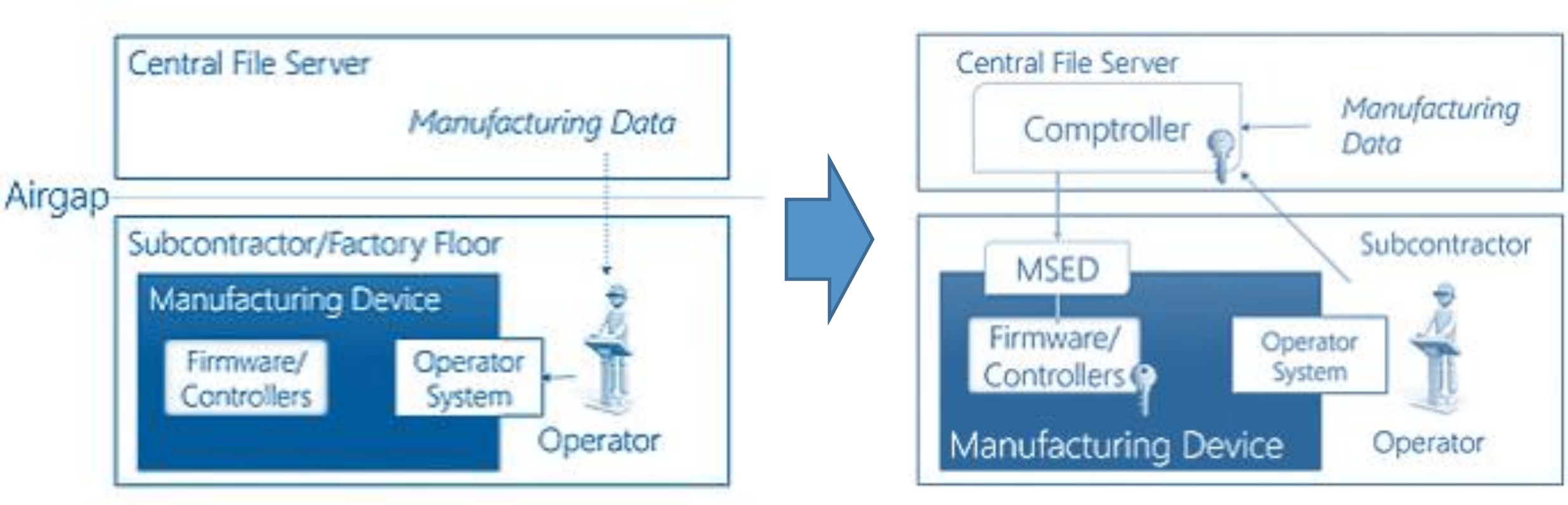
- Framework
  - International Standards Organization (ISO)
  - Institute of Electrical and Electronic Engineers (IEEE)
  - International Electrotechnical Commission (IEC)
  - Internet Engineering Task Force (IETF)
  - National Institute for Standards and Technology (NIST)

- Industrial Internet of Things Volume G4: Security Framework (Industrial Internet Consortium (IISF) 2016)
- Industrial Internet of Things, Volume G1: Reference Architecture (Industrial Internet Consortium (IIRA) 2016)

SOLUTION APPROACHES

Solution Approach

Controller and Manufacturing Security Enforcement Device (MSED)

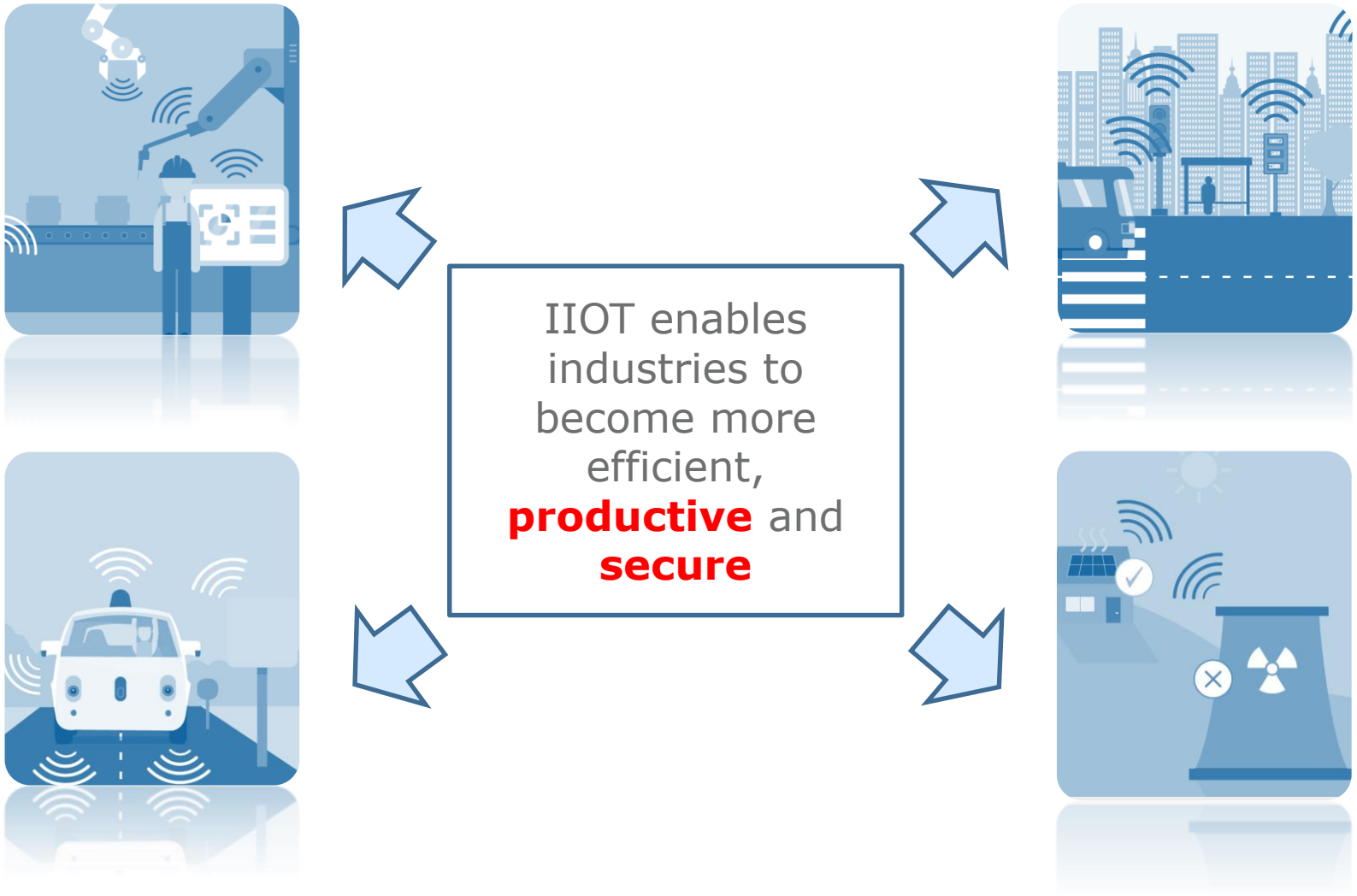


Quelle: ISBN 978-3-319-50659-3
Cybersecurity for Industry 4.0Analysis

SECURITY FOCUS IT VERSUS IIOT

SECURITY AND THE IIOT

Different Security Focus



SECURITY AND THE IIOT

libC TECHNOLOGIES

Different Security Focus

PRODUCTIVE + SECURE

Keep costs at the minimum

We will think about it later

Sophism

(argument apparently correct in form but actually invalid)

The market prefers inexpensive software with lots of features at the expense of security and reliability

SECURITY AND THE IIOT

libC TECHNOLOGIES

Different Security Focus

- Traditional security is largely centered around confidentiality

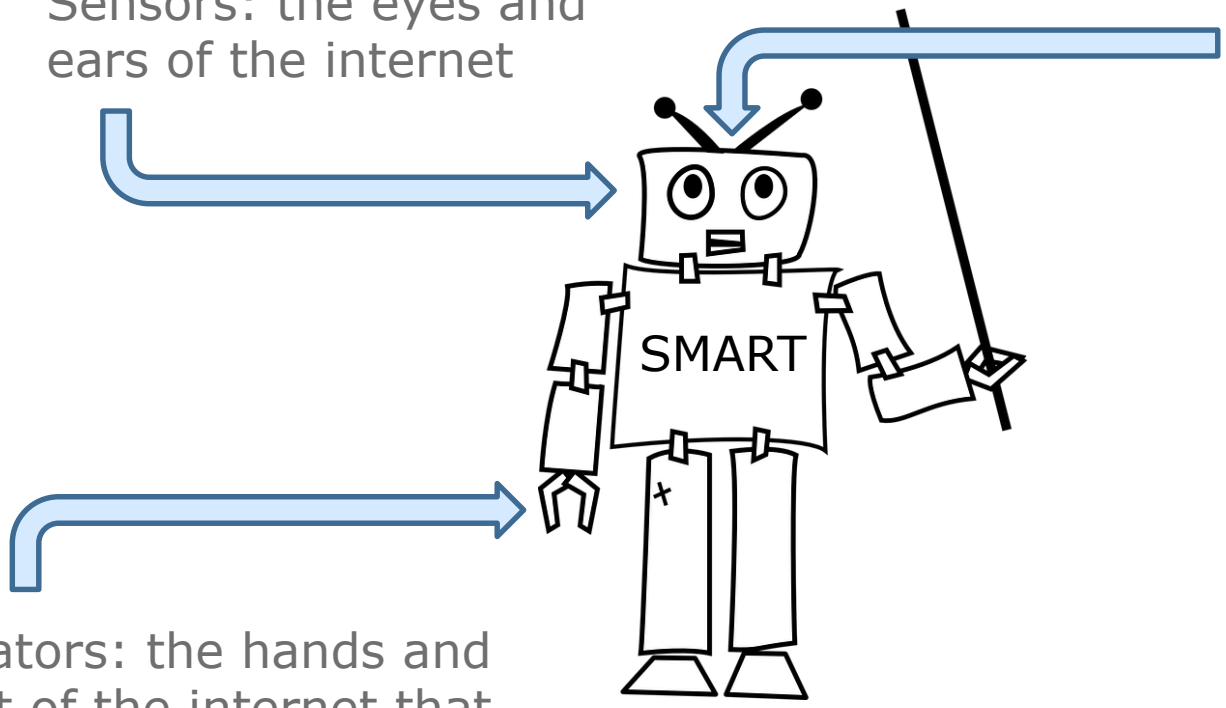
- With IIOT, integrity and availability threats are worse than confidentiality threats

«There is a difference between crashing your computer and loosing your Excel sheet and crashing your pacemaker and loosing your life»
(B. Schneier on IOT Security)

SECURITY AND THE IIOT

Sensors and Actuators

Sensors: the eyes and ears of the internet

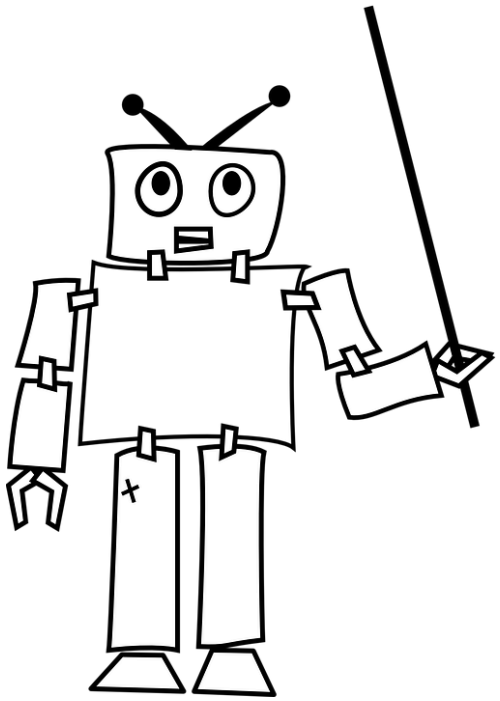


AI/SW: the «smarts» which figure out what the data means and what to do about it

Actuators: the hands and feet of the internet that which affect our environment

SECURITY AND THE IIOT

Sensors and Actuators



Connecting everything to each other will expose new vulnerabilities and IIOT is actually building a world-size robot

This robot is a combination of
- Decade old computers
- Mobile devices
- Cloud computing
- Databases
- Unpatched cheap devices

This gets dangerous: security was not part of the design

SECURITY AND THE IIOT

libC TECHNOLOGIES

Published IIOT/IOT hacks

IOT Inspector Project Princeton University

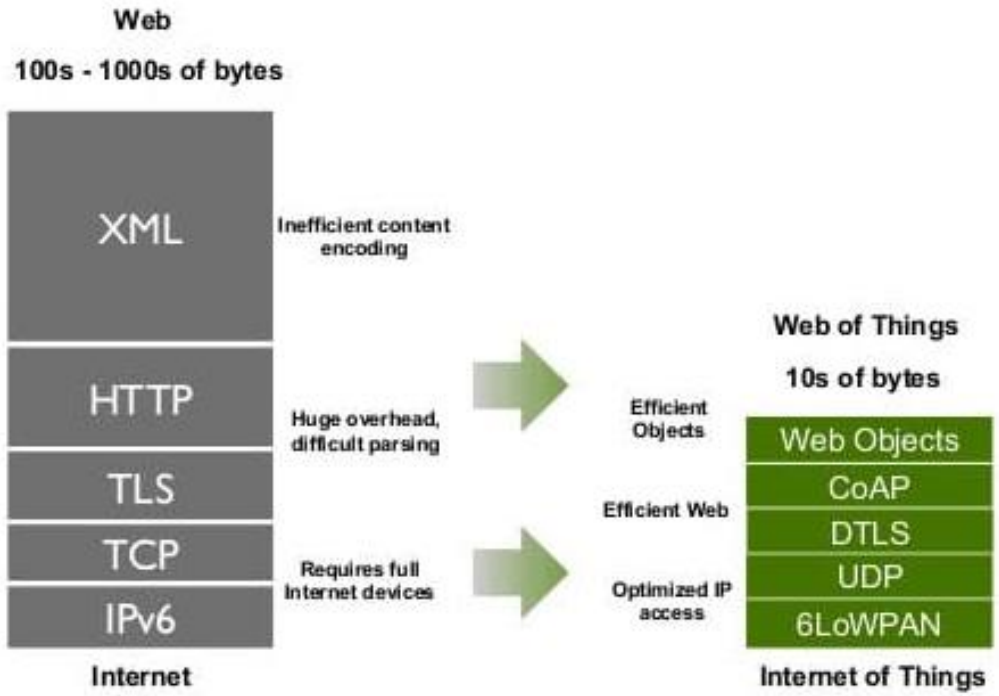
Year	Device/Product	Issues
2016 2018	Amazon's Echo speaker	Hide commands in white noise played over loudspeakers and through YouTube videos to get smart devices to turn on airplane mode or open a website. Add something to your shopping list.
2018	BMW with internet connection	Gain control of the CAN buses with the execution of arbitrary, unauthorized diagnostic requests of BMW in-car systems remotely.
2018	Phoenix Industrial Switches	Denial-of-service (DoS), execute arbitrary code, and gain access to potentially sensitive information
2018	GPON routers	Bypass all authentication on the devices
2018	Smart Home Hubs	Brute force attack DES key
2018	Western Digital Cloud	Gain root access to the devices
2018	ZyXEL modems	Access telnet and SSH daemons

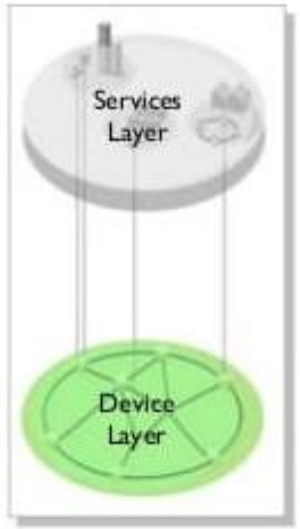
SECURITY AND THE IIOT

libC TECHNOLOGIES

IIOT/IOT Stack

1. **Infrastructure**
   (ex: 6LowPAN, IPv4/IPv6, RPL)
2. **Identification**
   (ex: EPC, uCode, IPv6, URIs)
3. **Comms / Transport**
   (ex: Wifi, Bluetooth, LPWAN)
4. **Discovery**
   (ex: Physical Web, mDNS, DNS-SD)
5. **Data Protocols**
   (ex: MQTT, CoAP, AMQP, Websocket, Node)
6. **Device Management**
   (ex: TR-069, OMA-DM)
7. **Semantic**
   (ex: JSON-LD, Web Thing Model)
8. **Multi-layer Frameworks**
   (ex: Alljoyn, IoTivity, Weave, Homekit)





SECURITY AND THE IIOT

libC TECHNOLOGIES

Organizations

- ETSI Connecting Things Cluster
- IETF CoRE working group, 6lowpan working group, ROLL working group
- IEEE IoT "Innovation Space"
- OMG Data Distribution Service Portal
- OASIS MQTT Technical Committee
- OGC (Open Geospatial Consortium)
- IoT-A
- OneM2M
- OSIOT
- IoT-GSI (Global Standards Initiative on Internet of Things)
- ISA International Society of Automation
- W3C
- EPC Global
- IEC
- RRG (Routing research group)
- HIPRG (Host identity protocol research group)

Alliances

- Eclipse Paho Project
- OpenWSN
- CASAGRAS
- AllSeen Alliance
- IPSO
- Wi-SUN Alliance
- OMA (Open Mobile Alliance)
- Industrial Internet Consortium

SECURITY AND THE IIOT

libC TECHNOLOGIES

Click here to kill eveyone

(Next Bruce Schneier Book on IIoT - September 2018)

SECURITY AND THE IIOT SOLUTION APPROACHES

Solution Approaches

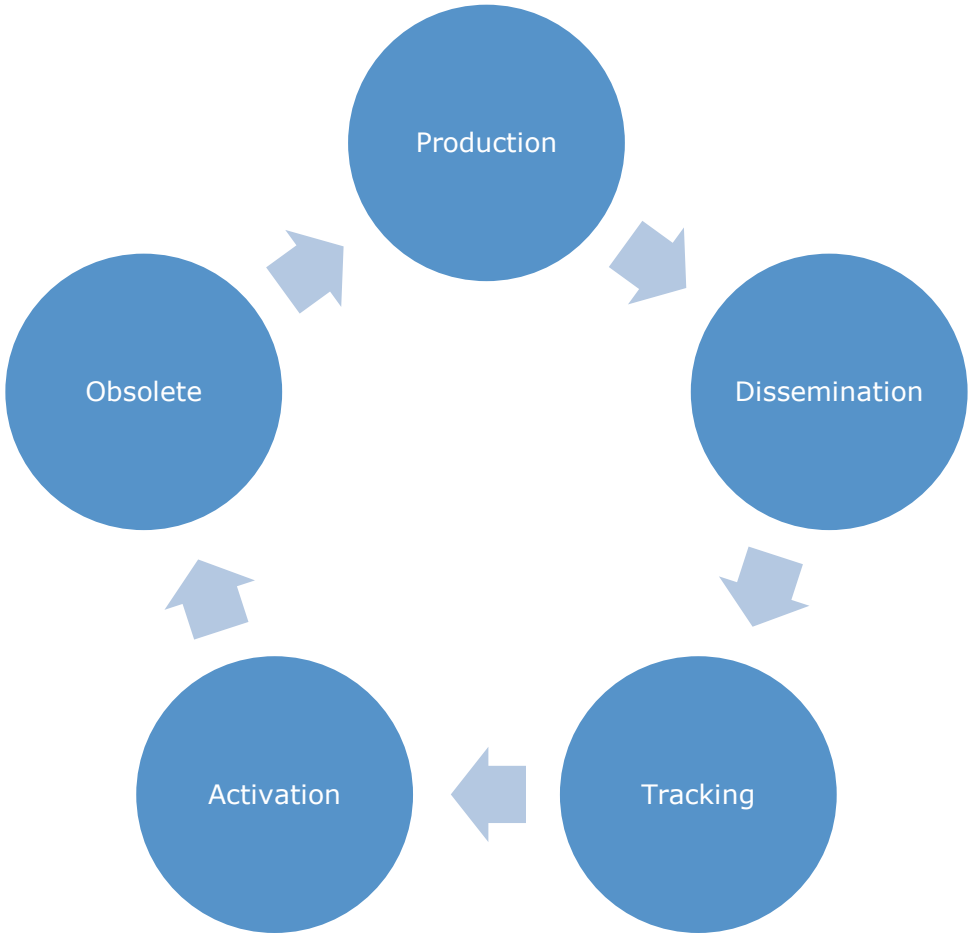
Key Management – Primus HSM

- Primus HSM embedded Key Management Service which delivers robust hardware based centralized key management backed up by strong cryptography to protect your business processes.
- Addresses large scale cryptographic key management life-cycle, online hardware-to-hardware key distribution, tamper proof audit as well as usage logs for compliance with standards.
- Integrate with the standard Primus HSM backup and replication mechanisms by securing all keys and objects directly in hardware on the HSM partition.
- Reduce operational overhead, increase security: no more licensing, maintenance and support of dedicated systems such as database servers, application and archive servers, monitoring and controls systems.

Solution Approaches

Key Management – Primus HSM

1. HW sym/assy. batch production which adresses
    a. industrial production lots
    b. HSM to device secure key injection
    c. Secure key storage. Keys never in the clear
2. Geographical dissemination of key material to remote HSM
3. Association of produced keys with devices
    a. Each key can have one or more attributes associated ith a device: lot/serial/date etc
4. Each key has a status which can be individually set: produced, associated, revoked etc
5. Key management performed via web UI or service interface
6. Key production and management is role based



Solution Approaches

libC TECHNOLOGIES

References

- https://www.postscapes.com/internet-of-things-protocols
- https://arxiv.org/pdf/1804.04159.pdf
- https://iot-inspector.princeton.edu/
- https://www.schneier.com/blog/archives/2017/02/security_and_th.htm
- https://codecurmudgeon.com/wp/iot-hall-shame

… yes we can

TEMET
end-to-end IT security

libC
TECHNOLOGIES

Thank you for your attention

TEMET AG
Basteiplatz 5
8001 Zürich
+41 44 302 24 42
info@temet.ch
www.temet.ch

libC SA
Avenue d'Ouchy 18
1006 Lausanne
+41 21 550 1562
info@libc.ch
www.libc.ch