UiO : Department of Technology Systems
University of Oslo

Seminar Security and Privacy, 14Feb2019

Measurable Security, Privacy and Trust for Autonomous Systems

Josef Noll,
Professor, University of Oslo, Department of Technology Systems
Kjeller, Norway, m: +47 9083 8066, e: josef@jnoll.net

Outline

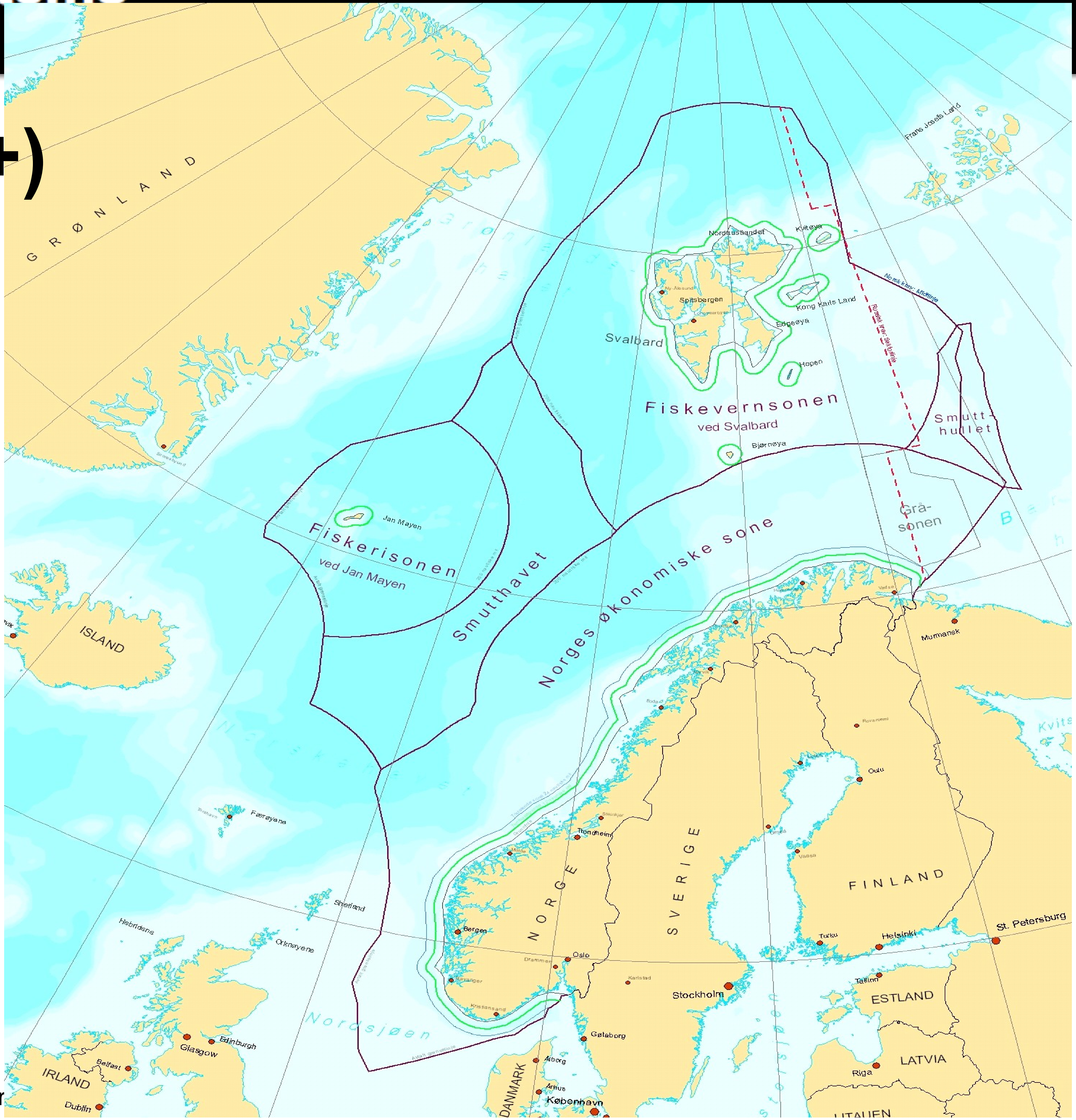
"The last time I was connected by wire was at birth"

- Mobile Network development
  - from 3G to 5G
  - "always online, always connected"?
- IoT Security
  - Measurable Security
  - Multi-Metrics Method
- Privacy, Internet and net-neutrality
  - Facebooks Free Basices
  - India: "We have been colonised once…"
- Smart Meters
  - Capabilities
  - online monitoring
- Conclusions

The Nordics (Scandinavia++)

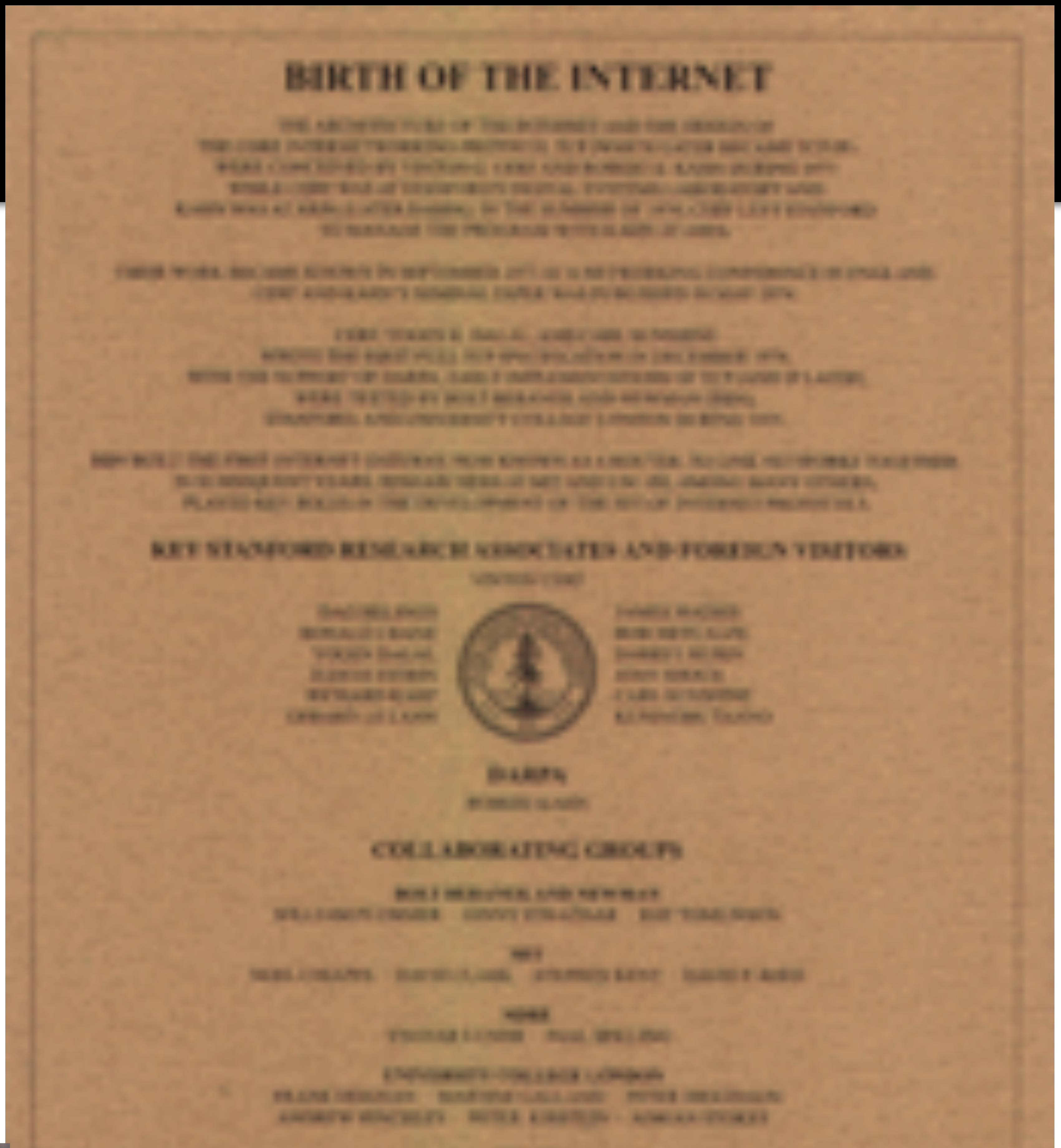
- Demanding customers
- Trusted authorities
- Competitive landscape
- Open Interfaces

- Large distances
- costly infrastructure
- high labour costs



The Internet and Scandinavia

- The first connection of Arpanet outside of the USA (and Hawaii) was to **Scandinavia** (Kjeller, June 1973)
- List_of_Internet_pioneers [Wikipedia]
  - ➡ Yngvar Lundh, Paal Spilling
- Application development
  - ➡ .php, OpenSource, Linux, Skype, Spotify
  - ➡ OperaSoftware, FAST Search
  - ➡ Nokia, Ericsson
  - ➡ Telenor, TeliaSonera
- Mobile Internet:
  - ➡ GSM
  - ➡ Adaptation



BIRTH OF THE INTERNET

[illegible]

KEY STANFORD RESEARCH ASSOCIATES AND FOREIGN VISITORS

[illegible]

DARPA

[illegible]

COLLABORATING GROUPS

BOLT BERANEK AND NEWMAN

[illegible]

NDRE

YNGVAR LUNDH PAAL SPILLING

UNIVERSITY COLLEGE LONDON

[illegible]

My Background

- ”Traditional German”
  - Radio, Communications, Remote Sensing
  - Siemens, European Space Agency (ESA)
  - Global: Sea surface, snow coverage, soil moisture
  - Cycling ”all year”, environment & health
- From Norway to the World
  - Telenor R&D: 3G/UMTS (Kjeller)
    - ”always online, always connected”
  - Took over from Internet Pioneer Pål Spilling
    ”Internet Lite for All” (2010)

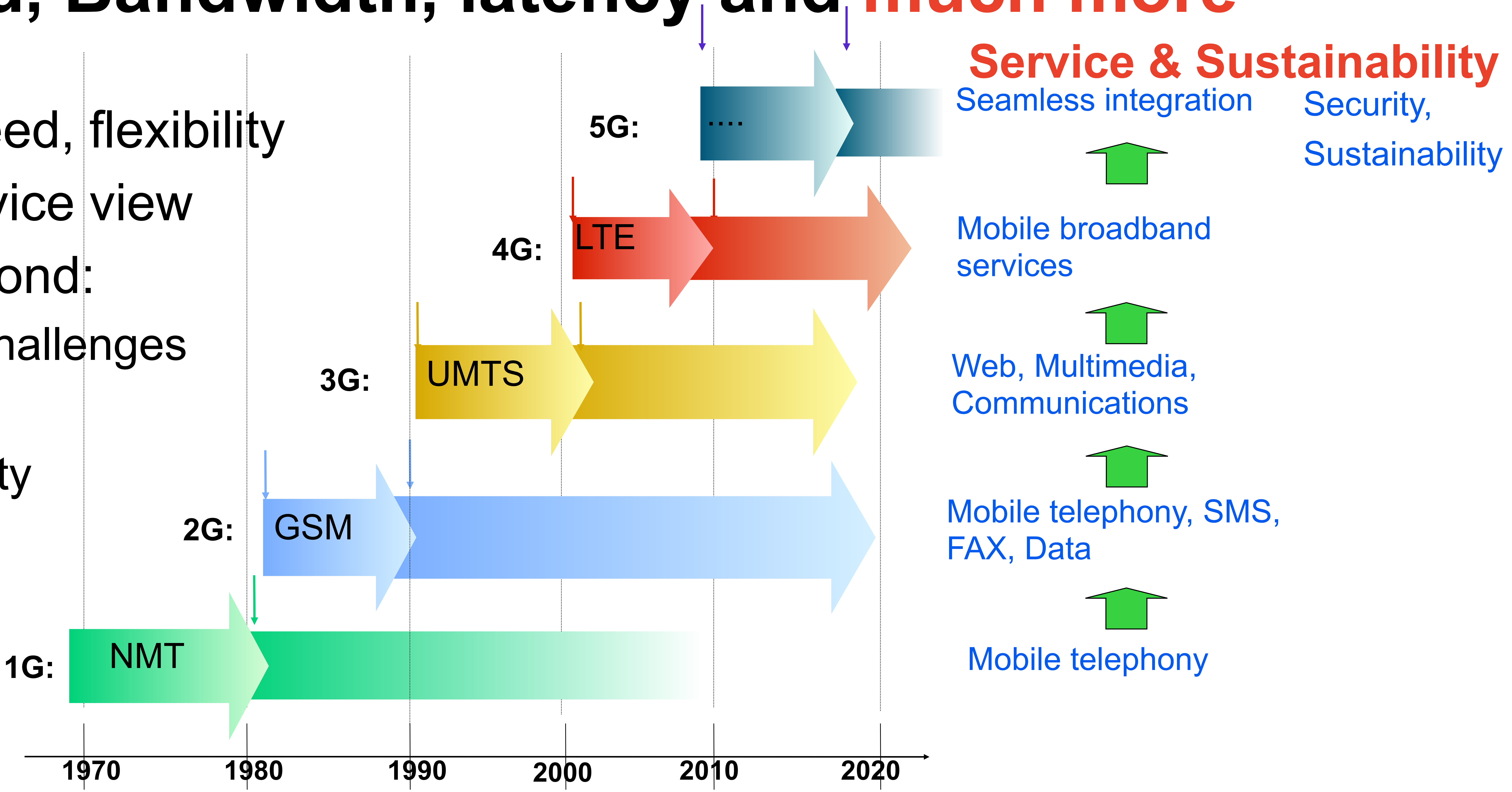
SYKKELENTUSIAST: Før han bosatte seg i Norge syklet Josef Noll Trondheim - Oslo. Selv om været nesten ikke var til å holde ut, ble han bitt av basillen. I dag sykler han distansen annethvert år, i tillegg sykler han til jobb på Kjeller fra hjemmet på Høybråten.

– Internett er en menneskerett

Source: Akers Avis Groruddalen, 2013

5G: Speed, Bandwidth, latency and much more

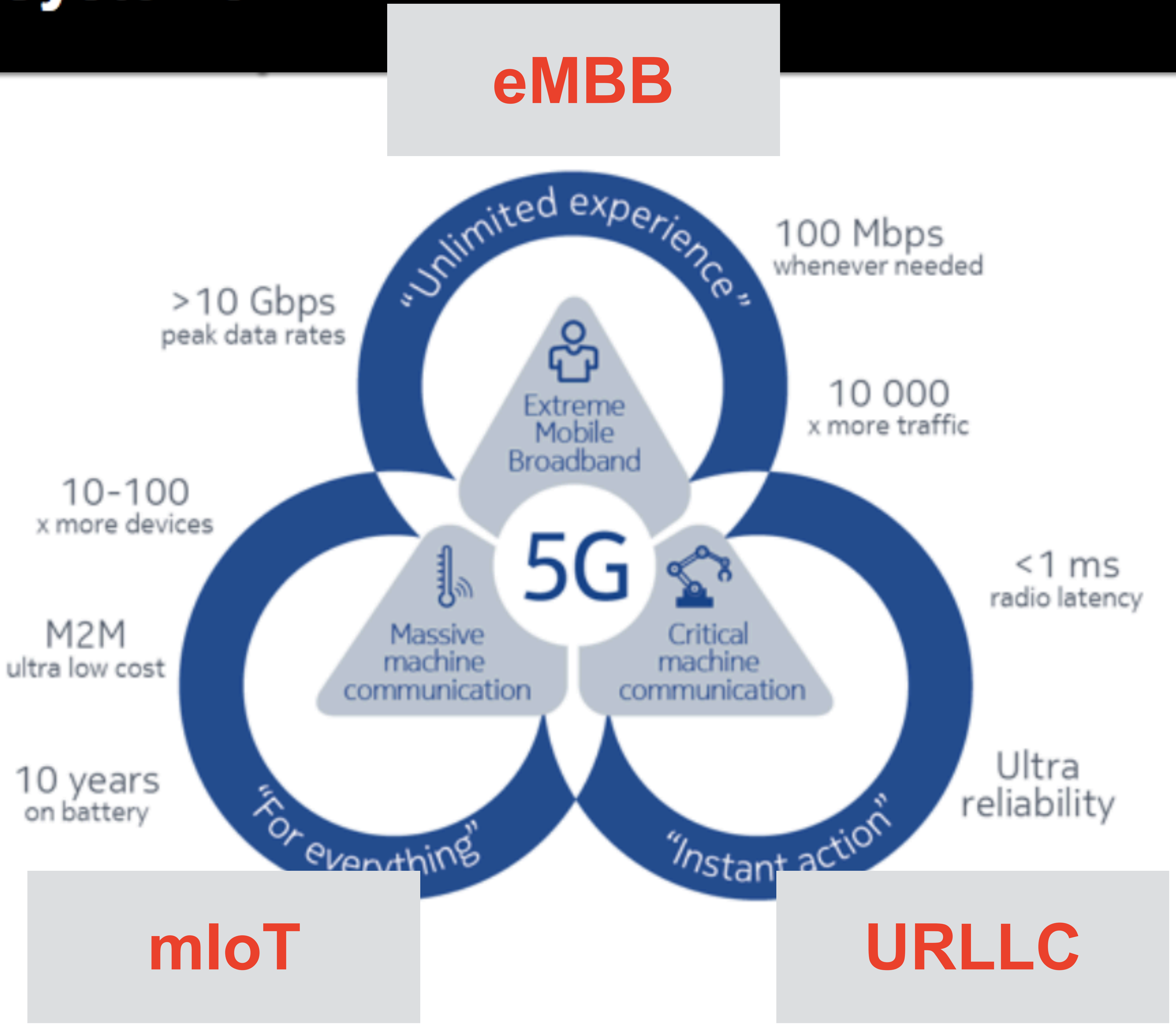
- 1G-3G: Speed, flexibility
- 3G-4G: service view
- 5G and beyond:
  - ➡ Business challenges
  - ➡ ownership
  - ➡ sustainability



[adapted from Per Hjalmar Lehne, Telenor, 2000]

5G

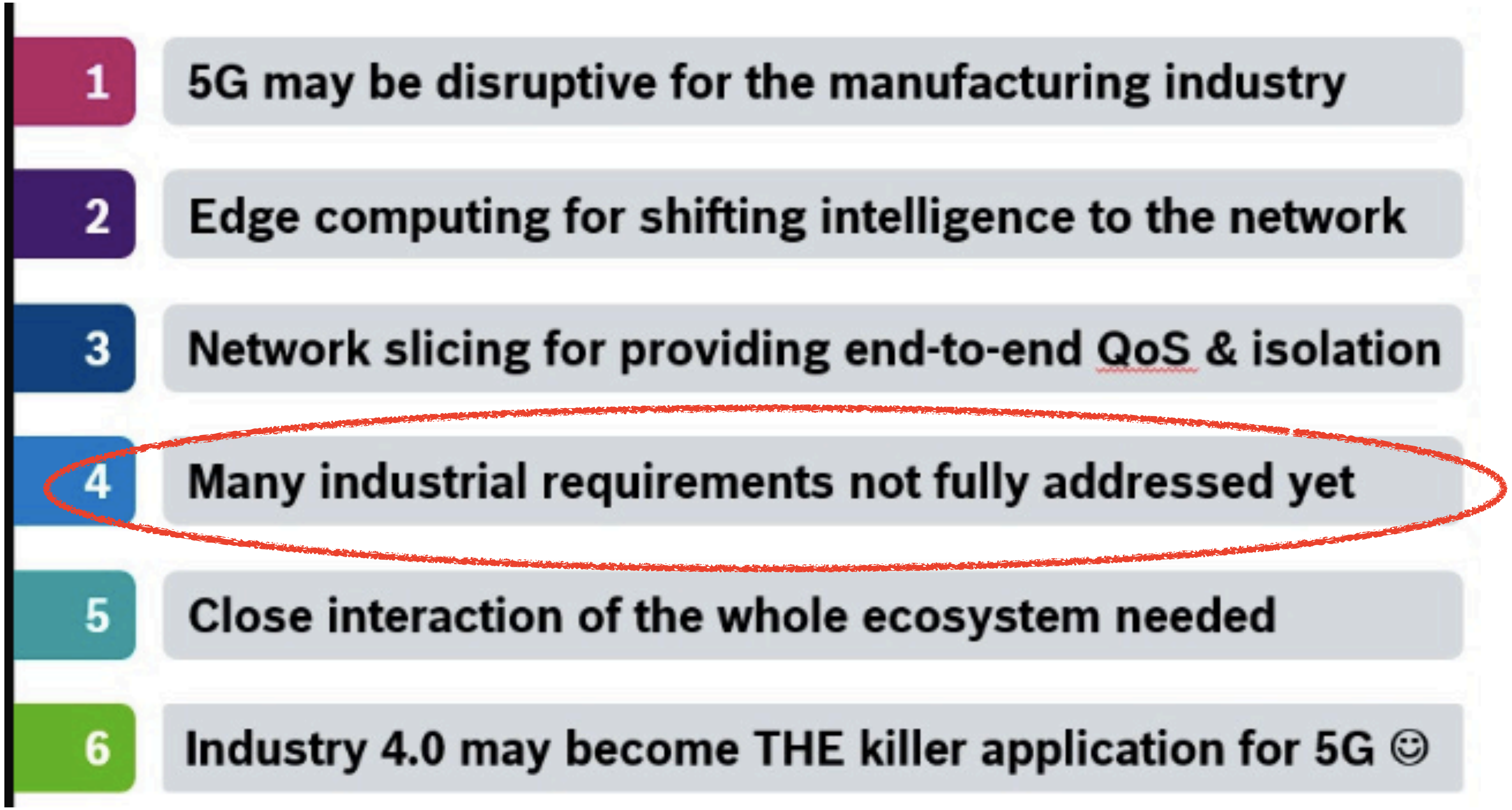
- Dhananjay Gore, Qualcomm Research, India at COMSNETS 2018
  - ➡ 3GPPP Rel-15 specifications aligned with Qualcomm Research white paper Nov2015
  - ➡ http://www.qualcomm.com/invention/technologies/5g-nr/mmwave



[source: Nokia https://networks.nokia.com/5g/get-ready]

5G Networks for Industry

- Core demand
- Edge intelligence
  - ➡ Edge/fog computing
- End-to-end QoS and isolation
  - ➡ network slicing
  - ➡ heterogeneity(?)



1 5G may be disruptive for the manufacturing industry

2 Edge computing for shifting intelligence to the network

3 Network slicing for providing end-to-end QoS & isolation

4 Many industrial requirements not fully addressed yet

5 Close interaction of the whole ecosystem needed

6 Industry 4.0 may become THE killer application for 5G ☺

[Source: Andreas Mueller, Bosch, 2018]

Security in IoT

- ➡ From Threat-based approach to Security by Design
- ➡ Measurable Security, Privacy and Dependability (SPD)

From Mobile Security to IoT Security

- Hollande (FR), Merkel (DE) had their mobile being monitored
- IoT security?

18. Dezember 2014, 18:14 Uhr Abhören von Handys

So lässt sich das UMTS-Netz knacken

Zwei Hacker zeigen: UMTS-Antennen lassen sich knacken. (Foto: dpa)

[source: Süddeutsche Zeitung, 18Dec2014]

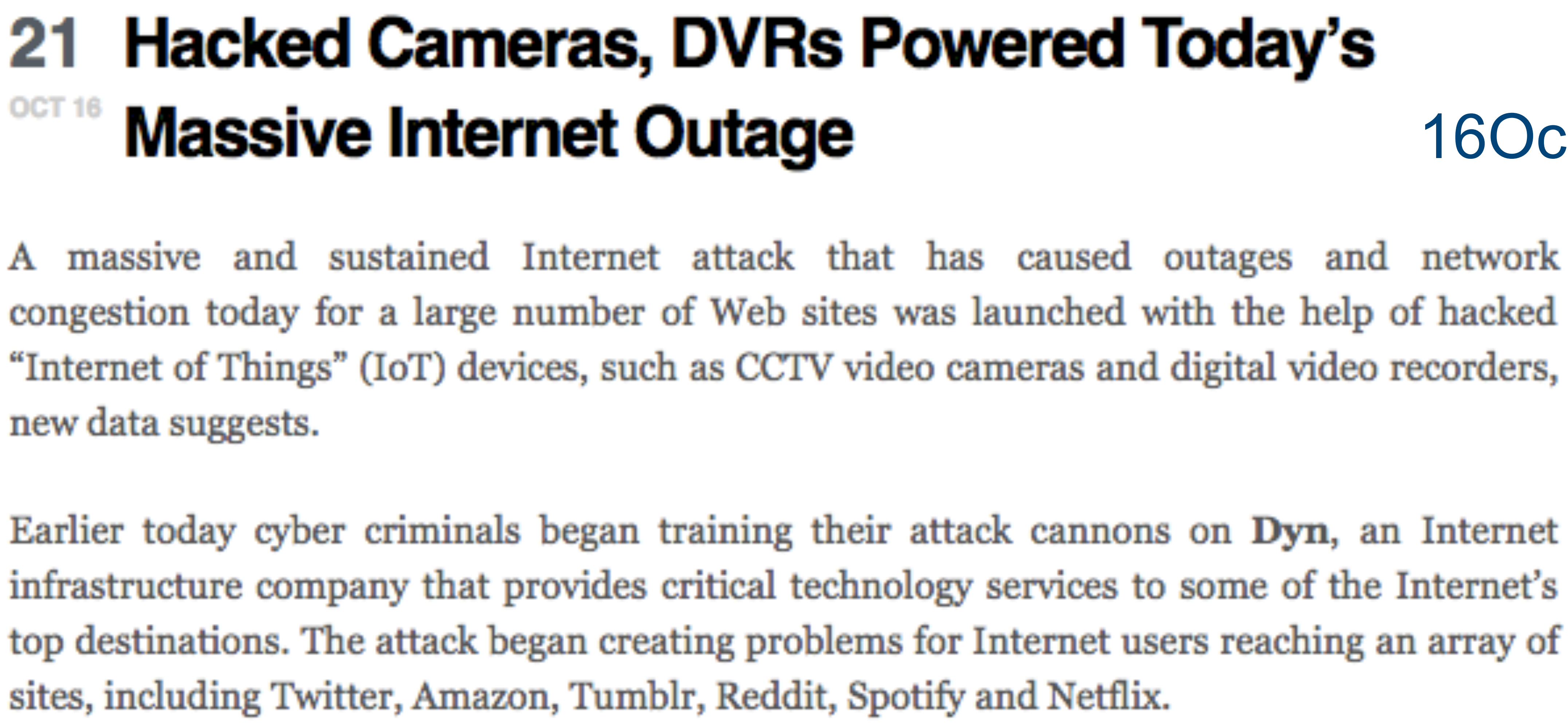
[source: www.rediff.com]

by IoT

IoT threats

- First massive attack from IoT devices
  - 16Oct2016 IoT botnet attack on Dyn
  - Camera (CCTV), video recorder, TV,…
  - 1.2 Gbps Denial-of-Service attack

- How?
- All using Linux BusyBox for authentication
  - admin - admin, root - root, admin - 1111…
  - simple “test” was enough to convert IoTs into bot

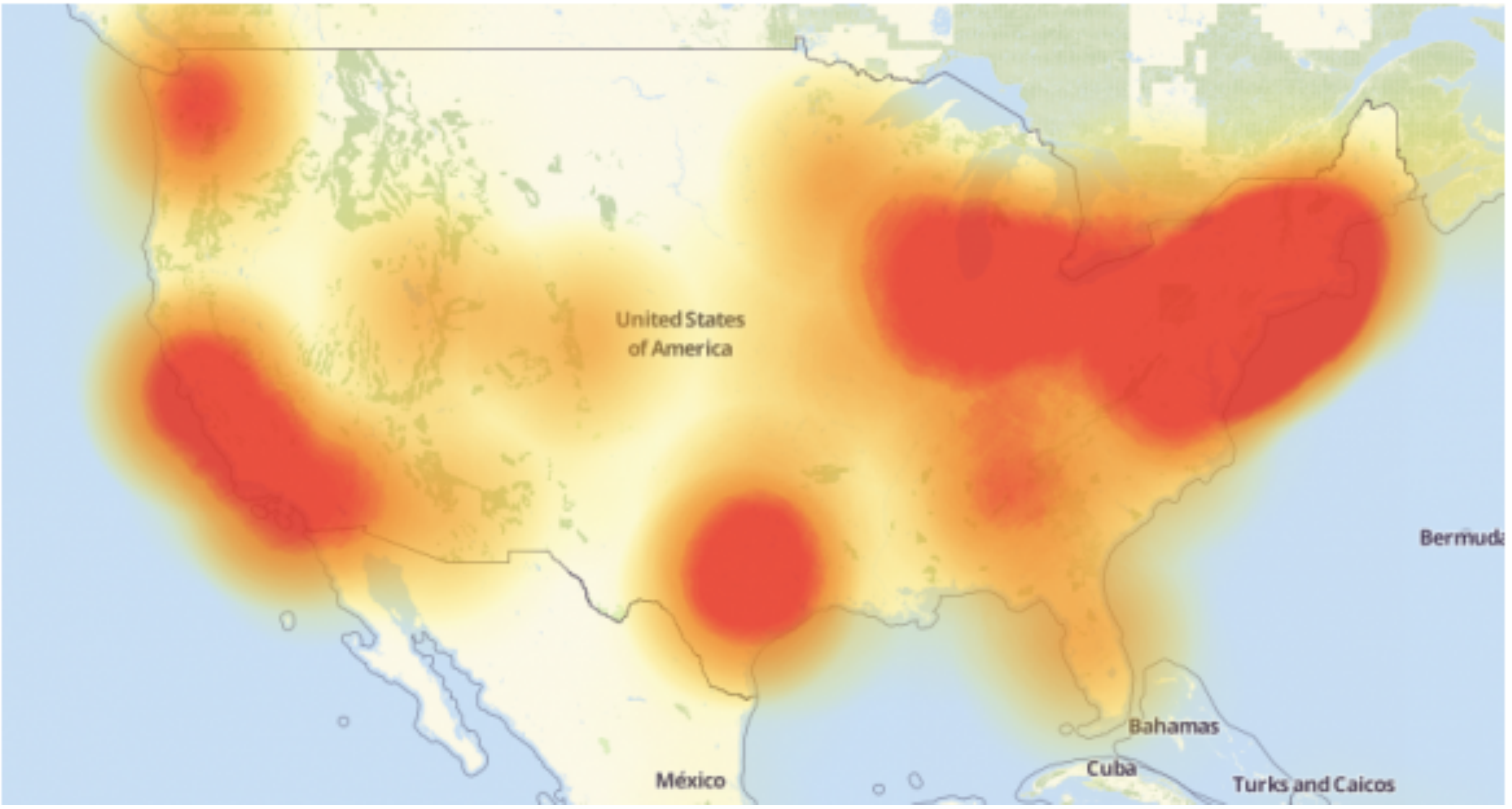


21 OCT 16 **Hacked Cameras, DVRs Powered Today’s Massive Internet Outage**

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked “Internet of Things” (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet’s top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.

16Oct



[Source: https://krebsonsecurity.com/2016

THERE WILL BE NO PEACE UNTIL ALL MEN LEARN TO UNDERSTAND EACH OTHER
TRUE... TRUE...
HOW ARE WE GOING TO GET EVERYBODY TO SPEAK NORWEGIAN ?

teach our sensors to talk Norwegian

Secure COnnected Trustable Things

Werner ROM / Michael KARNER
VIRTUAL VEHICLE Research Center, Graz/Austria

secure connected trustable things

SCOTT has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737422. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway.

SCOTT key message “elevator pitch”

largest security project in EU

57 partners from 12 countries

80 M€ budget 35 M€ EU&national

8 partners from Norway

IoT is the game changer and driver for digitalisation, and SCOTT contributes through:

- **Answer the IoT need for a new and more advanced security paradigm through security classes**
- **Create a Convincing privacy assessment through privacy labelling**
- **Establish a clear link between security and safety**

Automotive

Home

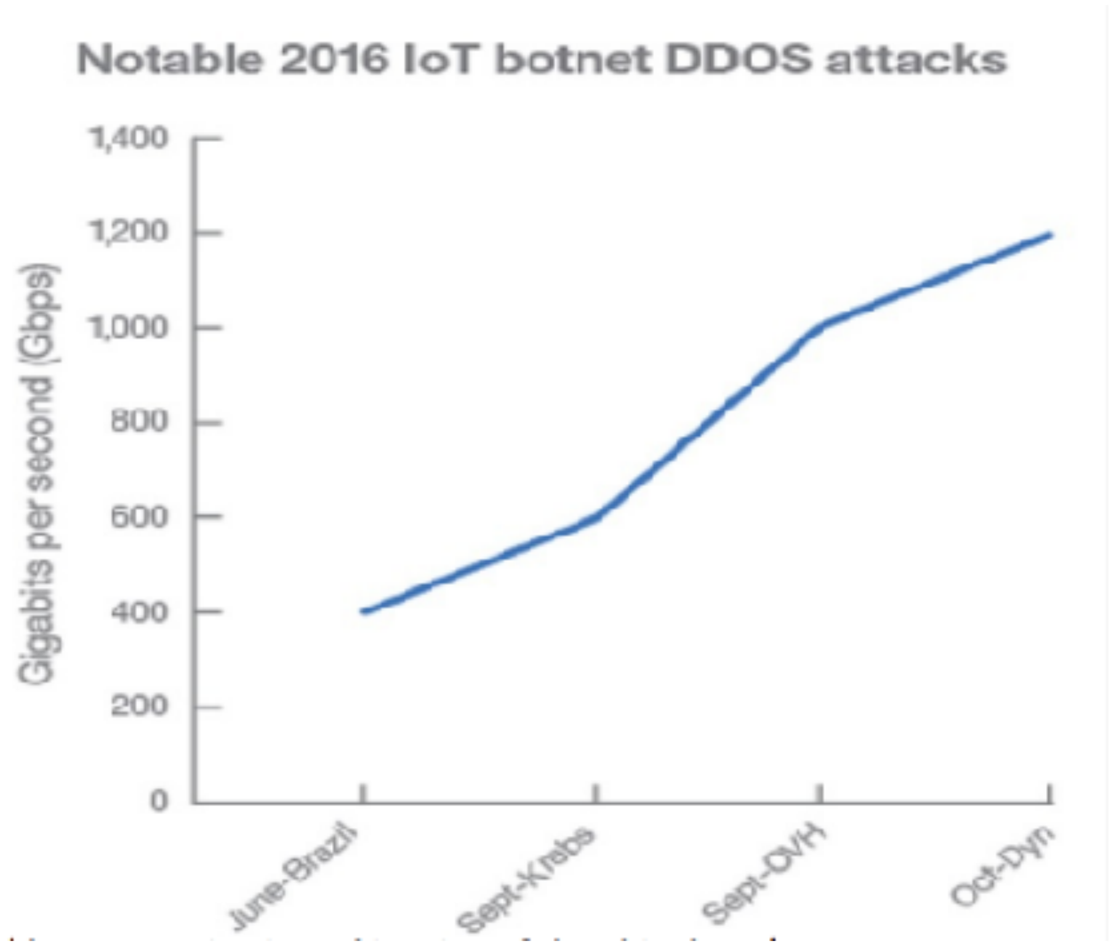
Rail

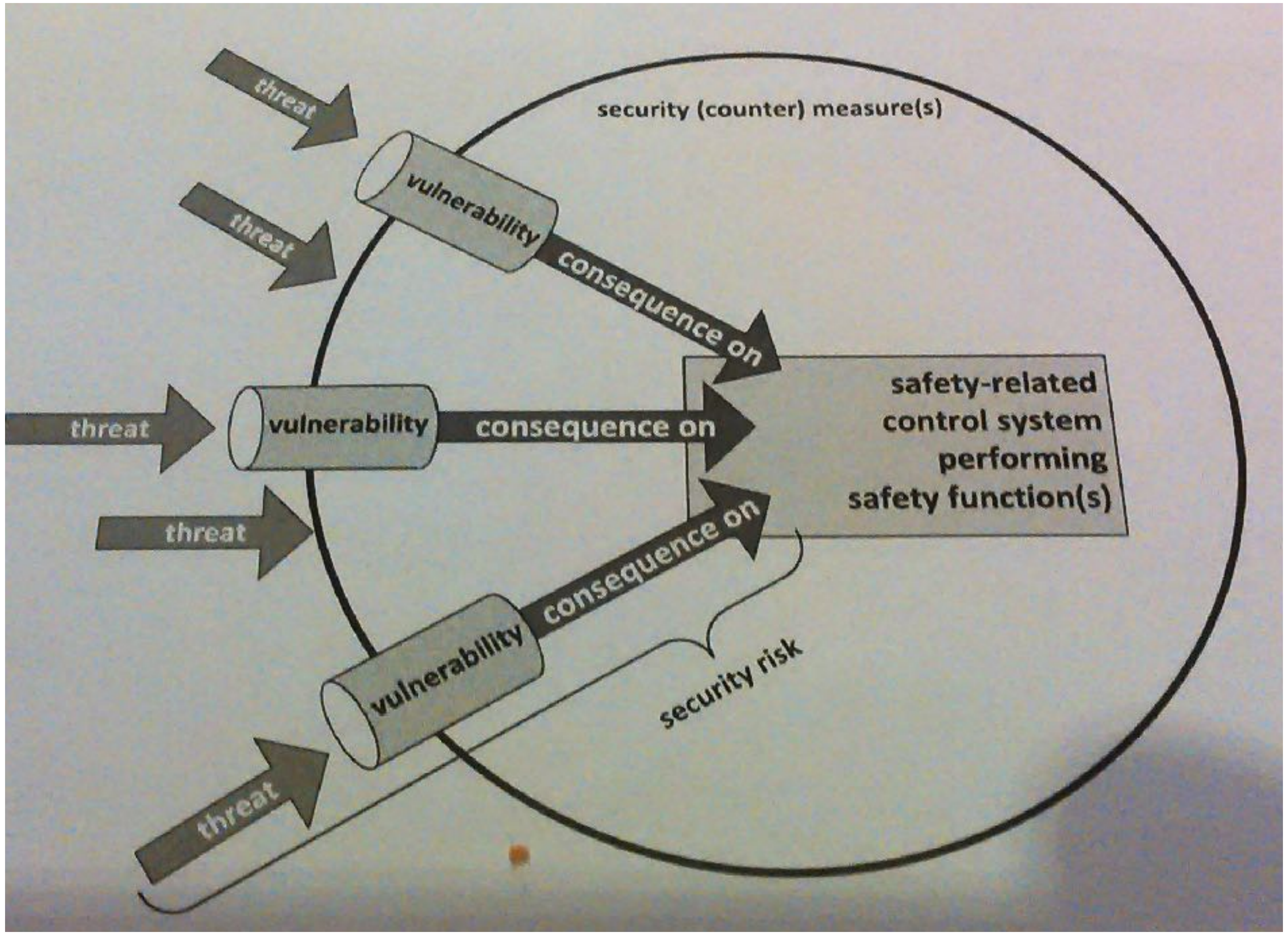
5G

Avionics

Roadmap for a more secure and privacy-aware society

- “Vulnerability analysis” is not sufficient
  - □ novel threats occur
  - □ installation base for 5-20 years
  - □ example: increase in DDoS attack capability

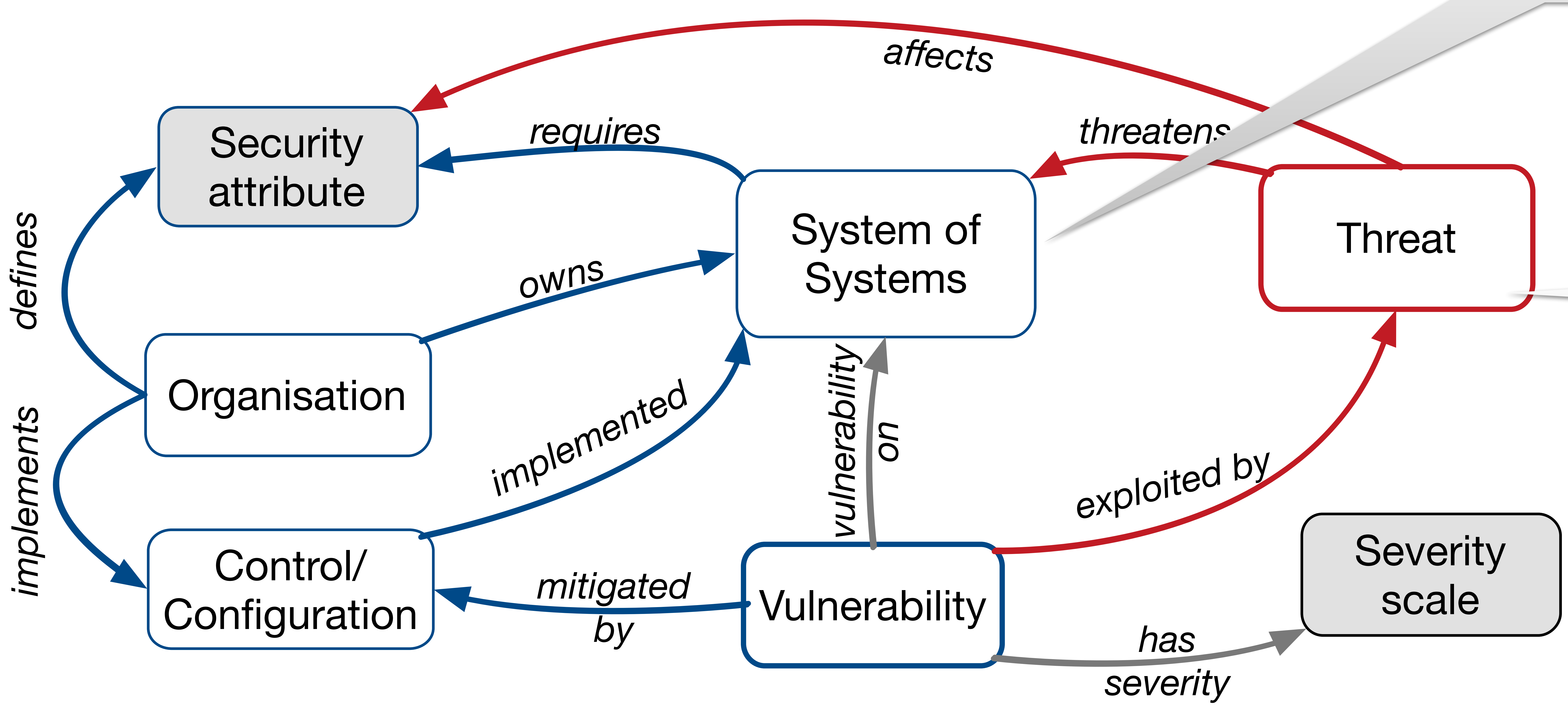




- Business advantage for European industries
  - □ Security classes/levels

. https://securityintelligence.com/the-weaponization-of-iot-rise-of-the-thingbots/

Traditional: Threat-based approach



Scalability?

Future Threats?

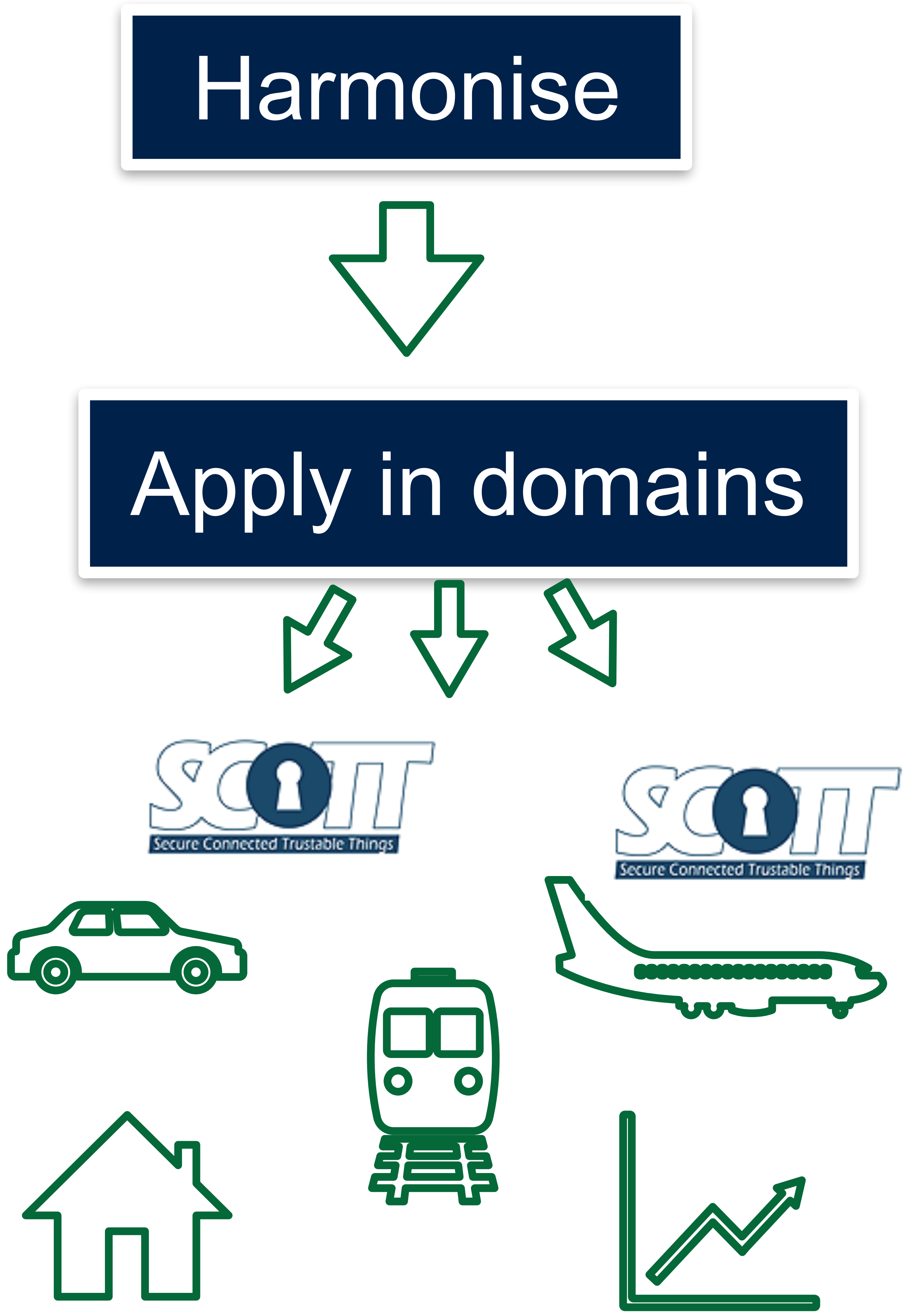
[source: http://securityontology.sba-research.org/]

IoT concerns regarding advanced security paradigm

Steps

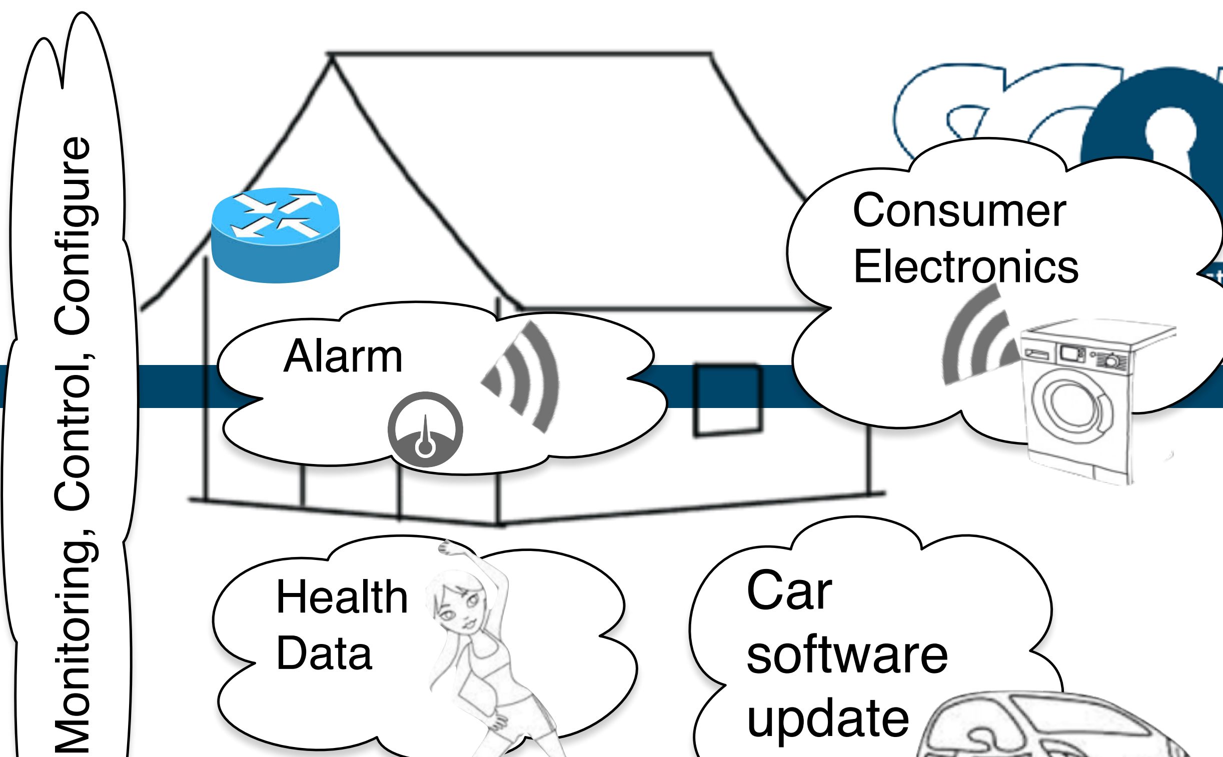
- **Answer the IoT need for a new and more advanced security paradigm**
  - *How to measure security of (complex) IoT systems, how to incorporate security it into designs, how to have a clear (understandable to end-users) security level assessment*
  - *Address cybersecurity through proactive safeguard*

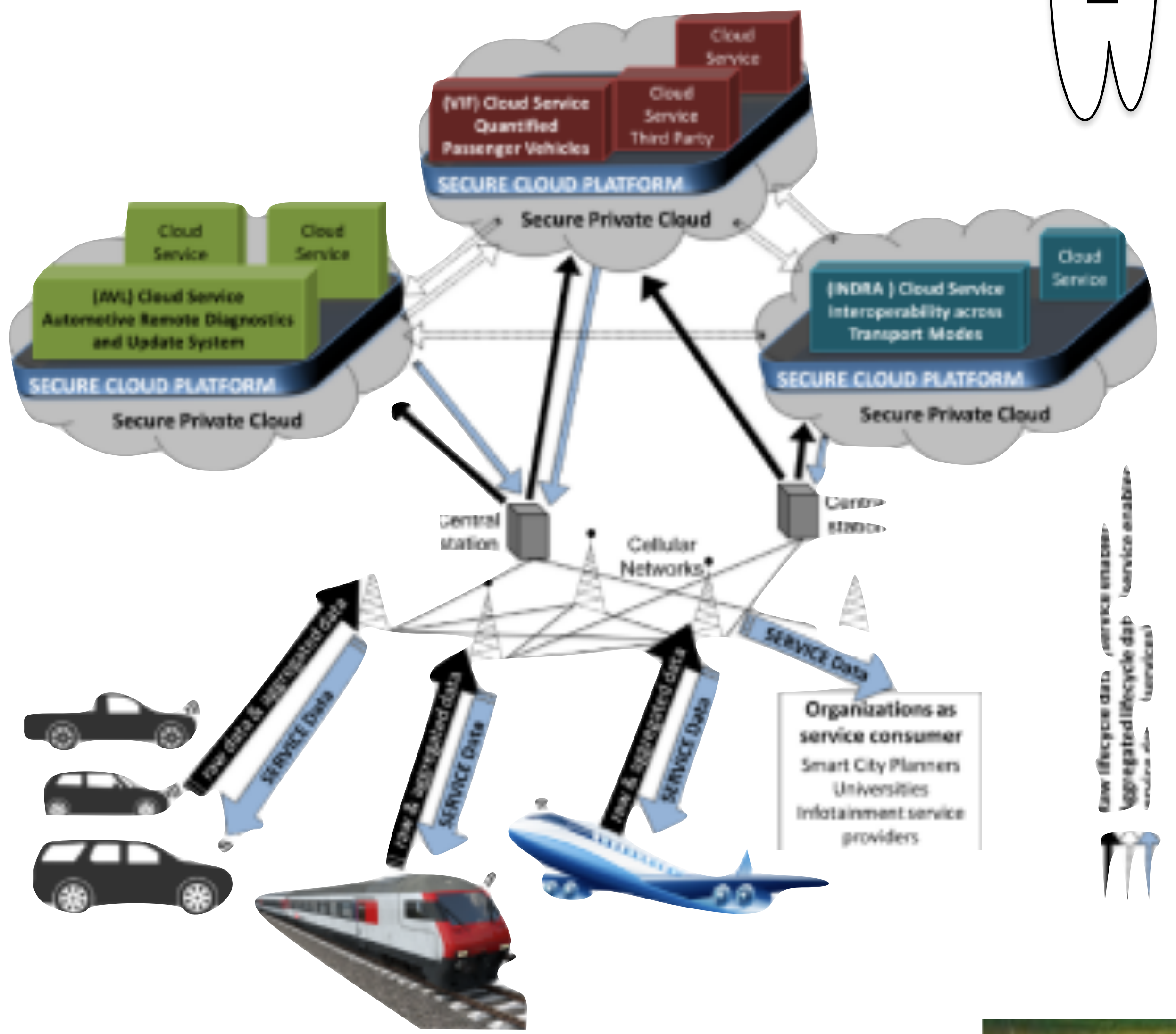
- **Main outcomes**
  - *Measurable security of (complex) IoT systems,*
  - *Security classes, defined through*
  - *Goal: Design paradigm for IoT systems*

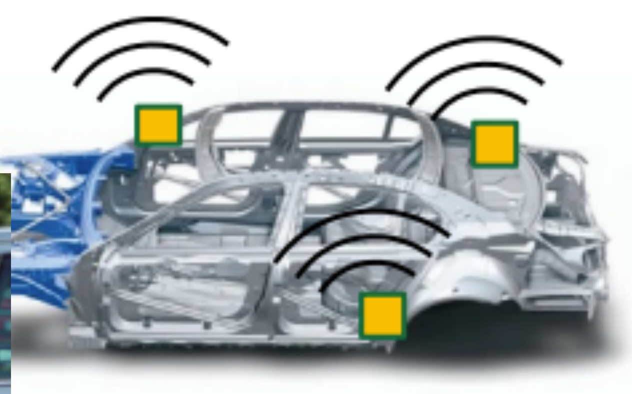

Harmonise
Apply in domains
SCOTT
Secure Connected Trustable Things
SCOTT
Secure Connected Trustable Things

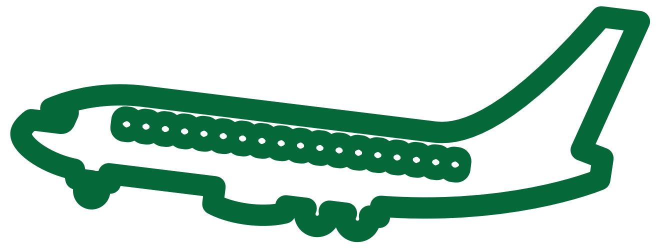
Suggestion:
High-level vision for each domain

- Home/Infrastructures: Cost-efficient monitoring and management for trusted services
- Mobile: Configurable networks providing reliable services
- Automotive: Security architecture for accident-free transport
- Rail: Highly flexible train composition
- Aeronautics: Security-Safety
- Support vision through
  - showcases
  - common security assessment
  - highlights, e.g. “InfoInternet: free access to Information for all”



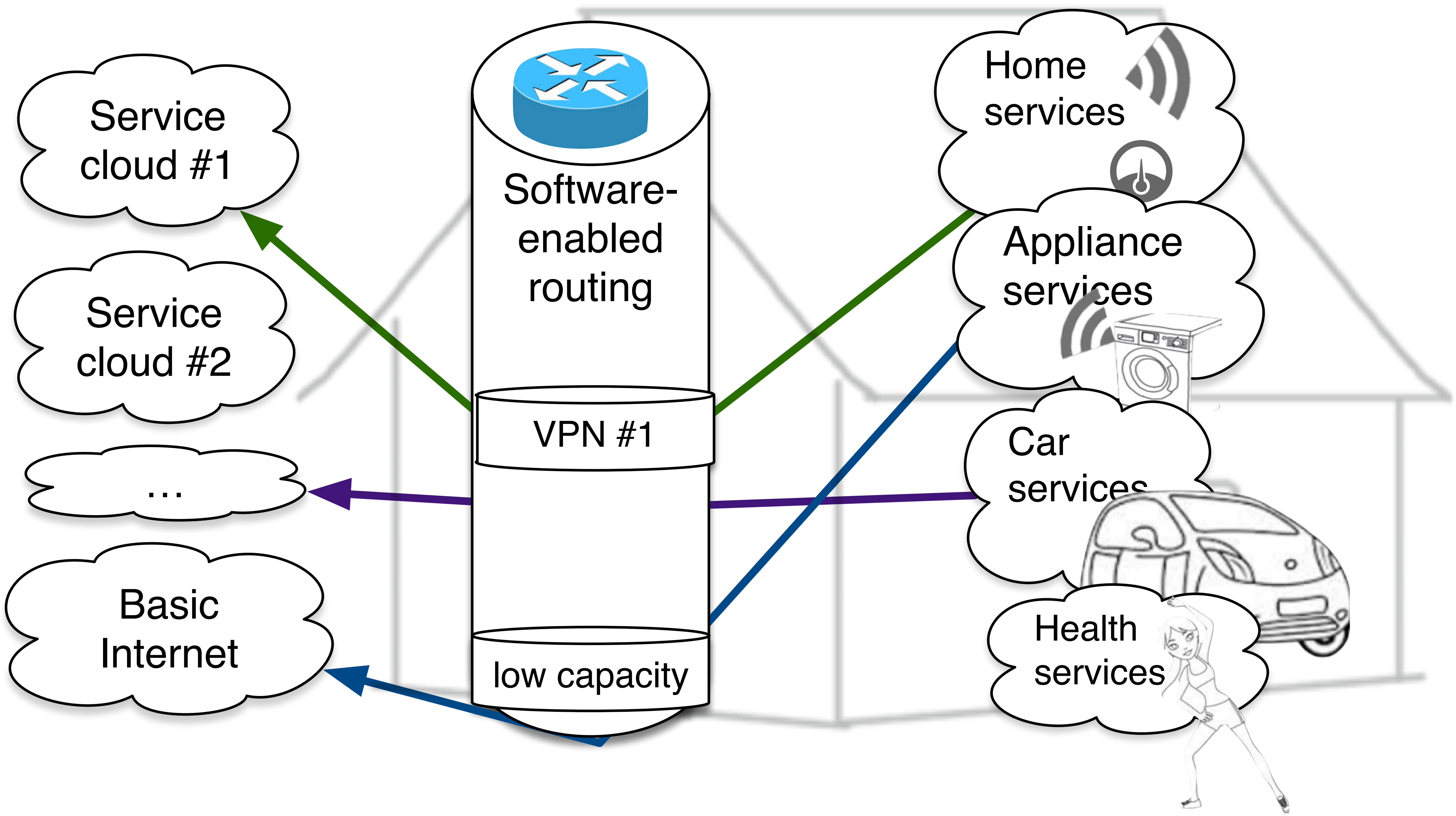






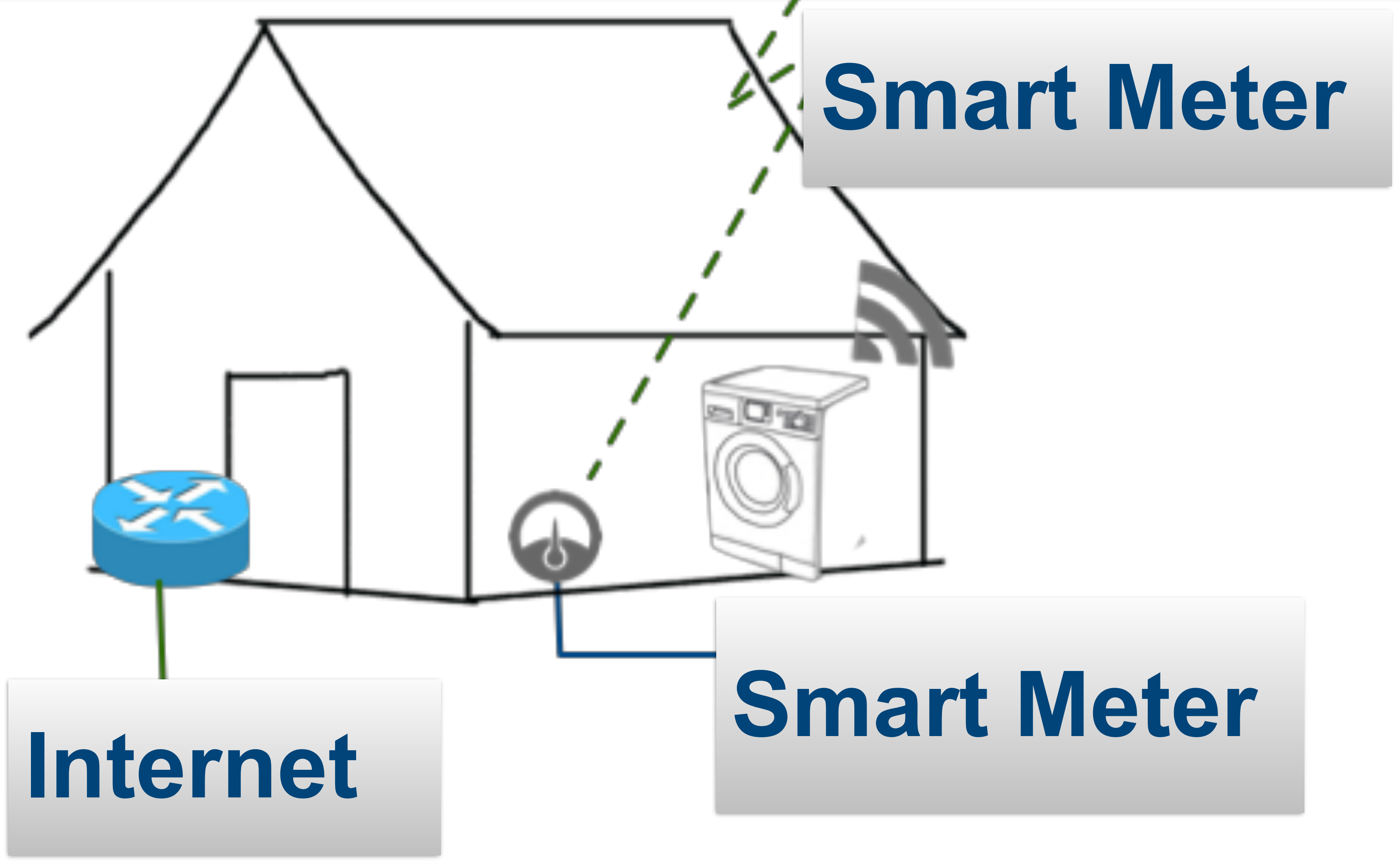
Learn from Industrial Automation and Mobile Networks

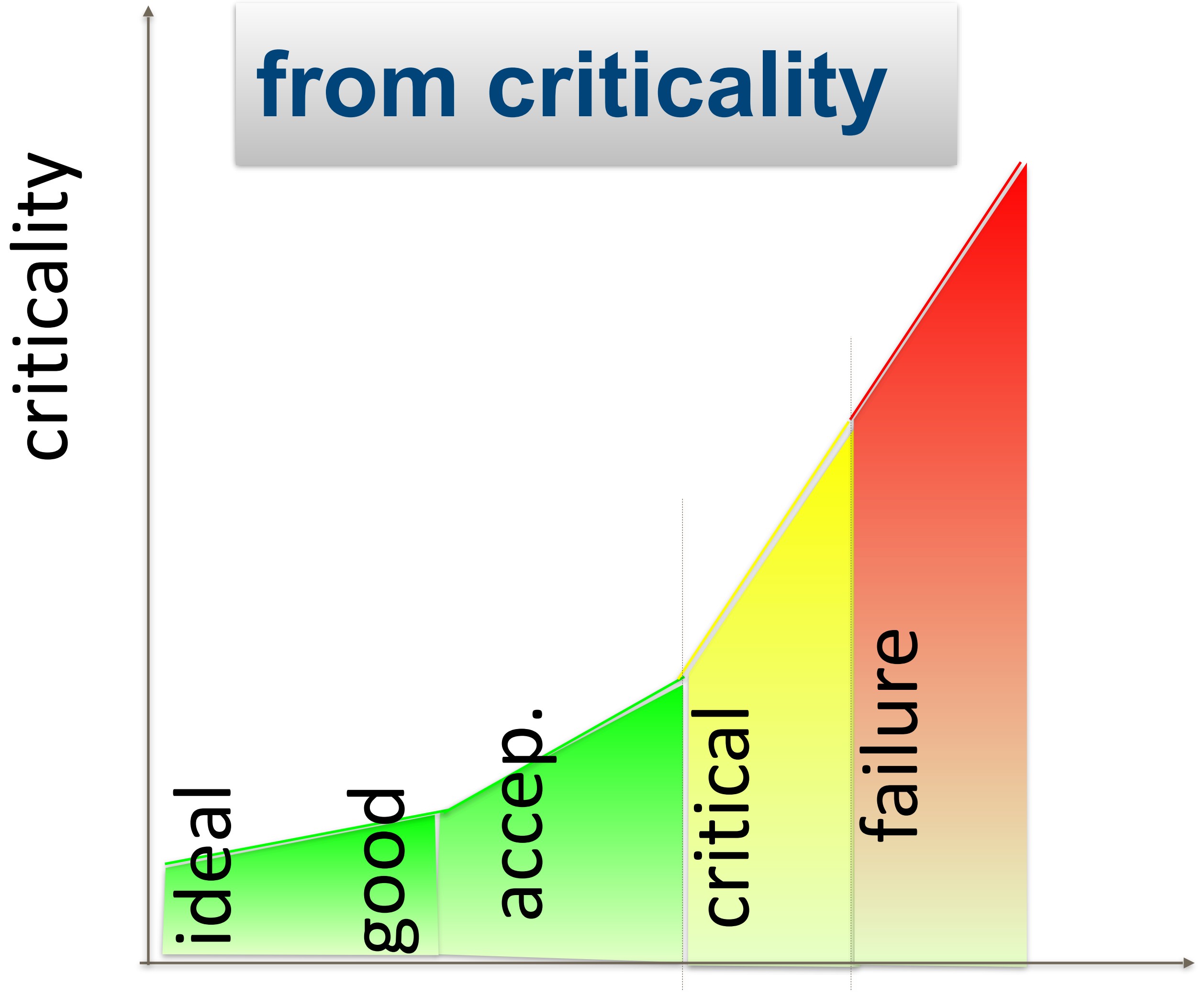
- “What to secure?”
- Network segregation
  - ➡ *Network slicing*
- From Confidentiality, Integrity, Availability (CIA)
- to Availability, Integrity, Confidentiality (AIC)



Security and Privacy challenges

- Smart Meter
  - ➡ read and control
  - ➡ logic?
- Smart Home
  - ➡ intelligent devices
  - ➡ on-demand regulation
- Challenges
  - ➡ Logic: Centralised ⟷ Fog
  - ➡ Smart Meter: Information ⟷ Control
  - ➡ Smart Grid Information ⟷ Internet Info





to measurable: security, privacy and dependability

SPD level	SPD vs SPD_{Goal}
(67,61,47)	(🔴,🟡,🟢)
(67,61,47)	(🔴,🟡,🟡)
(31,33,63)	(🔴,🟡,🟡)

Multi-Metrics Methodology for Assessment of Security, Privacy, and Dependability (SPD)

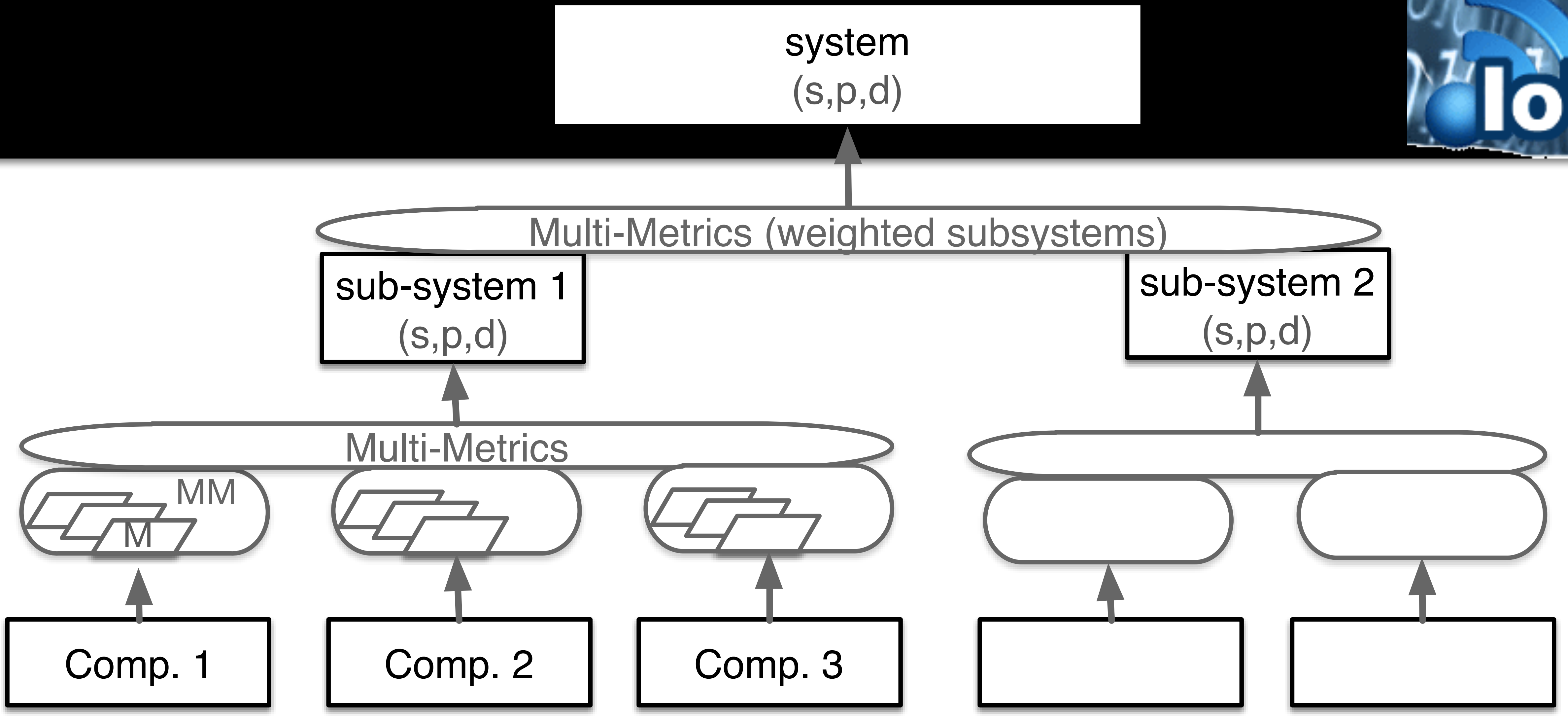
Thanks to our colleagues from SHIELD for the collaboration

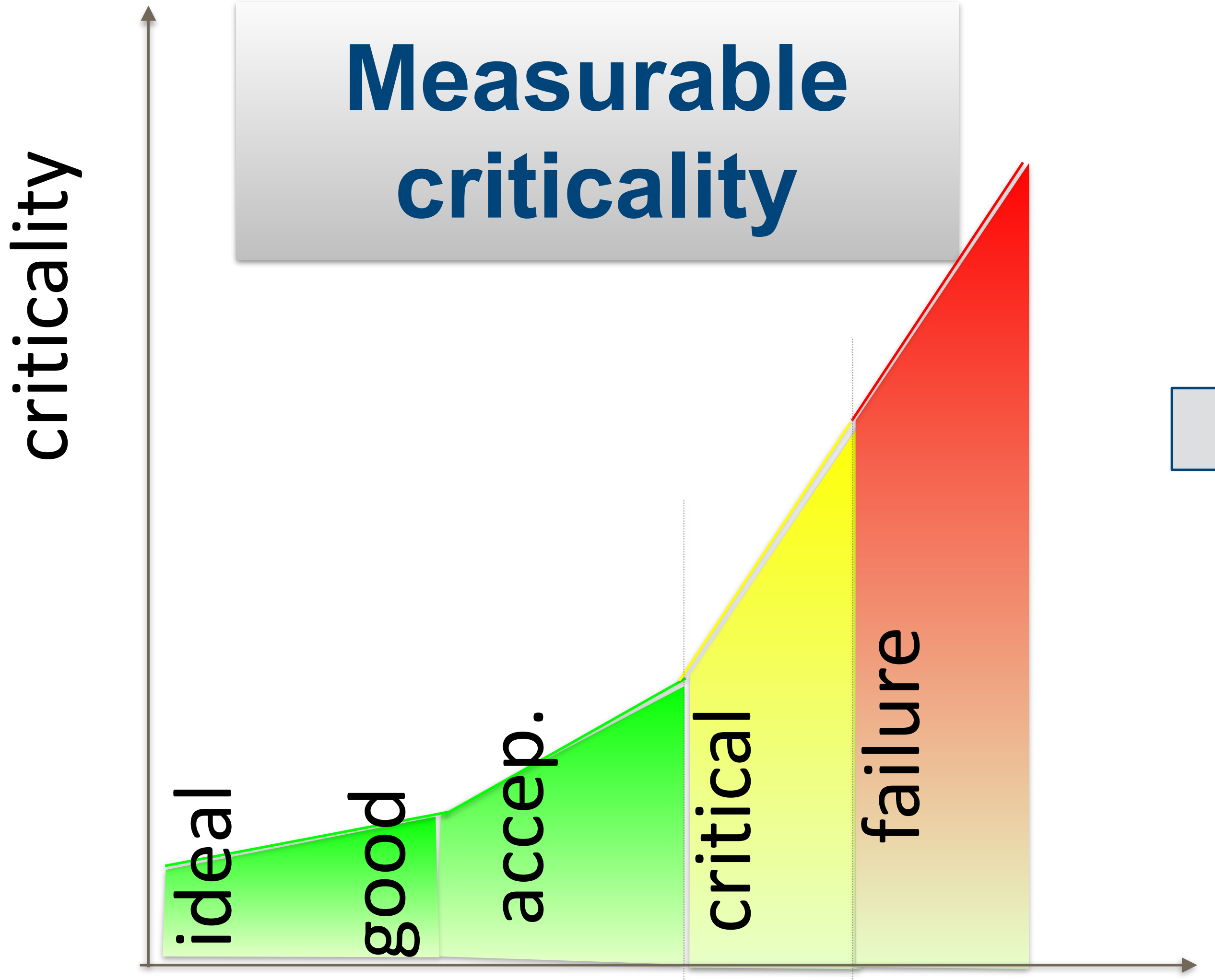
- Iñaki Equia, Frode van der Laak, Seraj Fayyad, Cecilia Coveri, Konstantinos Fysarakis, George Hatzivasilis, Balázs Berkes, Josef Noll

Feb2015

Accountable security

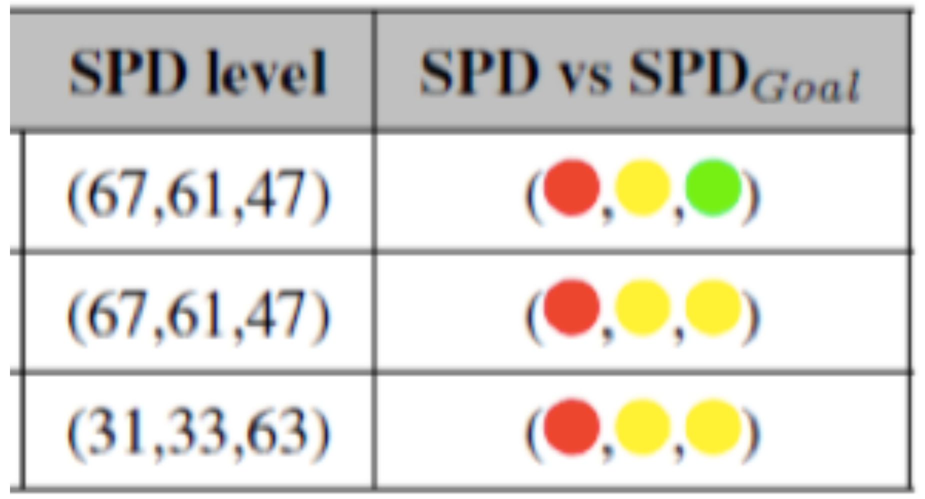
- Assessment
  - ➡ Comparison desired Class vs Calculated class
- Modelling
  - ➡ SPD Metrics, from criticality to SPD value
- Framework
  - ➡ Examples of applicability
- Measurable Security
  - ➡ Security is not 0/1


system
(s,p,d)
Multi-Metrics (weighted subsystems)
sub-system 1
(s,p,d)
sub-system 2
(s,p,d)
Multi-Metrics
MM
M
Comp. 1
Comp. 2
Comp. 3



Measurable criticality

to measurable: security, privacy and dependability



SPD level	SPD vs SPD$_{Goal}$
(67,61,47)	(🔴,🟡,🟢)
(67,61,47)	(🔴,🟡,🟡)
(31,33,63)	(🔴,🟡,🟡)

Methodology: From System description to SPD level

System/ Sub-system
Is made by
Components and functionalities
Could be
SPD Components, SPD functionalities
described by
Metrics description (SPD functionality)
define config. parameters and SPD values in Metrics
Run SPD Multi-metrics analysis

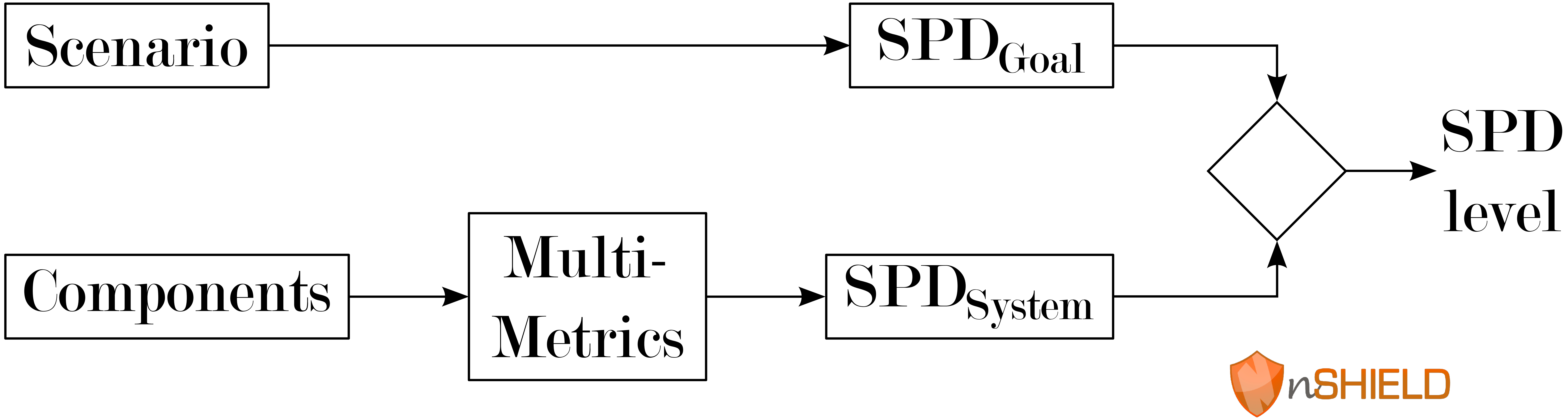
- System: Automatic Meter System (AMS) consists of reader (AMR), aggregator, communications, storage, user access
- Sub-systems: AMR consists of power monitor, processing unit, communication unit
- Component: AMR communication contains of a baseband processing, antenna, wireless link
- Configuration Parameter: Wireless link: f=868 MHz, output power=?, Encryption=?

Measureable Security, Privacy, Dependability (SPD)

- Focus on «entry the industrial market»

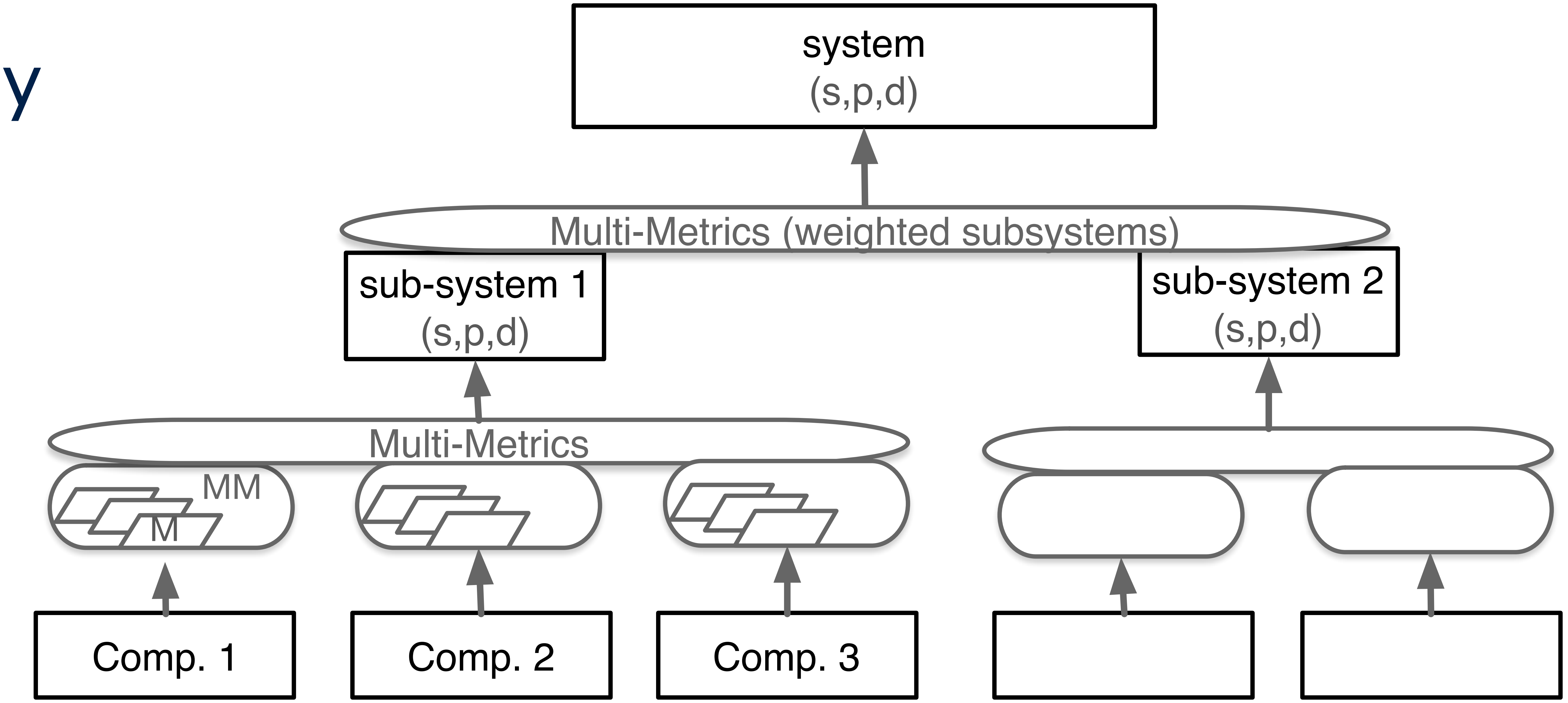
- Industry «needs security» - with entry models

- System Security, Privacy and Dependability is assessed
  - ➡ Application SPD_{Goal}
  - ➡ SPD_{System} asessment
  - ➡ Comparison SPD_{Level}

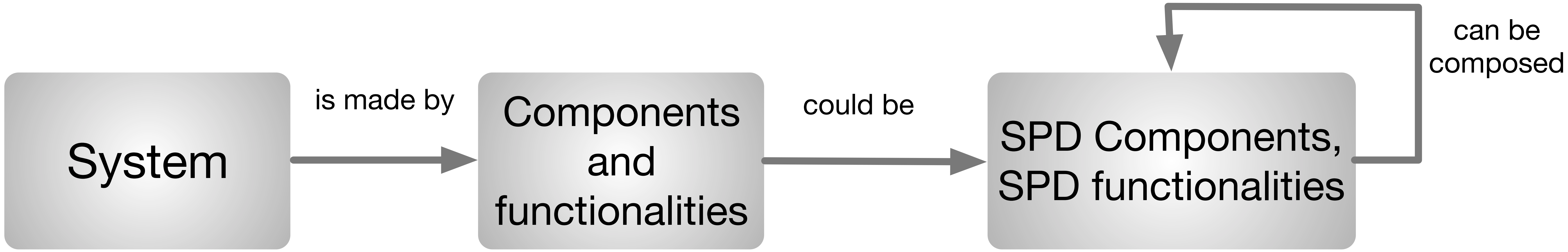


Measurable Security

- From people defined security classes
- To automated security decisions
  - *through metrics assessment*



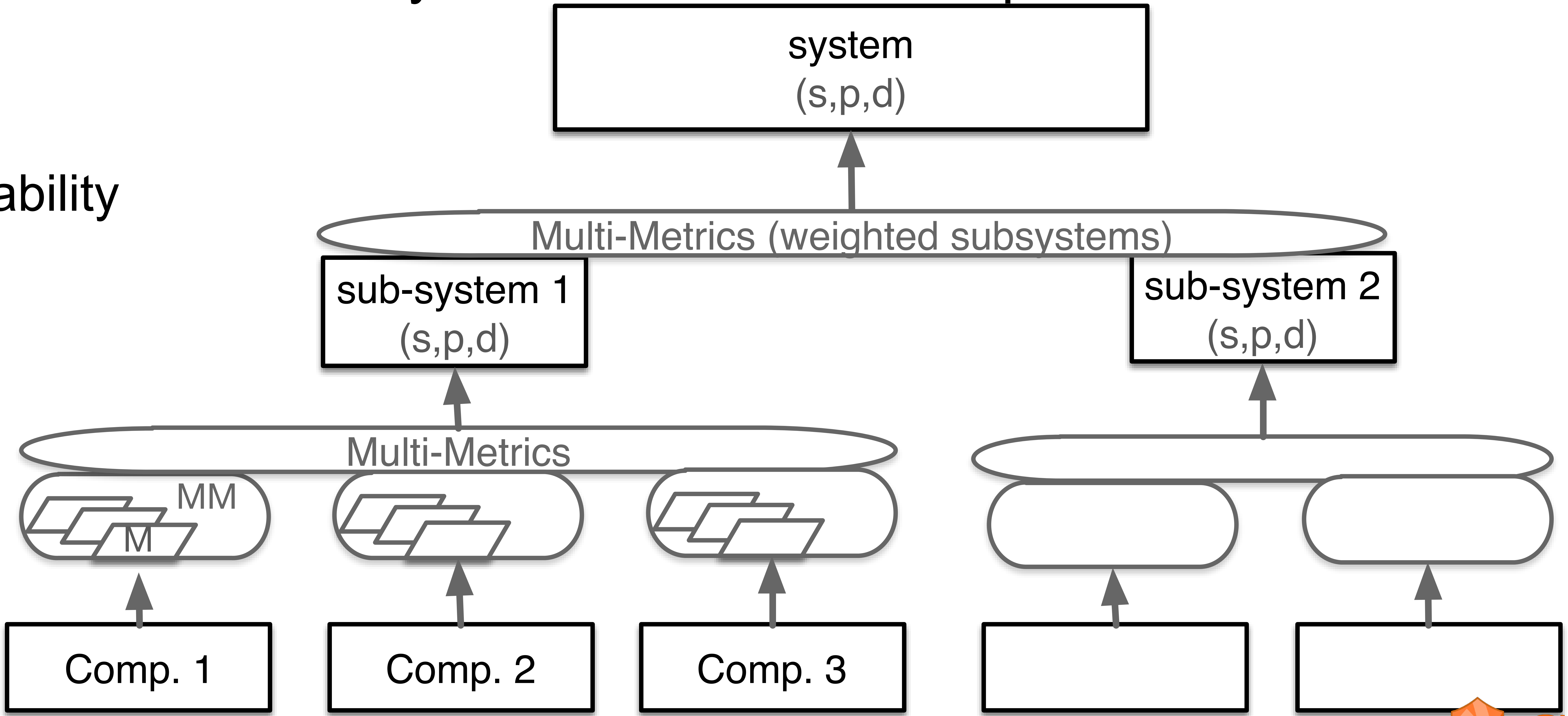
- based on
  - *security, privacy and dependability (SPD) functionalities*



System
is made by
Components and functionalities
could be
SPD Components, SPD functionalities
can be composed

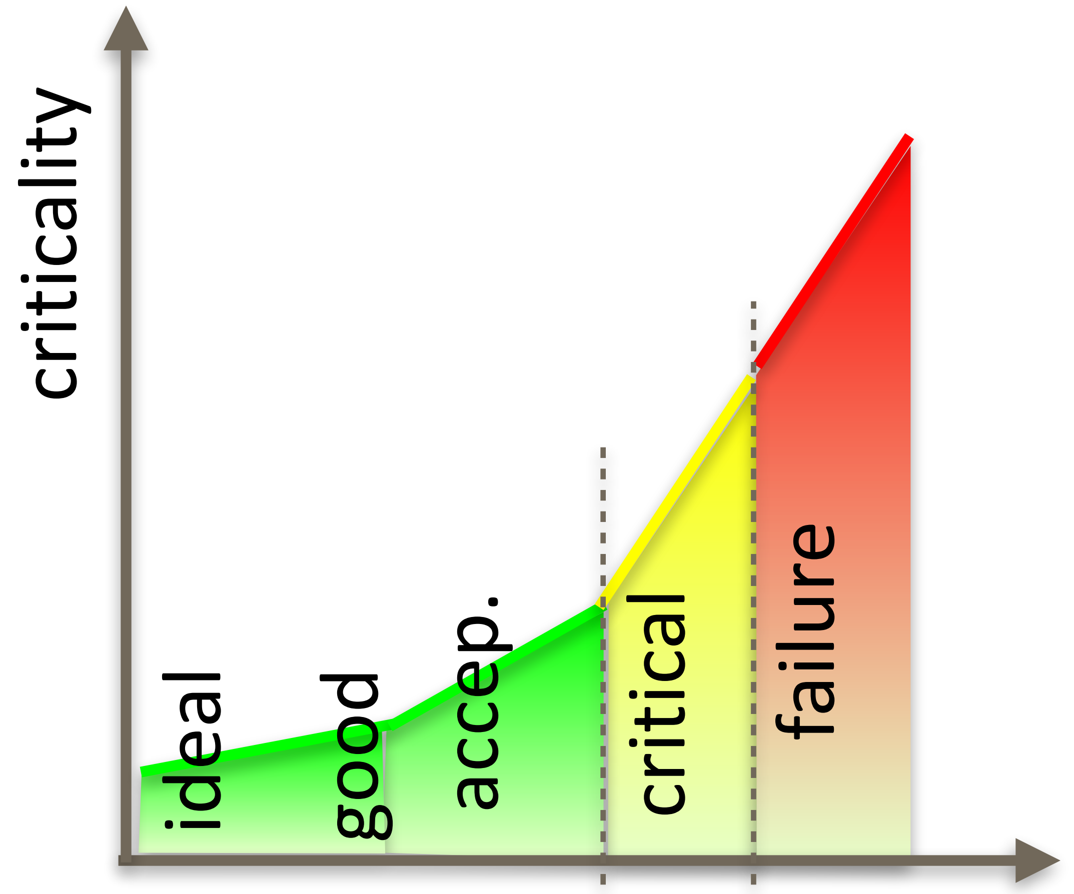
Multi-Metrics$_{v2}$ - system composition

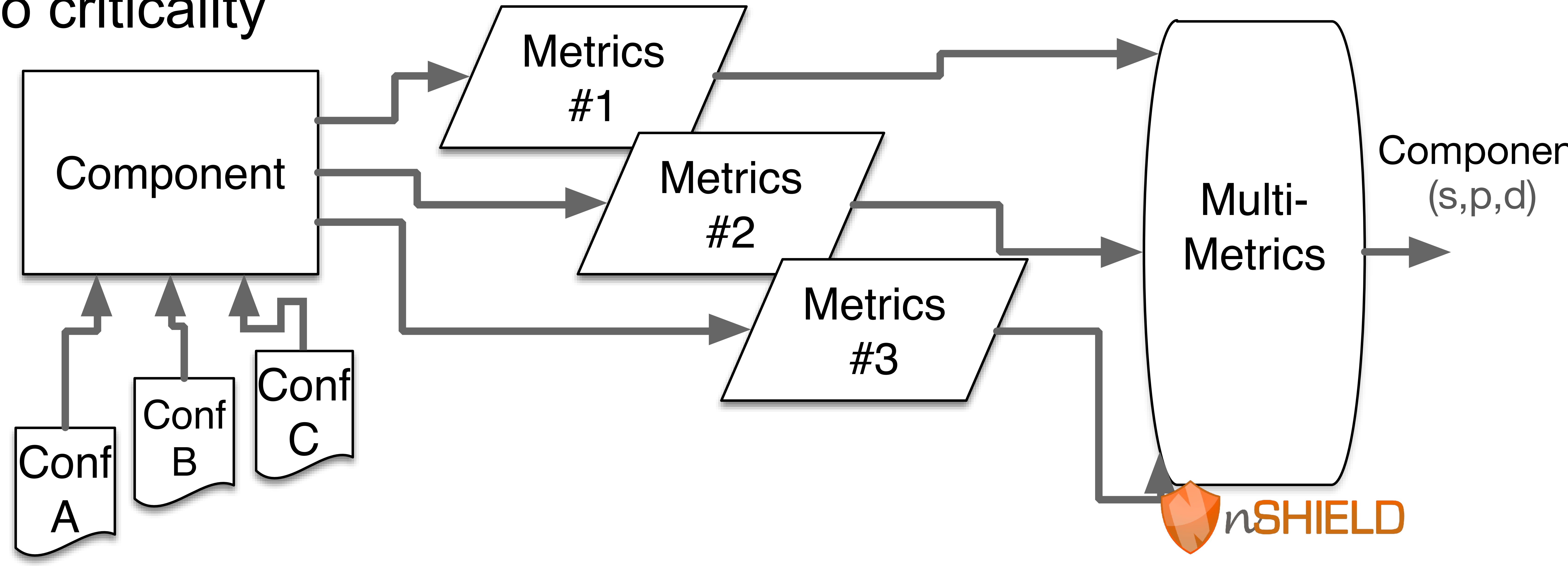
- System consists of sub-systems consists of components
  - ➡ security
  - ➡ privacy
  - ➡ dependability



Multi-Metrics components

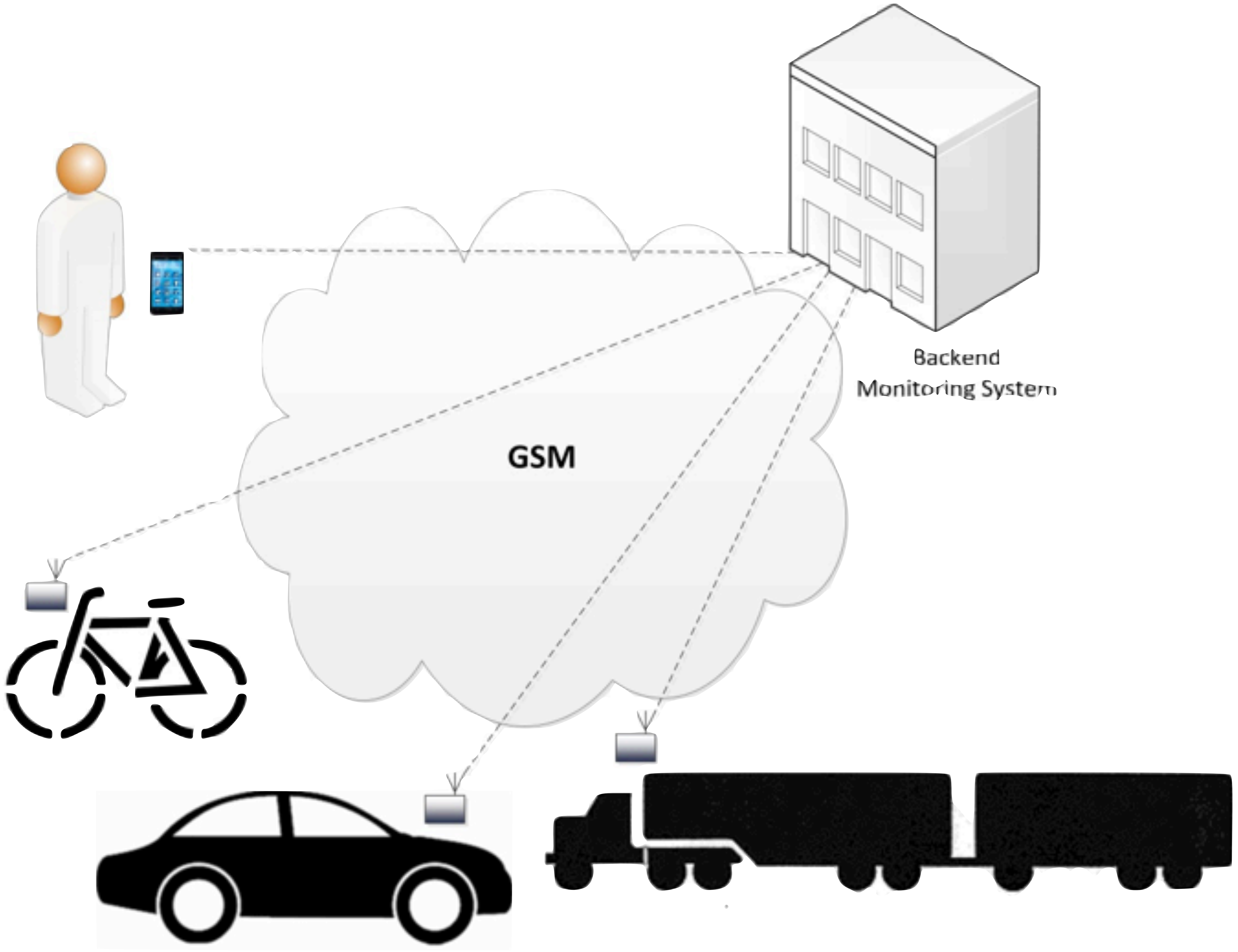
- Criticality (= 1 - Security) assessment
- Components have a security, privacy and dependability criticality
- Metrics assess the components
  - ➡ non-functional parameter to criticality
  - ➡ depend on configuration
  - ➡ weighting of metrics





Privacy: Loan of vehicle

- Scenario 1: privacy ensured, «user behaves»
- Scenario 2: track is visible as user drives too fast
- Scenario 3: Crash, emergency actions

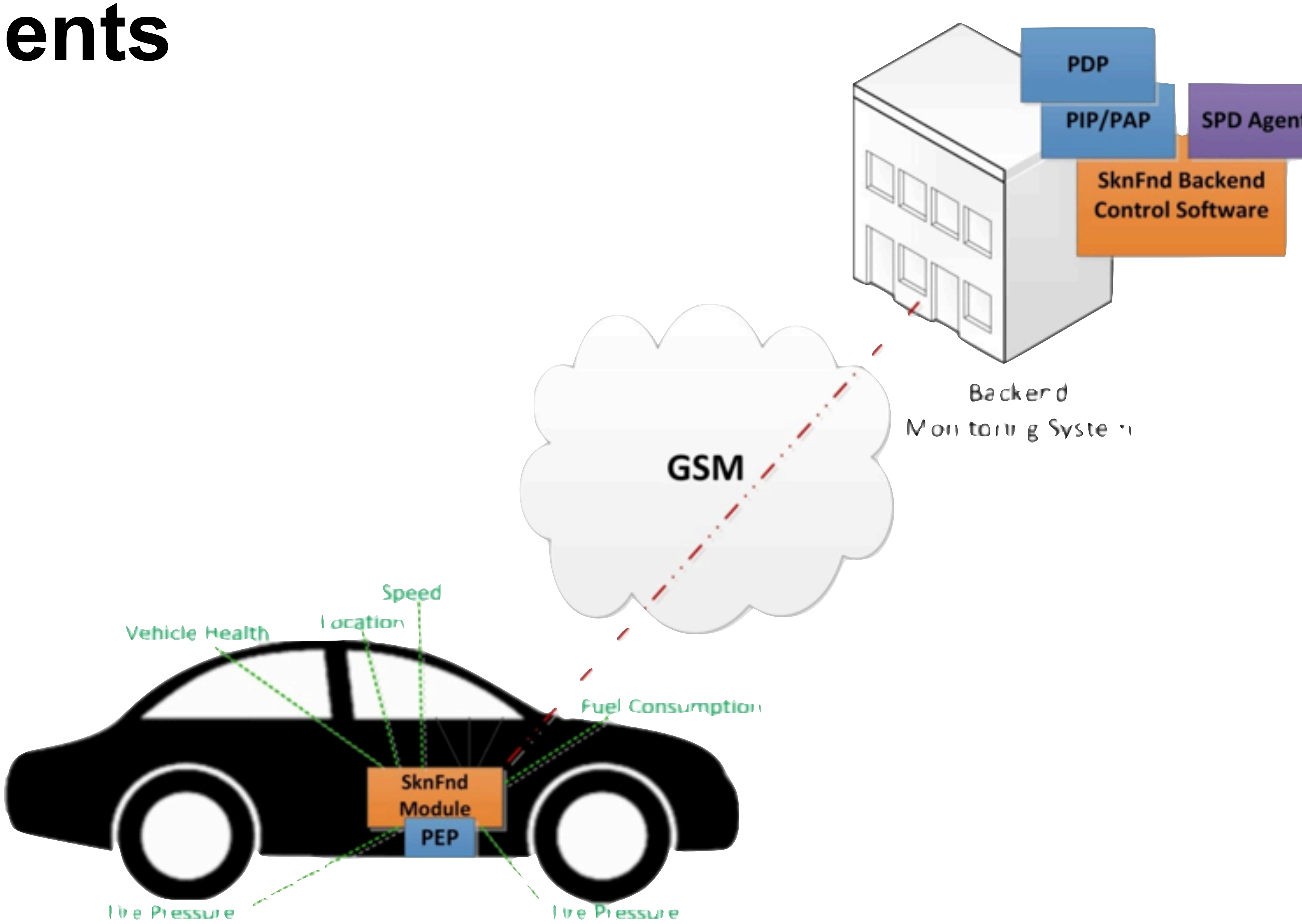


- Industrial applicability: Truck operation (Volvo), Autonomous operations on building places, add sensors (eye control)

Social Mobility Components

Applicable nSHIELD Components (Px):

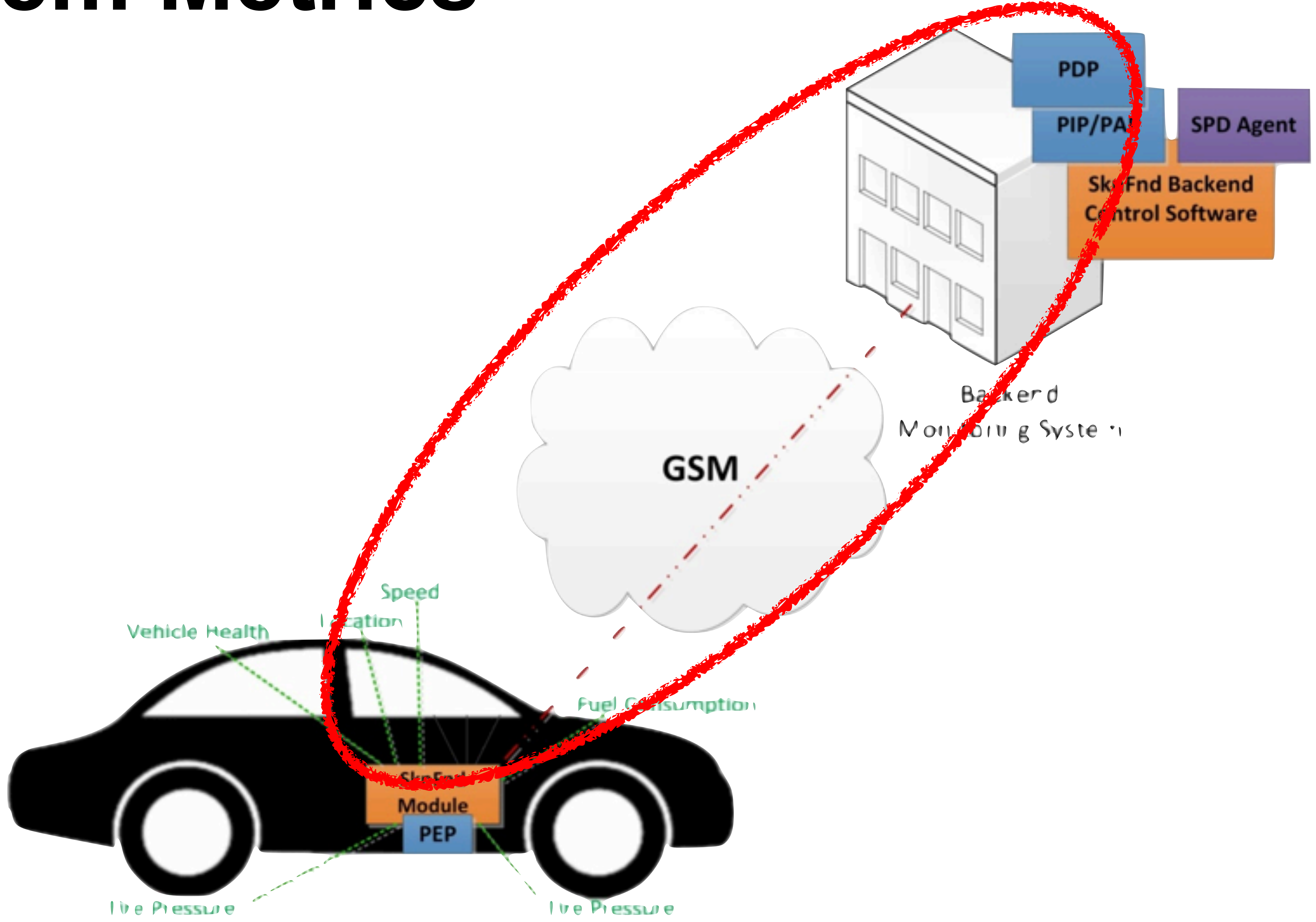
- 1- Lightweight Cyphering (P1)
- 2- Key exchange (P2)
- 3- Anonymity & Location Privacy (P10)
- 4- Automatic Access Control (P11)
- 5- Recognizing DoS Attack (P13)
- 6- Intrusion Detection System (P15)
- 7- Attack surface metrics (P28)
- 8- Embedded SIM, sensor (P38)
- 9- Multimetrics (P27)



Communication Subsystem Metrics

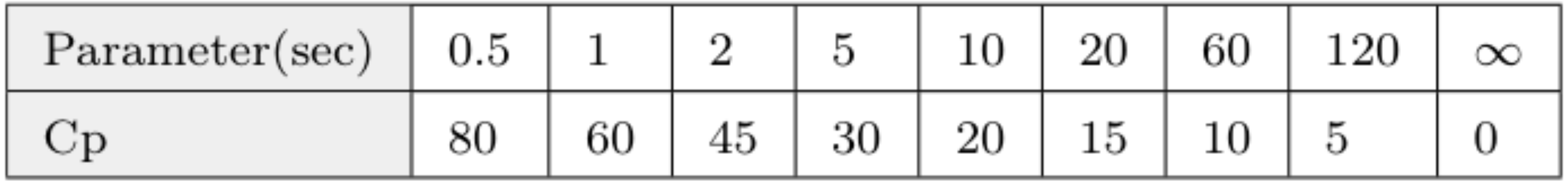
(SPD) Metrics

- ➡ Port metric
- ➡ Communication channel
- ➡ GPRS message rate
- ➡ SMS rate
- ➡ Encryption



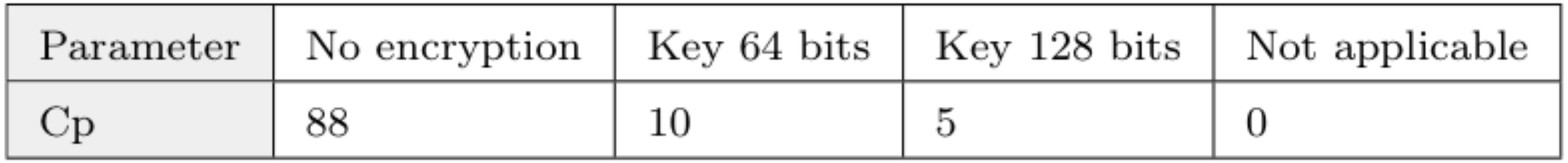
Social Mobility - Examples of Metrics

GPRS message rate metric



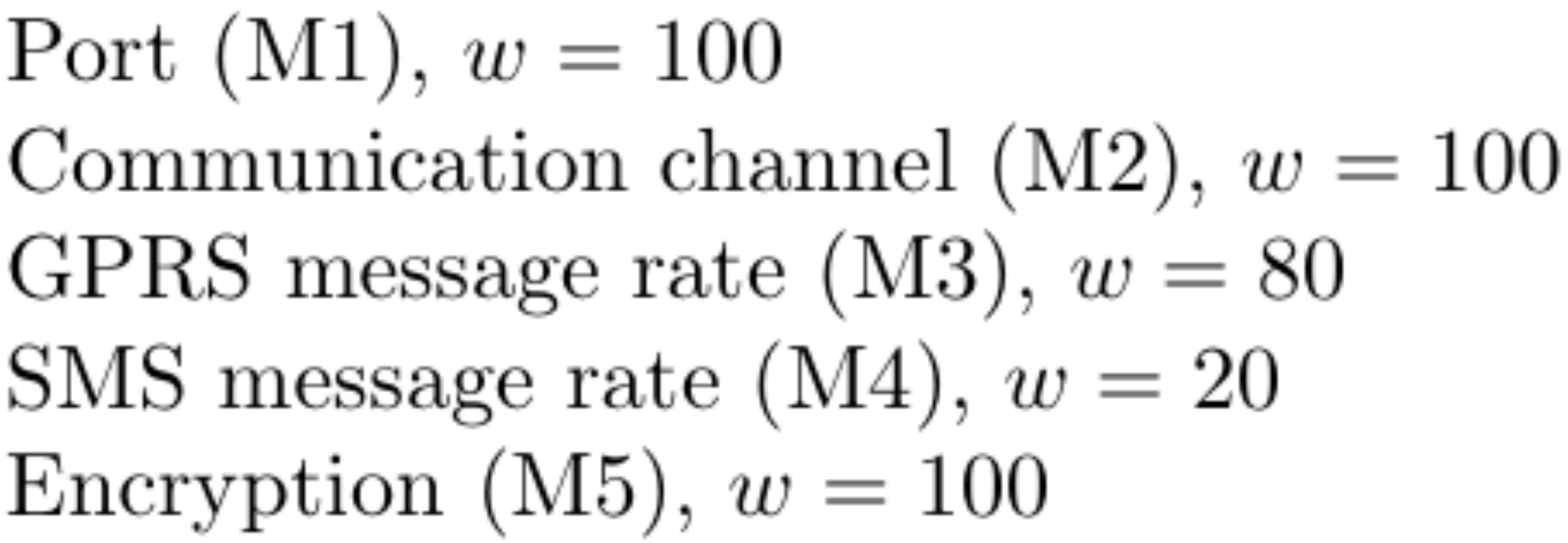
Parameter(sec)	0.5	1	2	5	10	20	60	120	∞
Cp	80	60	45	30	20	15	10	5	0

Encryption metric



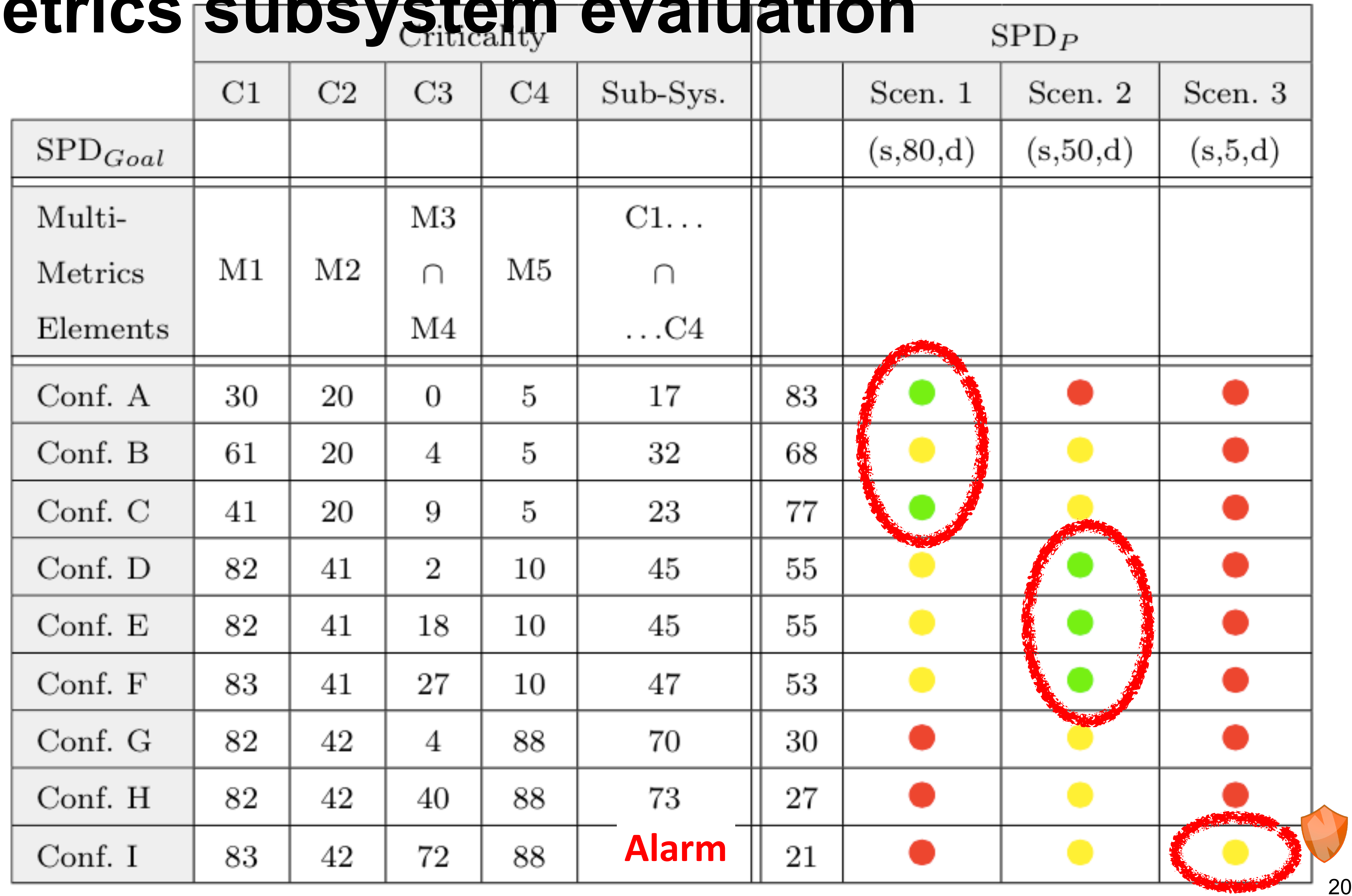
Parameter	No encryption	Key 64 bits	Key 128 bits	Not applicable
Cp	88	10	5	0

Metrics weighting



Port (M1), $w = 100$
Communication channel (M2), $w = 100$
GPRS message rate (M3), $w = 80$
SMS message rate (M4), $w = 20$
Encryption (M5), $w = 100$

Multi-Metrics subsystem evaluation



	Criticality					SPD$_P$			
	C1	C2	C3	C4	Sub-Sys.		Scen. 1	Scen. 2	Scen. 3
SPD$_{Goal}$							(s,80,d)	(s,50,d)	(s,5,d)
Multi-Metrics Elements	M1	M2	M3 $\cap$ M4	M5	C1... $\cap$ ...C4				
Conf. A	30	20	0	5	17	83	🟢	🔴	🔴
Conf. B	61	20	4	5	32	68	🟡	🟡	🔴
Conf. C	41	20	9	5	23	77	🟢	🟡	🔴
Conf. D	82	41	2	10	45	55	🟡	🟢	🔴
Conf. E	82	41	18	10	45	55	🟡	🟢	🔴
Conf. F	83	41	27	10	47	53	🟡	🟢	🔴
Conf. G	82	42	4	88	70	30	🔴	🟡	🔴
Conf. H	82	42	40	88	73	27	🔴	🟡	🔴
Conf. I	83	42	72	88	Alarm	21	🔴	🟡	🟡

SPD$_{Goal}$ versus System-SPD$_{Level}$

Smart Meter Application (Home)

- Application-based security goals
- Automated assessment

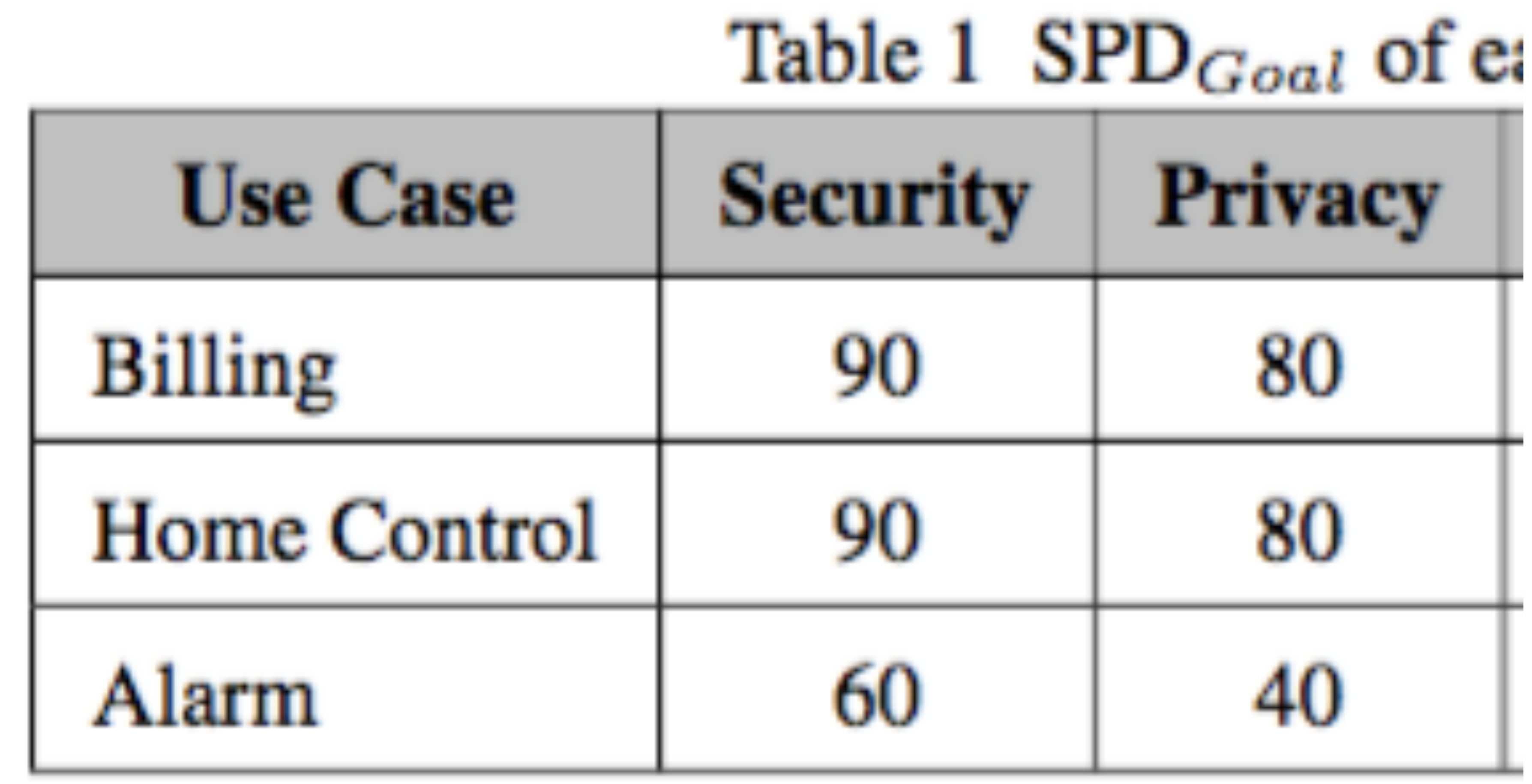


Table 1 SPD$_{Goal}$ of ea

Use Case	Security	Privacy
Billing	90	80
Home Control	90	80
Alarm	60	40

- Visualisation of "operating envelopes"
  - *Security good enough?*
  - *Too high Security*

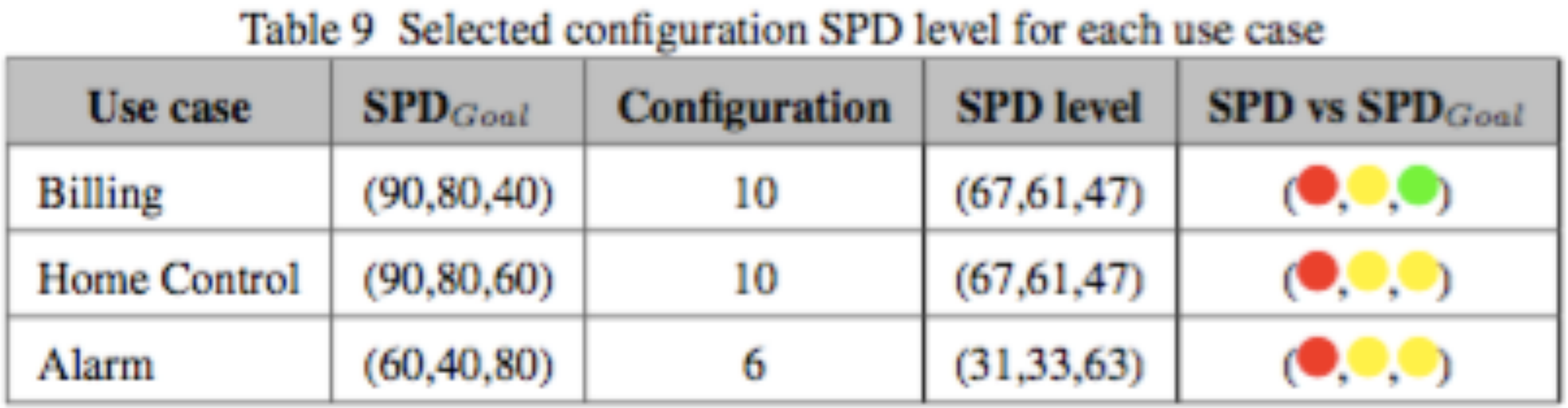


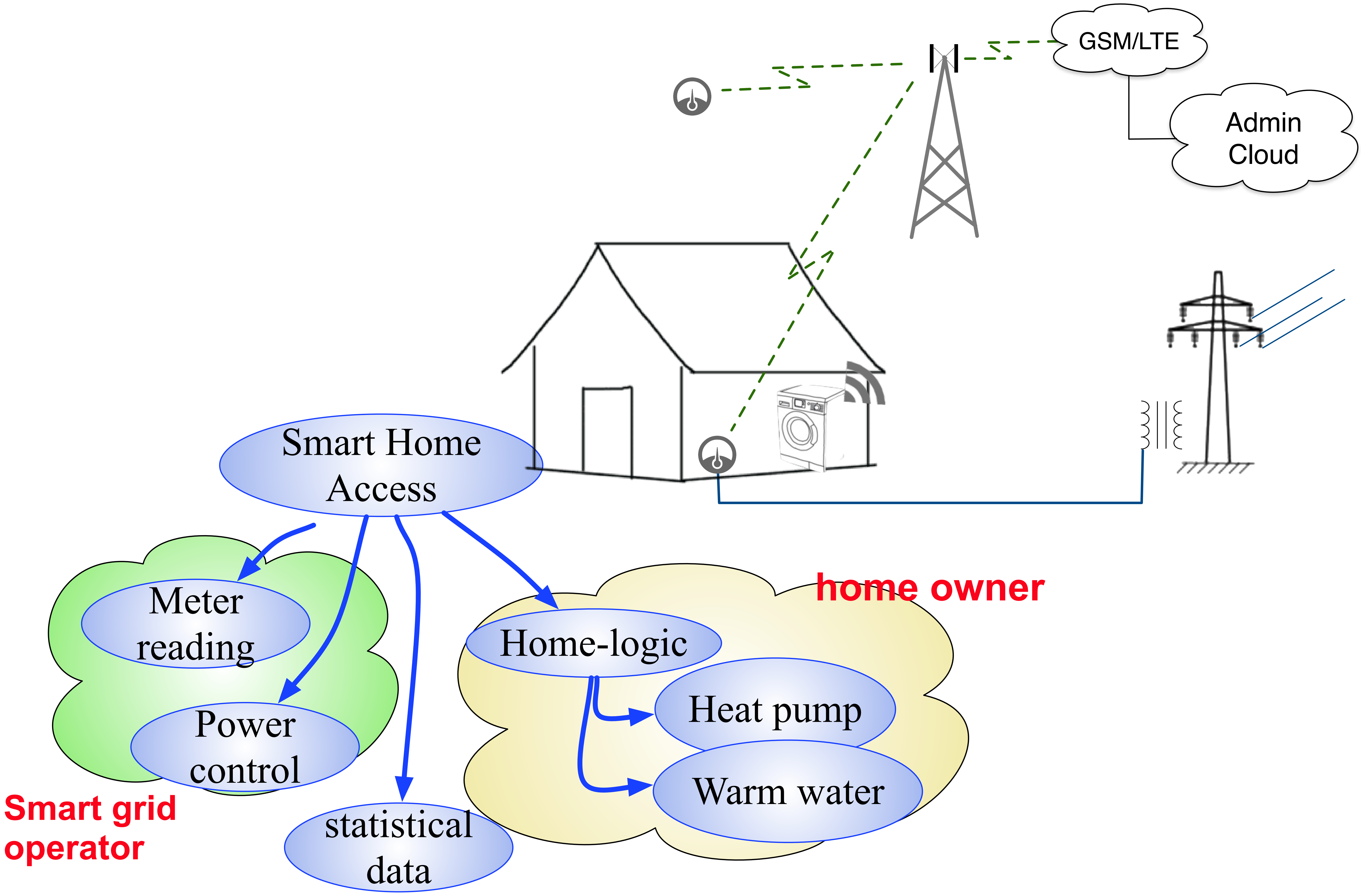
Table 9 Selected configuration SPD level for each use case

Use case	SPD$_{Goal}$	Configuration	SPD level	SPD vs SPD$_{Goal}$
Billing	(90,80,40)	10	(67,61,47)	(🔴,🟡,🟢)
Home Control	(90,80,60)	10	(67,61,47)	(🔴,🟡,🟡)
Alarm	(60,40,80)	6	(31,33,63)	(🔴,🟡,🟡)

- Critical component/sub-system assessment

Semantic attribute based access control (S-ABAC)

- Lifting the security class through S-ABAC
- Access to information
  - □ *who (sensor, person, service)*
  - □ *what kind of information*
  - □ *from where*
- Attribute-based access
  - □ *role (in organisation, home)*
  - □ *device, network*
  - □ *security tokens*
- Rules inferring access rights



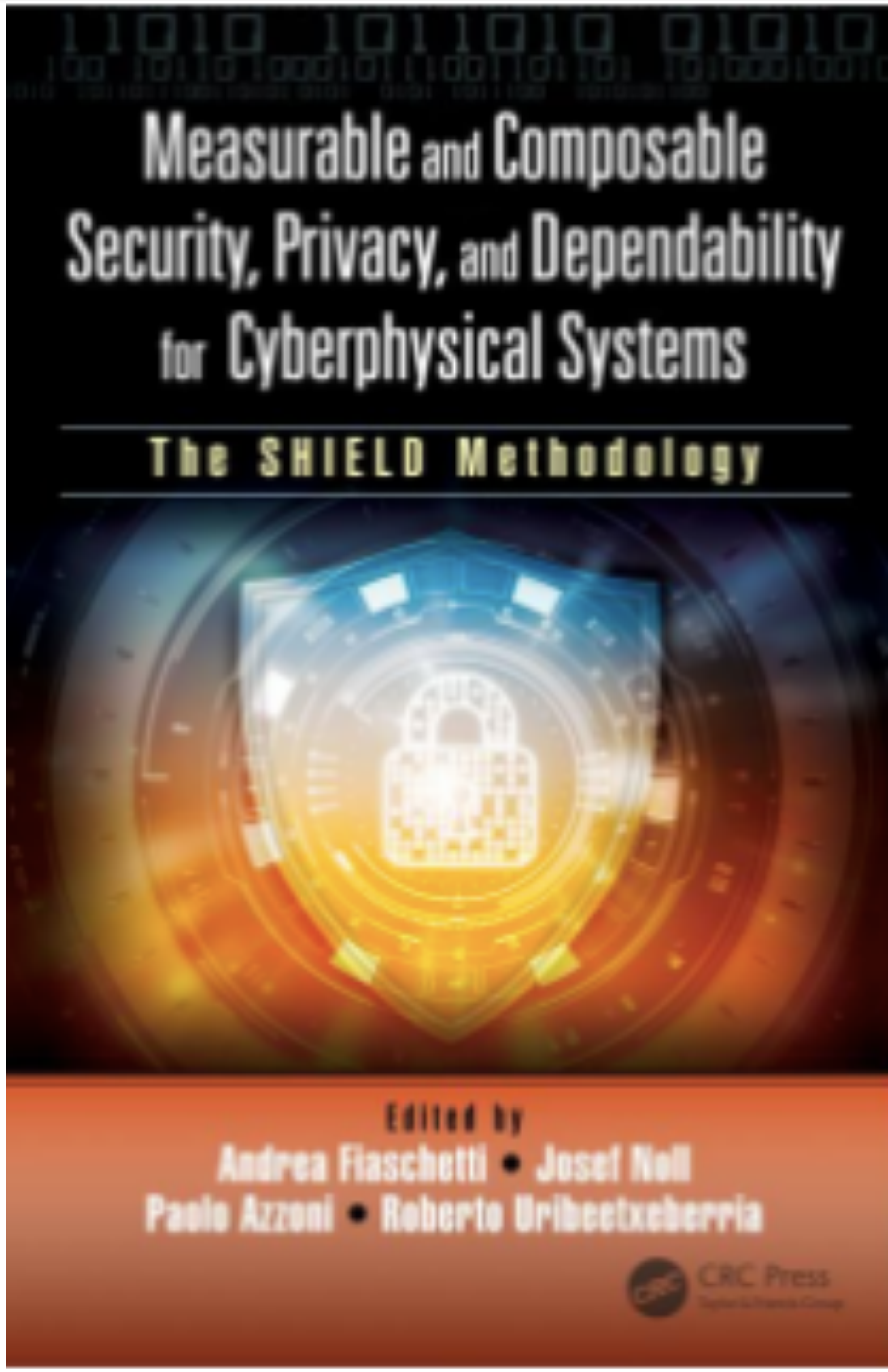
Attributes: roles, access, device, reputation, behaviour, ...

Further information

TEK5530 - Measurable Security for the Internet of Things
https://its-wiki.no/wiki/TEK5530

- L10: Multi-Metrics method for measurable security and privacy
  https://its-wiki.no/images/3/37/UNIK4750-L10_Multi-Metrics.pdf

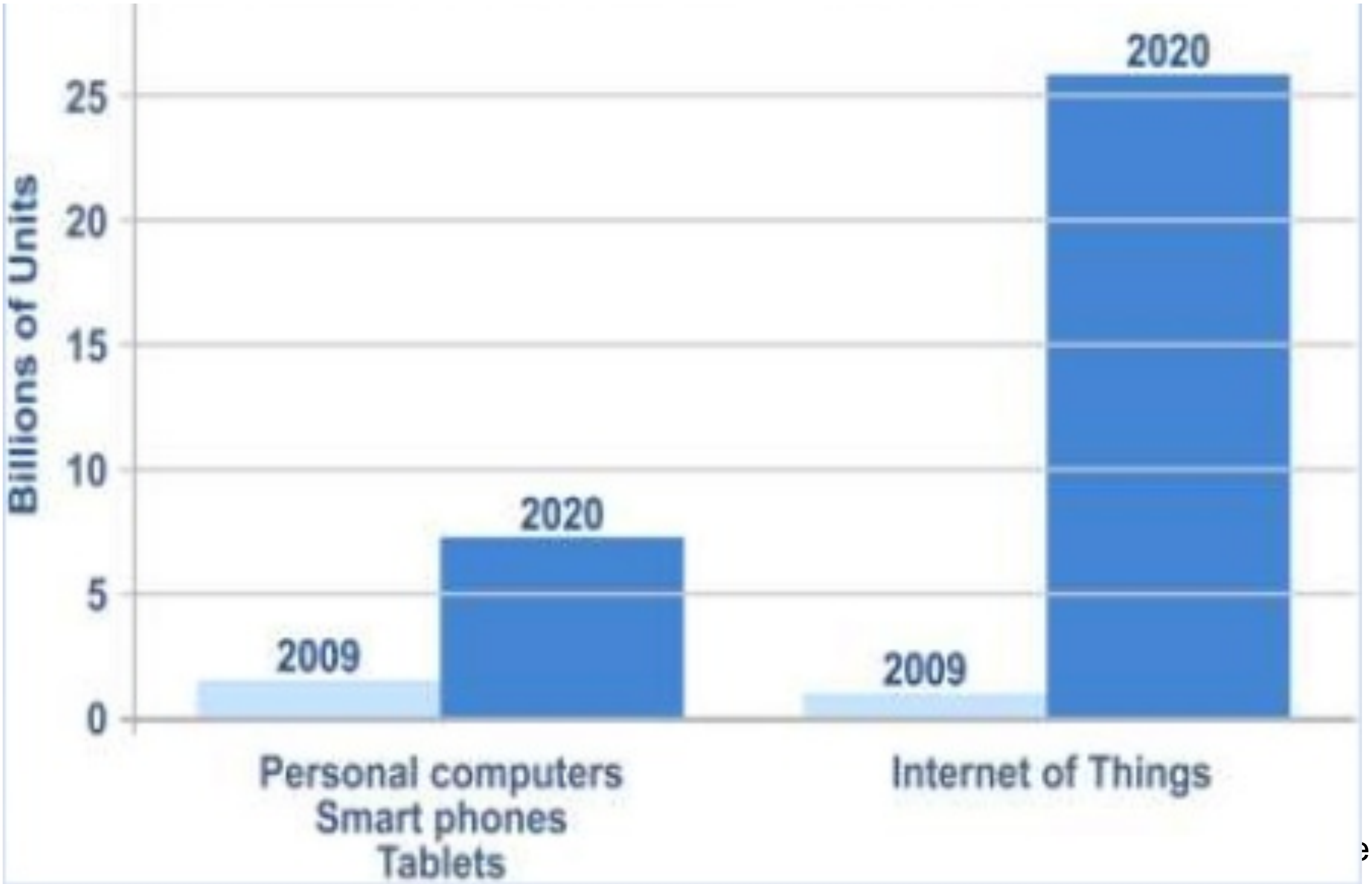
- L11: System Security and Privacy analysis, weighting of components and sub-systems
  https://its-wiki.no/images/b/b2/UNIK4750-L11_System_Security_Privacy.pdf


Measurable and Composable
Security, Privacy, and Dependability
for Cyberphysical Systems
The SHIELD Methodology
Edited by
Andrea Fiaschetti • Josef Noll
Paolo Azzoni • Roberto Uribeetxeberria
CRC Press

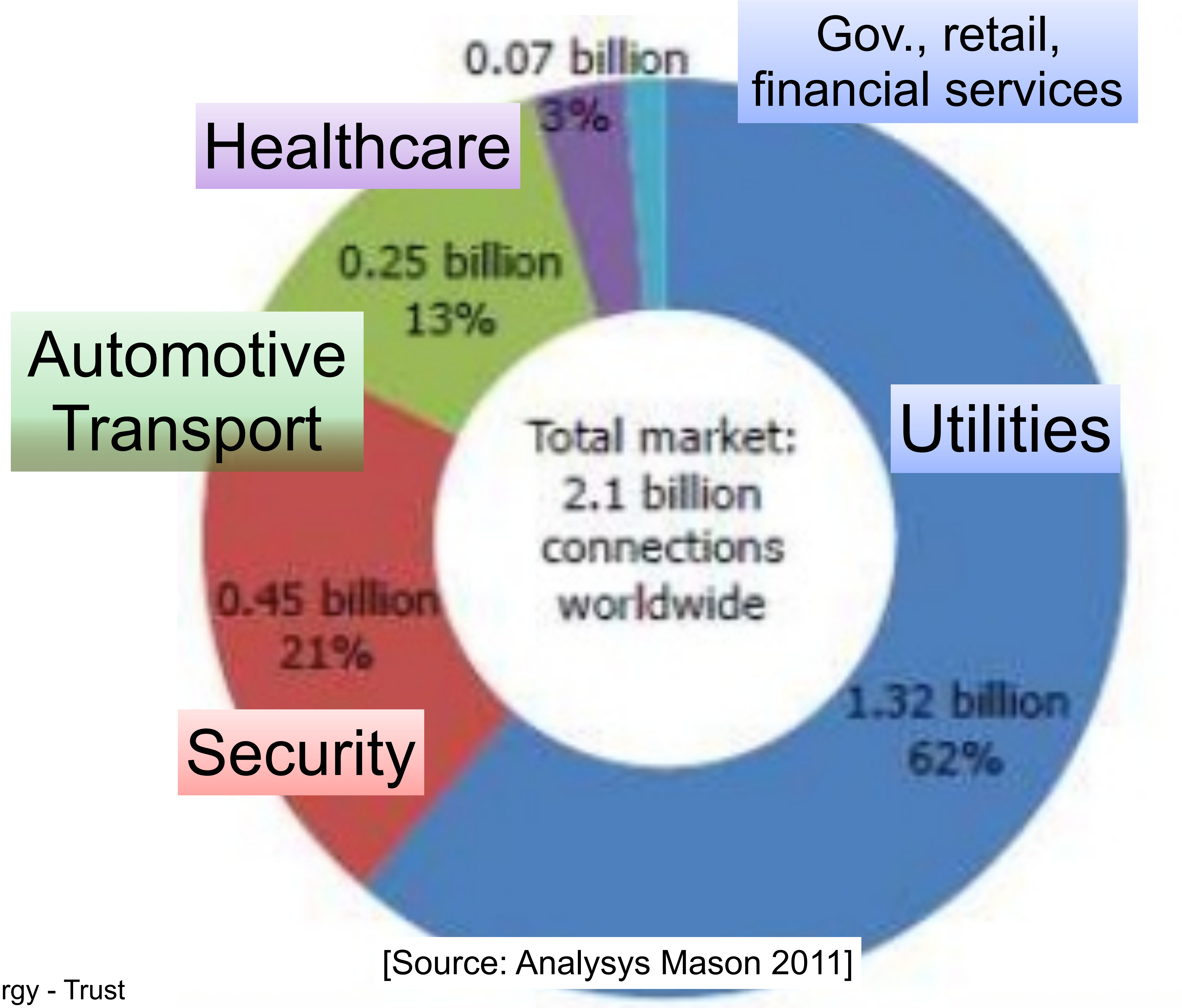
- Papers describing the Multi-Metrics_approach:
- I. Garitano, S. Fayyad, J. Noll, «Multi-Metrics Approach for Security, Privacy and Dependability in Embedded Systems», Wireless Pers. Commun. 81, pp1359-1376 (2015)
- J. Noll, I. Garitano, S. Fayyad, E. Åsberg, H. Abie, «Measurable Security, Privacy and Dependability in Smart Grids», Journal of Cyber Security, 3_4, (2015) -> http://riverpublishers.com/journal/journal_articles/RP_Journal_2245-1439_342.pdf

IoT & Automated processes

IoT - 10 x impact of Internet



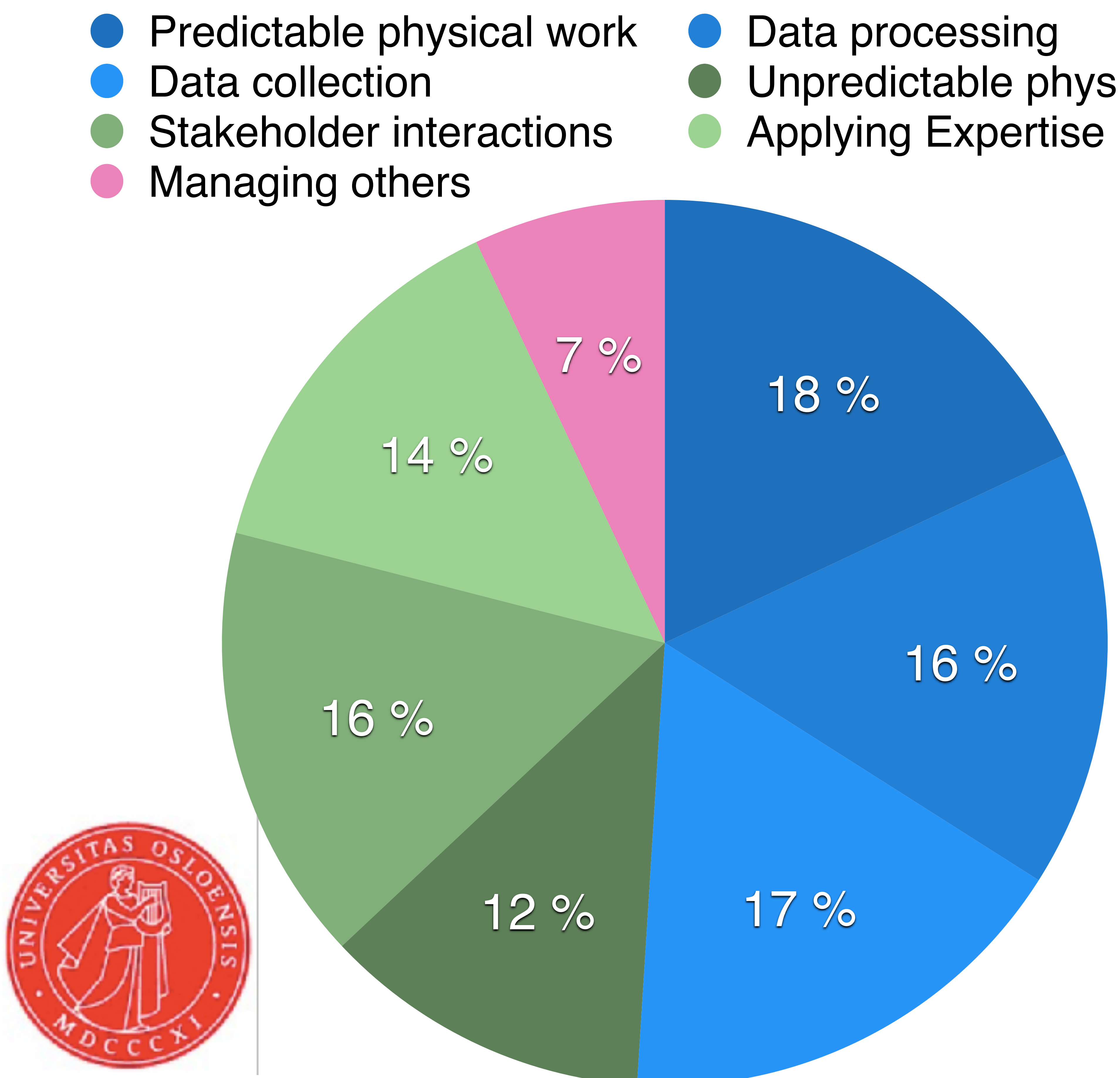
Commercial & Consumer M2M Device Connections Worldwide 2020



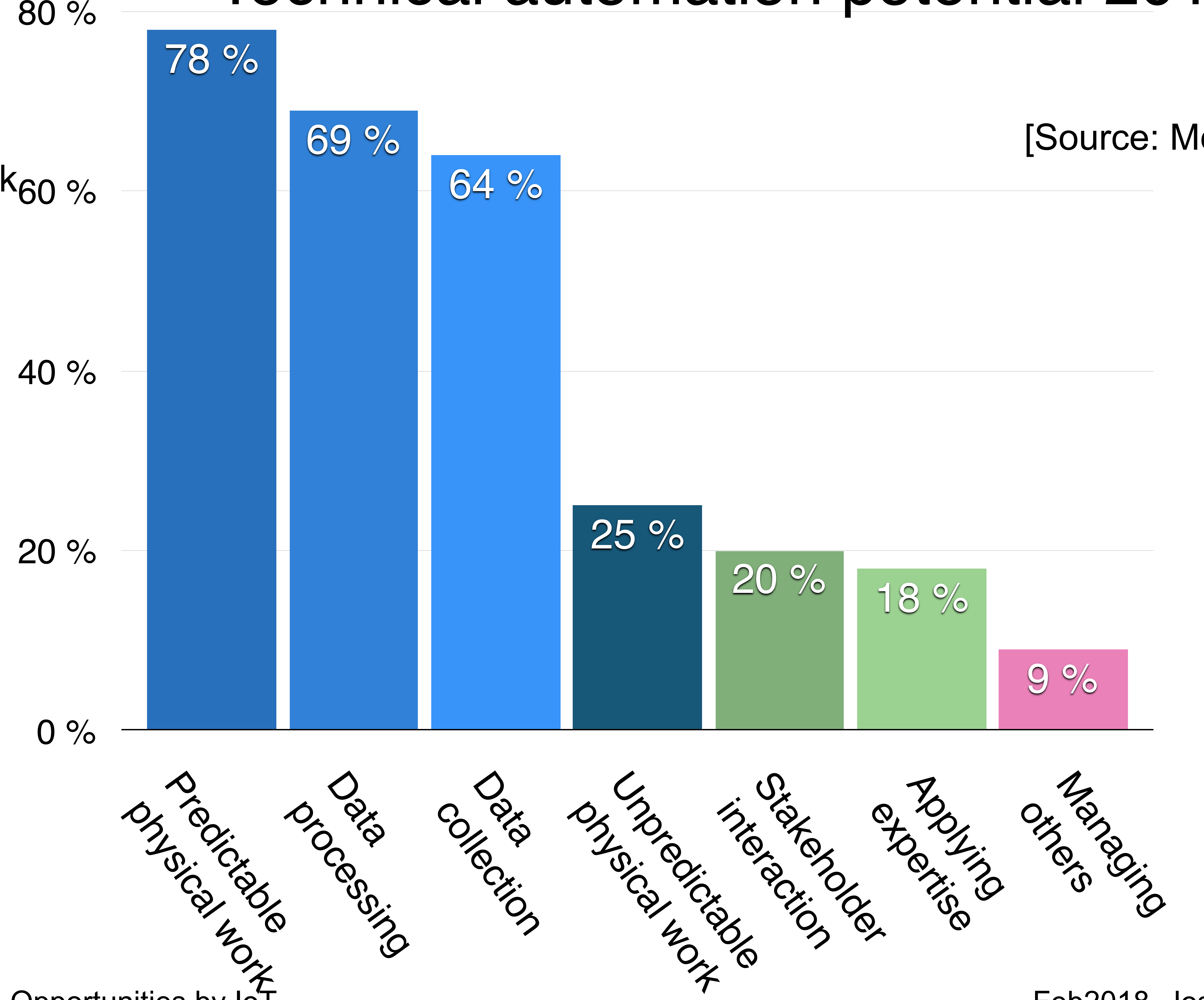
[Source: Analysys Mason 2011]

The challenge from automation

USA work force time spent [%]



Technical automation potential 2016 [%]



[Source: McKinsey, 2016]

Security classes and IoT lifecycle

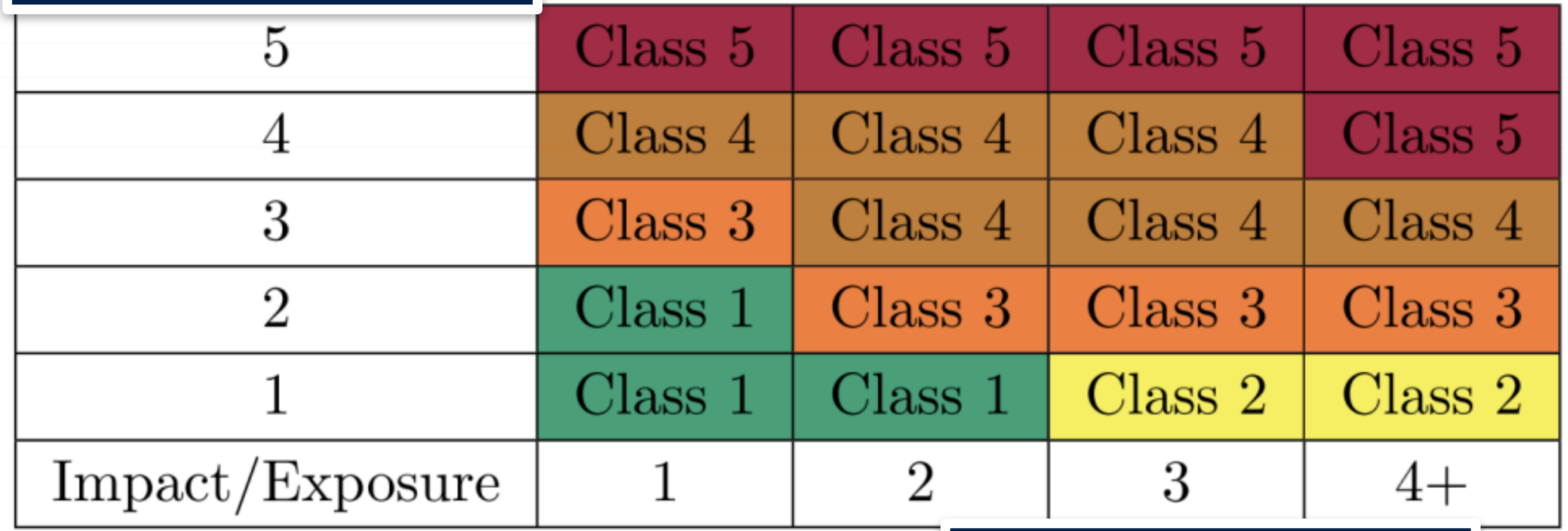
Security Classes and System design

- Security Classes in IoT
  - *Consequence*
  - *Exposure*
- Consequence
  - *as in risk map*
- Exposure
  - *Physical exposure*
    - people, building, physical ports,…
  - *IT exposure*
    - ports, firewall, connectivity
- Used to assess the security class ems and components

New postulate of securi ss

Security Class

Consequence



5	Class 5	Class 5	Class 5	Class 5
4	Class 4	Class 4	Class 4	Class 5
3	Class 3	Class 4	Class 4	Class 4
2	Class 1	Class 3	Class 3	Class 3
1	Class 1	Class 1	Class 2	Class 2
Impact/Exposure	1	2	3	4+

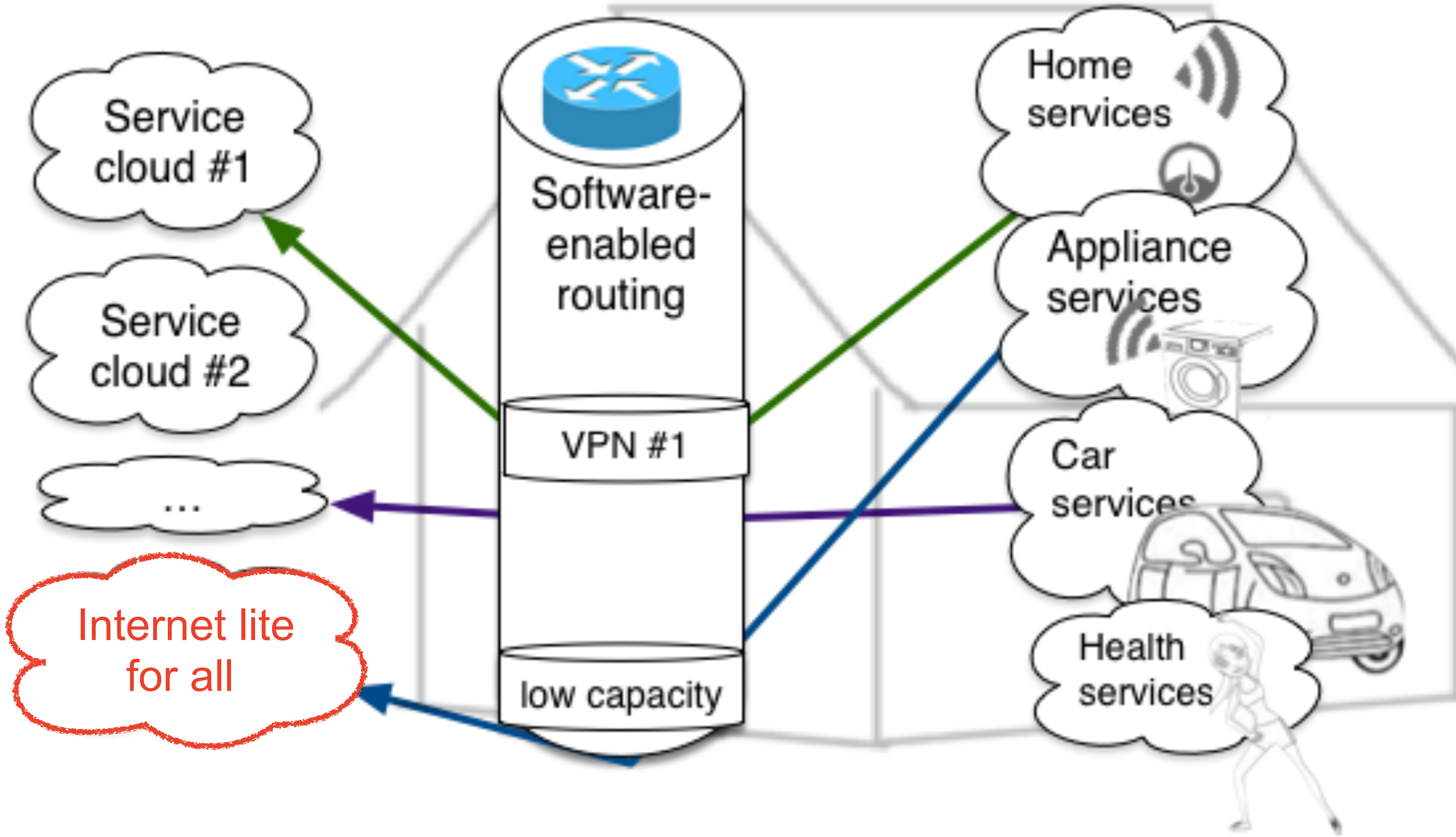
Exposure

Increase weak security:
- watchdog
- Attribute based access control (S-ABAC)

Vision for the Home Domain

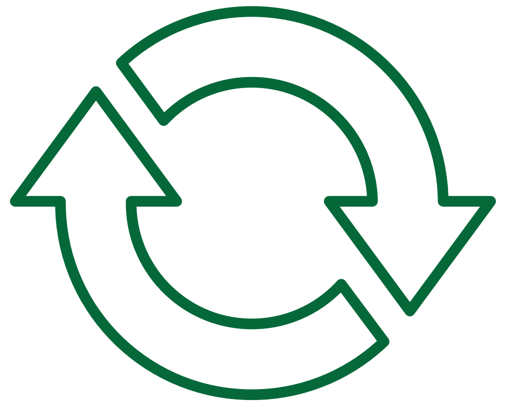
- Novel services in the home
  - ➡ Alarm, eHealth
    - high reliability
  - ➡ Appliances
    - convenience, “fridge door open”
  - ➡ Car/Home battery
    - balancing the grid

- Cost-efficient monitoring and management for trusted services
  - ➡ Wireless management
  - ➡ Security monitoring
  - ➡ Service harmonisation (5G@home)

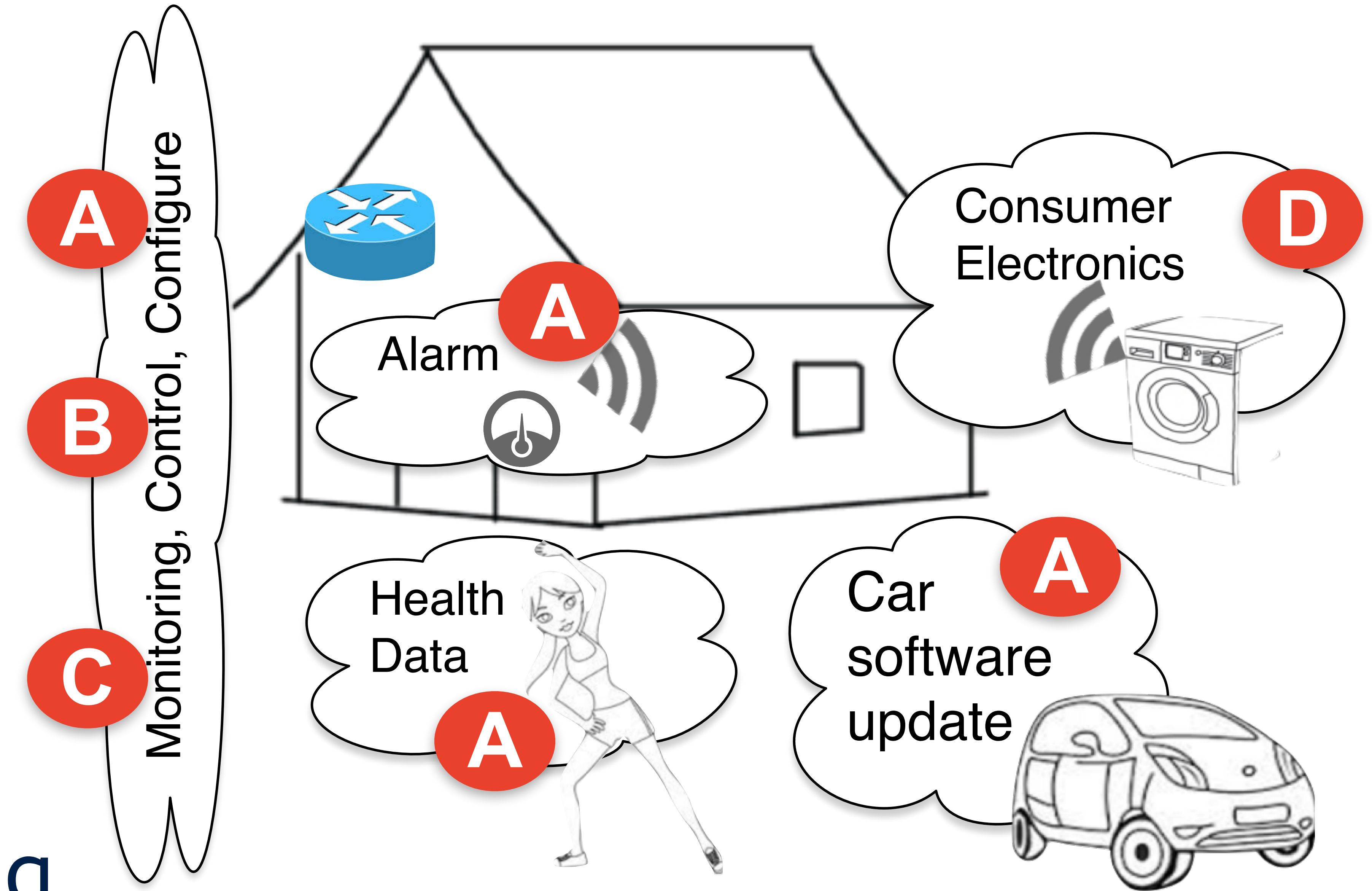


Security Paradigm / Security Classes

- Security classes A B C D
  - Target security goals for design (home alarm = Sec Class A)
  - build the system, security enhancing technologies
    - link data from Class D (consumer electronics) into Class A operation
  - validation, check against threats ("continuous update")
- Metrics and indicators for different stages of the IoT life-cycle
- Novel Risk Map: Impact over Exposure
  - Common weakness score system
  - Composite security metrics
- Certification methodologies
  - Risk database versus exposure database
- Benefits: quick security evaluation and budget planning



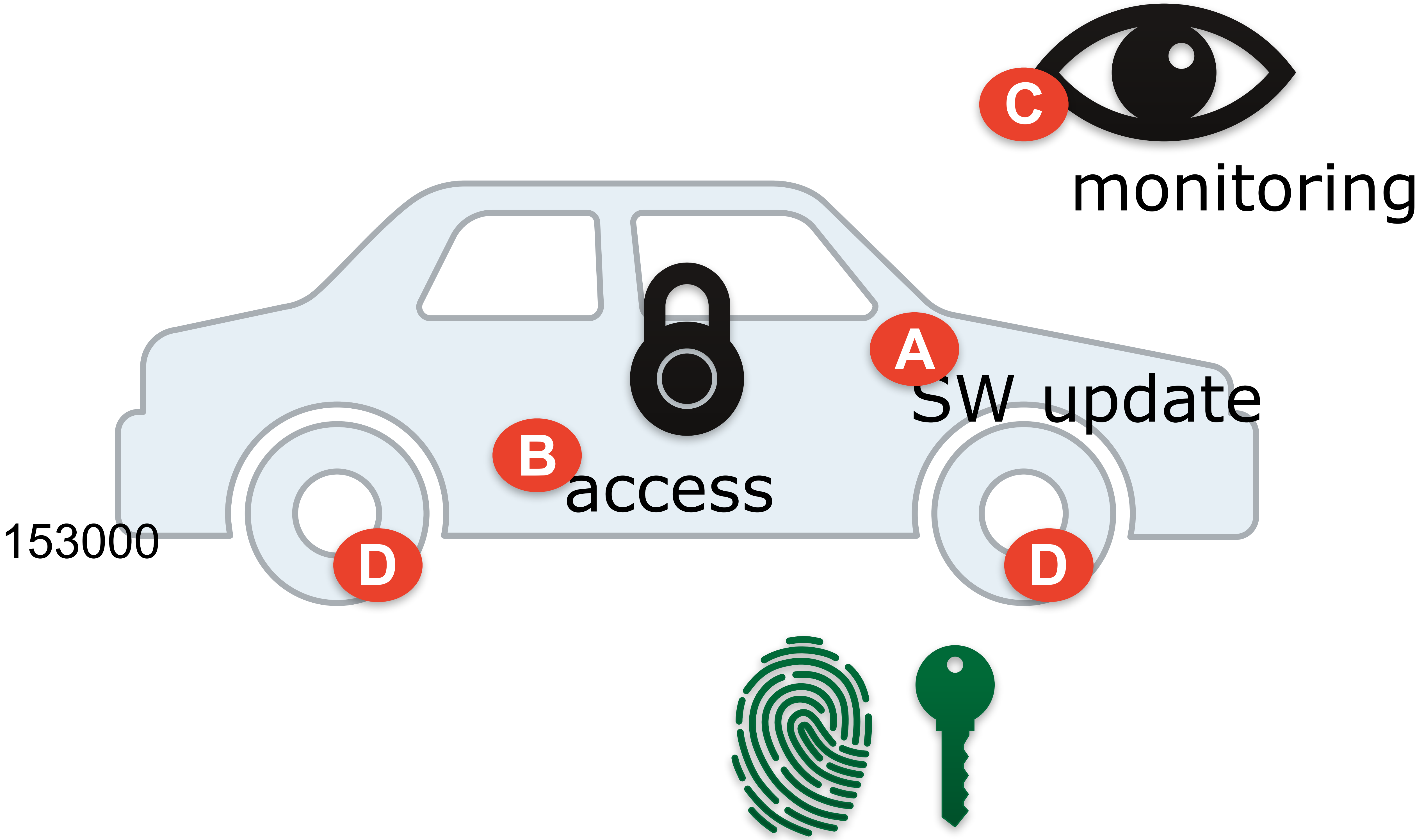
IoT lifecycle



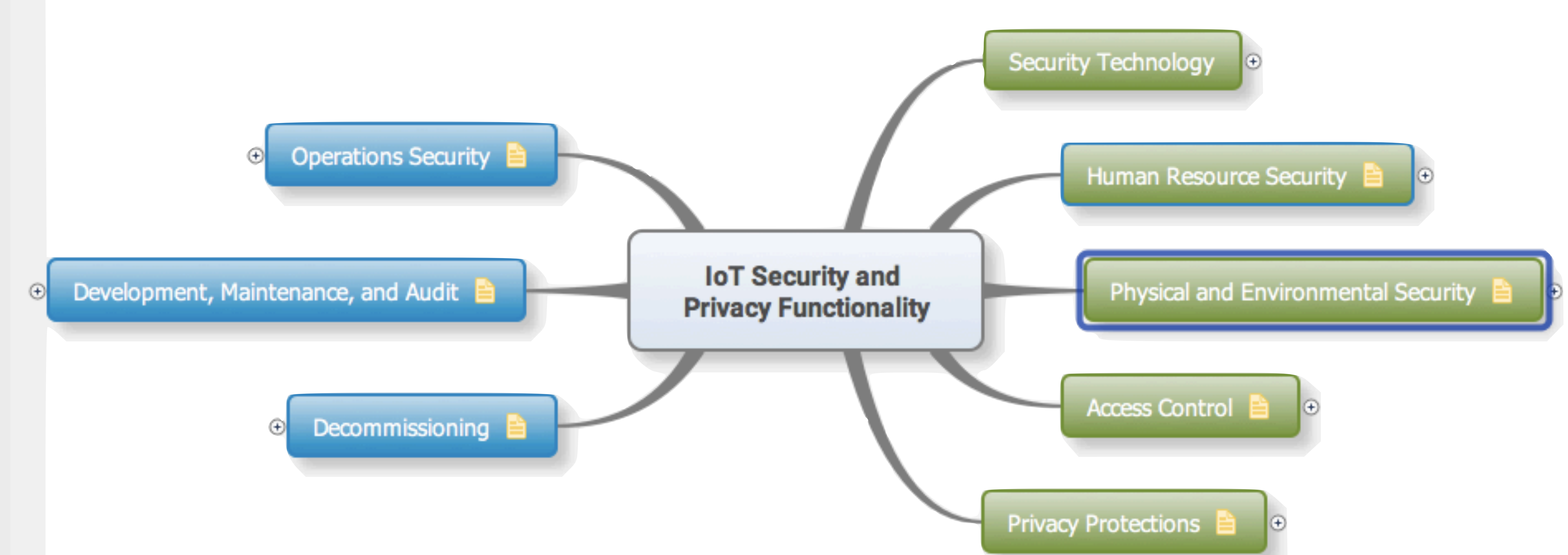
Example for Domain specific applicability: Automotive Security Classes

- Suggested methodology:
- The car as a system of systems
  - apply trust framework
  - apply security classes (car components)
  - security technologies

- For each subsystem, perform
- Security classes: A B C D
  - Exposure analysis of components
  - Threat analysis
  - Expected Impact

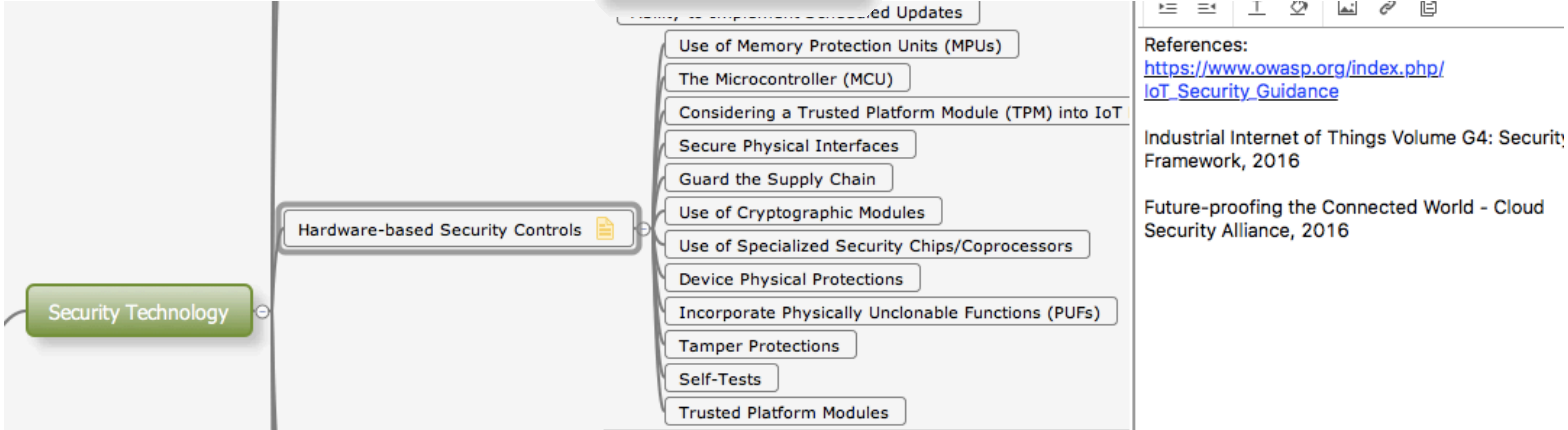


Security and Privacy Functionality



IoT Security and Privacy Functionality

- Operations Security
- Development, Maintenance, and Audit
- Decommissioning
- Security Technology
- Human Resource Security
- Physical and Environmental Security
- Access Control
- Privacy Protections



- Security Technology
  - Hardware-based Security Controls
    - Ability to implement Scheduled Updates
    - Use of Memory Protection Units (MPUs)
    - The Microcontroller (MCU)
    - Considering a Trusted Platform Module (TPM) into IoT
    - Secure Physical Interfaces
    - Guard the Supply Chain
    - Use of Cryptographic Modules
    - Use of Specialized Security Chips/Coprocessors
    - Device Physical Protections
    - Incorporate Physically Unclonable Functions (PUFs)
    - Tamper Protections
    - Self-Tests
    - Trusted Platform Modules

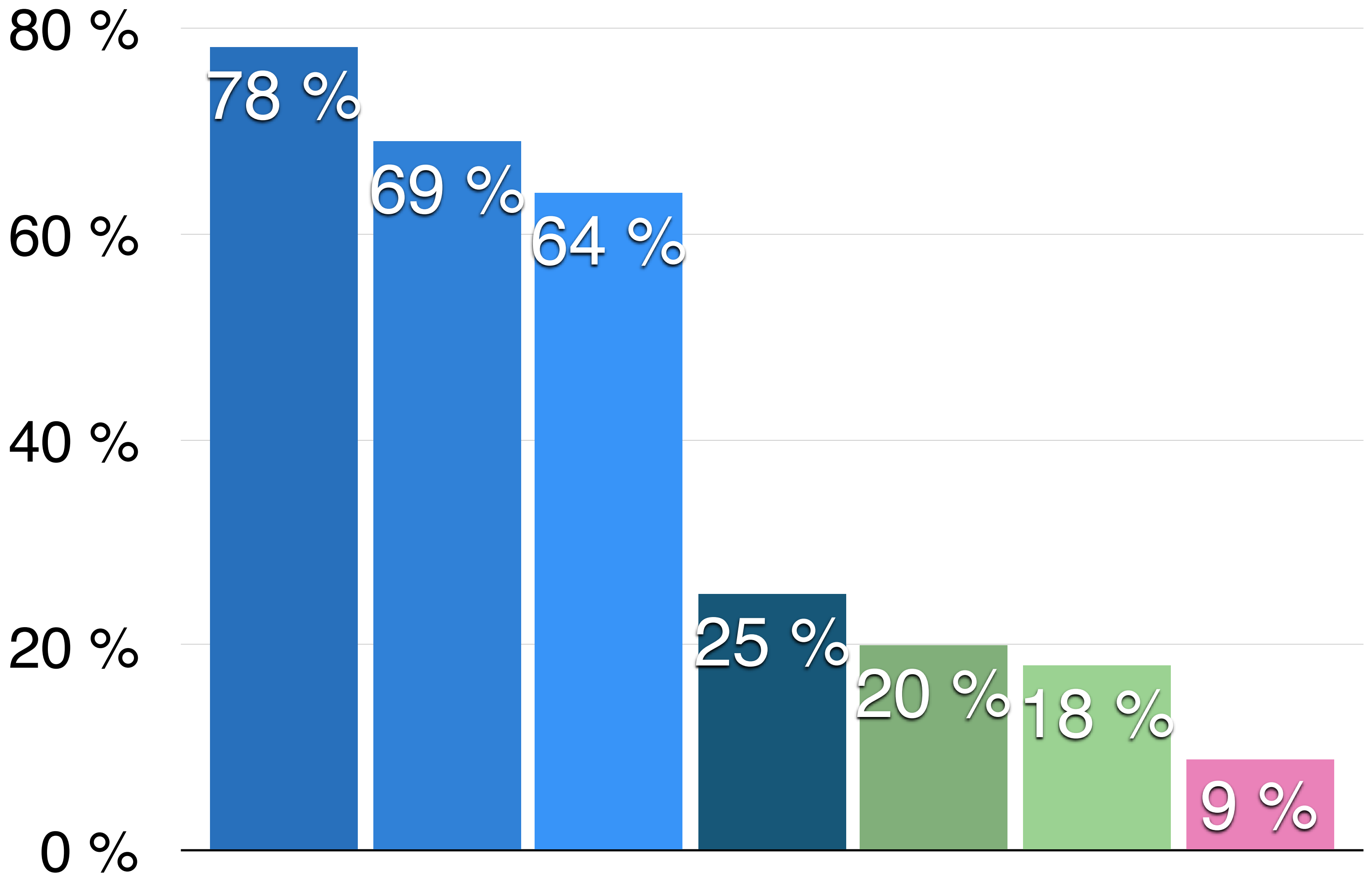
References:
https://www.owasp.org/index.php/IoT_Security_Guidance

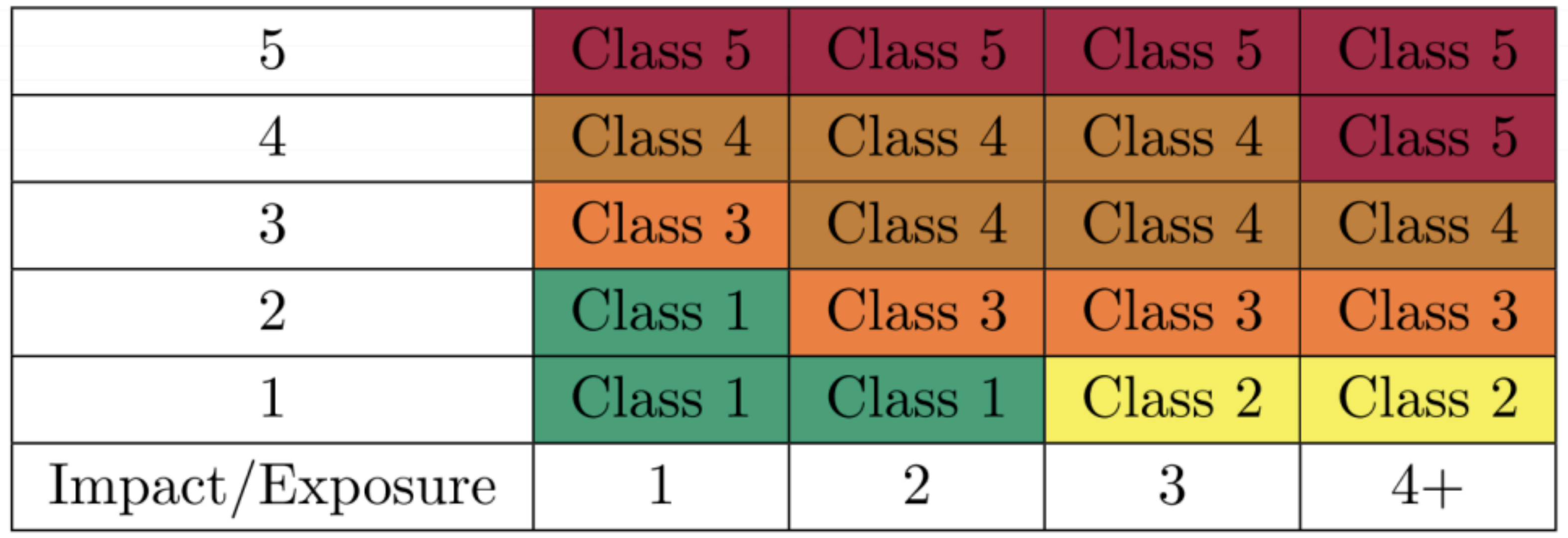
Industrial Internet of Things Volume G4: Security Framework, 2016

Future-proofing the Connected World - Cloud Security Alliance, 2016

Security - Conclusions

- Things (IoT) are driving the digital societies
- IoT: Business merger
  - Internet + Semantics + Things = IoT
  - Lifecycle of IoT
- Accountable Security
  - Attack-based & Vulnerability-based are not scalable
  - Security classes
  - Impact and Exposure





5	Class 5	Class 5	Class 5	Class 5
4	Class 4	Class 4	Class 4	Class 5
3	Class 3	Class 4	Class 4	Class 4
2	Class 1	Class 3	Class 3	Class 3
1	Class 1	Class 1	Class 2	Class 2
Impact/Exposure	1	2	3	4+

Autonomous system - Security considerations

- ➡ Trust in IoT systems
- ➡ Workforce
- ➡ Real systems

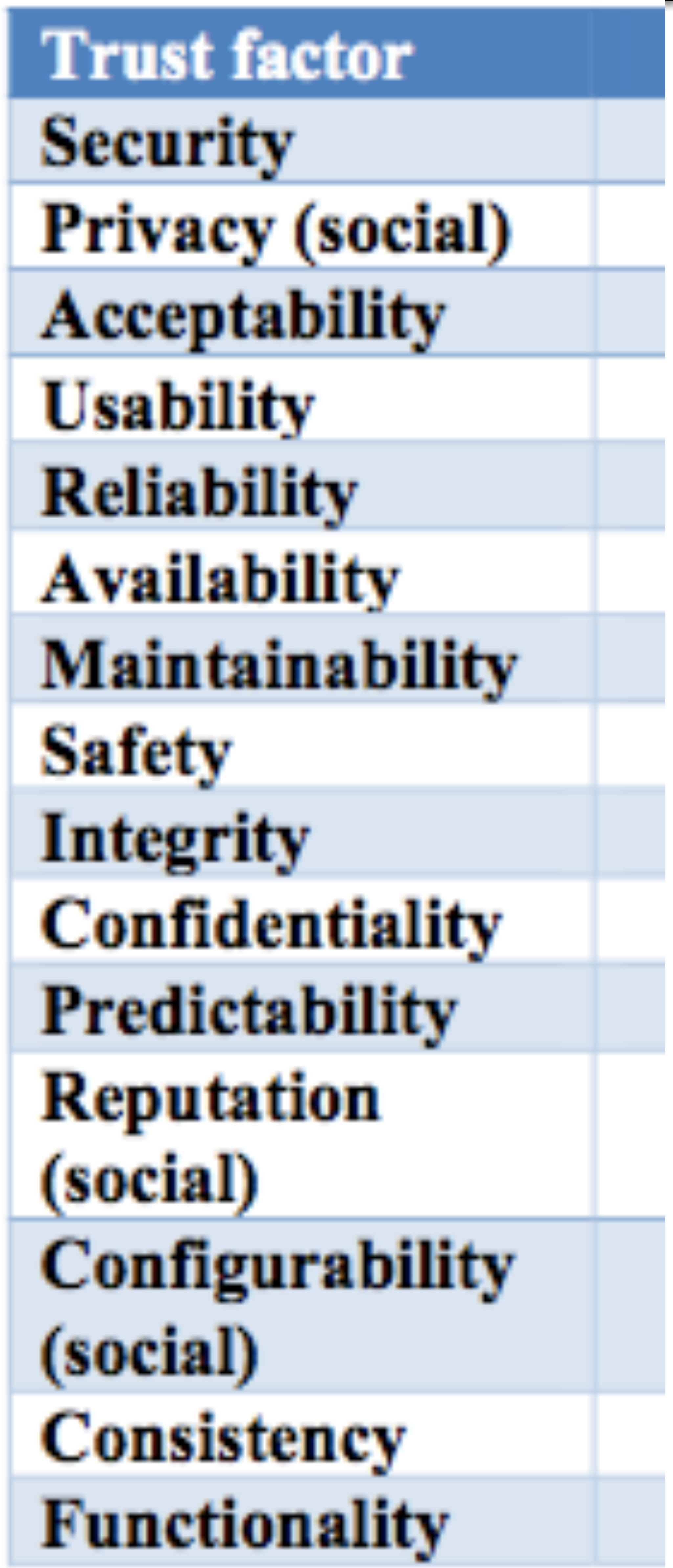
The trust matrix

- trust as a positive user attitude
  - ➡ engaging voluntarily
- security based trust issues
  - ➡ building trusted systems
- technological factors
  - ➡ data storage, distribution
  - ➡ insight
- human/societal factors
  - ➡ government
  - ➡ family, friends

If you had the choice, would you cross this bridge?

http://SCOTT.IoTSec.no

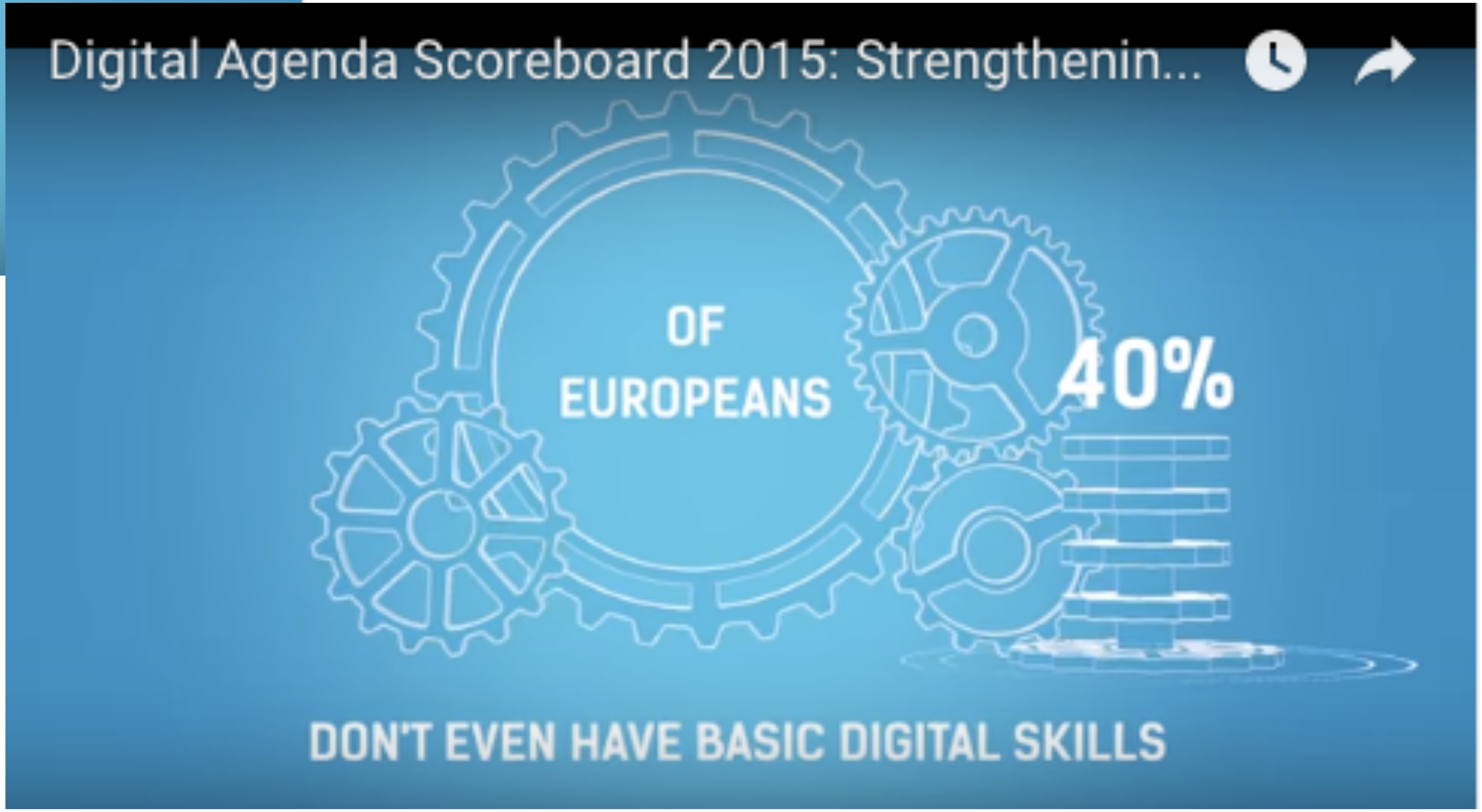
http://SCOTT-project.eu



Trust factor
Security
Privacy (social)
Acceptability
Usability
Reliability
Availability
Maintainability
Safety
Integrity
Confidentiality
Predictability
Reputation (social)
Configurability (social)
Consistency
Functionality

Digital Agenda Scoreboard 2015: Strengthenin...

A DIGITAL SOCIETY IS MADE OF DIGITALLY-SKILLED CITIZENS



Digital Agenda Scoreboard 2015: Strengthenin...

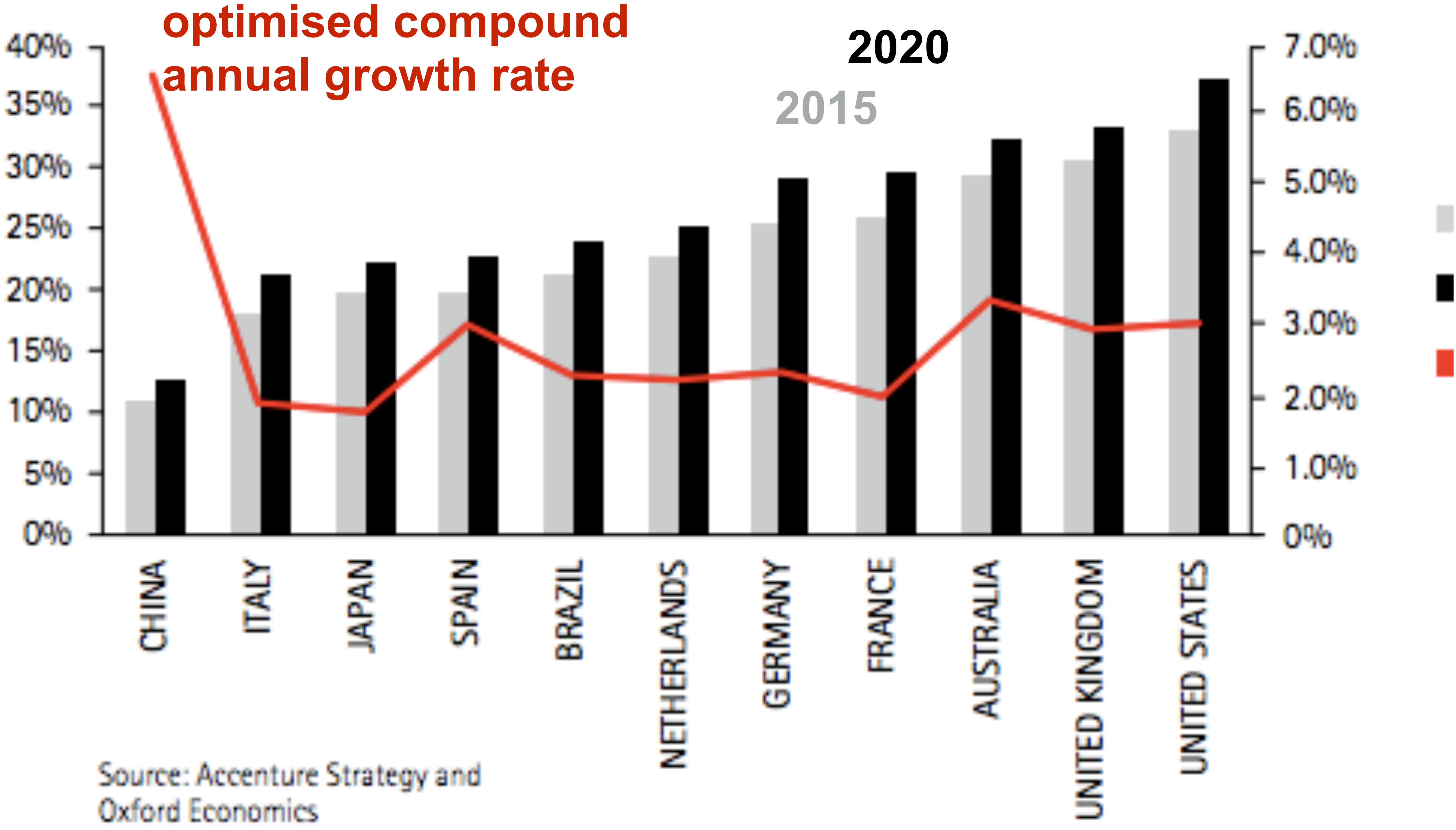
40% OF EUROPEANS DON'T EVEN HAVE BASIC DIGITAL SKILLS

Source: EU commission(2015)

Digital share of GDP (2015 - 2020)

- Accenture Strategy & Oxford Economics, 2016
- Today: USA, 33% og GDP due to digital
- Financial Services 57% digital
  Business Services 54%
  Communications 47%
- 22% of global retail from digital,
  28% in health,
  20% in consumer goods
- digital achievements: *technology, skills, accelerators*

Figure 1. Country-by-country digital share of gross domestic product (2015 and 2020) showing Compound Annual Growth Rate under optimized scenario* (right hand axis)

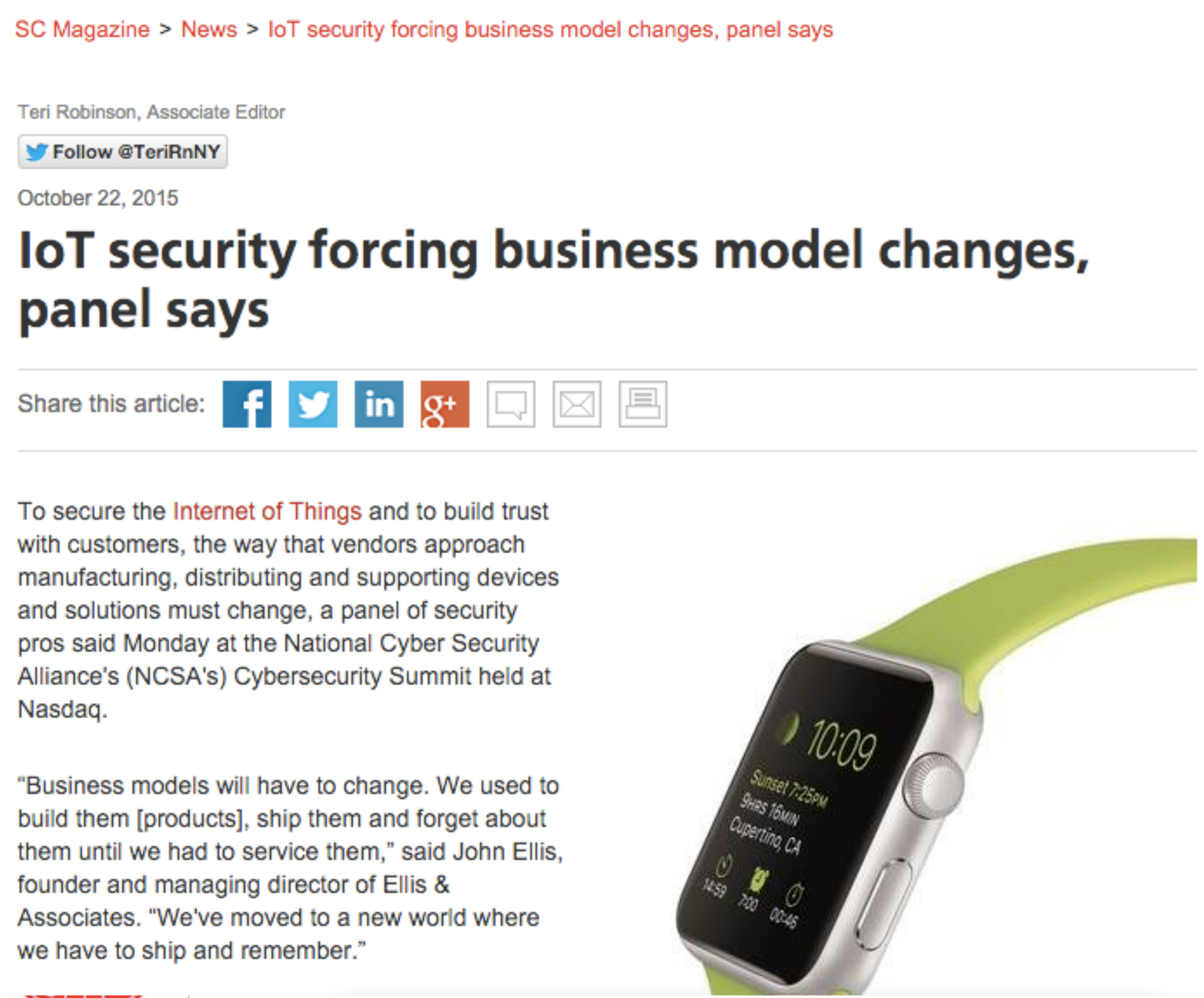


Source: Accenture Strategy and Oxford Economics

[Source:Accenture, "Digital Disruption Growth" 2016]

Jun2017, Noll et al.

http://www.scmagazine.com/iot-security-forcing-business-model-changes-panel-says/article/448668/



SC Magazine > News > IoT security forcing business model changes, panel says

Teri Robinson, Associate Editor

Follow @TeriRnNY

October 22, 2015

IoT security forcing business model changes, panel says

Share this article:

To secure the Internet of Things and to build trust with customers, the way that vendors approach manufacturing, distributing and supporting devices and solutions must change, a panel of security pros said Monday at the National Cyber Security Alliance's (NCSA's) Cybersecurity Summit held at Nasdaq.

"Business models will have to change. We used to build them [products], ship them and forget about them until we had to service them," said John Ellis, founder and managing director of Ellis & Associates. "We've moved to a new world where we have to ship and remember."

Volvo to 'accept full liability' for crashes with its driverless cars

But decide on rules so we can make the dang vehicles

UT-LAW.COM 68 22 78

ability" for collisions involving its autonomous vehicles, the company has

The "sharing economy" for energy companies?

Ved å bygge internett for alle, og ved å skape relevante og uunnværlige digitale tjenester, kan vi bidra til en bedre verden, skriver Sigve Brekke.

FOTO: Heiko Junge, NTB scanpix

IKT er den nye oljen! | Sigve Brekke

[Source: aftenposten.no]

Sharing Economy: "Telenor will create a digital ecosystem in Pakistan"

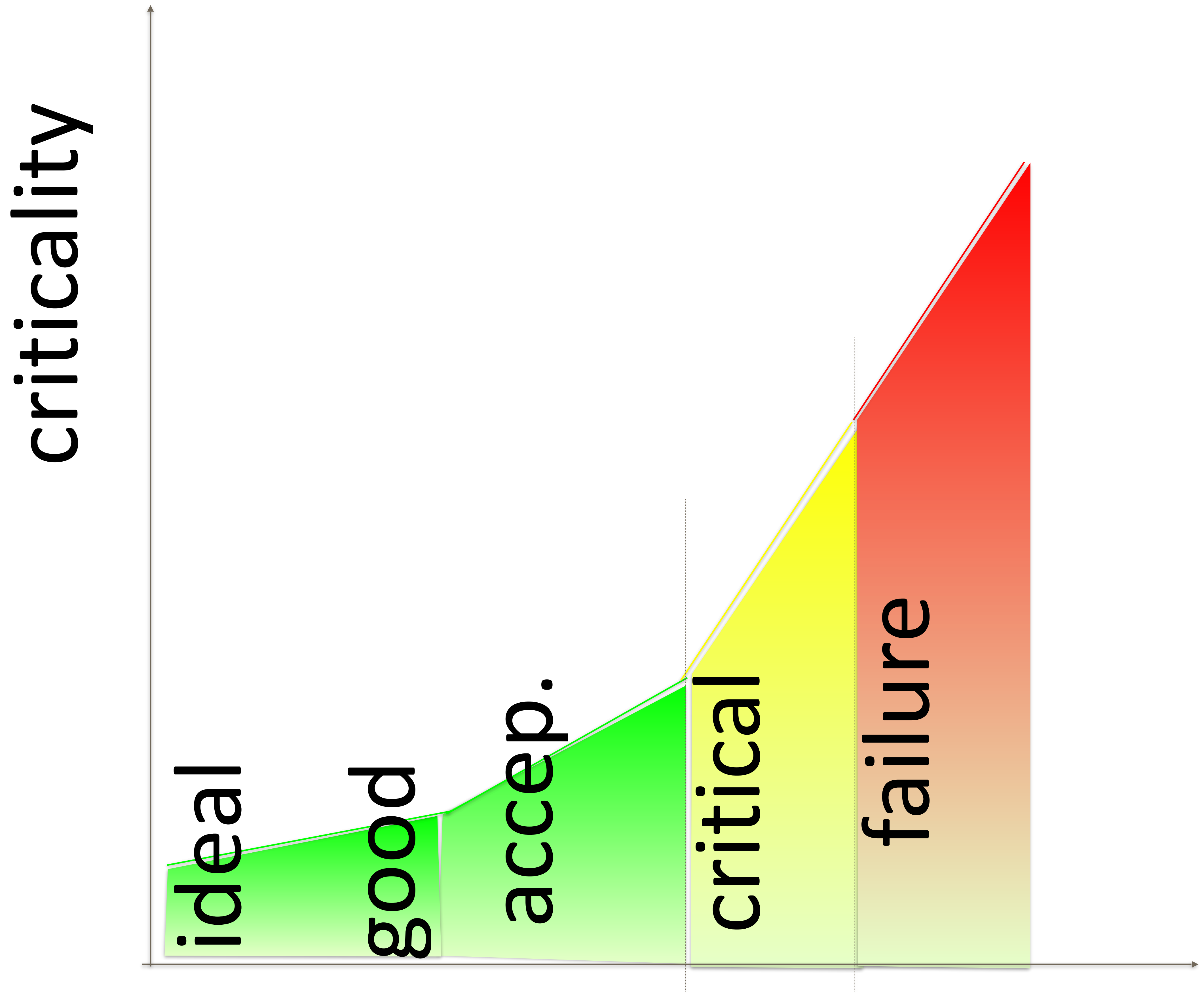
Prosumer bidding and scheduling in electricity markets

12. January 2016 Ukategorisert Administrator

[Source: eSmartSystems.com]

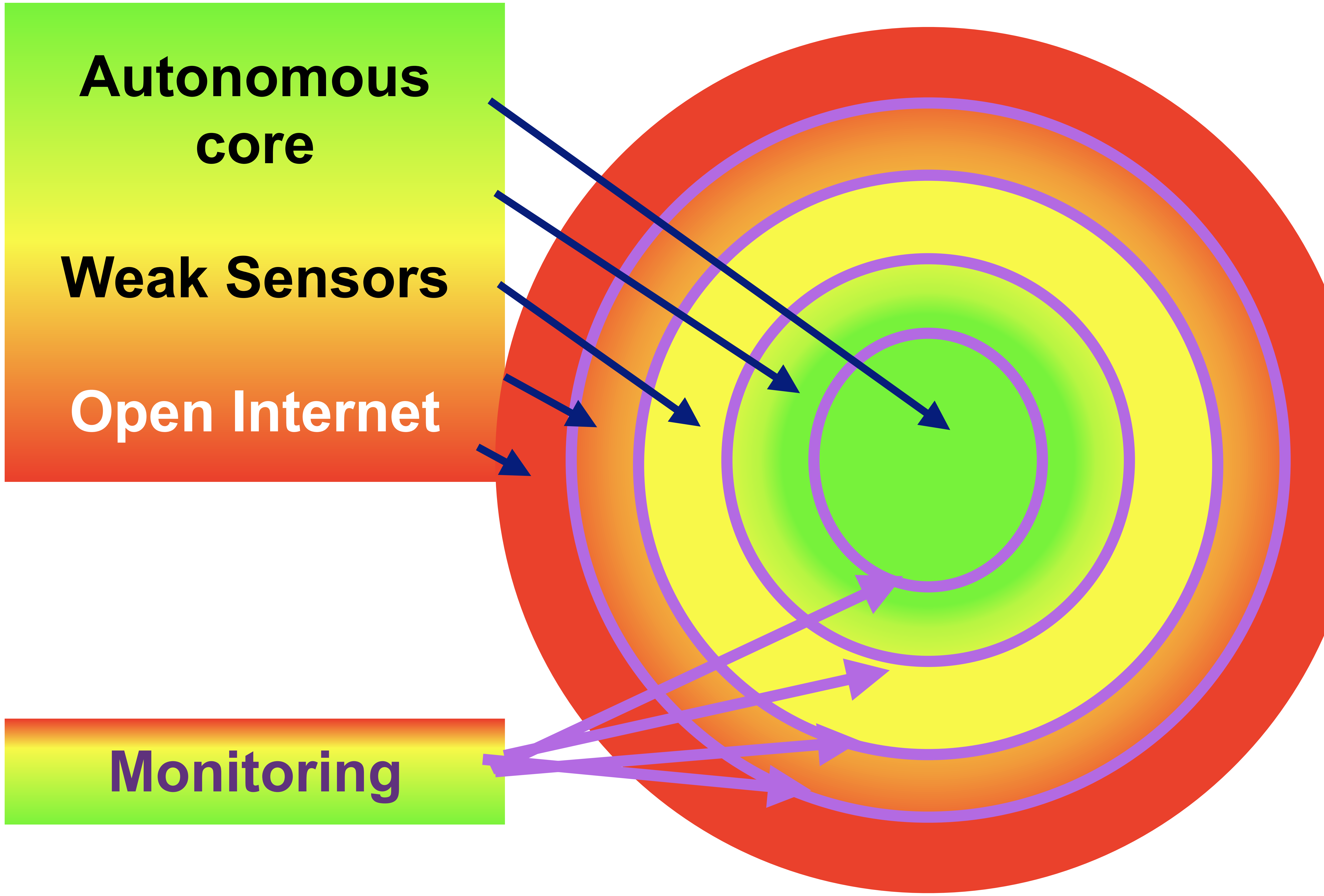
Autonomous, sensor-driven systems

- Design with optimal usage in mind
  - ideal operation
    - all sensors are working
    - no interference (wireless sensor networks)
    - non-hostile environment
- Real system
  - Sensors fusker
    - Øresund train crash (wind sensor)
  - Sensor fail
    - logic, modelling
  - System under attack



The new security paradigm

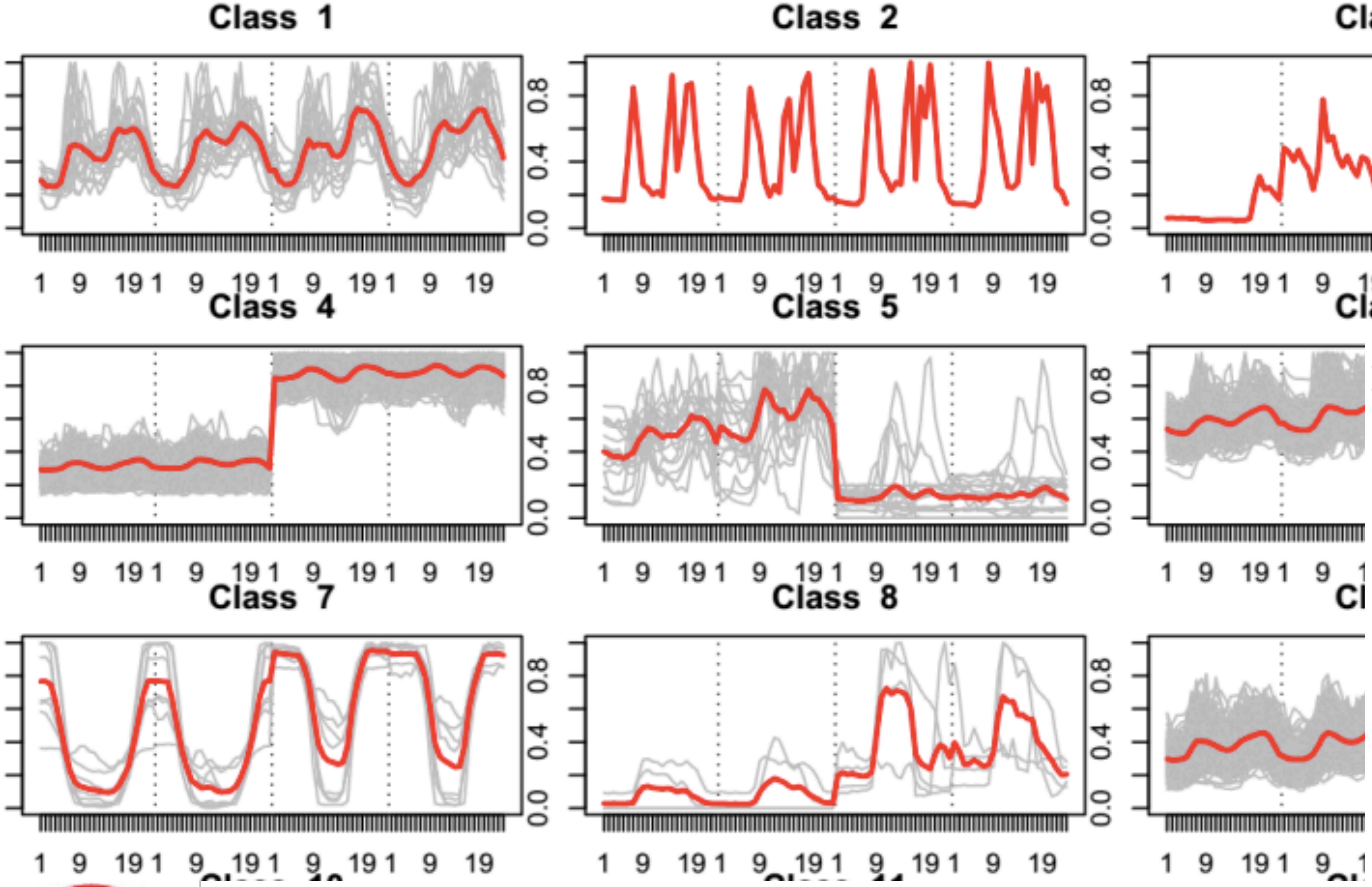
- Focus on attack is not sufficient
  - ➡ new vulnerabilities
  - ➡ 10+ years sensor life-time
- Onion approach
  - ➡ Autonomous Core
    - ‣ proven autonomy (ship, smart meter)
    - ‣ formally proven
  - ➡ Layers
    - ‣ monitoring
    - ‣ firewall

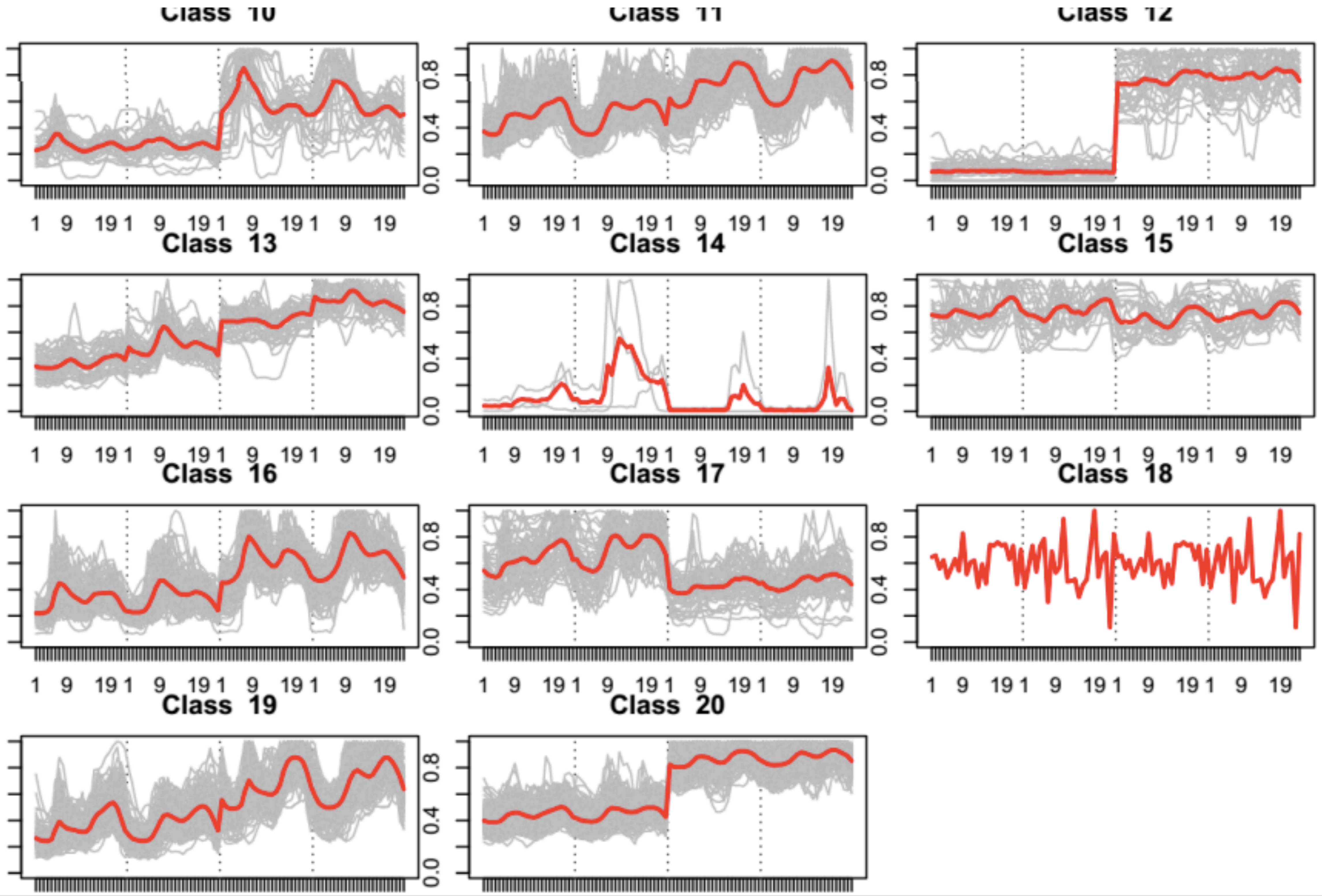


Big Data & Privacy

- Car industry: Liability in IoT driven business models
- Energy: Cost of providing of Energy -> Cost of Reliable Network
- Telecom: uO (MicroOperator), Partnership

What can we learn from meter reading? (1/h data)

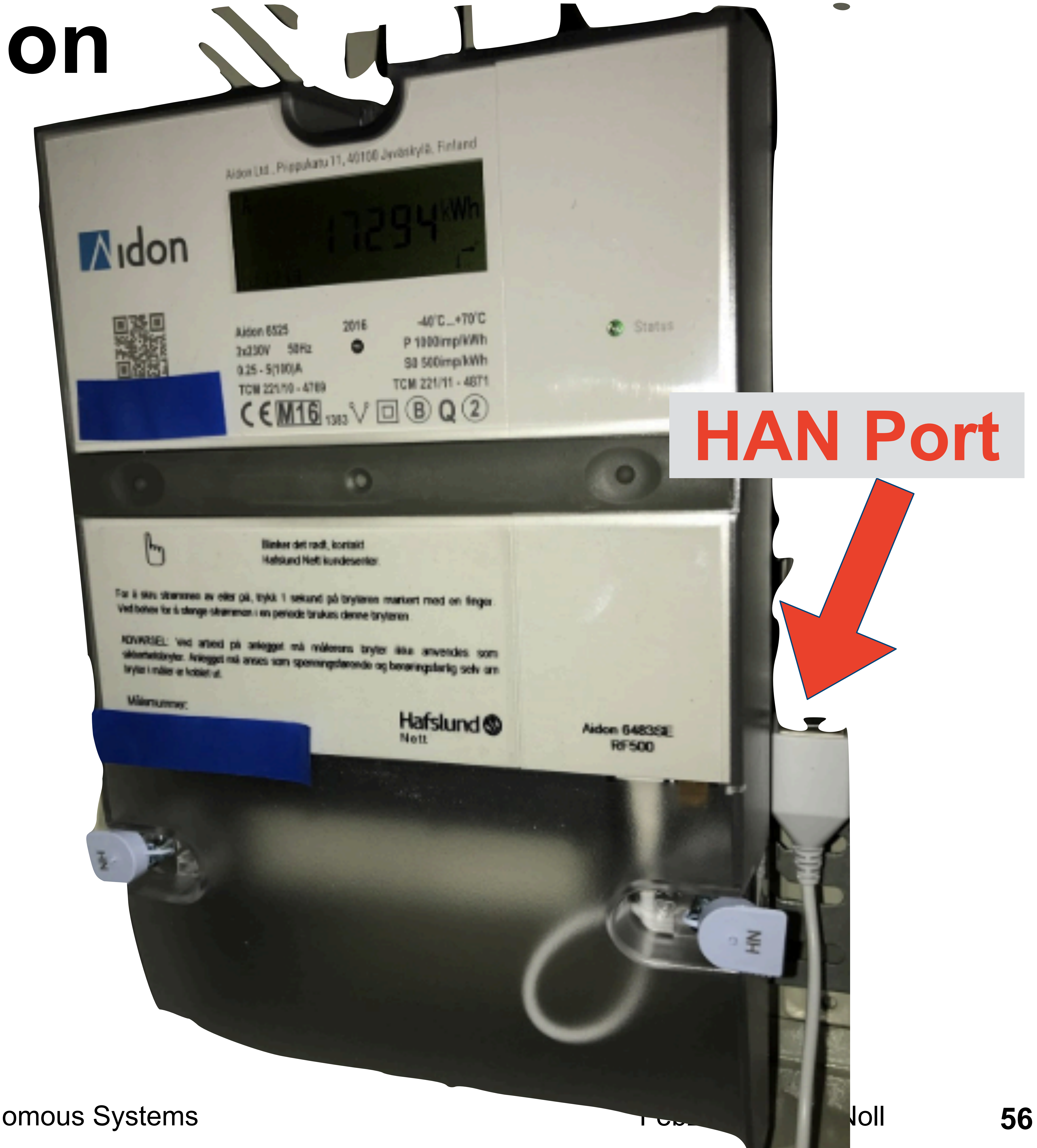




The-Hien Dang-Ha et. al. “Clustering Methods, 2017
https://arxiv.org/pdf/1703.02502.pdf

Instantaneous and high-resolution

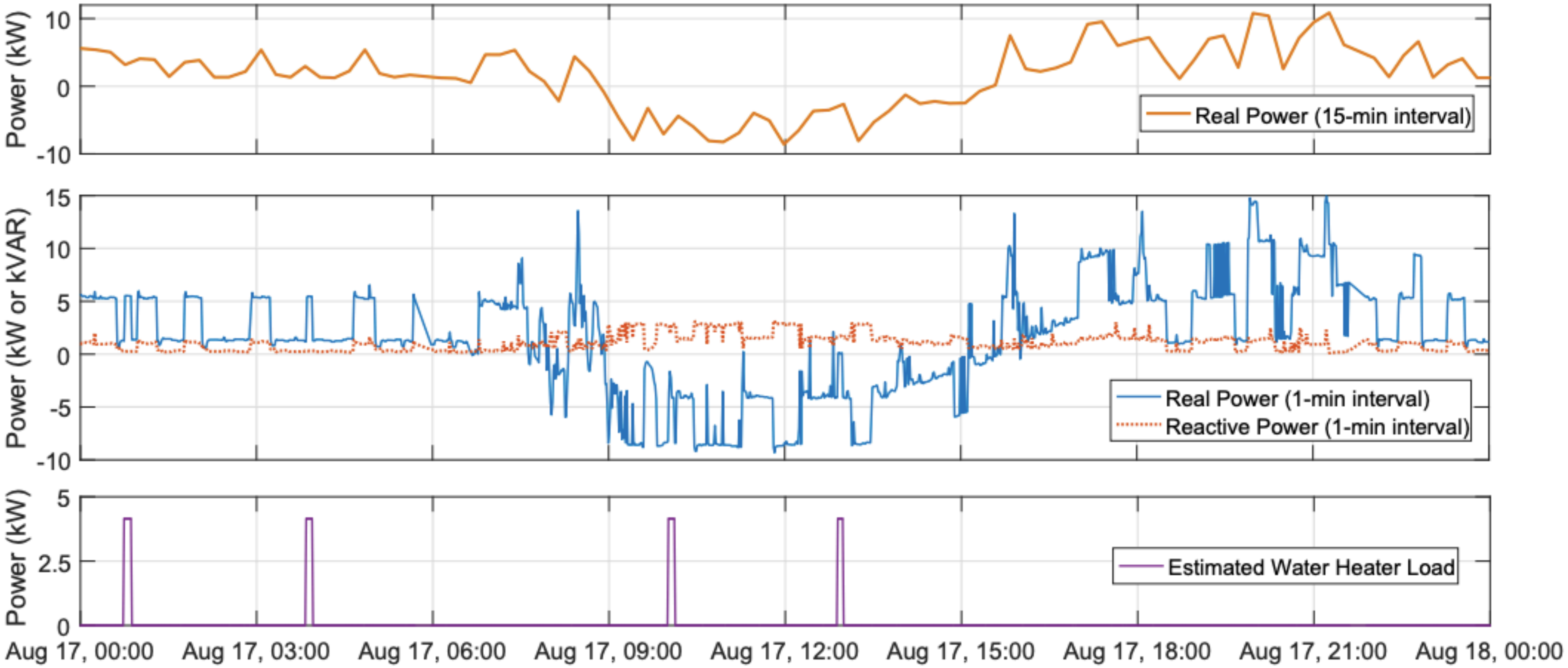
- HAN Port
  - energy usage
  - online monitoring (1/s … 1/min)
- Typical Norway
  - Power (every 2.5s)
  - Current (every 10s)
  - Voltage (every 10s)
- Connected devices
- Security
  - physical security, encryption



AMS HAN port (NEK)
https://www.nek.no/info-ams-han-brukere/

Meter analysis - knowledge about you

- Security
  - ➡ (unencrypted) wireless data
  - ➡ Cloud computing
  - ➡ “is my HAN port open?”
- Information & control
  - ➡ energy saving (water heater)
  - ➡ load control
  - ➡ Fridge, freezer, heat pump,…
  - ➡ usage pattern, “door is open”
  - ➡ “which TV channel do you watch” (every 2s)



http://nilmworkshop.org/2018/proceedings/Poster_ID17.pdf

Dites NON ! aux compteurs communicants LINKY

https://www.cnet.com/news/researchers-find-smart-meters-could-reveal-favorite-tv-shows/

“Amazon Echo” in your smart meter

- Amazon/Google/Apple home control
  - ➡ works on your command
- “Amazon HAN connect”
  - ➡ works all the time
  - ➡ brings all your information to the cloud

Amazon Echo/ Alexa

Apple Home Kit

Google Home/Nest

Comparison with the Mobile Network

- Facebook’s Free Basics
  - 0-rated content (free usage)
  - 3-months break even
- The con’s of Free Basics
  - every click goes to Facebook
  - Net-neutrality

- HAN port
  - who owns my power consumption?
  - cloud analysis?

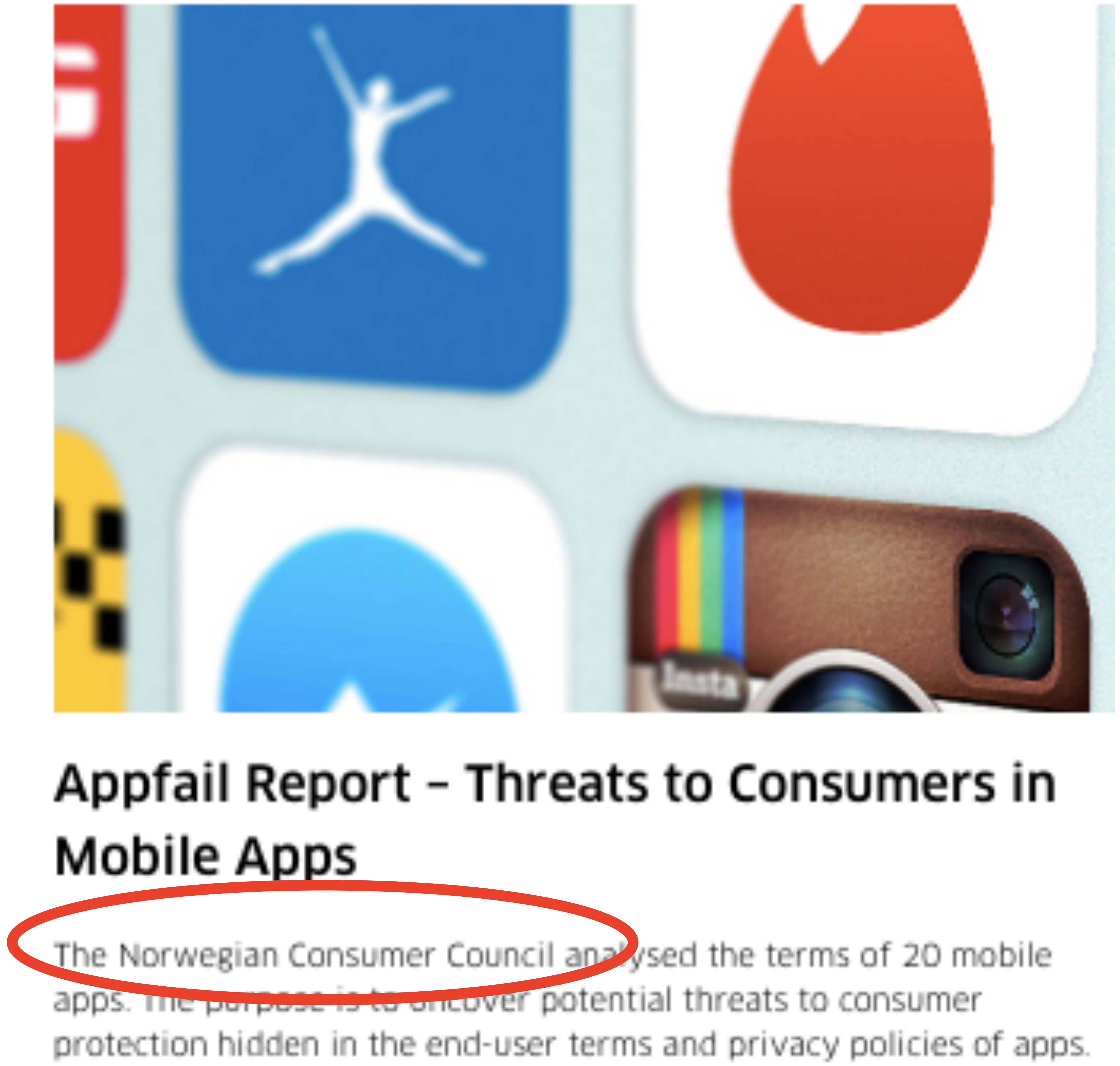
“no to Free Basics” we have been colonised once

Premier Minister Narendra Modi (India)

Towards Measurable Privacy - Privacy Labelling

A+++
A++
A+
A
B
C
D
A++
ENERGIA · ЕНЕРГИЯ
ΕΝΕΡΓΕΙΑ · ENERGIJA
ENERGY · ENERGIE · ENERGI
280
kWh/annum
1L
155 L
54 L
38 dB

- “Measure, what you can measure - Make measurable, what you can’t measure” - Galileo
- Privacy today
  - ➡ based on lawyer terminology
  - ➡ 250.000 words on app terms and conditions
- Privacy tomorrow
  - ➡ A++: sharing with no others
  - ➡ A: …
  - ➡ C: sharing with ….
- The Privacy label for apps and devices



Appfail Report – Threats to Consumers in Mobile Apps

The Norwegian Consumer Council analysed the terms of 20 mobile apps. The purpose is to uncover potential threats to consumer protection hidden in the end-user terms and privacy policies of apps.

The economic perspective

- The big 5 IT companies have a GDP as big as that of France
- Amazon largest sector in terms of revenue is selling of data
  - ➡ 20% of revenue

- How can SMEs compete?
  - ➡ Each service and device gets a privacy label

- Four areas for Privacy Label
  - ➡ which data are collected
  - ➡ sharing to my phone, my cloud, public cloud,...
  - ➡ data communication integrity and storage
  - ➡ further distribution of data, ownership of data, further processing

Privacy Label (A-F)

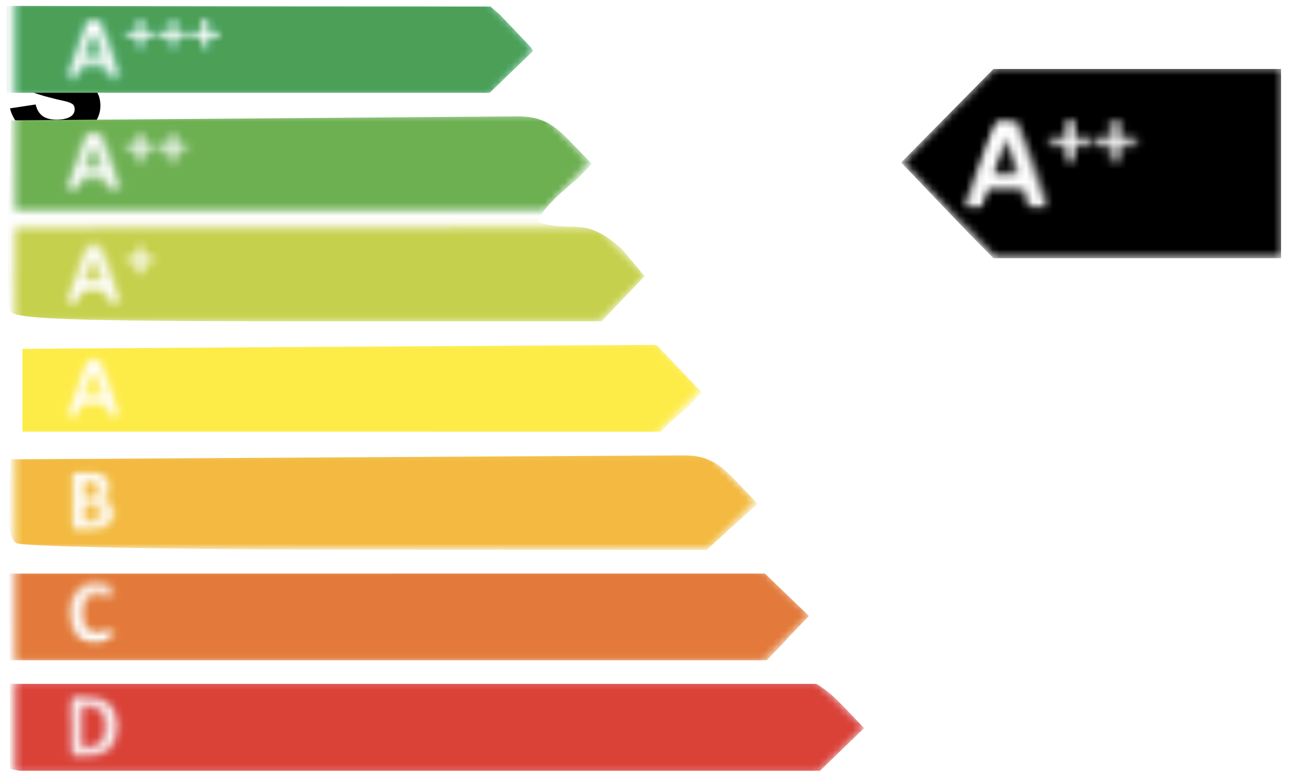
- easy visibility
- customer focus
- transparent

privacylabel.IoTSec.no

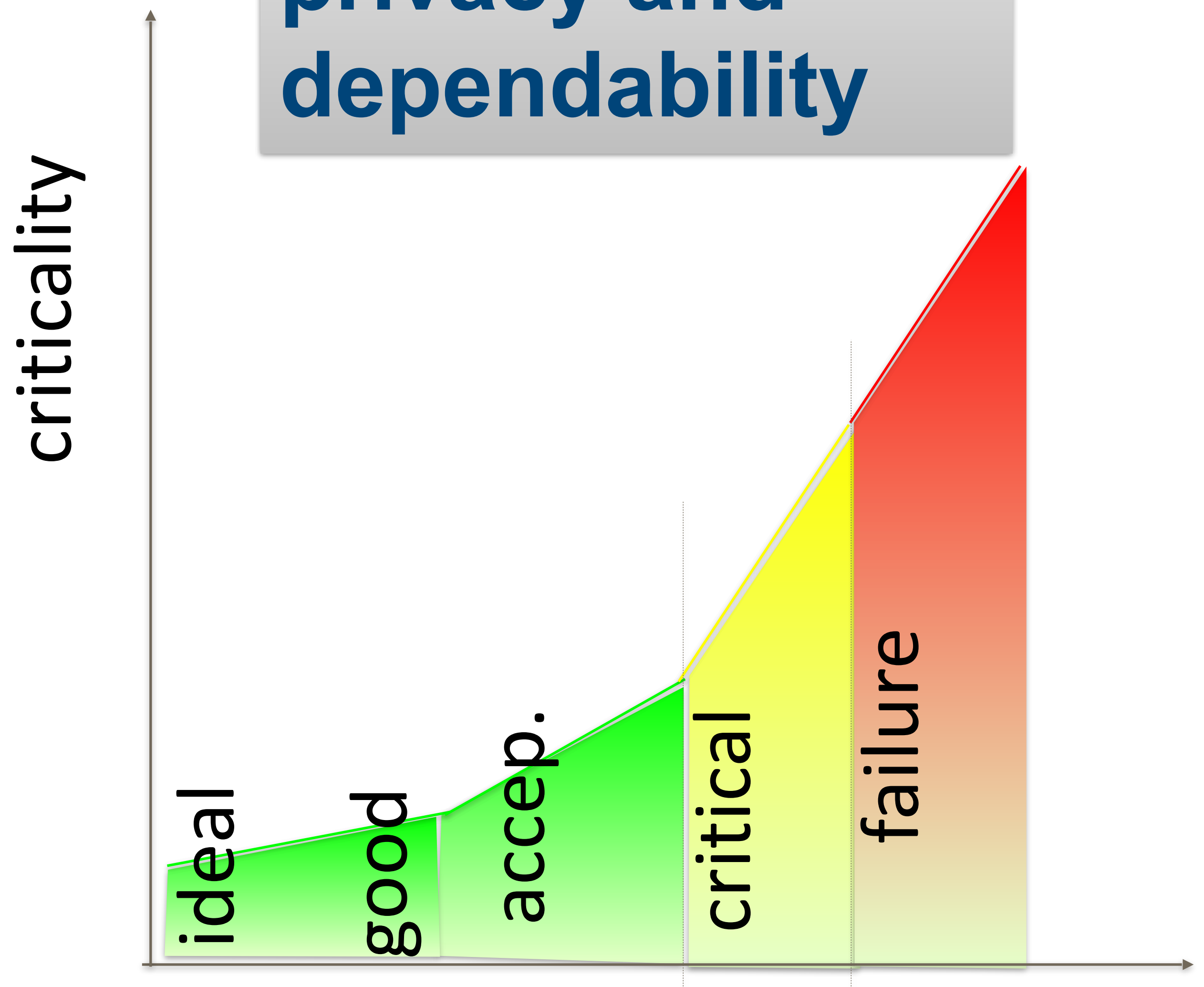
Privacy & Security Conclusions

- Home is the battlefield
  - Smart Home/Offices
  - Novel services: Control, Alarm, Health
    - Specific requirements for security, privacy
  - HAN port for continuous power monitoring
    - identification of user behaviour
- Collaborative approach for a (more) secure society
  - “the cloud is not the answer” - distributed security
  - partnership for security: threats, measures, counter activities
- Measurable Security and Privacy for IoT
  - Industrial impact: Security Centre for Smart Grid
  - Privacy labelling for apps and devices
- Innovation ecosystem for the IoT
  - Reducing the digital gap

Privacy Labels



Measurable: security, privacy and dependability



Logic: Centralised ⟷ Fog

Smart Meter: Information ⟷ Control

Societal challenges:

From IoT Security, Measurable Security & Privacy, to Societal Security

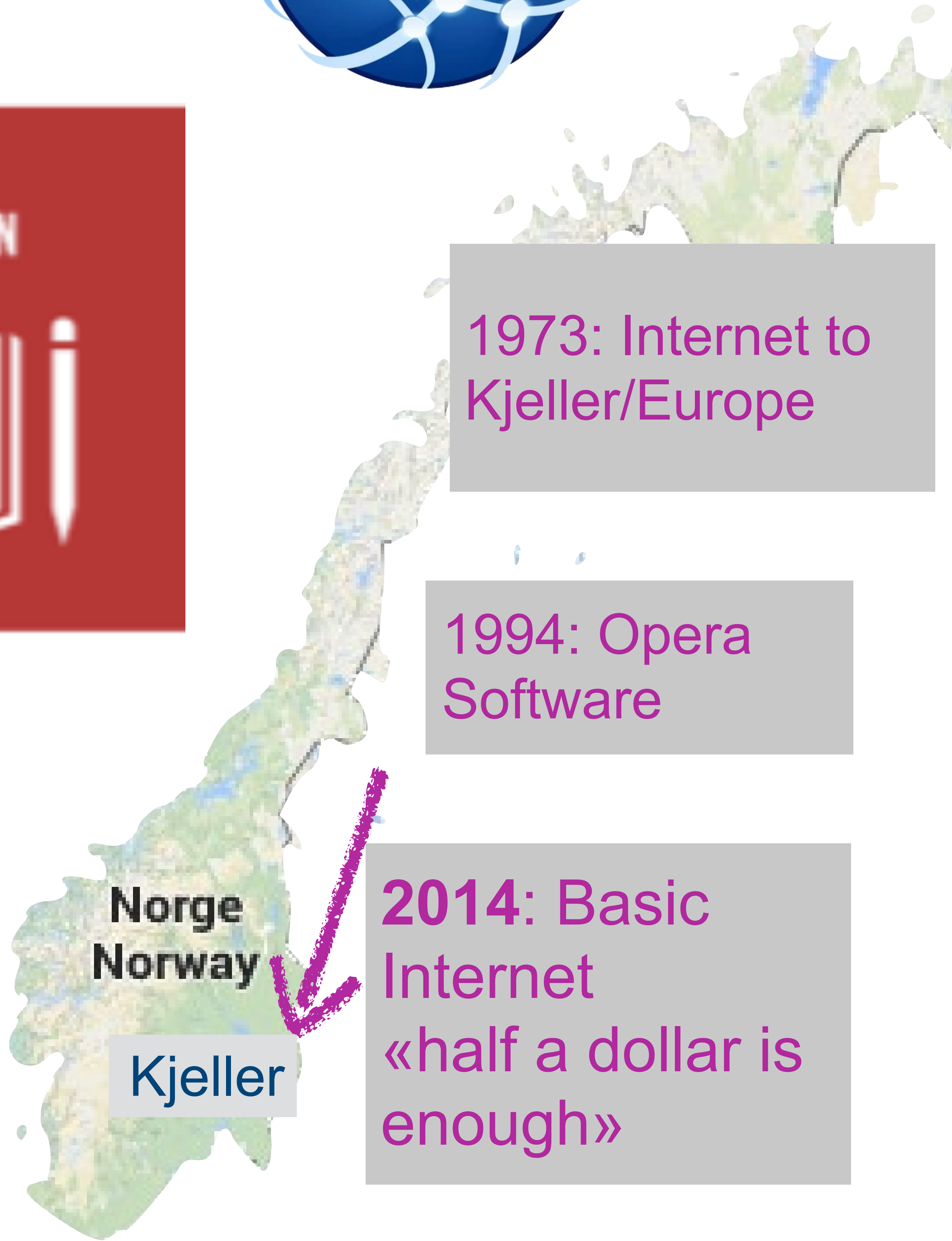
Motivation
"Need to close the digital gap"

- The Global Goals:
  Norway is the secretariat for Quality Education
- Internet history
  - ➡ 1973 Europe through Kjeller
  - ➡ 1994 Opera Software
  - ➡ 2014 Basic Internet Foundation

THE GLOBAL GOALS
For Sustainable Development

4 QUALITY EDUCATION

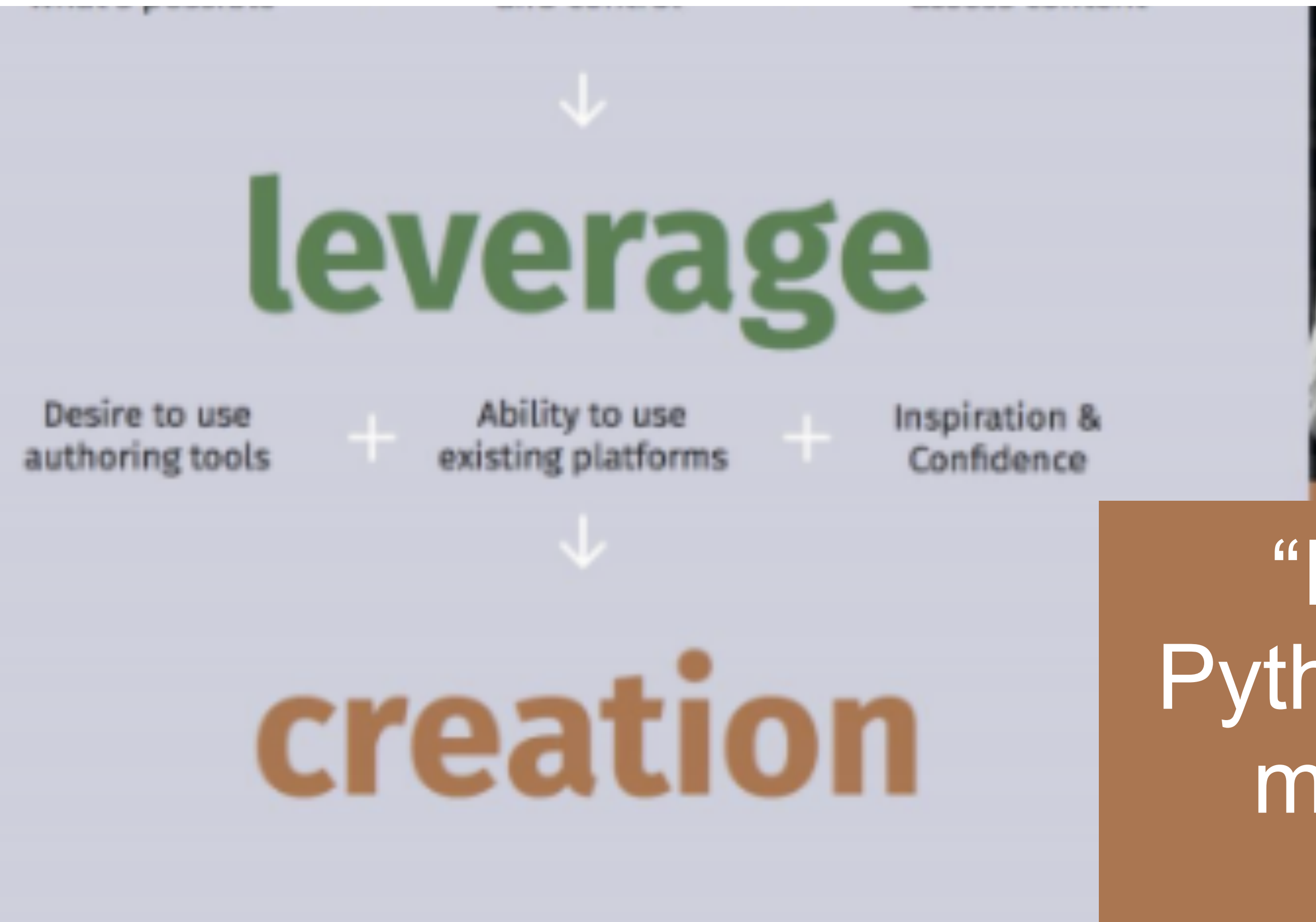
Basic Internet



1973: Internet to Kjeller/Europe

1994: Opera Software

2014: Basic Internet «half a dollar is enough»


leverage
Desire to use authoring tools
+
Ability to use existing platforms
+
Inspiration & Confidence
creation

"Internet is my teacher"

"I'm currently learning Python and HTML, so I can make a website for my parents' business"

Google translate

Partnership for Digital Africa

http://www.aftenposten.no/meninger/debatt/Kronikk-Som-gjesteland-pa-G20-toppmotet-ma-vi-bidra-til-a-endre-verden--Erna-

Comment: As a guest country at the G20 summit, we must change the world | Erna Solberg

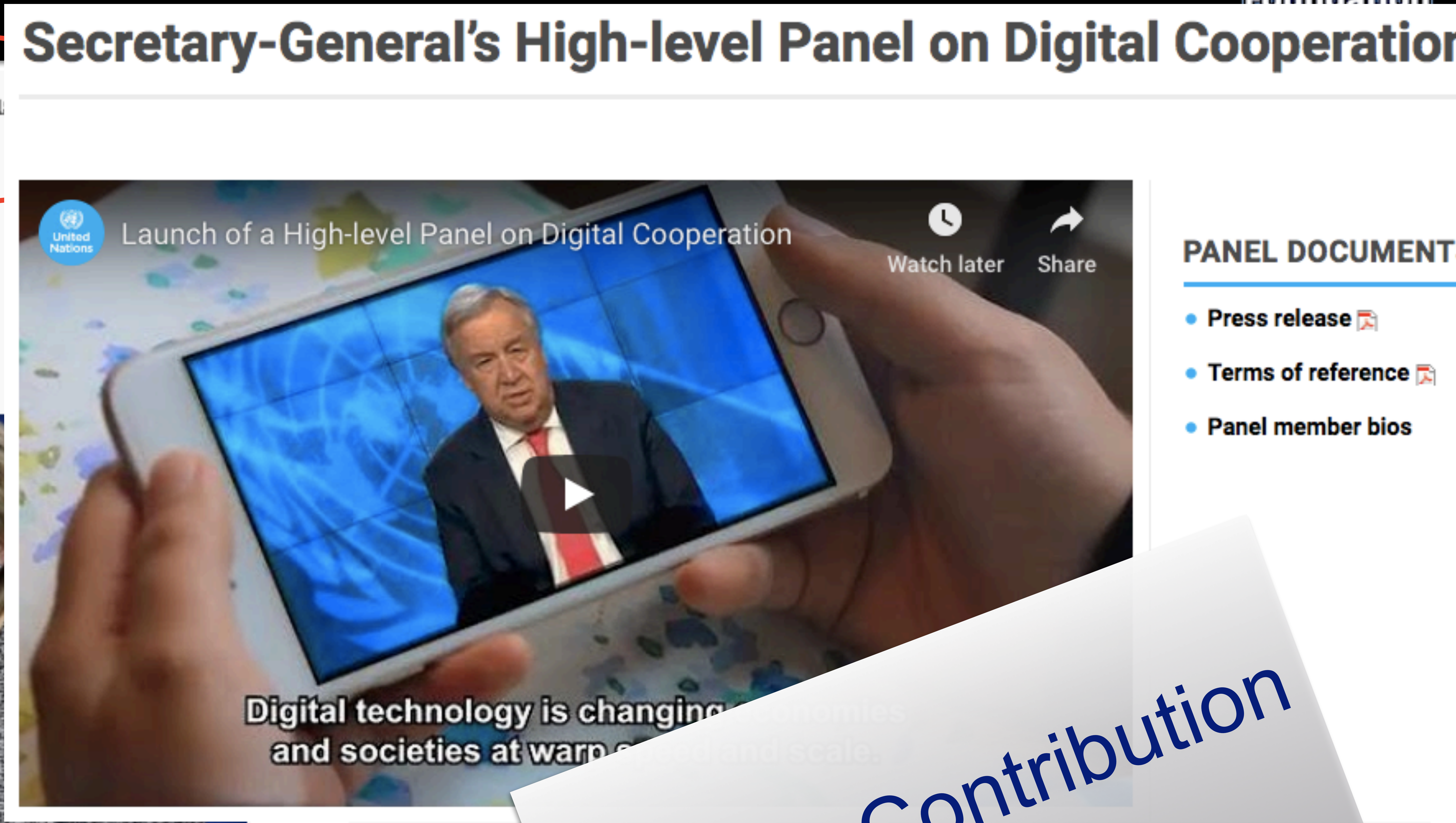
ERNA SOLBERG (H), PRIME MINISTER

7:58 P.M.

G20:
Compact with Africa

In July last year was Erna Solberg invited by Angela Merkel for this year's G20 meeting. Here from a meeting between the German Chancellor and the Norwegian Prime Minister in Berlin in November, where Norway's participation as guest country at the economic summit were among issues discussed.

Secretary-General's High-level Panel on Digital Cooperatio


United Nations
Launch of a High-level Panel on Digital Cooperation
Watch later
Share
Digital technology is changing economics
and societies at warp speed and scale.

PANEL DOCUMENT

- Press release
- Terms of reference
- Panel member bios

Call for Contribution

G20 can therefore help the countries and international organizations use their resources more ... which create growth and job creation.

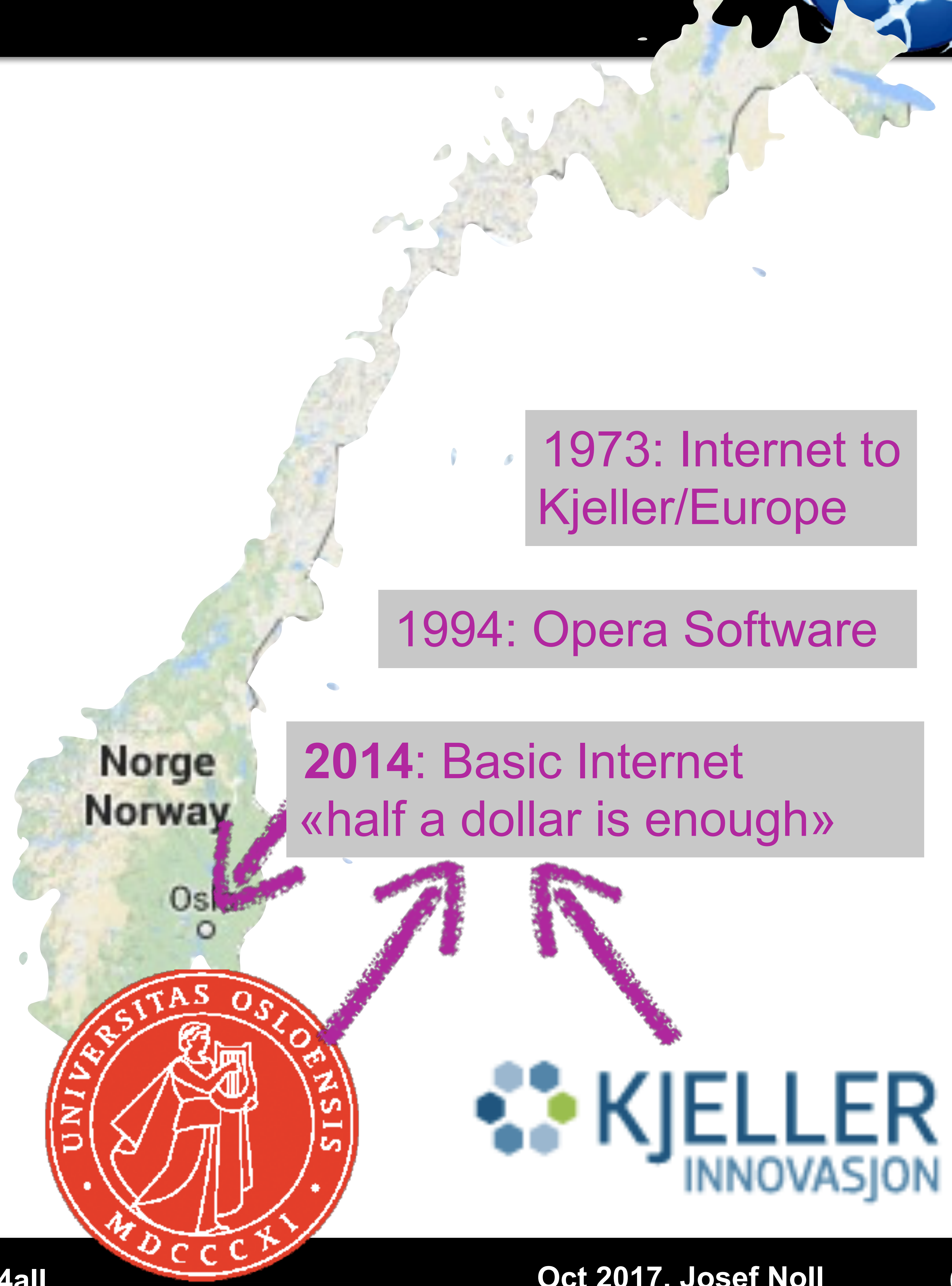
3. Health and education.

Norway has long had a heavy international involvement. Education and health are associated with economic growth.

About the Basic Internet Foundation

- Information is the basis for education, health and entrepreneurship
- Digitalisation is the engine of economic growth and wellbeing of people
- Sustainable development requires digital inclusion, which necessitates Internet for all
- Impact lives of the unconnected 3.5 billions of people in the world

- University of Oslo (UNIK) and Kjeller Innovation co-founded the Basic Internet Foundation
  - ➡ “**Internet Lite for All**”
  - ➡ Freemium model for access
    - ➡ free for information (text, pictures, local video)
    - ➡ premium for broadband

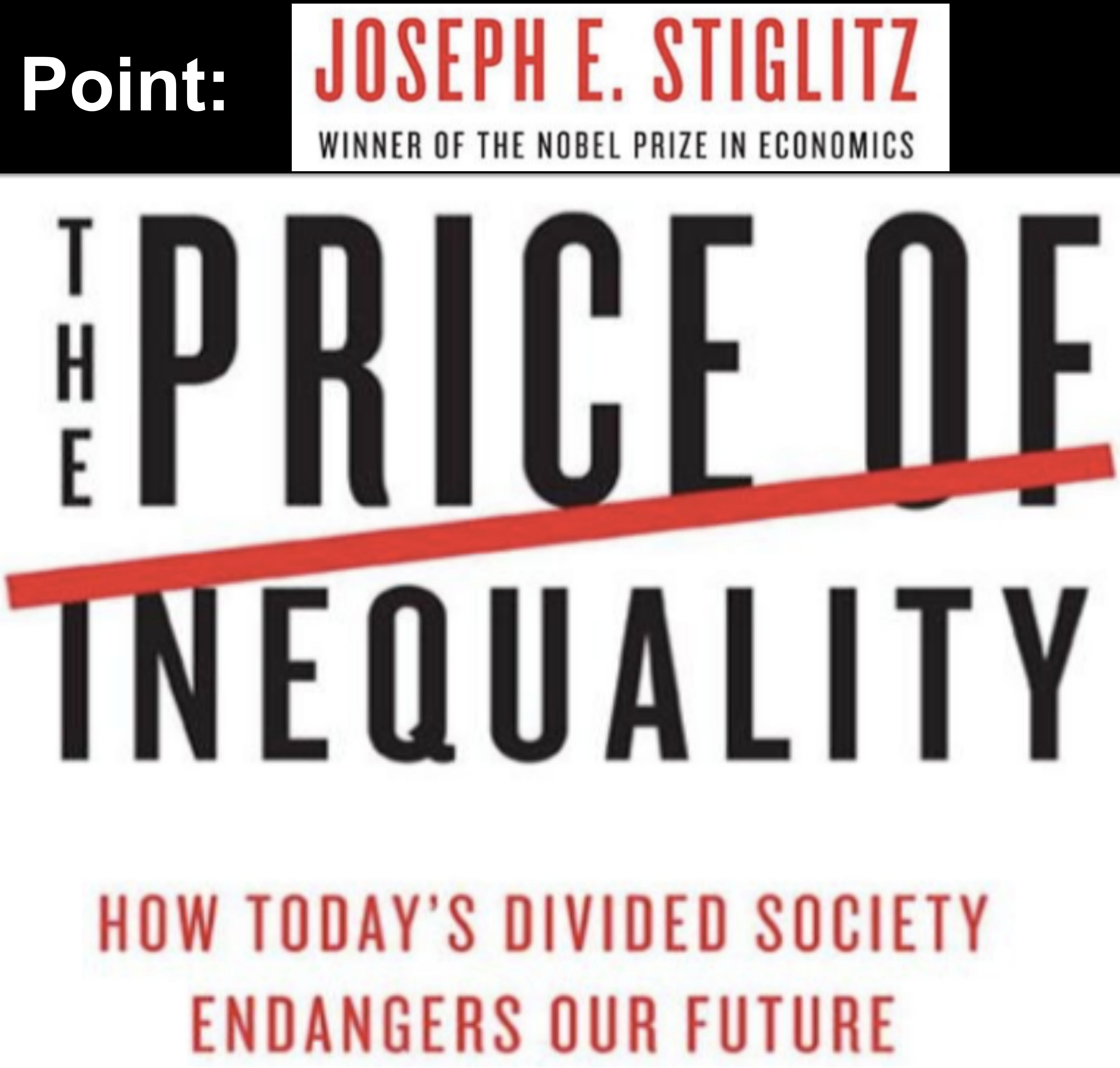


1973: Internet to Kjeller/Europe

1994: Opera Software

2014: Basic Internet «half a dollar is enough»

Starting Point:



JOSEPH E. STIGLITZ

WINNER OF THE NOBEL PRIZE IN ECONOMICS

THE PRICE OF INEQUALITY

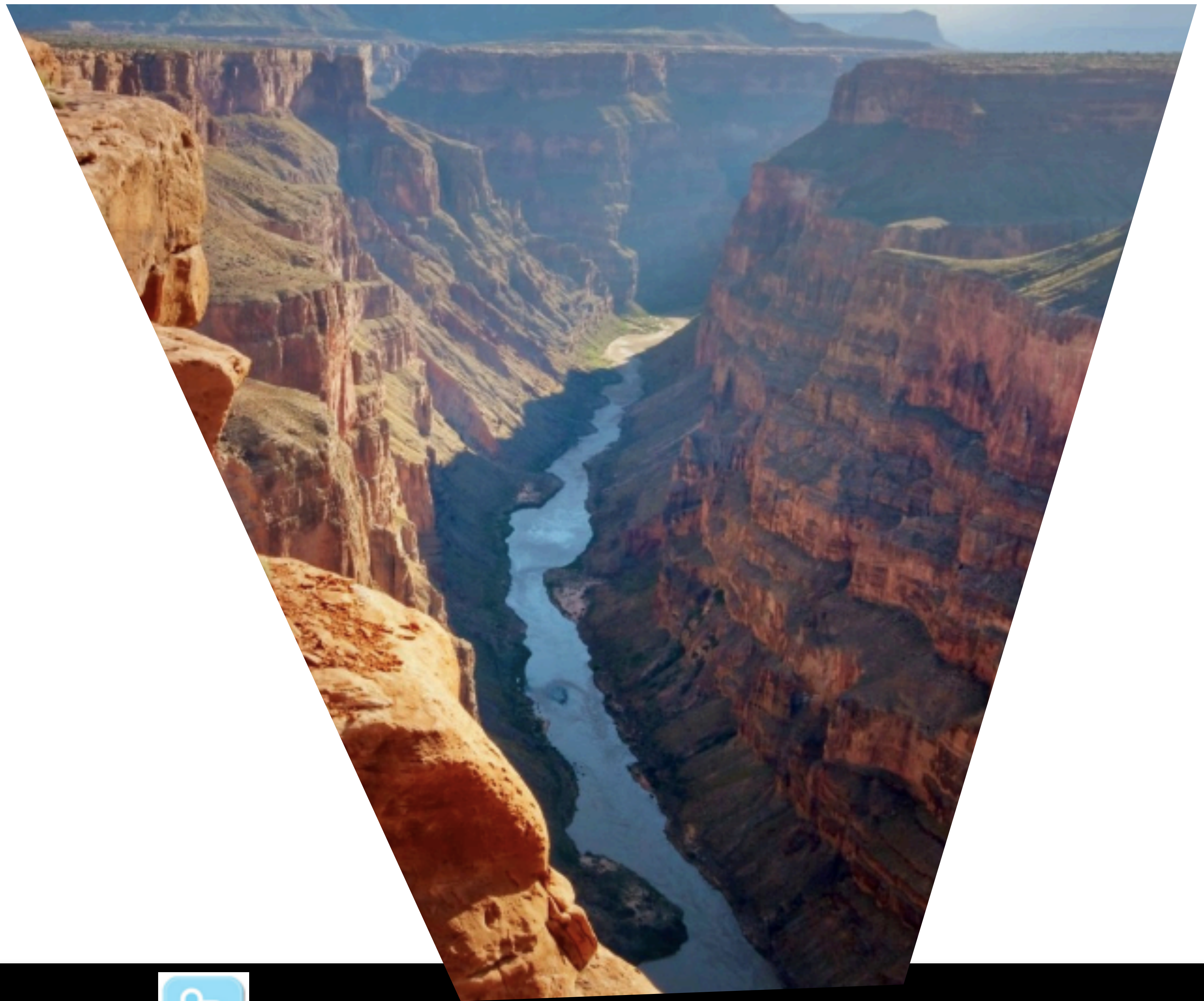
HOW TODAY'S DIVIDED SOCIETY ENDANGERS OUR FUTURE

Grand Challenges - a.o. Digital Divide

- Grand Challenges
  - ➡ Climate
  - ➡ Resources (radio, minerals)
    - ‣ Kobald (East - DR Congo)
  - ➡ Divide

- Digitisation
  - ➡ Mobile Networks
  - ➡ IoT
  - ➡ Automation
  - ➡ …

- Will enhance
  - ➡ the digital divide



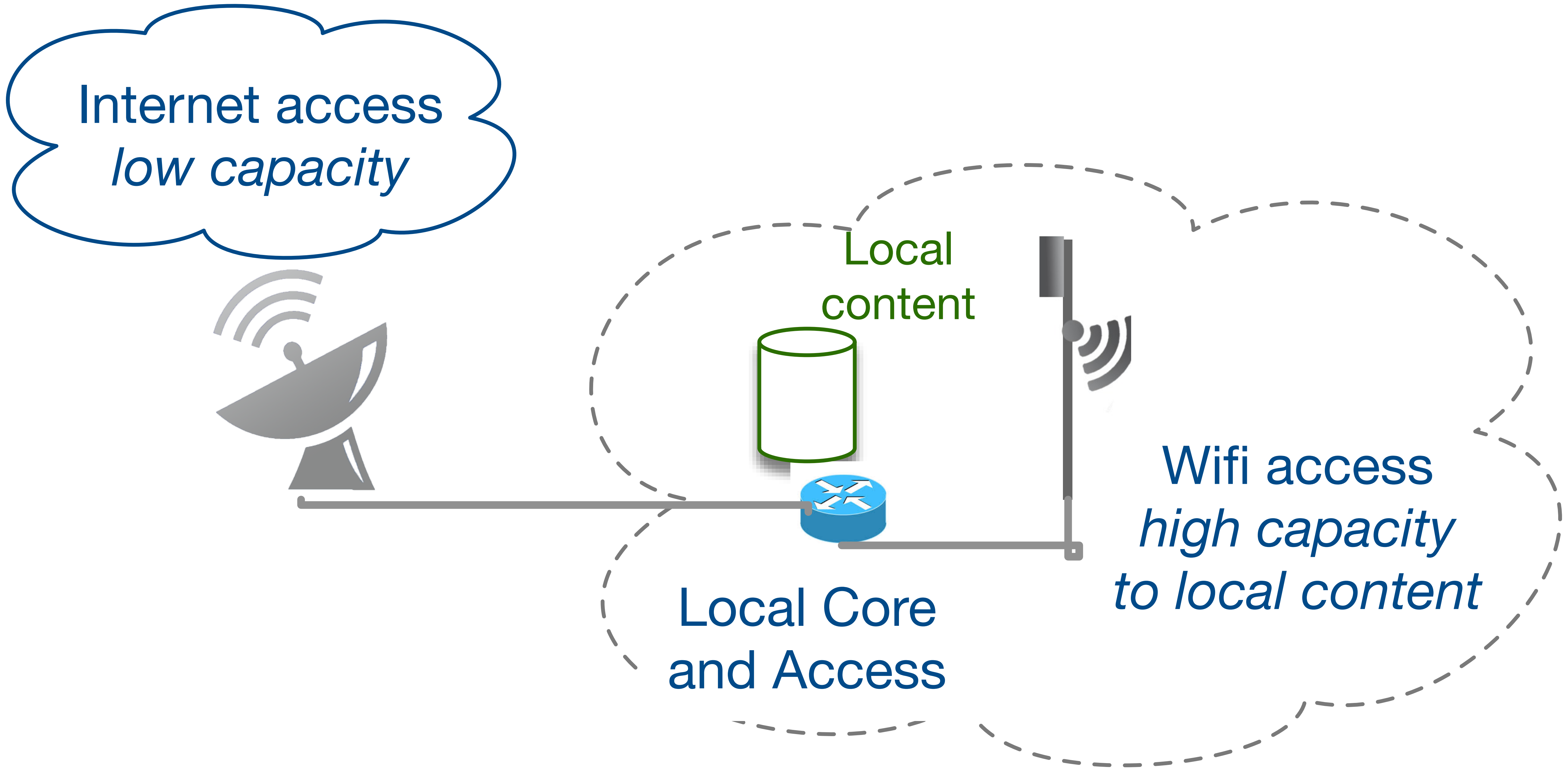
Basic Internet Focus

- How are **we** going to address the challenges?
- Digital Inclusion and Empowerment
  - ➡ Specific Solution:
    - ➡ Internet Lite for All
    - ➡ Freemium Model for Access

“Internet Lite for All”

the walk on the Internet

- Freemium model
  - ➡ Free: text, pictures & local video
  - ➡ Premium: broadband services
- Ensure Network Neutrality
  - ➡ Content type filtering
- 1 premium pays for 300 free
  - ➡ “10 months of Information, or 10 min of video”?



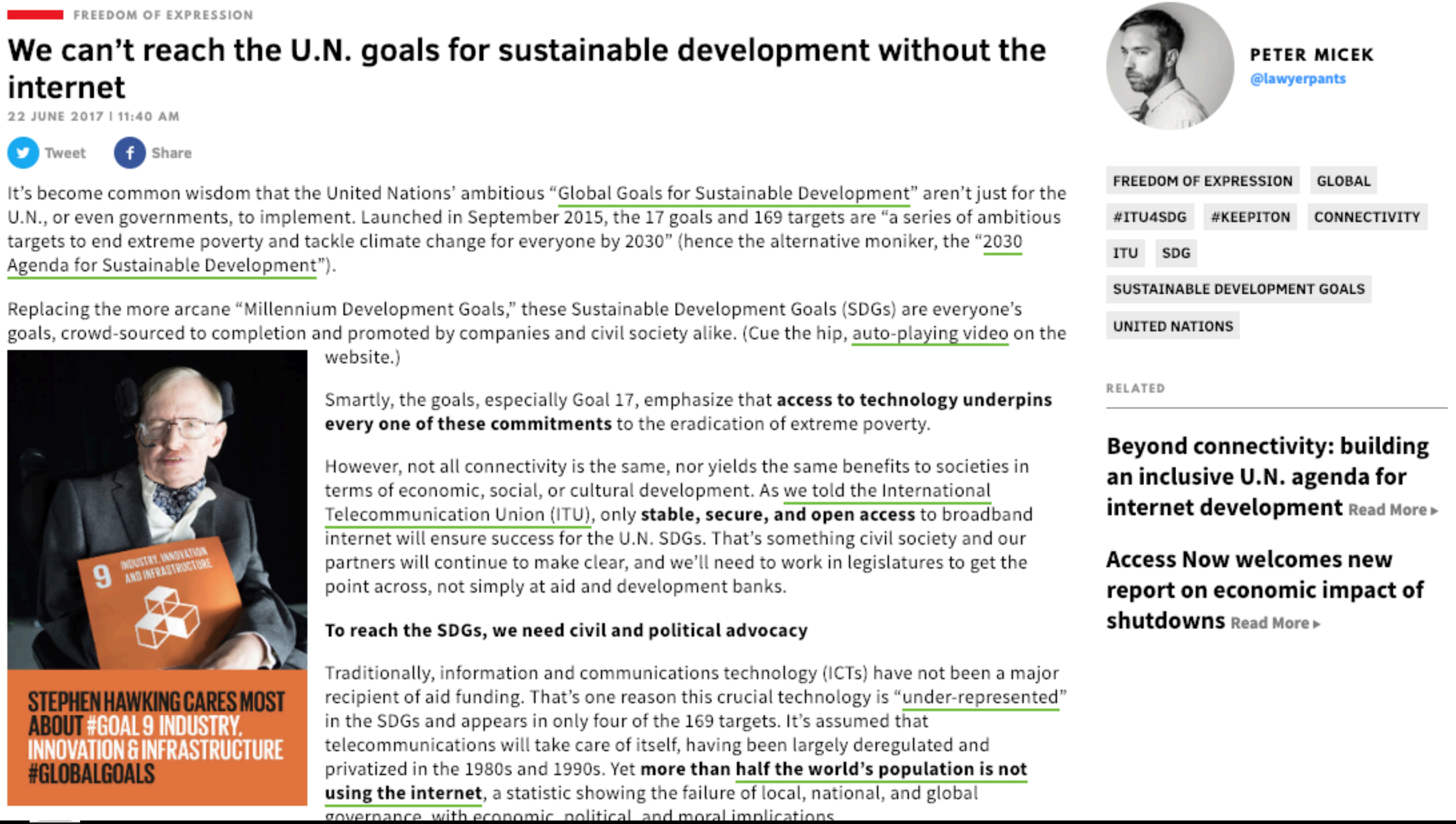
Satellite: 1 Mbit/s = 2000 US$/month

Tanzania: 4Mbit/s = 600 US$/month

SUSTAINABLE DEVELOPMENT GOALS

And what about IoT?

https://www.accessnow.org/cant-reach-u-n-goals-sustainable-development-without-internet/



FREEDOM OF EXPRESSION

We can't reach the U.N. goals for sustainable development without the internet

22 JUNE 2017 I 11:40 AM

Tweet Share

PETER MICEK
@lawyerpants

FREEDOM OF EXPRESSION · GLOBAL · #ITU4SDG · #KEEPITON · CONNECTIVITY · ITU · SDG · SUSTAINABLE DEVELOPMENT GOALS · UNITED NATIONS

It's become common wisdom that the United Nations' ambitious "Global Goals for Sustainable Development" aren't just for the U.N., or even governments, to implement. Launched in September 2015, the 17 goals and 169 targets are "a series of ambitious targets to end extreme poverty and tackle climate change for everyone by 2030" (hence the alternative moniker, the "2030 Agenda for Sustainable Development").

Replacing the more arcane "Millennium Development Goals," these Sustainable Development Goals (SDGs) are everyone's goals, crowd-sourced to completion and promoted by companies and civil society alike. (Cue the hip, auto-playing video on the website.)

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
STEPHEN HAWKING CARES MOST ABOUT #GOAL 9 INDUSTRY, INNOVATION & INFRASTRUCTURE #GLOBALGOALS

Smartly, the goals, especially Goal 17, emphasize that **access to technology underpins every one of these commitments** to the eradication of extreme poverty.

However, not all connectivity is the same, nor yields the same benefits to societies in terms of economic, social, or cultural development. As we told the International Telecommunication Union (ITU), only **stable, secure, and open access** to broadband internet will ensure success for the U.N. SDGs. That's something civil society and our partners will continue to make clear, and we'll need to work in legislatures to get the point across, not simply at aid and development banks.

To reach the SDGs, we need civil and political advocacy

Traditionally, information and communications technology (ICTs) have not been a major recipient of aid funding. That's one reason this crucial technology is "under-represented" in the SDGs and appears in only four of the 169 targets. It's assumed that telecommunications will take care of itself, having been largely deregulated and privatized in the 1980s and 1990s. Yet **more than half the world's population is not using the internet**, a statistic showing the failure of local, national, and global governance, with economic, political, and moral implications.

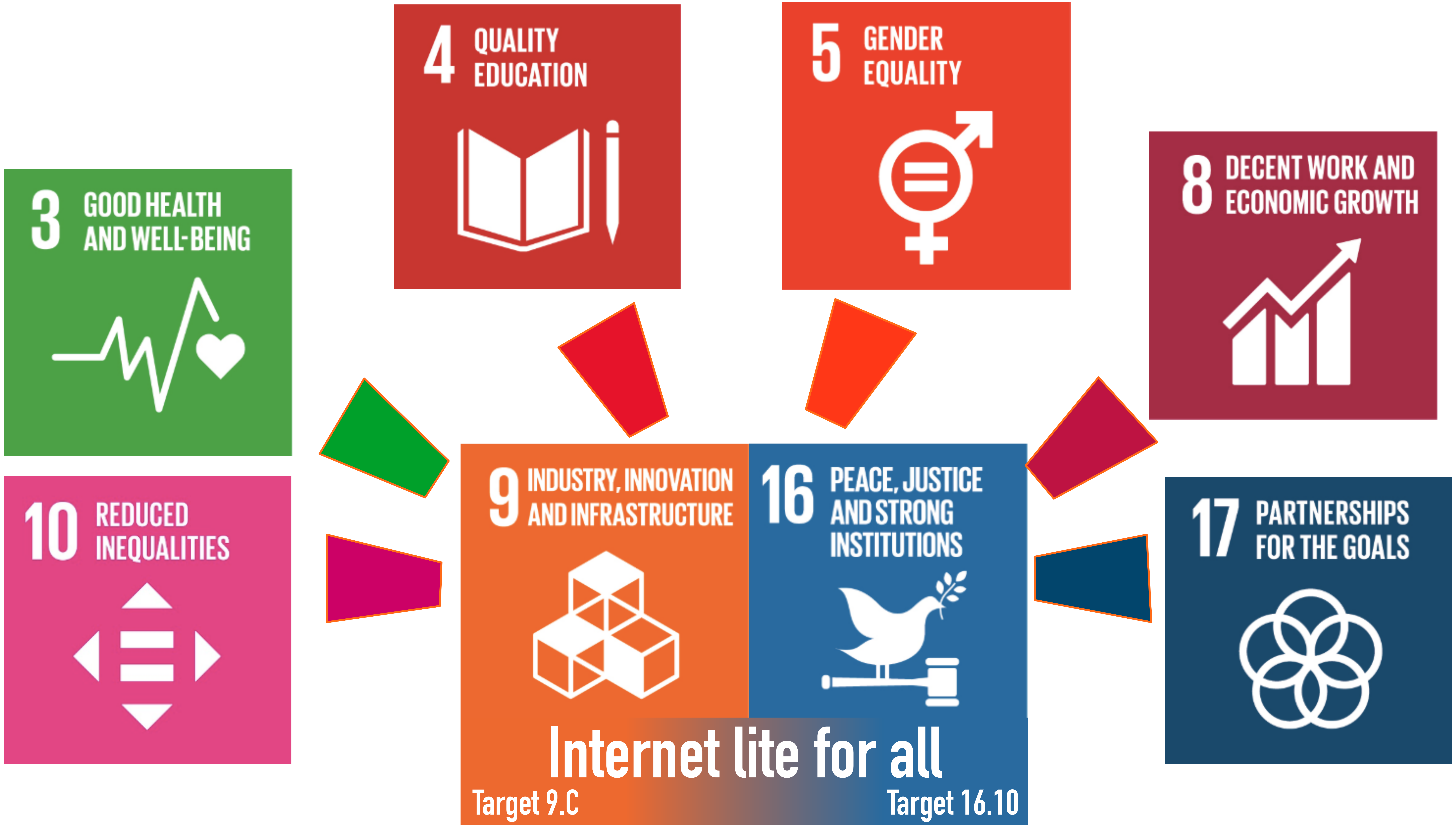
RELATED

Beyond connectivity: building an inclusive U.N. agenda for internet development Read More ▸

Access Now welcomes new report on economic impact of shutdowns Read More ▸

Internet lite for all

the catalyst for the goals



3 GOOD HEALTH AND WELL-BEING

4 QUALITY EDUCATION

5 GENDER EQUALITY

8 DECENT WORK AND ECONOMIC GROWTH

10 REDUCED INEQUALITIES

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE

16 PEACE, JUSTICE AND STRONG INSTITUTIONS

17 PARTNERSHIPS FOR THE GOALS

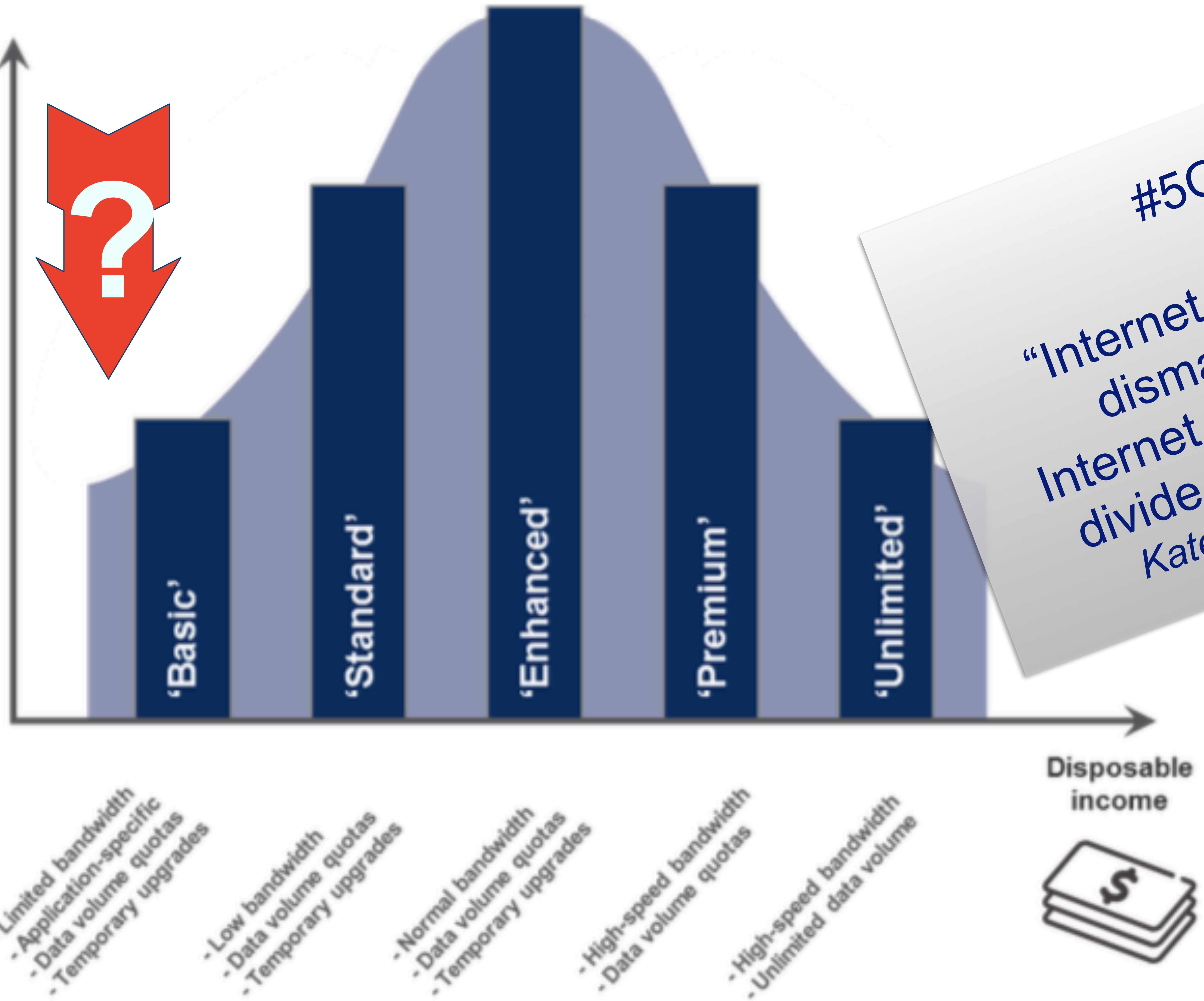
Internet lite for all

Target 9.C

Target 16.10

Telecom view on digital inclusion

Addressable Market



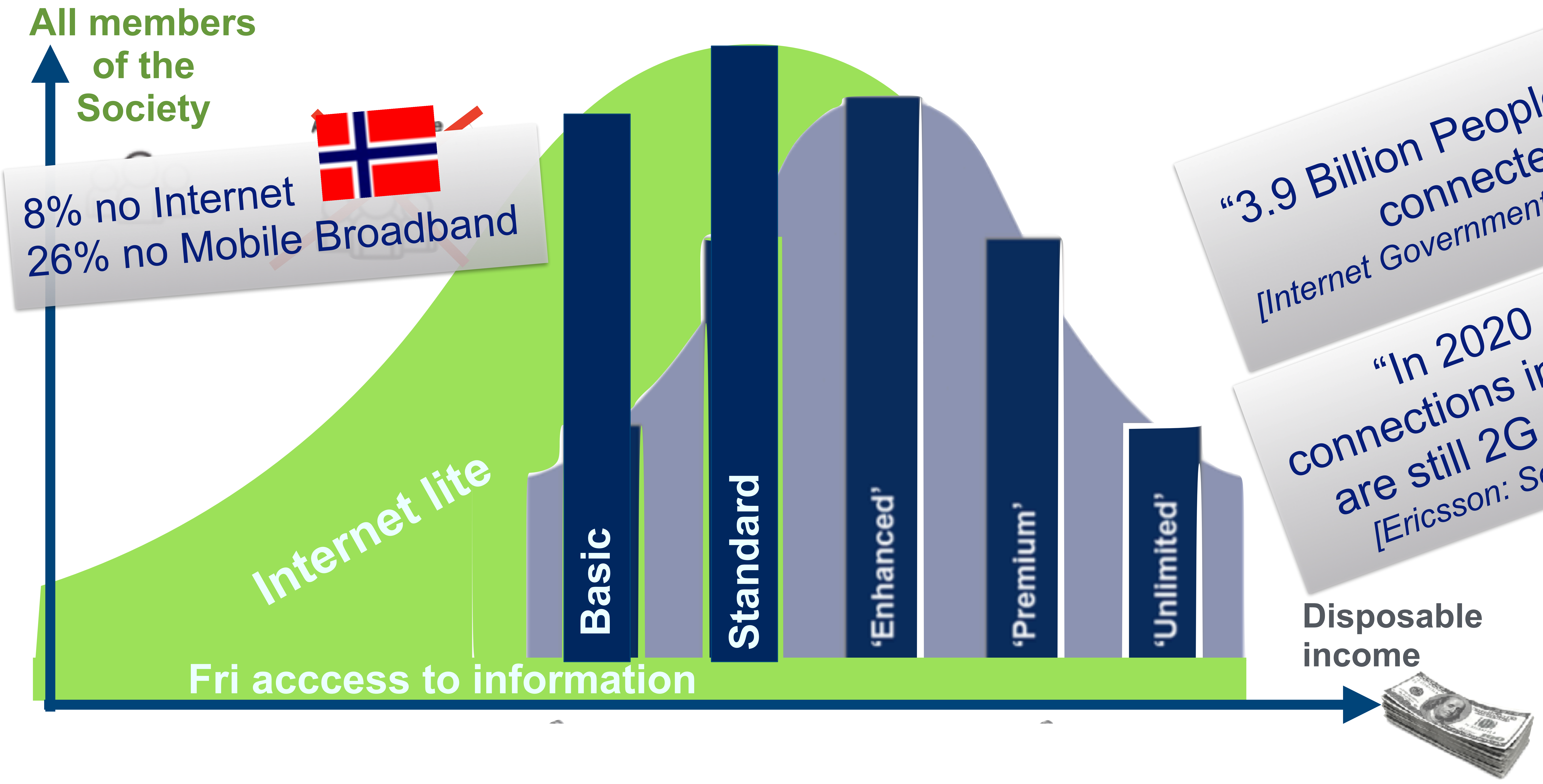
#5Gfor All?

"Internet had the ability to dismantle the divide. Internet failed miserably, the divide is bigger than ever."

Kate Gilmore, Human Rights, UNO

Source: Service Innovation through Smart Networks, Ericsson, https://www.ericsson.com/assets/local/networks/documents/service-innovation-through-smart-networks.pdf

6G (#5GforAll) for digital inclusion



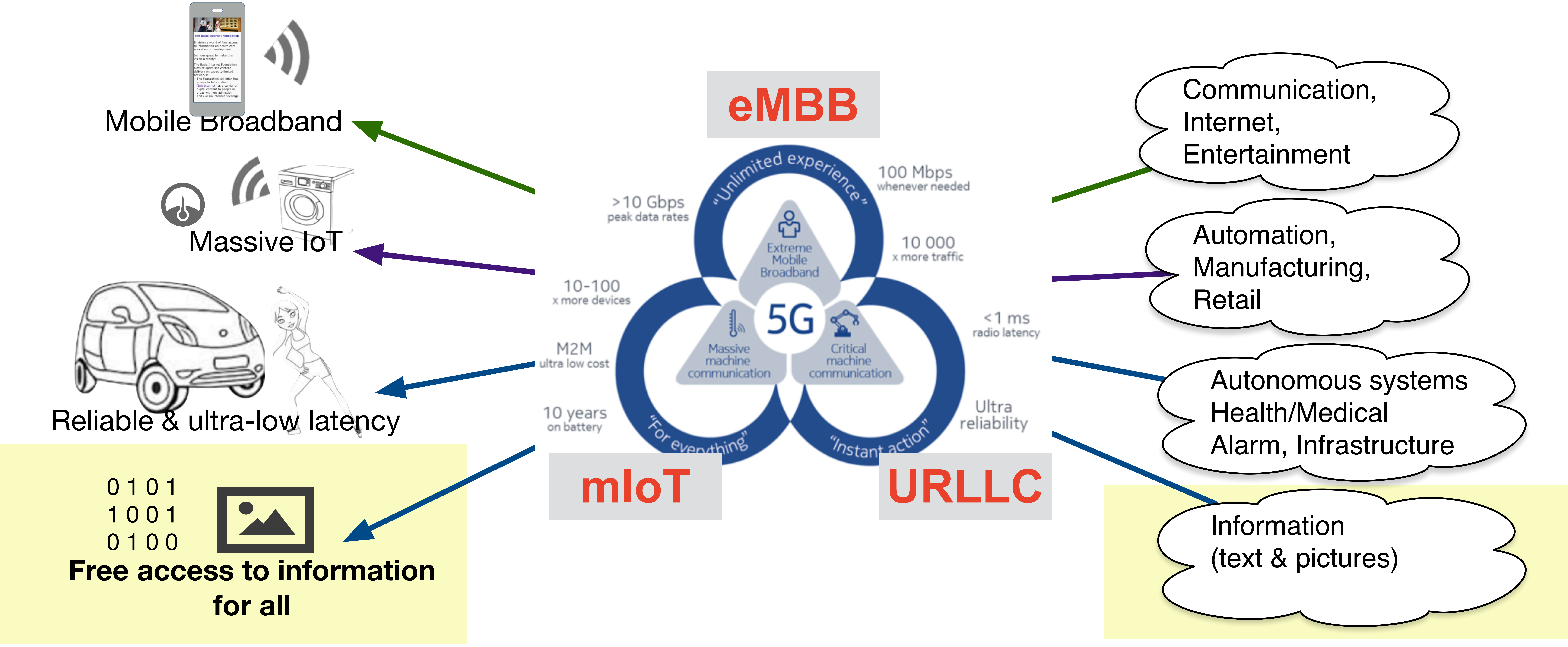
8% no Internet
26% no Mobile Broadband

"3.9 Billion People are not connected"
[Internet Government Forum, 2018]

"In 2020 45% of connections in Africa (SSA) are still 2G connections"
[Ericsson: Service Innovation]

[Adapted from: Service Innovation through Smart Networks, Ericsson, 2018]

5G network slicing for Free Access to Information for All



Mobile Broadband

Massive IoT

Reliable & ultra-low latency

0 1 0 1
1 0 0 1
0 1 0 0

Free access to information for all

eMBB

mIoT

URLLC

Communication, Internet, Entertainment

Automation, Manufacturing, Retail

Autonomous systems Health/Medical Alarm, Infrastructure

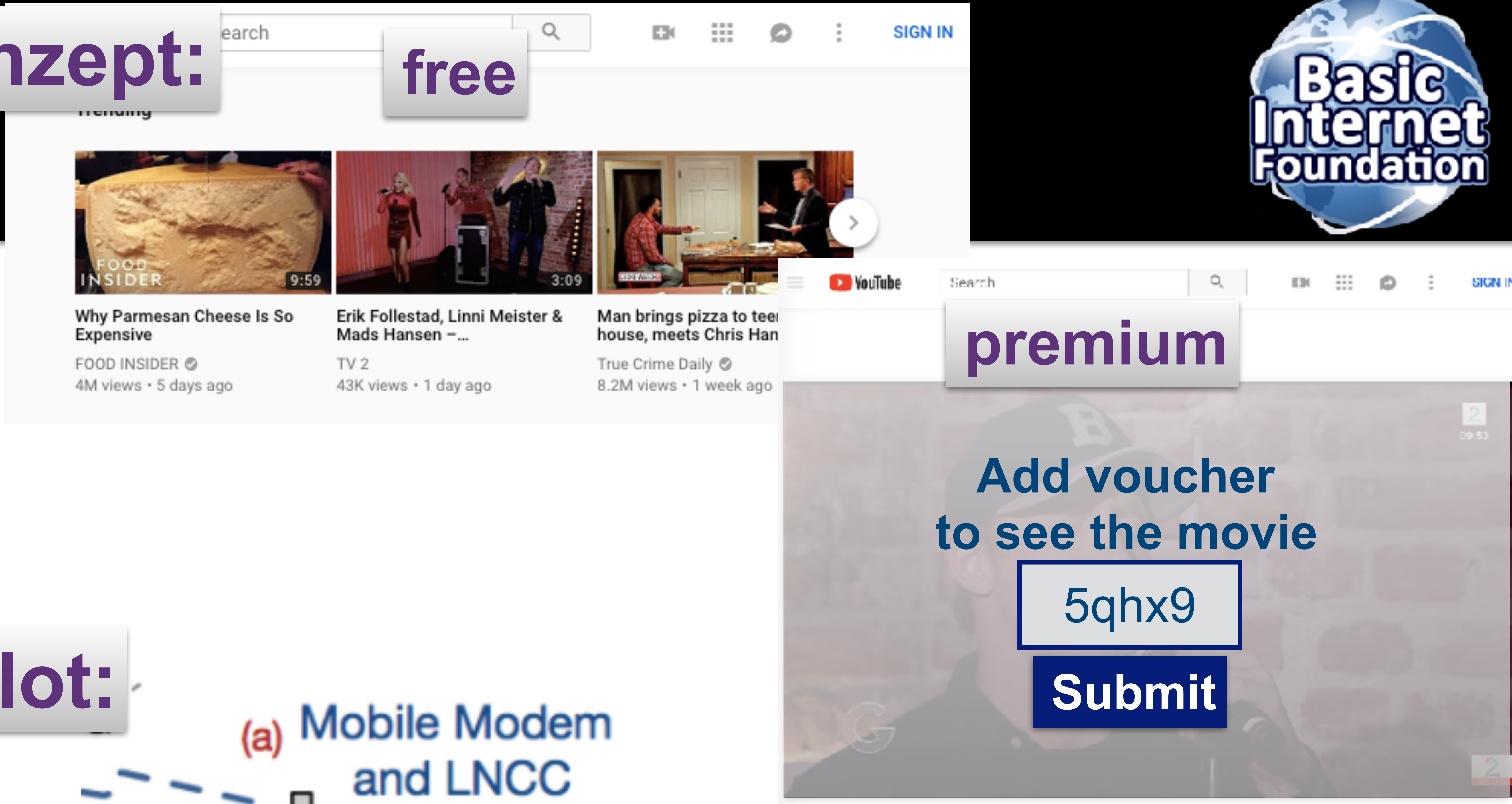
Information (text & pictures)

InfoInternet Standard

- Network responsiveness

- InfoInternet Standard development
  - ➡ **Konzept**: www-filtering
    - free: text & picture, premium: video
  - ➡ **Pilot**: www metadata & inspection
    - address, port & deep packet analysis
  - ➡ **Standard**: proxy & html5 standard,
    - http://BasicInternet.org&standard=InfoInternet

Konzept:



free

earch

SIGN IN

Trending

Why Parmesan Cheese Is So Expensive
FOOD INSIDER
4M views • 5 days ago

Erik Follestad, Linni Meister & Mads Hansen –...
TV 2
43K views • 1 day ago

Man brings pizza to teen house, meets Chris Han
True Crime Daily
8.2M views • 1 week ago

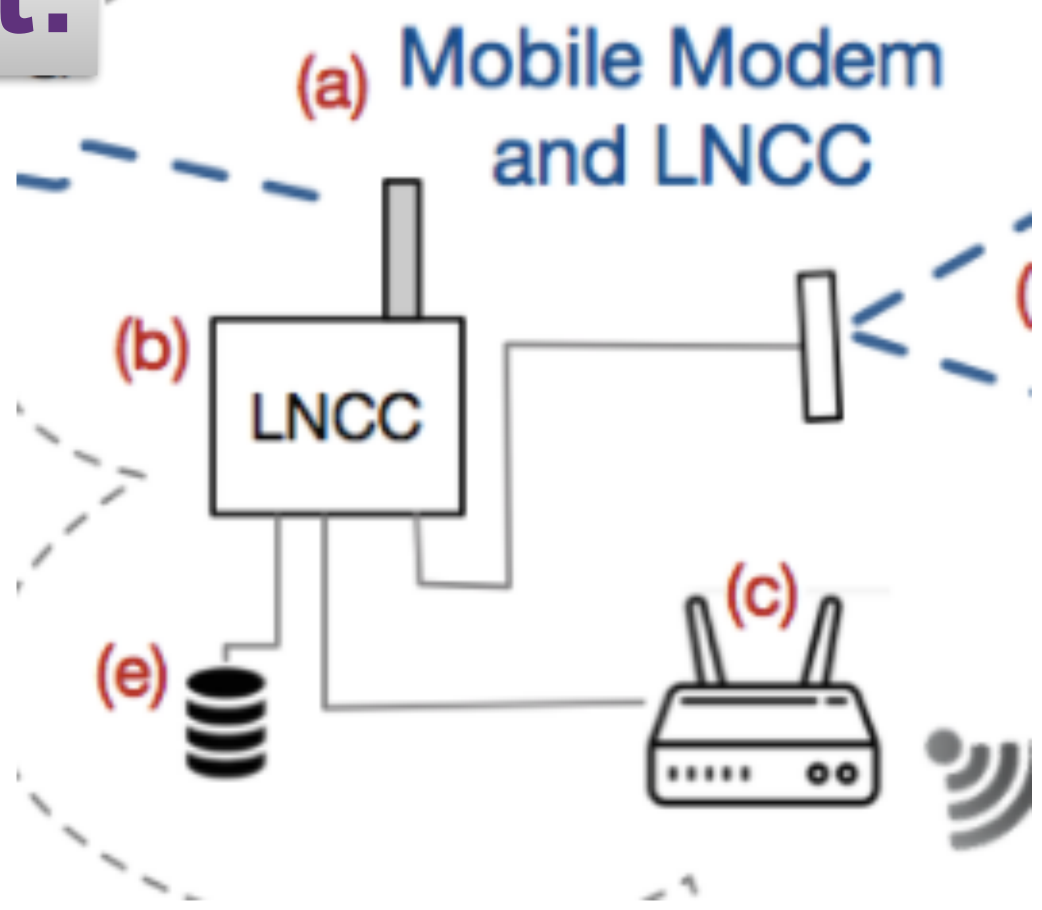
premium

Add voucher
to see the movie

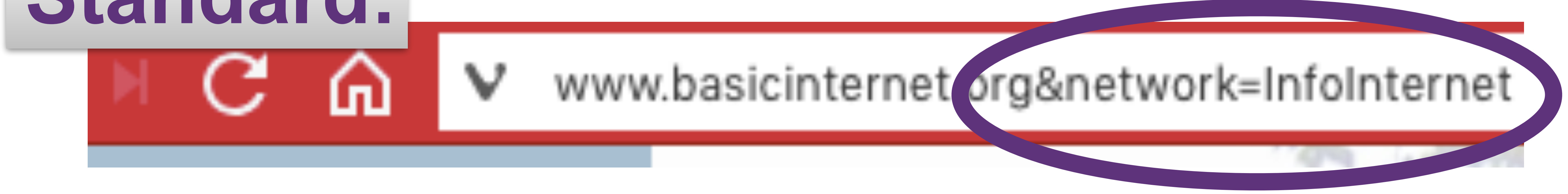
5qhx9

Submit

Pilot:



Standard:

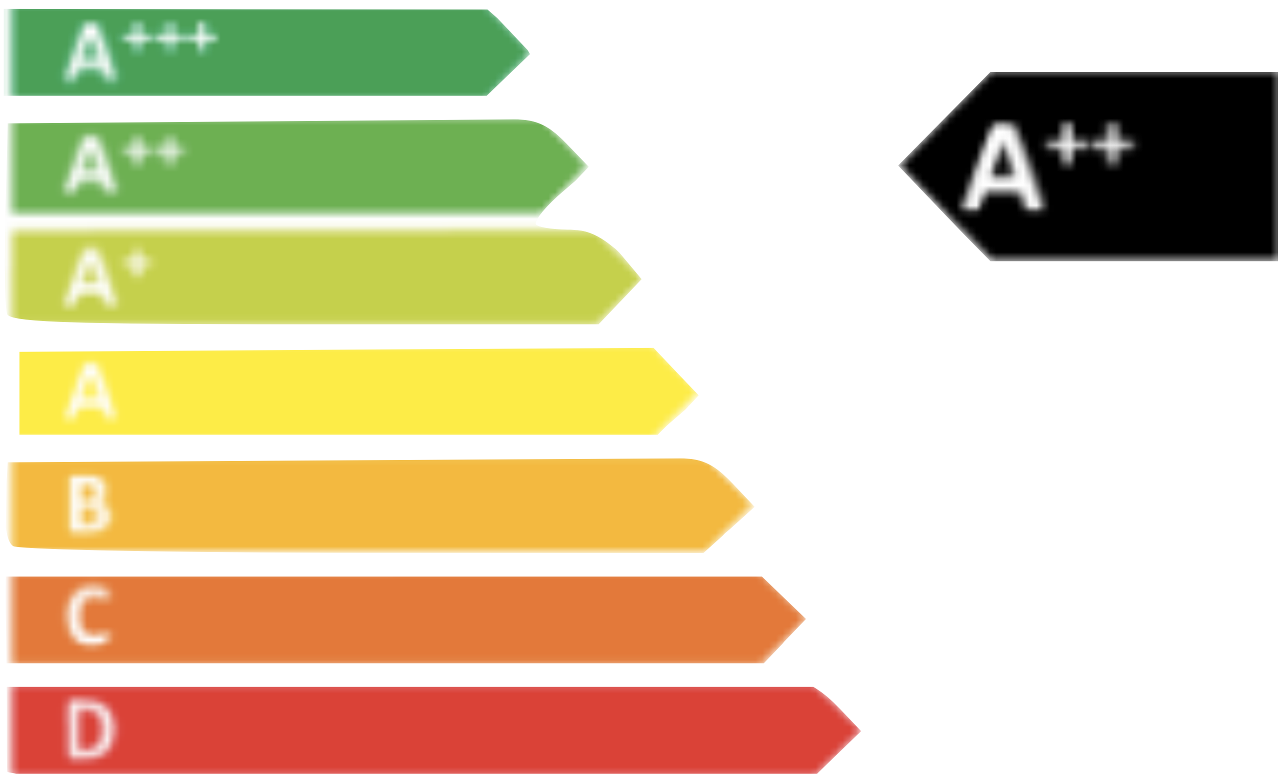


www.basicinternet.org&network=InfoInternet

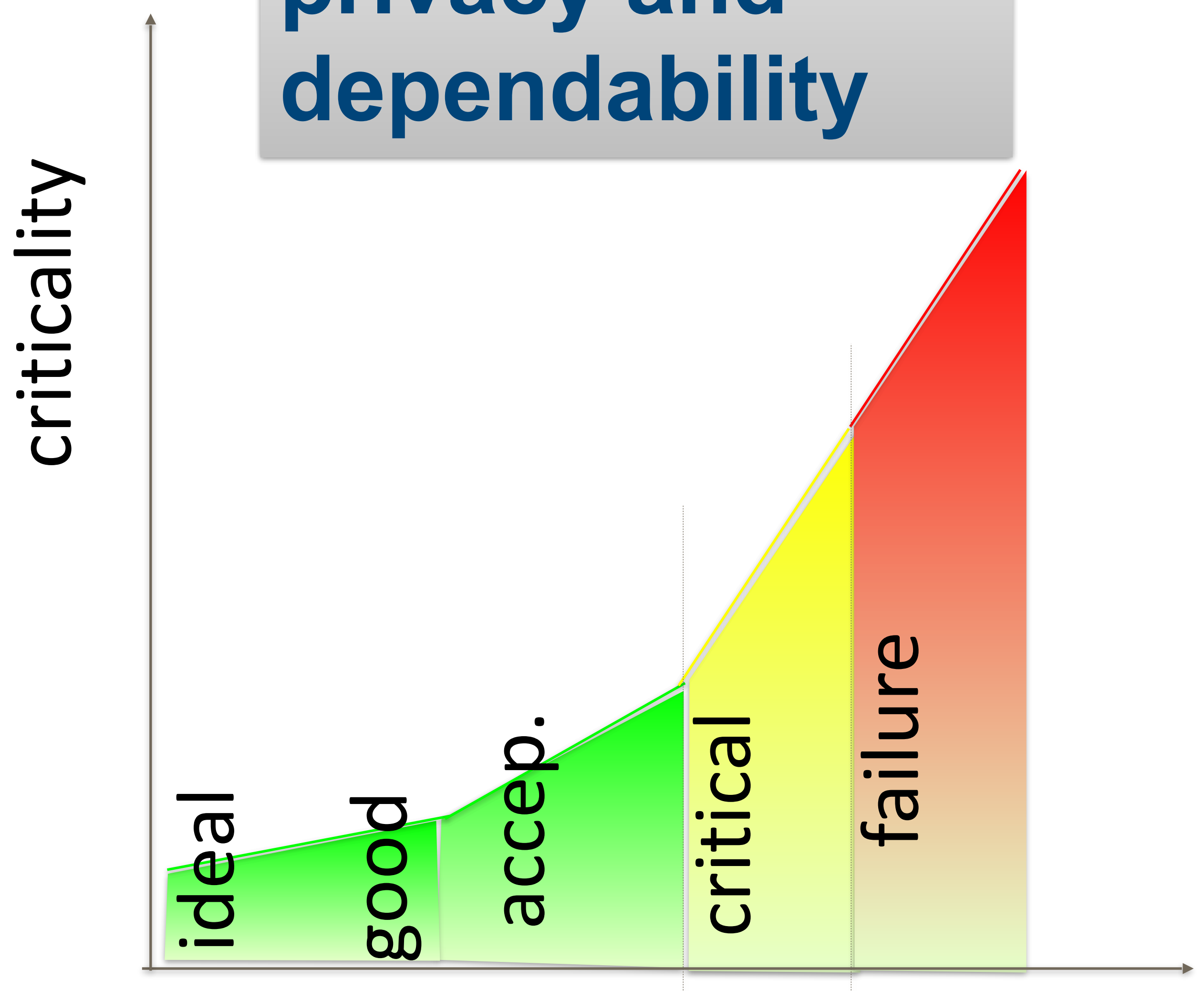
Privacy Conclusions

- Home is the battlefield
  - ➡ Smart Home/Offices
  - ➡ Novel services: Control, Alarm, Health
    - ➡ Specific requirements for security, privacy
  - ➡ HAN port for continuous power monitoring
    - ➡ identification of user behaviour
- Collaborative approach for a (more) secure society
  - ➡ “the cloud is not the answer” - distributed security
  - ➡ partnership for security: threats, measures, counter activities
- Measurable Security and Privacy for IoT
  - ➡ Industrial impact: Security Centre for Smart Grid
  - ➡ Privacy labelling for apps and devices
- Innovation ecosystem for the IoT
  - Reducing the digital gap

Privacy Labels



Measurable: security, privacy and dependability



Logic: Centralised ⟷ Fog
Smart Meter: Information ⟷ Control