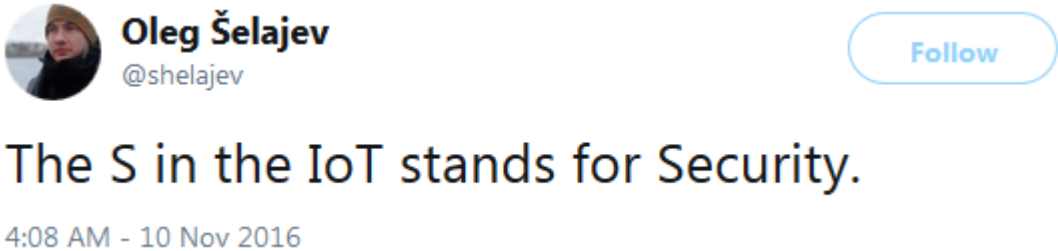
Prof. Dr.-Ing. Jochen H. Schiller
Computer Systems & Telematics @ Freie Universität Berlin
Einstein Center Digital Future

Security aspects in the Internet of Things –
think of risks and side-effects in advance!

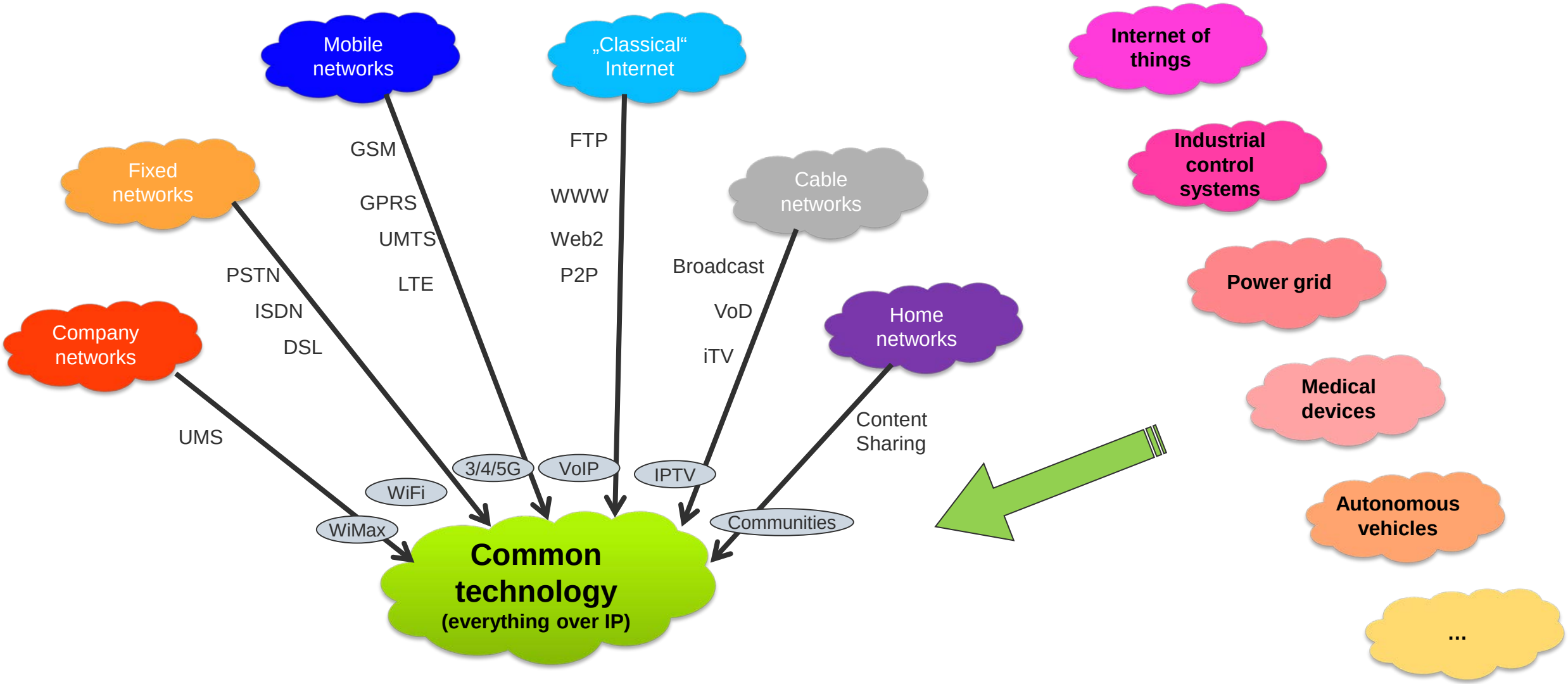
Leibniz-Konferenz „Lokalisierungstechniken für IoT, Telematik und Industrie 4.0“

22.-23. November 2018



(lead developer, Oracle Labs)

New: Convergence with new applications



Current Hype: The Internet of Things

Cars, animals, people, monitoring

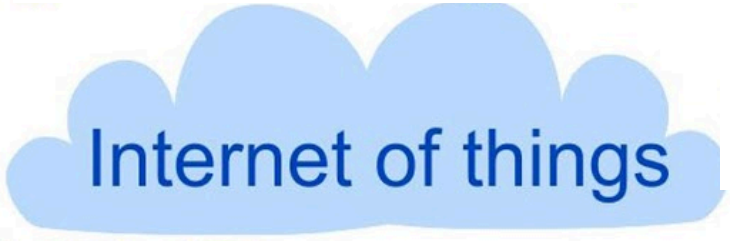
Agriculture

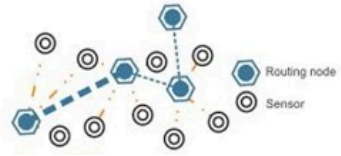
Energy

Security, surveillance

Building automation

Embedded systems





Machine-to-machine com., Sensor networks

Everyday things

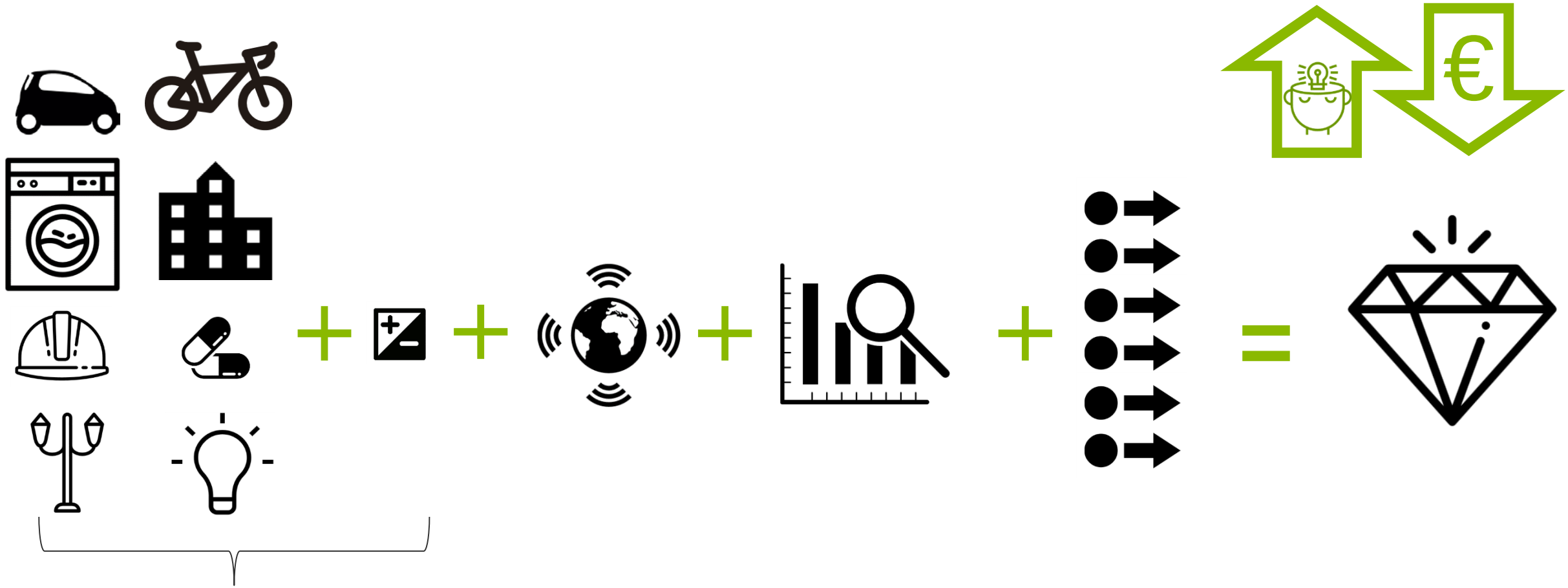
Smart Home / City

Health care

Source: The Telecare Blog, thetelecareblog.blogspot.de, 24.10.14

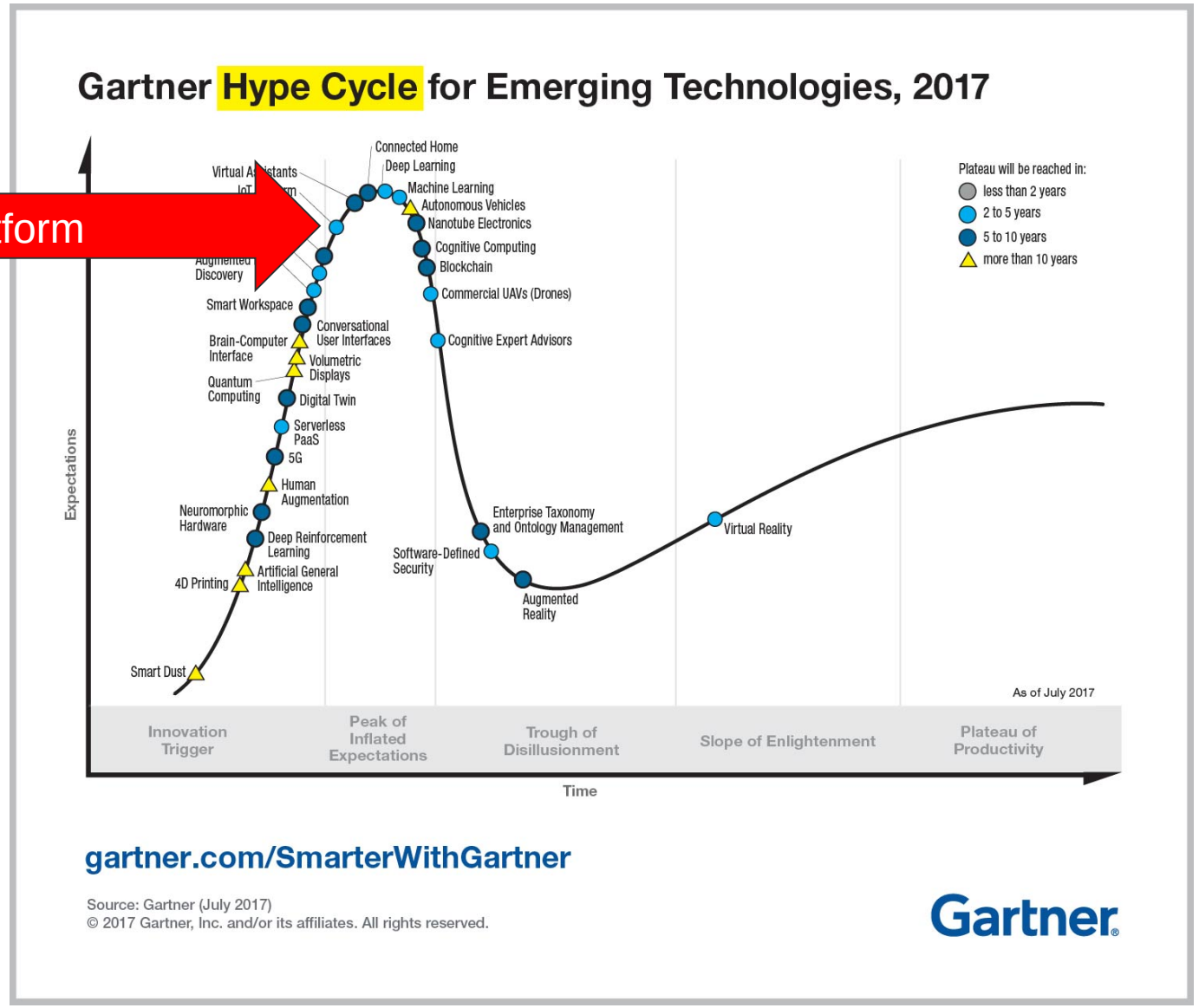
One common technology for everything!

The Internet of Things: Drivers



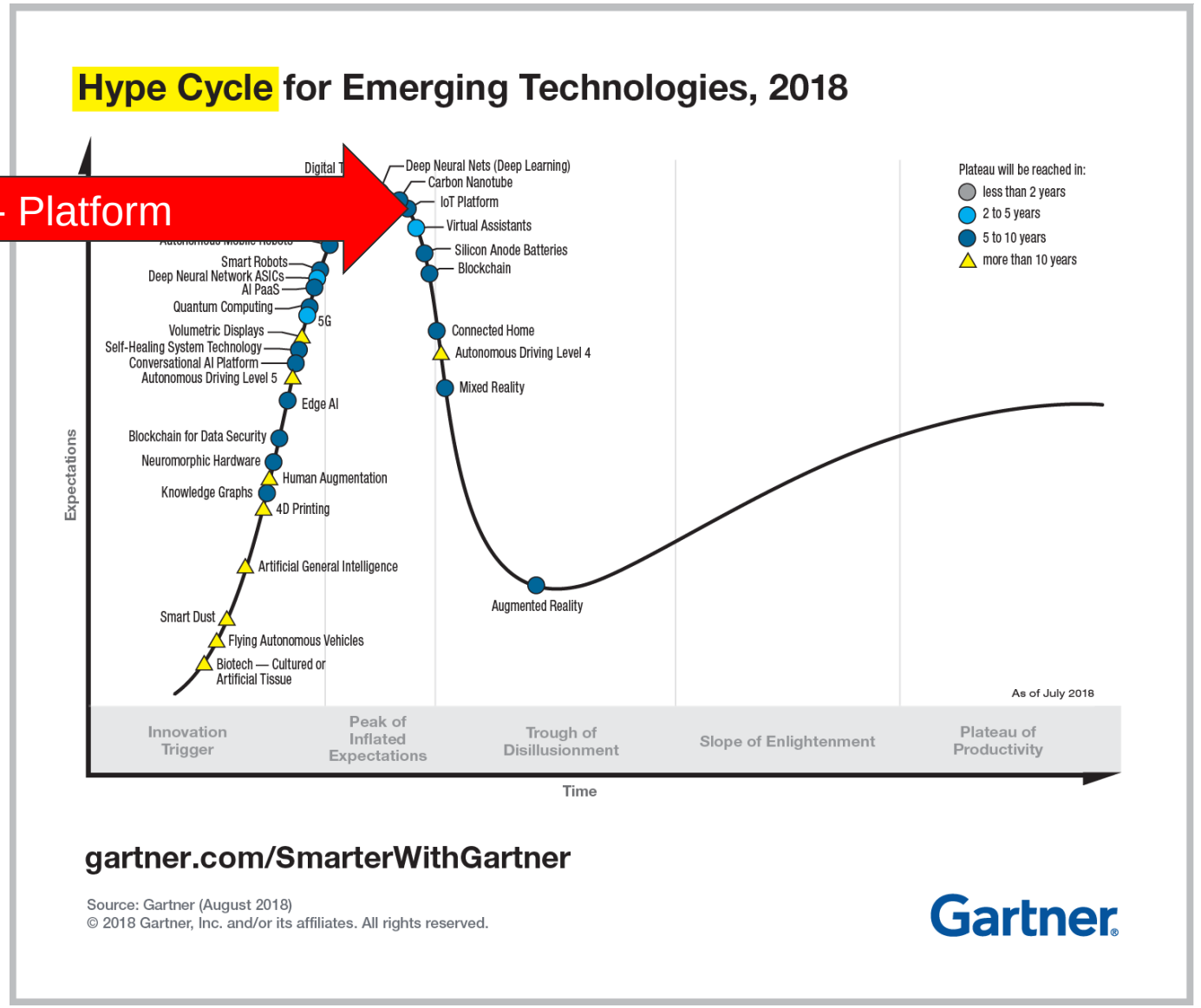
Current Hype

IoT - Platform



Current Hype

IoT - Platform



Internet of Things – is it really new?

1991: Mark Weiser

- *The Computer for the 21st Century,* ubiquitous use of IT, disappearing computer

1999: Kevin Ashton

- Coined the term *Internet of Things* in the context of logistics/supply chains, enhanced radio tags

Network of inter-connected, embedded mini computers

- Collecting and distributing data, Internet technologies as common platform, comprises enhanced RFIDs, wireless sensor networks, actors, mobile communications, “smart” objects, cyber physical systems, …
- Next generation embedded systems + wireless sensor networks + actors + Internet protocols + …

Already today, there are many more communicating systems compared to people – more than 10 billion

In the future:

- Some estimate > 25 billion in 2020, others estimate > 50 billion – ok, there will be MANY…
- As always great expectations: 202x - 1 trillion $ revenue p.a. estimated by GSMA

Internet of Things: What is really new?

Miniaturization

- MEMS, *smart everything*, embedded objects

Availability of many "new" technologies

- *Cloud/edge computing*, *big data*, IPv6, 6LoWPAN, *content centric networking*, adapted operating systems…

Restricted devices

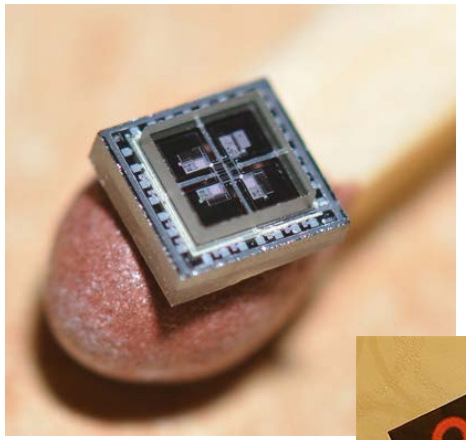
- At least at the beginning wrt. Firewalls, Antivirus, …
- BUT we all use the same or similar protocols and interfaces

Complexity

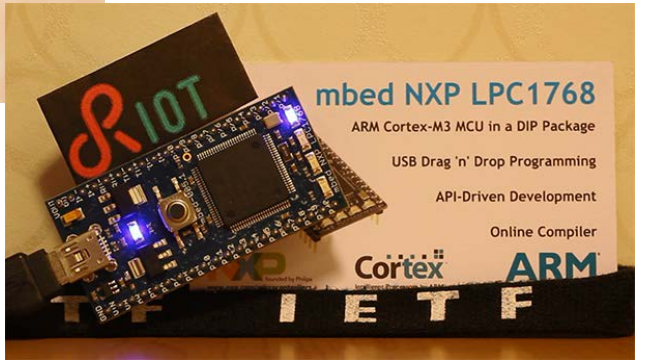
- function(#nodes, topology, traffic pattern, stability, legacy, ?)

➔ **All this comes together now!**

- Possibilities and vulnerabilities…



© iecetech.org



Source: RIOT OS, www.riot-os.org
1,5 kByte RAM, 5 kByte ROM, real-time, multi-threaded

Security risks in the Internet of Things

Facts

- Variety of platforms and manufacturers
- Very long life-cycles/short product cycles
- Low interest in security
- Low-performance devices
- Unclear liability

Higher risks

- Things are directly connected to values
  - Cameras → privacy, situation monitoring
  - Doors → admission control
  - Cars, medical devices → personal safety
  - Valves → industrial production
  - …

Compromised things can cause much higher damage compared to the majority of classical systems (e.g., PC on the desktop)

Examples for the variety– RIOT OS (www.riot-os.org)

Architectures	Boards
AVR	Airfy Beacon
ARM7	Arduino Due, Mega 2560, Zero
Cortex-M0	Atmel samr21-Xplained Pro
Cortex-M0+	f4vi
Cortex-M3	mbed NXP LPC1768
Cortex-M4	Micro::bit
Cortex-M7	Nordic nrf51822, nrf52840 (DevKit)
ESP8266	Nucleo boards
MIPS32	senseBox
MSP430	STM32F4DISCOVERY
PIC32	TelosB
X86	Texas Instruments cc2538 Developer Kit, EZ430-Chronos,UDOO Board
…	Waspmote-pro
	Zolertia Z1
	…

Right now RIOT supports more than 130 different hardware platforms

Security risks in the Internet of Things

© GE Lighting 2017

Even the simplest things are complex – although their function may be trivial

- The networked light switch includes operating system, communication software, web server etc.
- A simple valve uses (secured) connections, security algorithms, memory management etc.

Security is difficult for an application developer **to understand** and to achieve

- Focus is on the functionality of a product
- Use of (hopefully available) security functions of the underlying platform
- Platform developer do not no the application, cannot really prove security

Many more **tests/evaluations** are **needed**

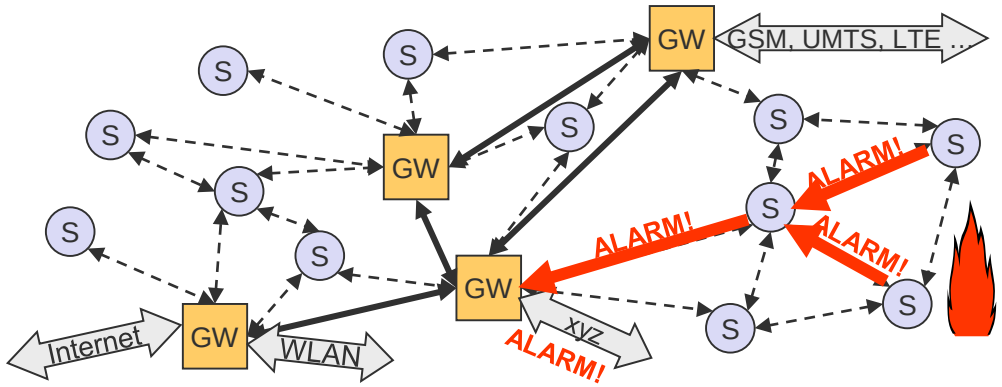
- In reality way too many combinations of platforms, applications, products
- Additionally, life-cycle vs. product cycle plus scalability of all approaches

Chances – Challenges – Risks

Fact: many new developments based on miniaturization

Chances

- Lower costs due to unified technologies (everything „speaks“ Internet)
  - Avoids vendor lock-in, uses COTS components, benefits from general IT improvements, simpler interfaces integration of commercial/public systems, …
- Improved situation awareness due to higher resolution of real-time data
  - increased number of simpler sensors, mobile systems, pre-processing, …
- Better interaction based on distributed actors
  - Actors can directly interact with environment, local control loops, …
- Robustness due to semi-autonomous systems
  - Lower failure rates due to edge computing, simplified redundancy, decentralization, …
- …



Networked systems – Things communicate with things (and humans)

Source: Spiegel Online

IoT Challenges - what is really new

- „The Internet of Things (IoT) will present **new attack surfaces** as most of the IoT devices do not offer integrated security and, furthermore, it is **often not possible to update** security mechanisms later on. If compromised, these devices may serve as a backdoor for hackers to enter clinical IT systems – undiscovered for months.“ (DarkReading, www.informationweek.com, 22.12.16)

- Large variety of systems (hardware, interfaces, operating systems), typically “weak”
- Real interaction with the environment (CPS)
- Longer (but also much shorter!) life cycles, deeply embedded
- Complete unclear patching/updating strategy, responsibility
- SME problem: do they know what they do?

- How to integrate today the security needed in 30 years?

- First steps in the right direction: certified IoT devices and liability

Typical attack scenarios with things

28.2.2018: OMG-Botnet uses IoT devices as proxys

- https://www.heise.de/security/meldung/OMG-Botnet-macht-aus-IoT-Geraeten-Proxys-3982037.html

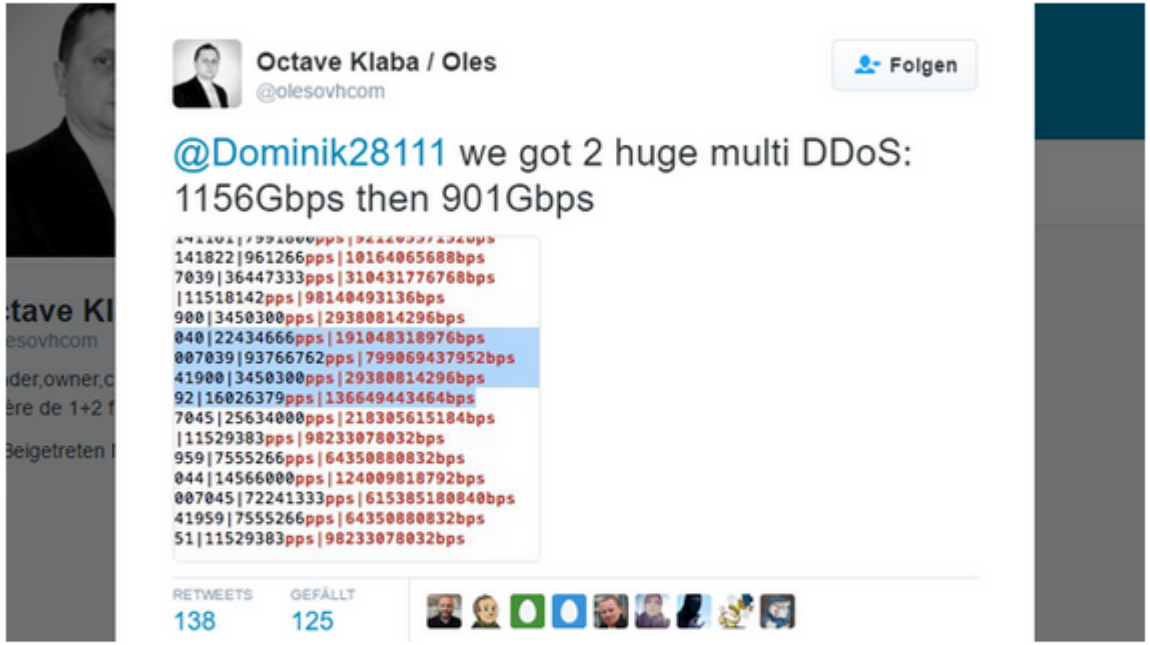
„There are more than 5.3 million vulnerable IoT devices in Spain. More than 493.000 in Barcelona, which currently hosts the MWC.“ (heise, 03/2017)

Erst vergangene Woche brach die Internetseite des Security-Bloggers Brian Krebs unter massiven DDoS-Attacken zusammen und der Anti-DDoS-Dienst Akamai kapitulierte vor den Angriffen. In diesem Fall wurden Spitzen von 620 Gigabit die Sekunde gemessen.

Auch bei diesem Übergriff soll ein Botnetz bestehend aus mehr als einer Million Geräte aus dem Internet der Dinge (IoT) die Kapazitäten für den Angriff zur Verfügung gestellt haben. Klaba vermutet, dass die Attacken auf OVH vom gleichen Botnetz

Rekord-DDoS-Attacke mit 1,1 Terabit pro Sekunde gesichtet

29.09.2016 10:25 Uhr – Dennis Schirrmacher vorlesen



(Bild: Screenshot)

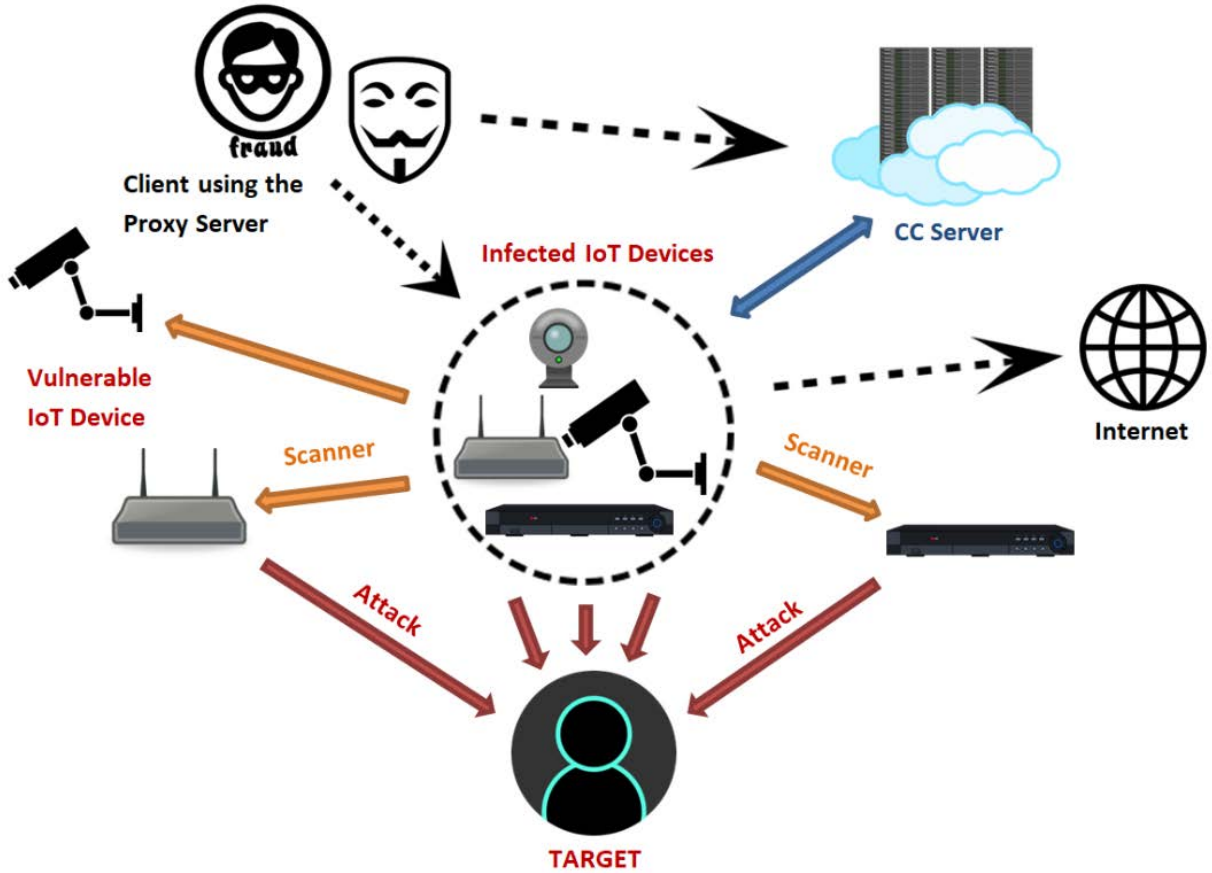
Höher, schneller, weiter: Ein stetig wachsendes IoT-Botnet soll die Server eines französischen Web-Hosters mit gewaltigen Datenmengen bombardiert haben. Dabei handelt es sich offensichtlich um den bisher größten dokumentierten DDoS-Angriff.

http .html

Typical attack scenarios with things

28.2.2018: OMG-Botnet uses IoT devices as proxys

- https://www.heise.de/security/meldung/OMG-Botnet-macht-aus-IoT-Geraeten-Proxys-3982037.html

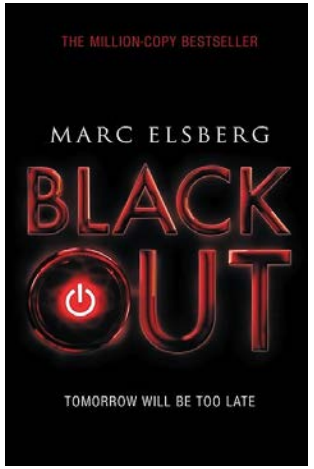


https://www.fortinet.com/blog/threat-research/omg--mirai-based-bot-turns-iot-devices-into-proxy-servers.html

Example: Photovoltaics

Headline: Cyber-attack on solar panels could shut down power grids via domino effect

- The Horus Scenario (https://horusscenario.com/) – see also the 50.2 Hz problem, Blackout, …
- 30-50% solar power in Germany – switching this on and off repeatedly most likely brings down the power grid
- Many vulnerabilities found in the inverters – and reported to the manufacturer before disclosure at SHA2017



Interesting answers of the manufacturer (https://www.sma.de/fileadmin/content/global/specials/documents/cyber-security/Whitepaper-Cyber-Security-AEN1732_07.pdf)

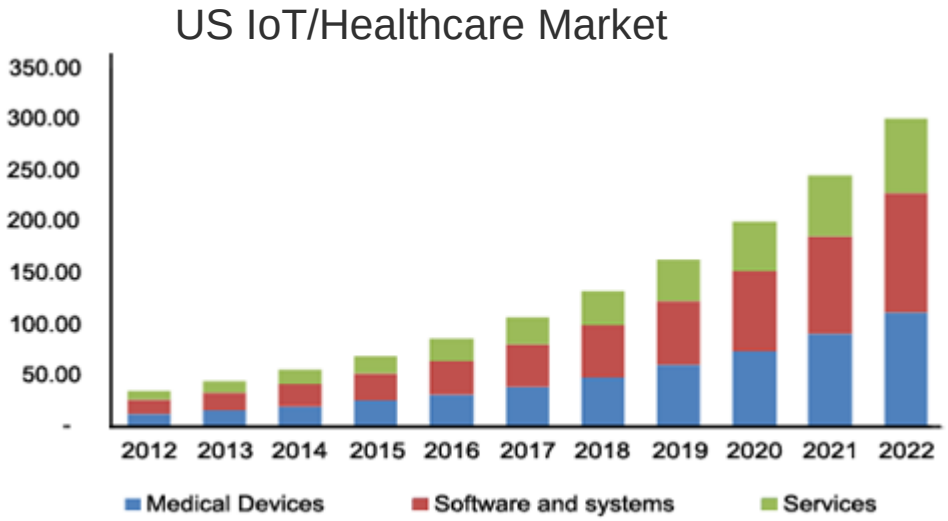
- Only some models are affected, all the others use “the latest security standards”
- **Any device not connected to the Internet is not affected.**

BUT:

- DC/AC inverters have to be remotely controllable by the power grid operator – it’s the law
- Additionally, the webservice some manufacturers use operates on unencrypted data, exchanges usr/pwd for Internet connectivity including the PIN for the SIM to the portal operator for the PV portal – it’s the reality …
- Why? Don’t know …

IoT and Healthcare

- “Global Internet of Things (IoT) in Healthcare Market is expected to reach nearly $410 billion by 2022” (GrandView Research).
- Collateral damage possible
- But also direct attacks ➔ **MEDJACK** (medical device hijack)
- Unsecure systems „inside“: HW, SW, building automation/IoT, door locks, WLAN, etc. but also the patients
- Updating/patching devices difficult or simply not allowed
- Firewalls often cannot detect “old” attack schemes



The devices vulnerable to MEDJACK … include “diagnostic equipment (PET scanners, CT scanners, MRI machines, etc.), therapeutic equipment (infusion pumps, medical lasers, surgical machines), life support equipment (heart/lung machines, medical ventilators, extracorporeal membrane oxygenation machines and dialysis machines) and more.”

Internet of things in safety-critical applications?

Important **differences** wrt. “classical” mobile or fixed networks

- Higher degree of inter-connectivity
  - Things communicating with other things, ad-hoc, spontaneous
- Many more interfaces
  - Fixed and wireless, always on
- Many more “network operators” and vendors with less experience compared to classical systems
  - Installed and operated at home but also in industrial production lines – but often not by networking professionals

Similarities

- Operating systems and communication protocols
- Enough computing power (for the application – but also for attacks)

Is there any hope that things will get better wrt. attacks, threats, vulnerabilities etc.?

- Blackouts, viruses, software bugs, insufficient updates, cyber crime, …

Can we control the complexity of our (IoT) networks?

NO

- If we continue to connect “just because the interface fits somehow”
- Yes, many new applications, but we do not know all side-effects?

Can we *regain* control of our (IoT) networks?

NO

- If we continue to connect “just because the interface fits somehow”
- Yes, many new applications, but we do not know all side-effects?

YES

- If we go back to the classical engineering principles used in many disciplines
- Unfortunately, network “engineering” today quite often ignores basic rules
- Unfortunately, often there is no strong business case for solid engineering

Terra incognita – even for IT professionals

Many still think computer = PC

- Classical thinking of the 80ies/last century
- Quite often buzzwords only:
  - Smartphone, Phablet, Tablet, Cloud, Fog, smart grid, smart city, smart xy, **Internet of Things**, BYOD (Bring Your Own Device) etc.
  - With knowing what is really behind it!

BUT IoT means

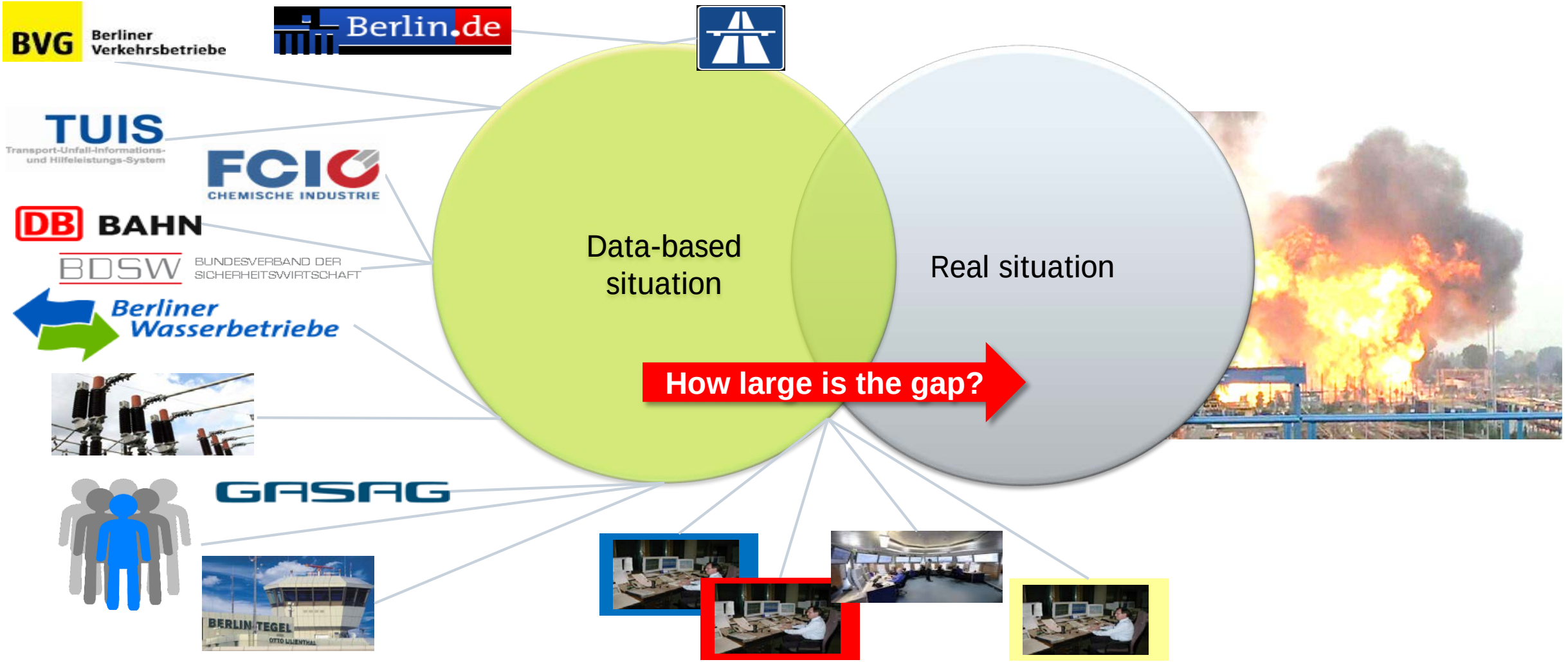
- Full-featured computer (with operating system, memory, processor, I/O, …) embedded in many “things”
  - Printer, BIOS, USB stick, lighting, batteries, keyboard, headset, glasses etc.
- „Always on“ – there is no switch to take it off-line
  - Permanent connection to the Internet and the environment possible
- Many (unknown) interfaces!!

IoT and security – a permanent process

approach: Try to avoid the loss of control, but be prepared for a complete failure

- Pure technical approaches are limited
  - Helps only with simple attackers, not useful to protect against the professionaly
  - Complete system often not understood, e.g., mobile phone/BYOD/company networks/new and unknown interfaces
- Do only things you understand
  - Better less functionality, but secure (e.g., own cloud/edge/…)
  - Fewer, simpler and understandable interfaces (e.g. VPN box instead of software client)
- Use well-known practices
  - Encrypted file systems, smart cards instead of passwords, multi-way authentication, …
  - Many best practices do exist – but have to be used!
  - See certification, ISO, BSI, …

Mind the gap between data and the real world!



Conclusion

The biggest challenges today are **not so much technical problems** as they are matters of awareness

- We have a lot of security architectures, protocols, algorithms … at hand
- But we do not really use them in a proper way! (and sometimes we don't know how to do it…)

Know what you do before you introduce IoT in safety and security critical systems!

- Otherwise history is repeating and we will (again) enter the permanent fight of patches and updates vs. abuse and attacks.

Unfortunately, right now there is **no strong business case for** manufacturers to add a ubiquitous **security** element into the development process

- It is up to the professional consumers in safety critical environments to call for sound standards and guaranteed common security settings.
- Plus legislation, certification, liability…

Localization…

- Zakaria Kasmi et al.: ***Algorithms and Position Optimization for a Decentralized Localization Platform Based on Resource-Constrained Devices***, September 2018, IEEE Transactions on Mobile Computing PP(99):1-1, DOI: 10.1109/TMC.2018.2868930
- Zakaria Kasmi et al.: ***Accurate 3D Positioning for a Mobile Platform in Non-Line-of-Sight Scenarios Based on IMU/Magnetometer Sensor Fusion***, January 2018, Sensors 18(1):126, DOI: 10.3390/s18010126
- Simon Schmitt et al.: ***Fast Routing Graph Extraction from Floor Plans***, September 2017, DOI: 10.1109/IPIN.2017.8115868, IEEE International Conference on Indoor Positioning and Indoor Navigation, Sapporo, Japan
- Enrico Köppe et al.: ***An advanced method for pedestrian dead reckoning using BLSTM-RNNs***, October 2015, DOI: 10.1109/IPIN.2015.7346954, 2015 International Conference on Indoor Positioning and Indoor Navigation (IPIN)
- Yi Sun et al.: ***A Running Step Length Estimation Model for Position Tracking***, 12th Workshop on Positioning, Navigation and Communication 2015 (WPNC'15), Dresden, Germany
- Yubin Zhao et al.: ***An Indoor Positioning System based on Inertial Sensors in Smartphones***, March 2015, DOI: 10.1109/WCNC.2015.7127812, Wireless Communications and Networking Conference (WCNC), 2015 IEEE, New Orleans, LA, USA
- …