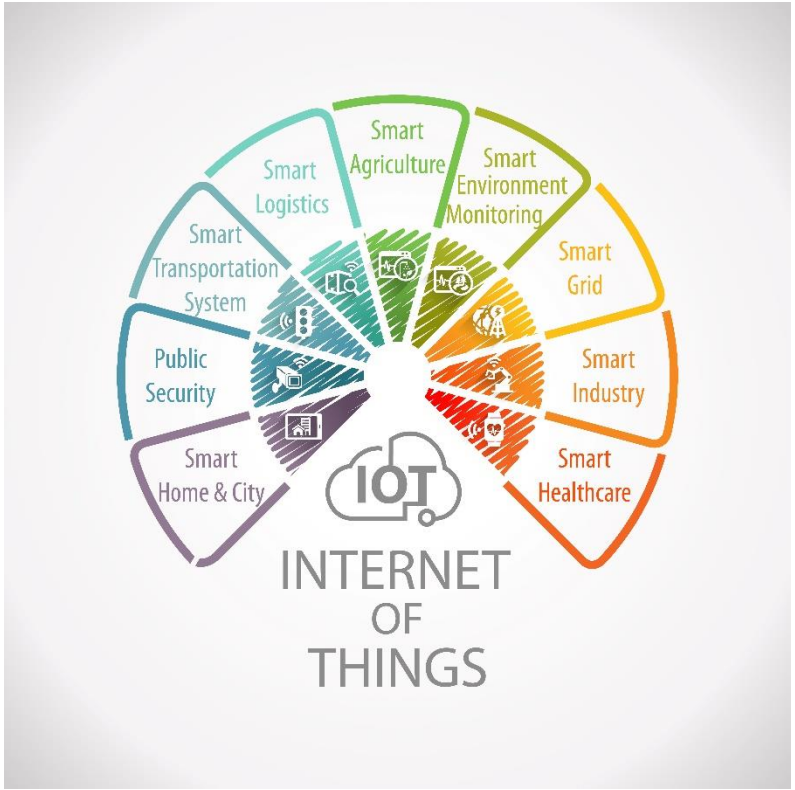
Datensicherheit und IoT

Michael Isler
Dr. iur., Attorney at Law, Partner
Walder Wyss

Nicolas Grunder
Chief Counsel Digital & Data Privacy
ABB

Was ist das Internet of Things?

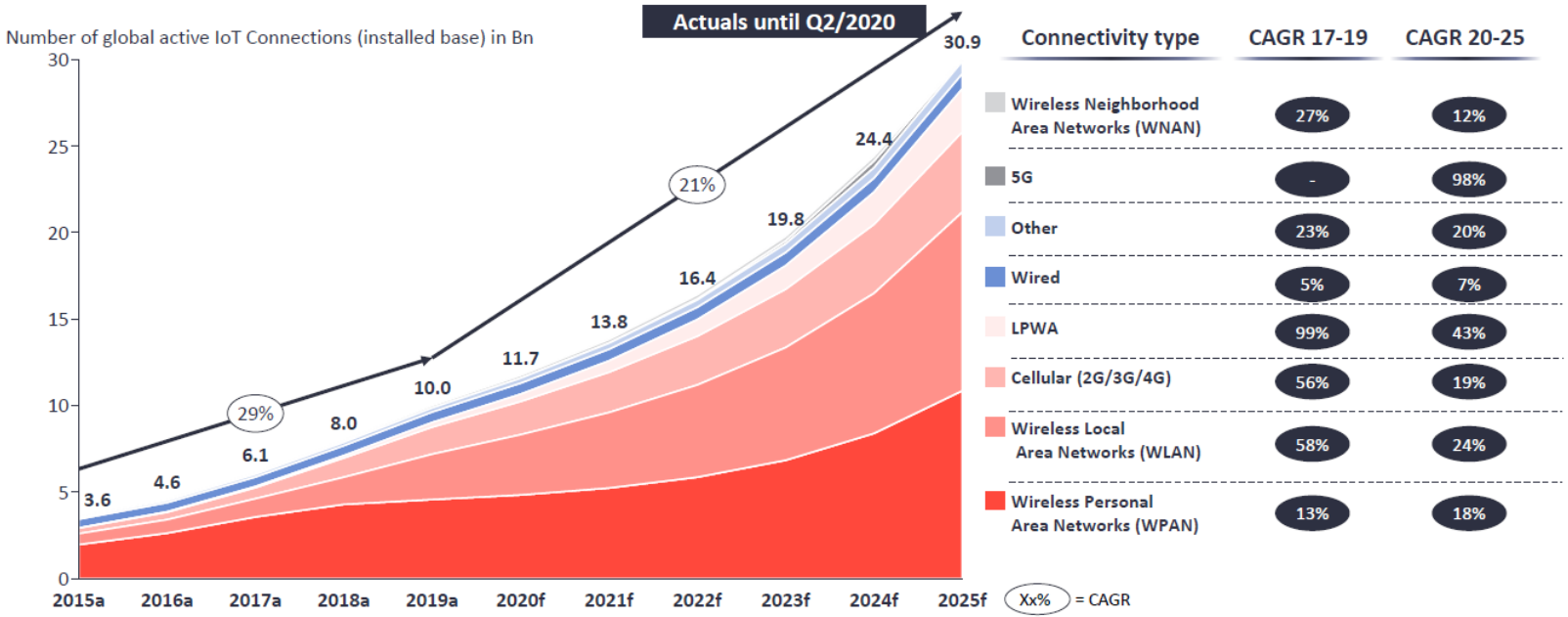
- Netzwerk von physischen (und virtuellen) Objekten, in die Sensoren, Software und andere Technologien eingebettet sind
- Jedes dieser Objekte hat seine eigene digitale Identität
- Objekte können kommunizieren und Daten austauschen
- Anwendungsbereich nahezu unbeschränkt – alle Objekte in allen Sektoren könnten vernetzt werden



Relevanz des Internet of Things

Global IoT Market Forecast [in # of connected IoT devices]

10.3Bn in 2019



Connectivity type	CAGR 17-19	CAGR 20-25
Wireless Neighborhood Area Networks (WNAN)	27%	12%
5G	-	98%
Other	23%	20%
Wired	5%	7%
LPWA	99%	43%
Cellular (2G/3G/4G)	56%	19%
Wireless Local Area Networks (WLAN)	58%	24%
Wireless Personal Area Networks (WPAN)	13%	18%

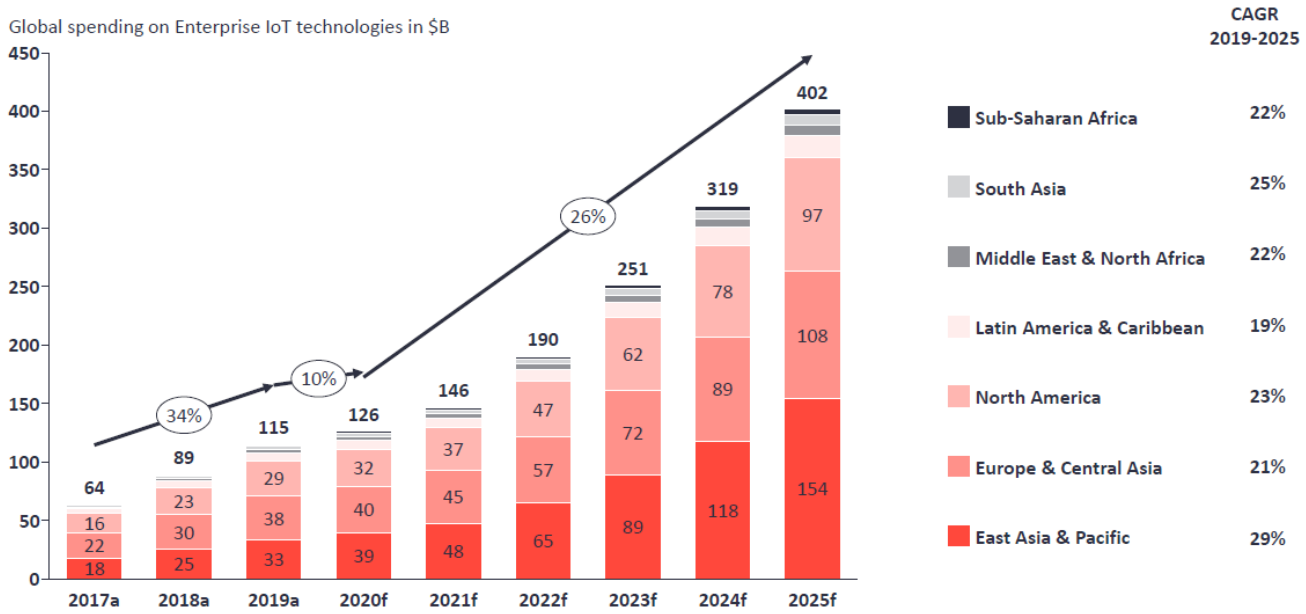
Note: IoT Connections do not include any computers, laptops, fixed phones, cellphones or tablets. Counted are active nodes/devices or gateways that concentrate the end-sensors, not every sensor/actuator. Simple one-directional communications technology not considered (e.g., RFID, NFC). Wired includes Ethernet and Fieldbuses (e.g., connected industrial PLCs or I/O modules); Cellular includes 2G, 3G, 4G; LPWAN includes unlicensed and licensed low-power networks; WPAN includes Bluetooth, Zigbee, Z-Wave or similar; WLAN includes Wi-fi and related protocols; WNAN includes non-short range mesh, such as Wi-SUN; Other includes satellite and unclassified proprietary networks with any range.
Source: IoT Analytics Research 2020

Source: IoT Analytics: State of IoT, FALL 2020 Report

Relevanz des Internet of Things

Global IoT Enterprise Market Forecast by region – Revenue in $B

East Asia & Pacific is expected to grow with a CAGR of 29% until 2025 and be biggest market by 2021



IoT Analytics defines the Internet of Things(IoT) as a network of internet-enabled physical objects. Objects that become internet-enabled (IoT devices) typically interact via embedded systems, some form of network communications, as well as a combination of edge and cloud computing. The data from IoT-connected devices is often (but not exclusively) used to create novel end-user applications. Connected personal computers, tablets, and smartphones are not considered IoT, although these may be part of the solution setup. Devices connected via extremely simple connectivity methods such as RFID or QR-codes are not considered IoT devices. Source: IoT Analytics Research

Source: IoT Analytics: State of IoT, FALL 2020 Report

Was ist das Industrial Internet of Things?

Anwendung von IoT im verarbeitenden Gewerbe

- Vernetzung industrieller Assets
- Verknüpfung von Operational Technology (z.B. DCS, SCADA, PLC)* mit Information Technology
- Bisher unerreichte Verfügbarkeit von Daten – überwinden von Datensilos

- Internet connected devices
- Ad-hoc connected devices
- Connected systems

* DCS – Distributed control system; SCADA – Supervisory control and data acquisition; PLC – Programmable logic controller

Asset Performance Management – an IIoT use case

Predictive maintenance

Why?

- Reduce total cost of ownership
- Maximize uptime
- Avoid energy waste
- Improve safety

How?

- Online condition monitoring
- Offline data assessment and analysis
- Site and multi-site asset health analysis
- Simulation

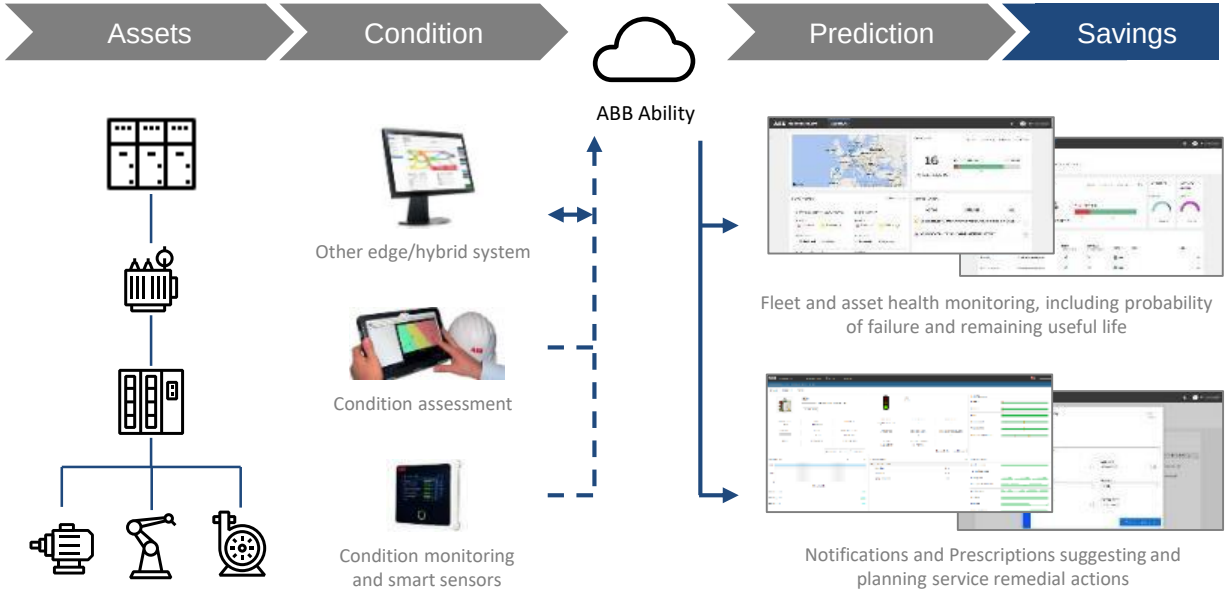
Asset condition data collection

Assets in the plant can be monitored and conditions can be tracked.

ABB Ability™: gain insights on assets

Asset health dashboard

Predictive analytics to optimize maintenance and improve availability and reliability



Was wir unter Datensicherheit verstehen

- Vertraulichkeit - Schutz vor nicht autorisiertem Zugriff
- Integrität - Schutz vor Datenmanipulation
- Verfügbarkeit - Schutz vor (temporärem oder dauerhaftem) Datenverlust

Warum Datensicherheit für das IoT zentral ist

- Daten als Kernelement von IoT basierten Geschäftsmodellen
- Dilemma Sicherheit vs Kosten? -> Bedenken zur Datensicherheit können ein Haupthindernis bei der Umsetzung von IoT Geschäftsmodellen sein
- Regulatorische Vorgaben
- Haftungs- und Reputationsrisiken
- Schutz von Knowhow und IP
- Zunehmende Frequenz von Cyber Angriffen sowie Aggressivität und Gewandtheit der Angreifer
- Verknüpfung mit realer Welt beschlägt nicht nur Datensicherheit, sondern auch Produktsicherheit

Warum Datensicherheit im IoT herausfordernd ist

Schulthess FORUM

Vertikale Zersplitterung

Rechtliche Einflussfaktoren (Haftung, Sanktionen)

Hersteller
- Produziert und vertreibt IoT Devices:
  - Konnektivität
  - Kosten
  - Convenience

Betreiber
- Setzt IoT-Systeme ein:
  - Mehrwert
  - Zuverlässigkeit
  - Betriebliche Effizienz

Nutzer
- Greift auf IoT-Systeme zu:
  - schnell
  - sicher
  - günstig

Horizontale Zersplitterung

- Vernetzung / offene Ökosysteme:
  - Zahlreiche Einfallstore für Angriffe
  - Verknüpfung von OT und IT
  - Hohe Reichweite von Angriffen
- Massenphänomen:
  - Stark steigende Anzahl IoT Objekte
  - Big Data

IoT als Ziel und Mittel von Angriffen

Warum Datensicherheit im IoT ein rechtliches Thema ist

Schulthess FORUM §

Treiber der Verrechtlichung	Rechtsfolgen bei Verletzung der Datensicherheit
Verletzung der Datensicherheit als unternehmerisches Risiko	- Organhaftung - Vertragliche Haftung - Produkthaftung

Regulierung der Datensicherheit:
- Datenschutz
- Sektorielle Aufsicht (z.B. Finanzinstitute)
- Sektorielle Produktregulierung (z.B. Medtech, Telekom)
- Technologiespezifische Regulierung (z.B. Kalifornien: Security of Connected Devices Act)
	- Meldepflichten
	- Informationspflichten
	- Sanktionen:
	  - Bussen
	  - Verwaltungsmassnahmen
	- Verlust der Verkehrsfähigkeit von Produkten

Normung der Datensicherheit: - Internationale Standards (best practices)	- Vertragliche Haftung - Produkthaftung

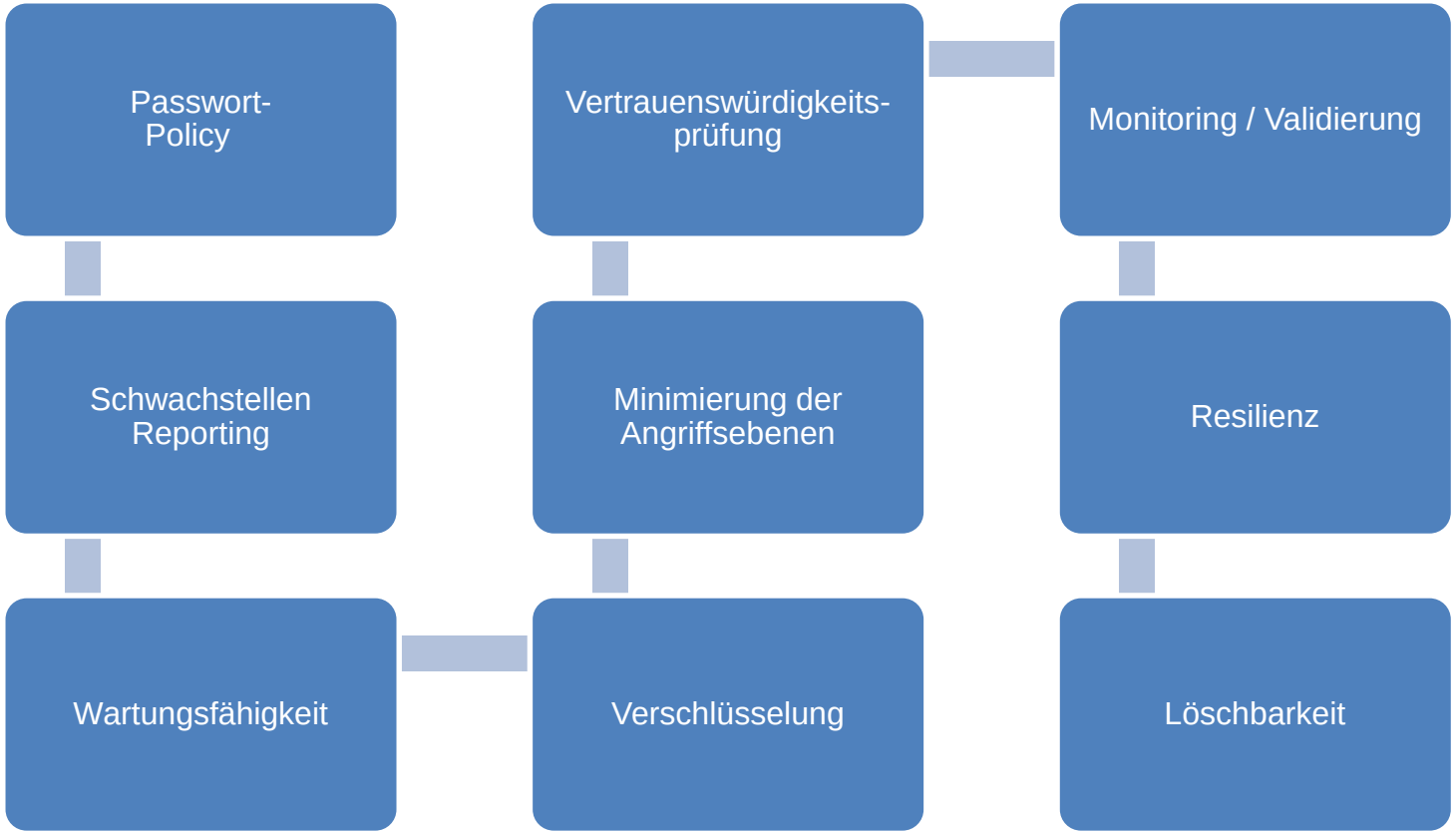
Wer für Datensicherheit im IoT verantwortlich ist

Akteur	Anknüpfungspunkt	Präventionskatalog	Reaktionskatalog
Hersteller	“Inverkehrbringen”	Produktbeobachtung Security by design Produktzertifizierung Produktzulassung	Meldepflichten bei Schwachstellen Produkthaftung Rückruf Vertriebsverbote
Betreiber	“Verwenden, Anwenden, Bereithalten” “Bearbeiten”	Produktbeobachtung Privacy by design DFA TOMs Audits (Pentests) Betriebsbewilligungen	Meldepflichten Sanktionen Betriebsverbote
Nutzer	“Bearbeiten” “Nutzen”	Acceptable use policies Sorgfaltspflichten	Schadloshaltung Verlust von Ansprüchen

Regulierungstrends

- **Staatliche Normen:**
  - Entwicklung des Personendatenschutzes zur umfassenden Daten-Governance
  - Sektorspezifische Regulierung für kritische Infrastrukturen
  - Vorverlagerung des Datenschutzes auf Hersteller (Security by Design)
- **Standards:**
  - Konkretisierung verfahrensorientierter Standards auf Ebene des “Bearbeitens”
  - Konkretisierung technischer Standards auf Ebene des “Inverkehrbringens”
  - Initiativen von Industriekonsortien
  - Verdichtung zu rechtsverbindlichen Standards / Zertifizierungen

Technische Cybersicherheit für Consumer IoT Devices: ETSI EN 303 645



Rechtliche Herausforderungen bei Sicherheitsvorfällen

Schulthess FORUM

Prävention

- Policies/Standards
- Incident Response Pläne
- Einbezug externer Leistungserbringer
- Beziehung zu relevanten Behörden
- Security in Design, Development und Operations
- Versicherung
- Training, Schulung
- IoT Sicherheit spezialisierte Resourcen

Spezifischer Fokus auf IoT Szenarien

Reaktion

- Technische und forensische Untersuchung (intern/extern)
- Meldepflichten (Regulator(en), Individuen)
- Kommunikation (intern/extern)
- Versicherung (Obliegenheiten)
- Behebung und Schadenminderung
- Vertragliche Pflichten
- Untersuchungen und Ermittlungen durch Behörden
- Ansprüche Dritter und Prozesse

Schlussbetrachtung

- Ökosystem-Architektur macht das IoT zum attraktiven **Ziel und Mittel** von Angriffen
- **Datensicherheit ist zentral** für die weitere erfolgreiche Entwicklung des IoT
- Die **Regulierungsdichte** wird zunehmen – sowohl auf der Ebene der Hersteller wie auch auf der Ebene der Betreiber/Nutzer, mit gegenseitigen Reflexwirkungen
- Geopolitische Trends deuten auf zunehmende **Datenlokalisierungstendenzen** und sich potentiell widersprechende Anforderungen hin

Danke für Ihre Aufmerksamkeit

Kontakt
Dr. Michael Isler
Walder Wyss
Seefeldstrasse 123
Postfach
8034 Zürich
058 658 55 15
michael.isler@walderwyss.com

Kontakt
Nicolas Grunder
ABB
nicolas.grunder@ch.abb.com