



**UiO** : **Department of Technology Systems**  
University of Oslo

**Guest Lecture at UPM - 28May2020**

# **Measurable Security for the Internet of Things**

Josef Noll,  
Professor, University of Oslo  
[josef.noll@its.uio.no](mailto:josef.noll@its.uio.no)



<http://IoTSec.no> , [#IoTSec](https://twitter.com/IoTSec), <http://SCOTT-project.eu>

***“The last time I was connected by wire was at birth”***

- ◉ Background: Nordic Perspective
  - ◉ Internet of Things (IoT)
    - ➔ Cyber-, IoT-, Societal-Security
  - ◉ Systems of Systems
    - ➔ Security, Privacy, Dependability
    - ➔ Measurable Security
    - ➔ Goal versus System
  - ◉ The Multi-Metrics Method
    - ➔ Mobility services
    - ➔ Walk through
  - ◉ Conclusion
- Questions - for you - keep awake

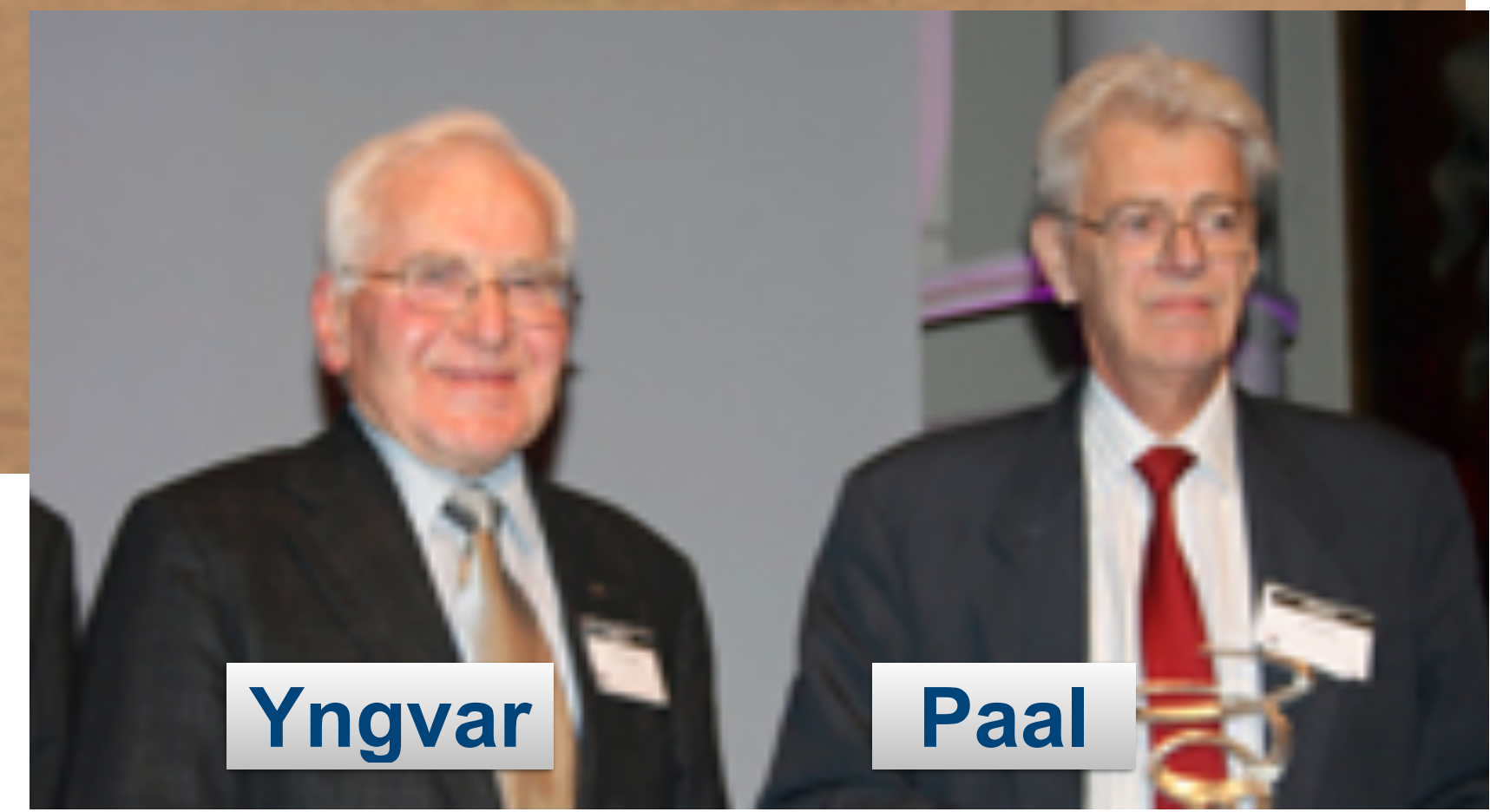
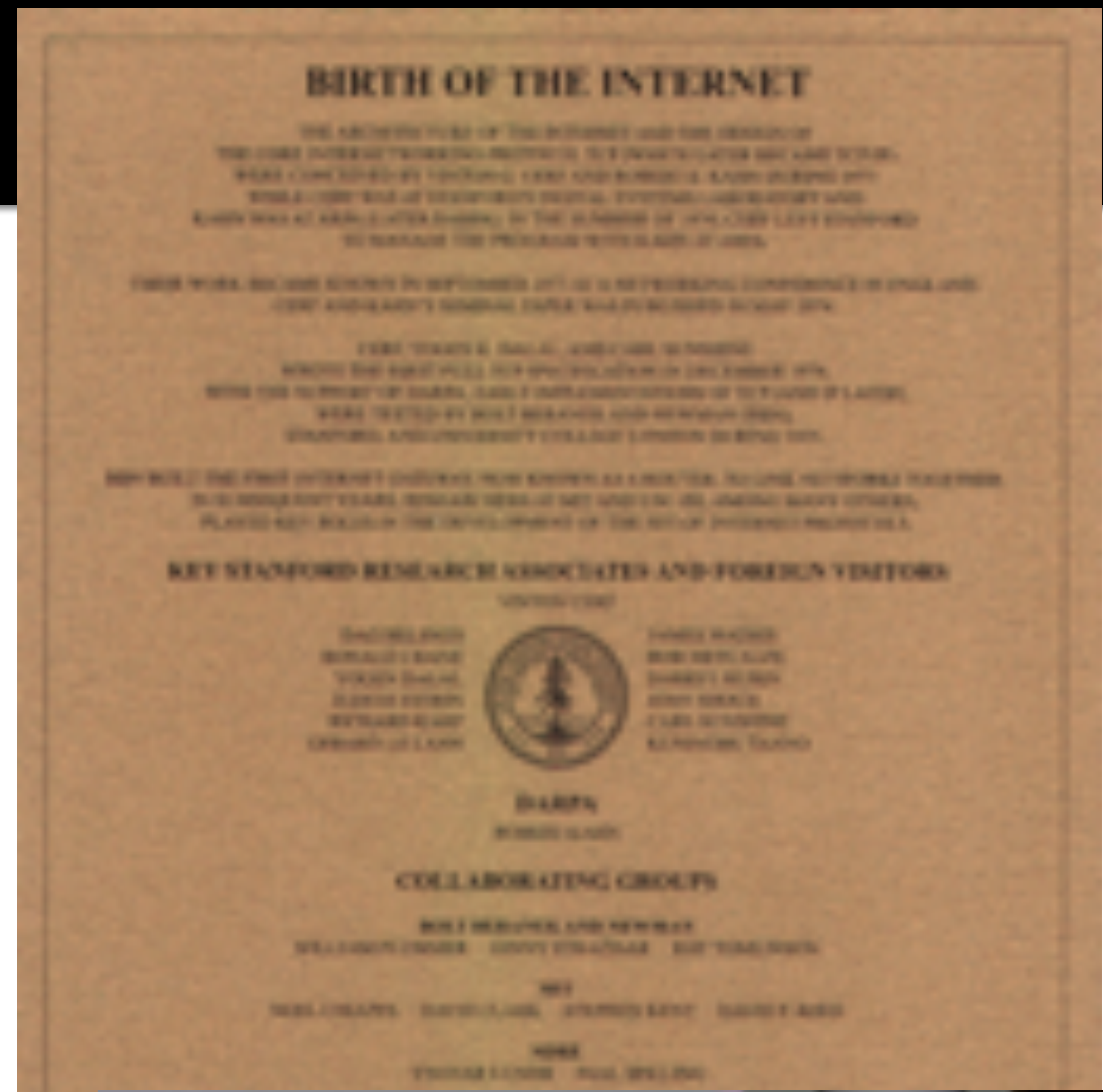


# The Internet and the Nordics

- First Arpanet Connection to **Kjeller** (June 1973)
  - (except Hawai)
- List\_of\_Internet\_pioneers [Wikipedia]
  - Yngvar Lundh, **Paal Spilling**
- Application development
  - .php, OpenSource, Linux, Skype, Spotify
  - **OperaSoftware**, FAST Search (Bing)
  - Nokia, Ericsson
  - **Telenor**, TeliaSonera
- Mobile Internet:

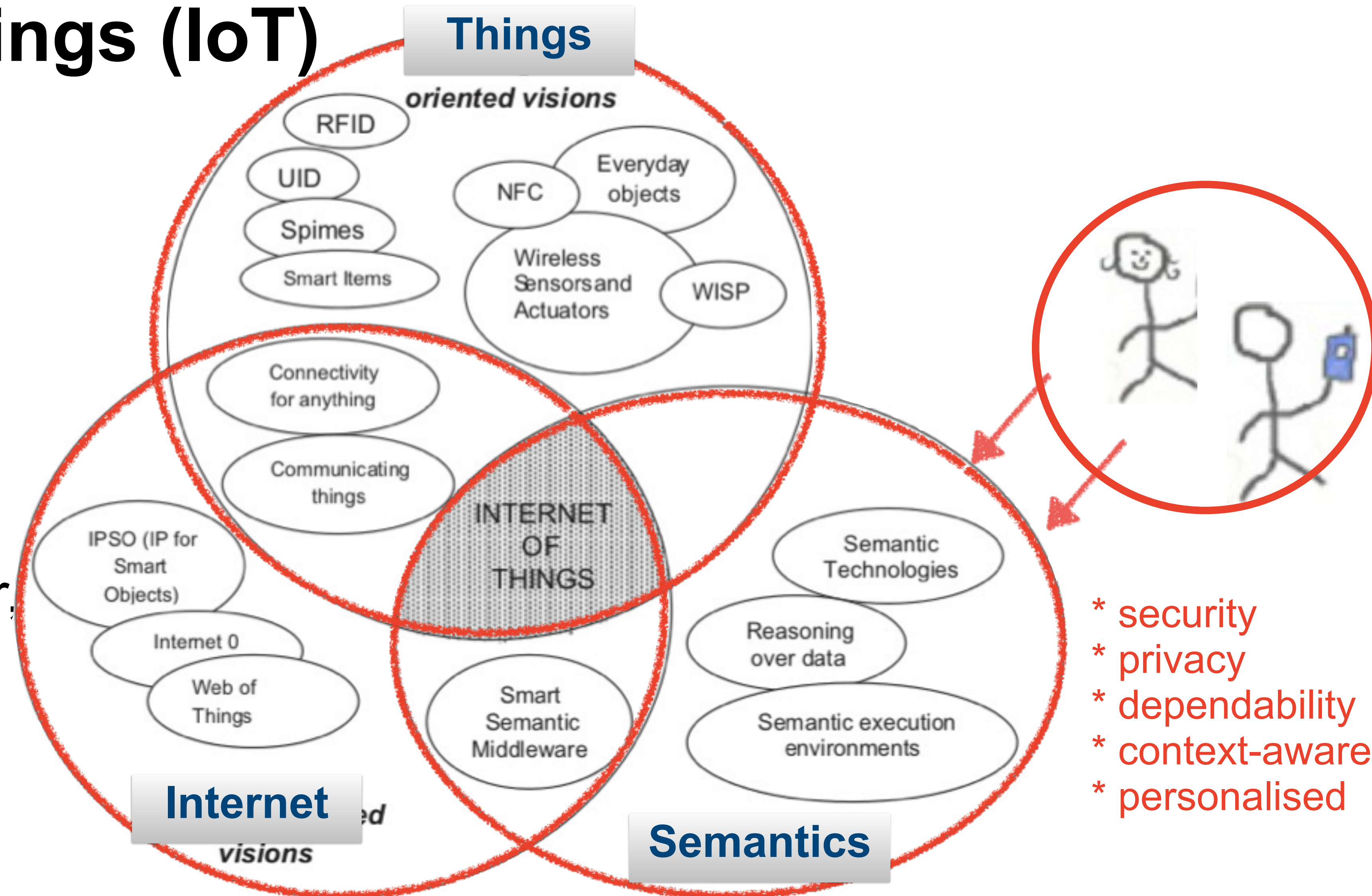


**GSM**  
 Mobile Applications, 6G



# The Internet of Things (IoT)

- IoT =
  - Things +
  - Internet +
  - **Semantics**
- Things that communicate
  - with Things: computer,
  - understand the meaning,
  - takes own decisions



# Why Semantics?

- Conceptual Level



lunch (.no)



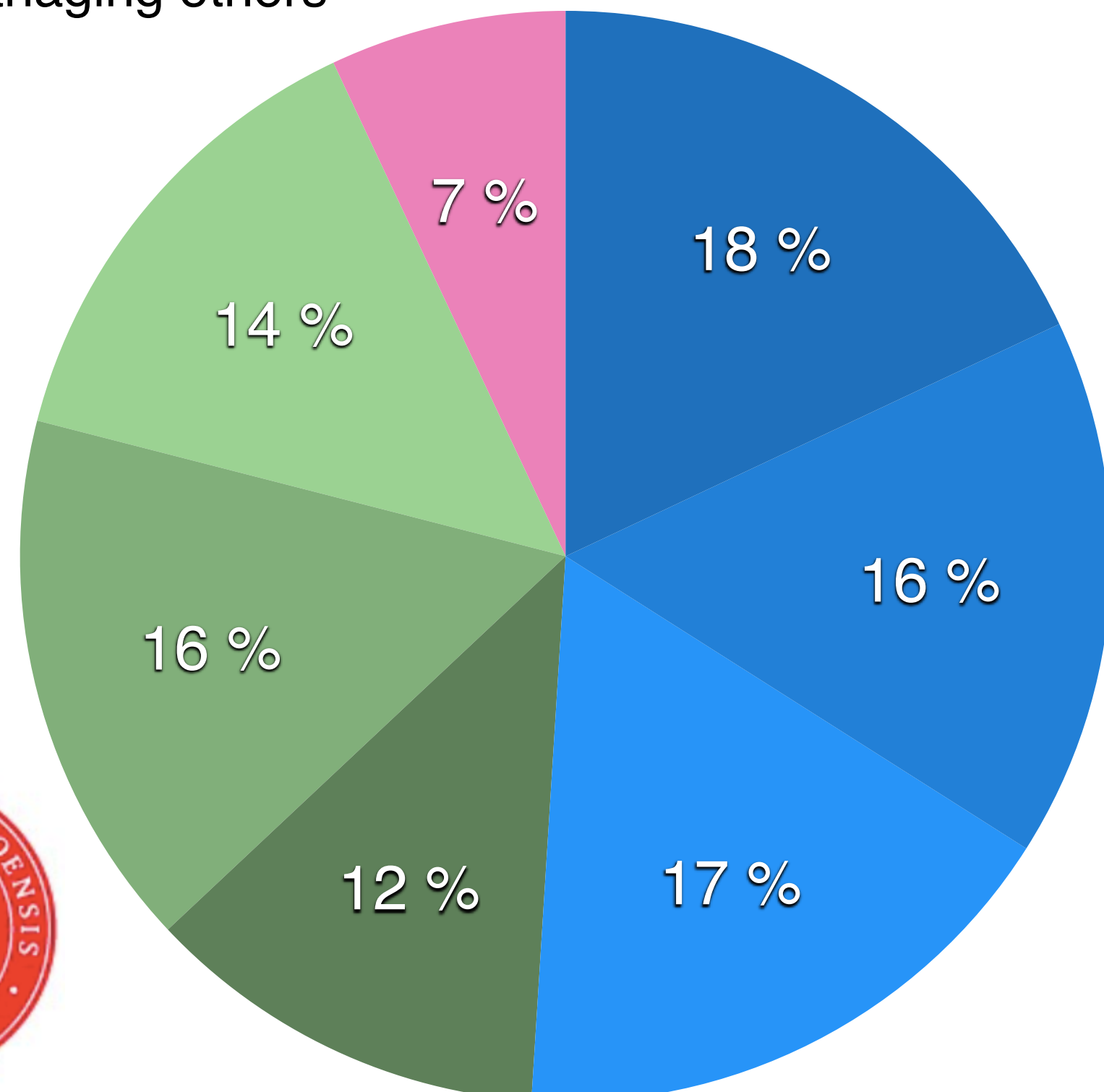
lunch (.es)

Source: Juan Miguel Gomez, University Carlos III de Madrid

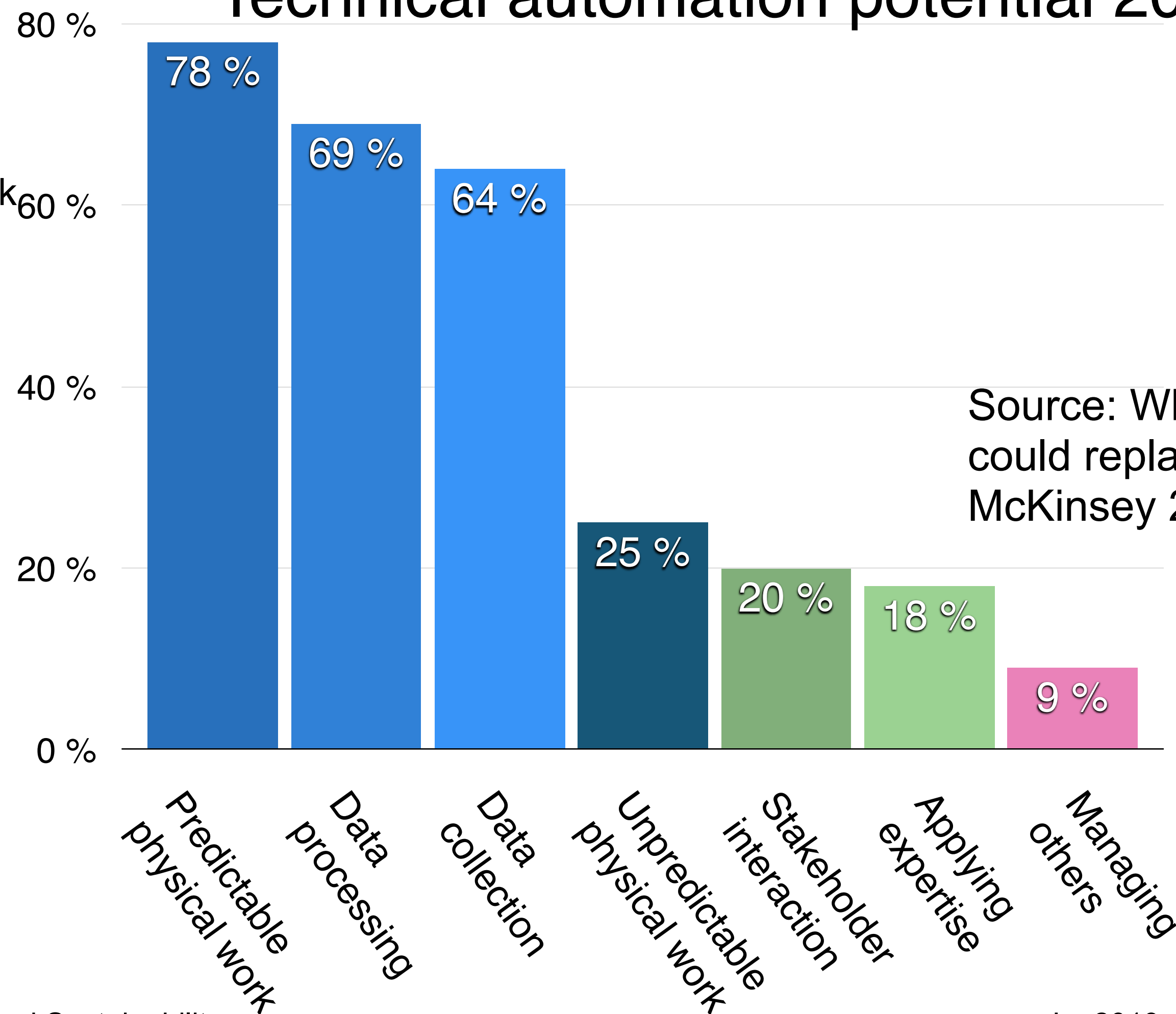
# Automation will come

USA work force time spent [%]

- Predictable physical work
- Data collection
- Stakeholder interactions
- Managing others
- Data processing
- Unpredictable physical work
- Applying Expertise

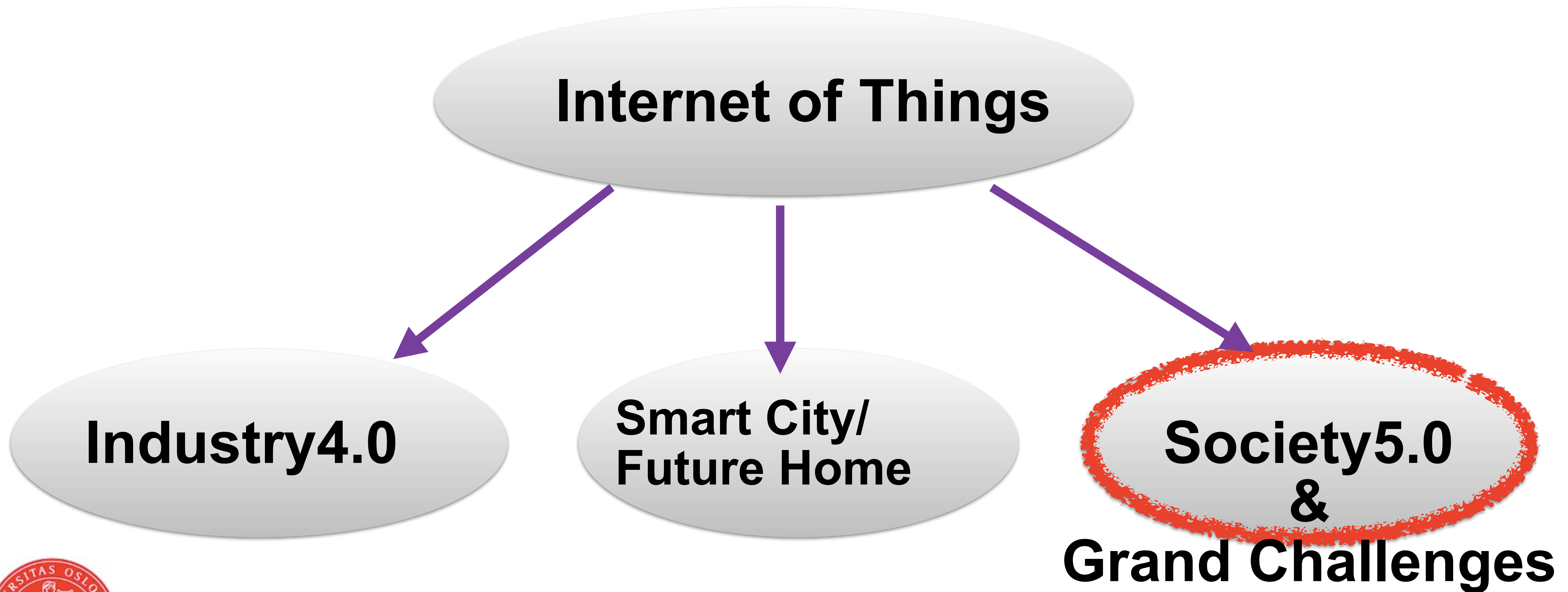


Technical automation potential 2016 [%]



Source: Where Machines could replace humans, McKinsey 2016





# 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



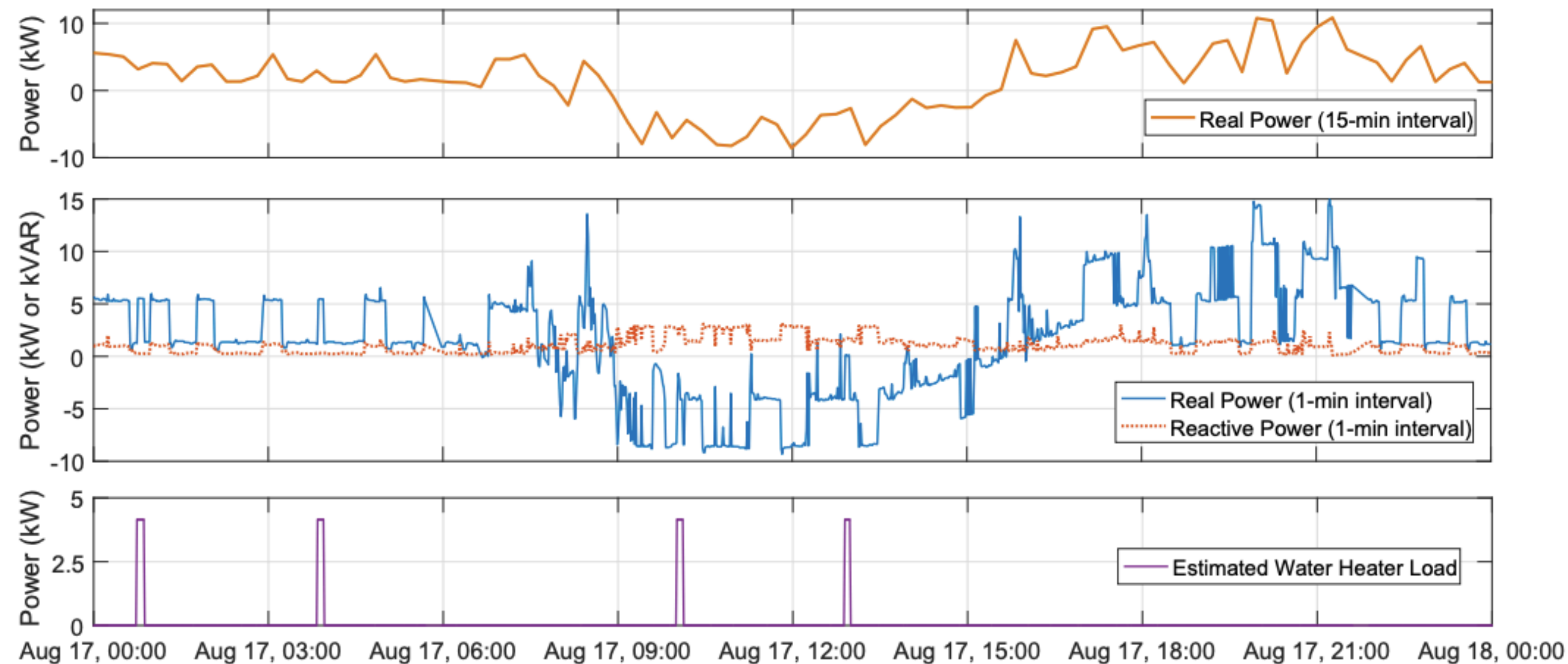
AMS HAN port (NEK)

<https://www.nek.no/info-ams-han-brukere/>IoT and Sustainability



## 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](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**

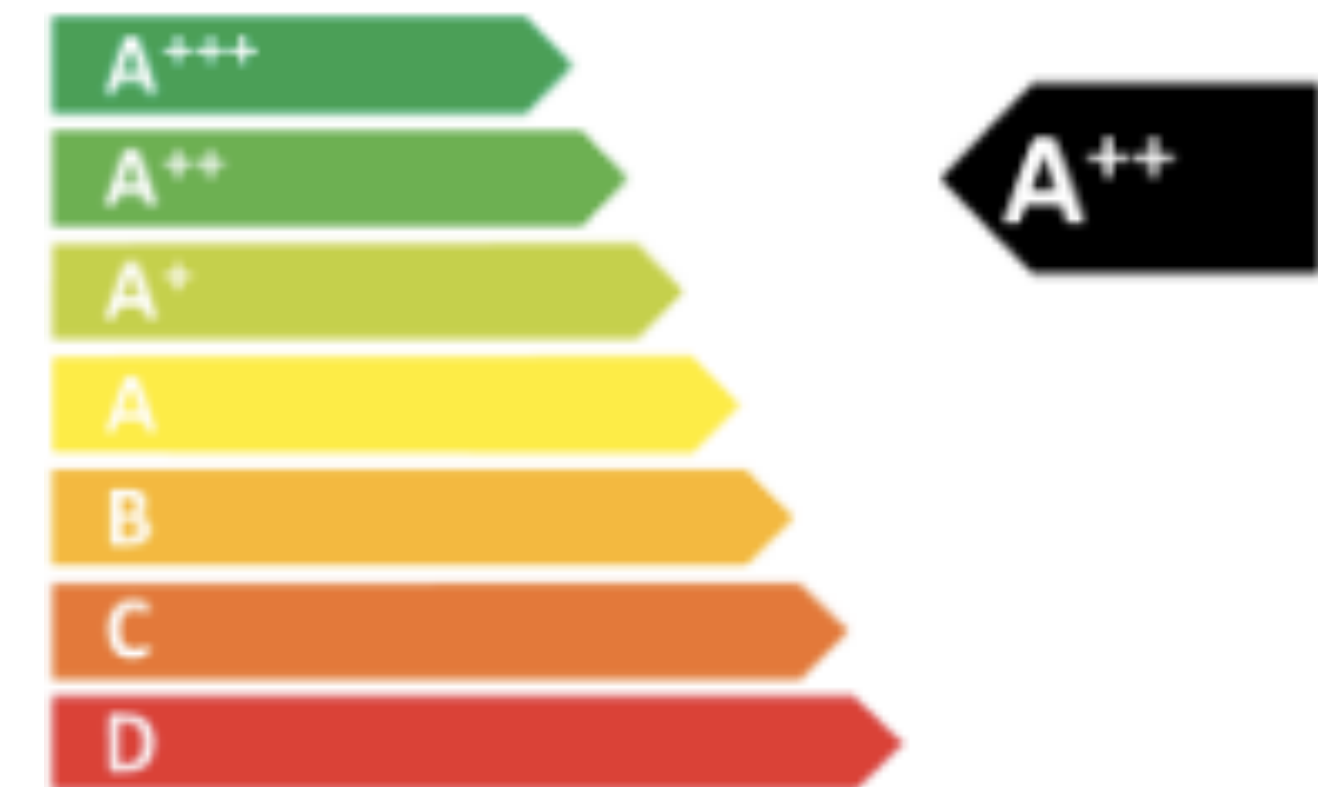


## The economic perspective

- 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

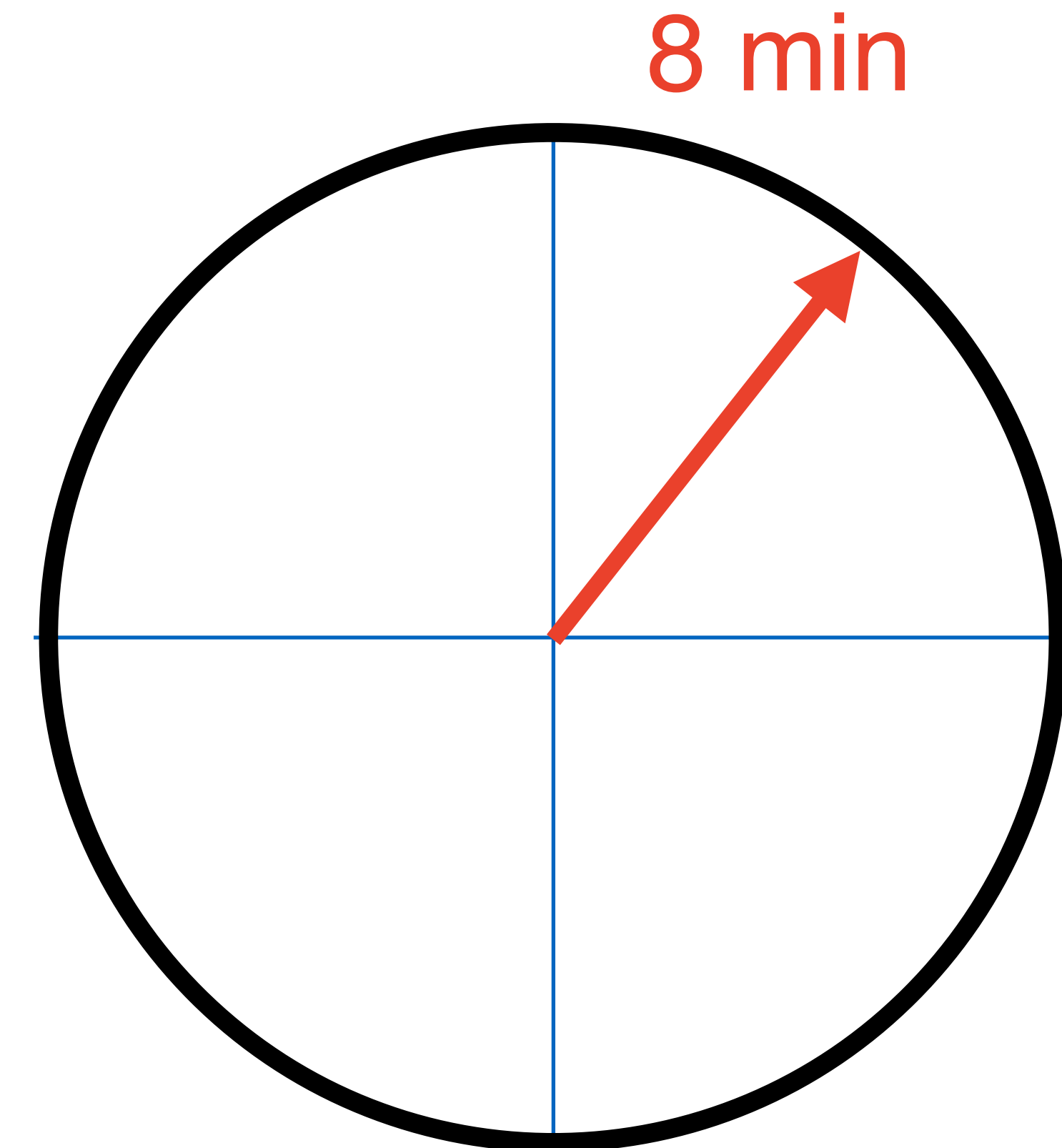


[privacylabel.ioTSec.no](https://privacylabel.ioTSec.no)



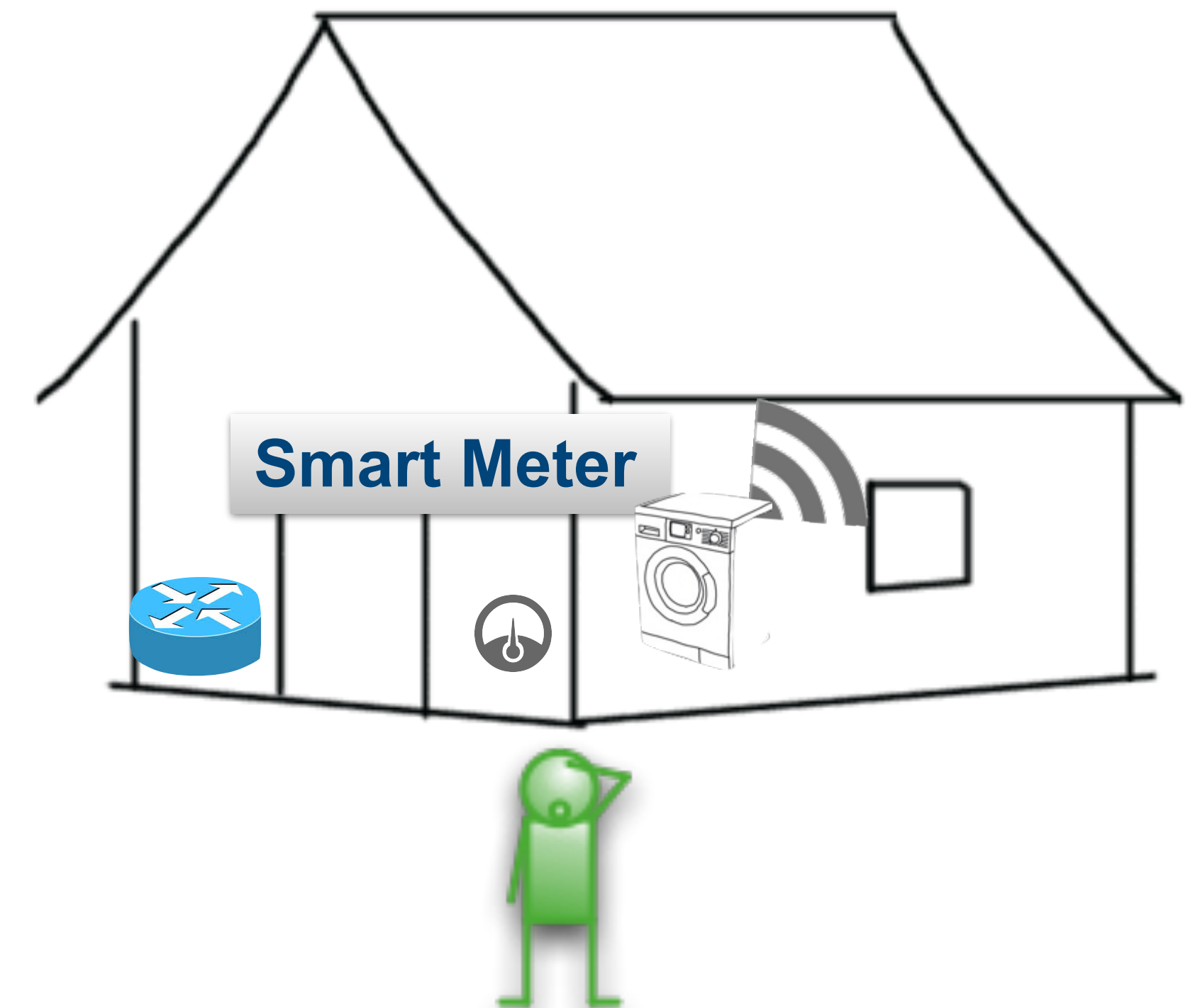
# IoT take-away - discuss (4 x 2 min)

- ◉ IoT consists of ...
- ◉ What is ..... and why do we need it?
- ◉ Which areas will IoT influence? - and why
- ◉ Economic perspective of IoT



## Resource-related challenges

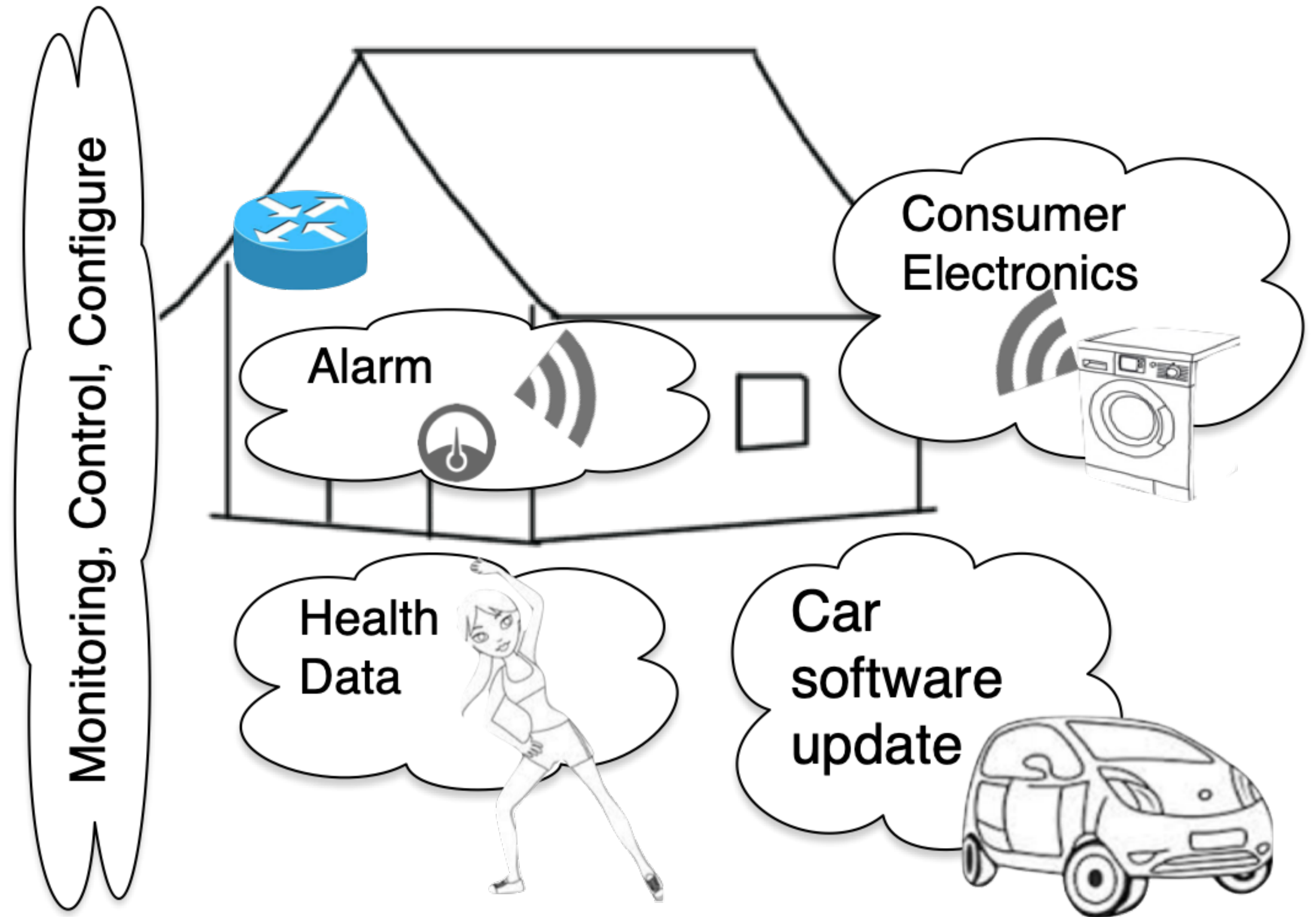
- Limited bandwidth
- Latency
- Reliability
- Not feasible to create a "perfect" system: be prepared to be compromised
  - ➔ Redundancy, reconfiguration, backup
- Security focus points
  - ➔ the edge: Sensors, Appliances
  - ➔ Gateway/router
  - ➔ Cloud services



## Internet of Things (IoT)

- Interconnected power systems
  - ➔ measure:
    - Voltage,
    - Frequency variation
  - ➔ automatic control
- Controlling home appliances
  - ➔ Power consumers:
    - heat pump, water heater
    - car charger
    - washing machine, dish washer

Convenience & Security



## Converged IoT infrastructure-related challenges

- ◉ From closed networks to cloud computing. Not only new possibilities, but also new threats
- ◉ Heterogenous infrastructure connects a wide range of devices with a life-cycle mismatch
- ◉ Opens up new interfaces to attack
  - ➔ Risk for loss of privacy, functionality, fraud
  - ➔ Physical consequences
- ◉ Security measures
  - ➔ shall be budgeted in accordance with the possible damage,
  - ➔ not with the price of the asset
- ◉ IoT devices can introduce unexpected traffic into corporate networks (e.g. IPv6), which can be a challenge for the IDS system (if e.g. rules include IPv4 parameters) – one should enforce security controls both on IPv6 native and IPv6 tunnelled traffic



# Significance

## IoT security challenges

- Mirai attack
  - ➔ “security by obscurity”
  - ➔ different security viewpoint
- “it is just the beginning”
  - ➔ 4x increase in capability in 2018
- 2020: 36 different classes of IoT virus



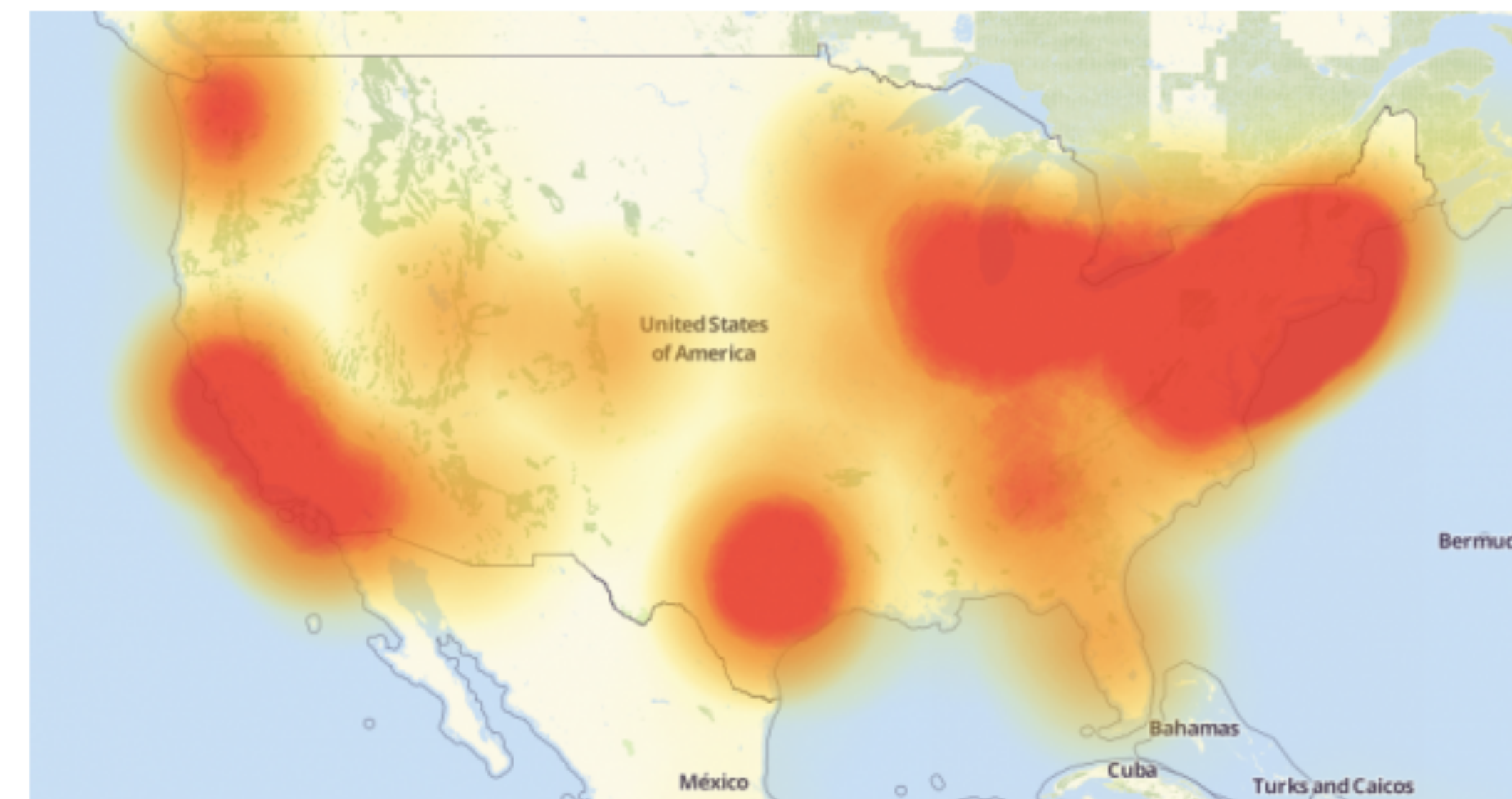
## 21 Hacked Cameras, DVRs Powered Today's Massive Internet Outage

OCT 16

16Oct2016

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.



[Source: <https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/>]

## Security challenges

- ◉ IoT introduces a dramatically larger attack surface
- ◉ Wide range of technologies involved:
  - ➔ Sensors: AV, positioning, acceleration, temperature, proximity
  - ➔ Communication: cellular, wireless, wired, light
  - ➔ Identification: RFID, barcodes, tags, biometry
  - ➔ Localisation: gps, indoor solutions
- ◉ From closed networks to cloud computing:
  - ➔ Security solutions should not build on and depend on to the network technology (heterogeneous infrastructure)
- ◉ Cost of security:
  - ➔ Possible mismatch between the value of the device and the data handled
- ◉ Misconception: device focus. IoT has many attack surfaces, each of these shall be evaluated.
- ◉ All elements of the system have to be considered:
  - ➔ End devices, cloud infrastructure, the application, network interfaces, software environment, use of crypto
- ◉ Public acceptance of IoT depends on security of the systems
  - ➔ Trust in IoT



## Security analysis

### Increasingly Hostile Threats

Source: Dept. of Homeland Security; ICS-CERT

Disclosed ICS Vulnerabilities\*

High Profile Attacks



- It's not about the device. One shall see the big picture
  - IoT as entry point for "system control"
- Structured approach with well-known steps: e.g. securing a web interface, analysis and setup of protocol parameters (avoid fallback to weak crypto), analysis of data to select correct protection
- Insecure network services: unfortunately, typical for industrial applications
- Transport encryption: use appropriate technological solutions
- Cloud interface
- Mobile interface
- Appropriate granularity in security configuration: e.g. monitoring, logging, password and lockout parameters
- Insecure software
- Physical security



## Security needs of IoT

- ◉ User identification
  - ◉ Identity management
  - ◉ Tamper resistance
  - ◉ Secure storage
  - ◉ Secure content
  - ◉ Secure software execution
  - ◉ Secure communication
    - ➔ Over-the-air updates
  - ◉ Secure network access
- 
- ◉ Gateway as a key customer component: edge device for the LAN, concentrator



## Security needs of IoT

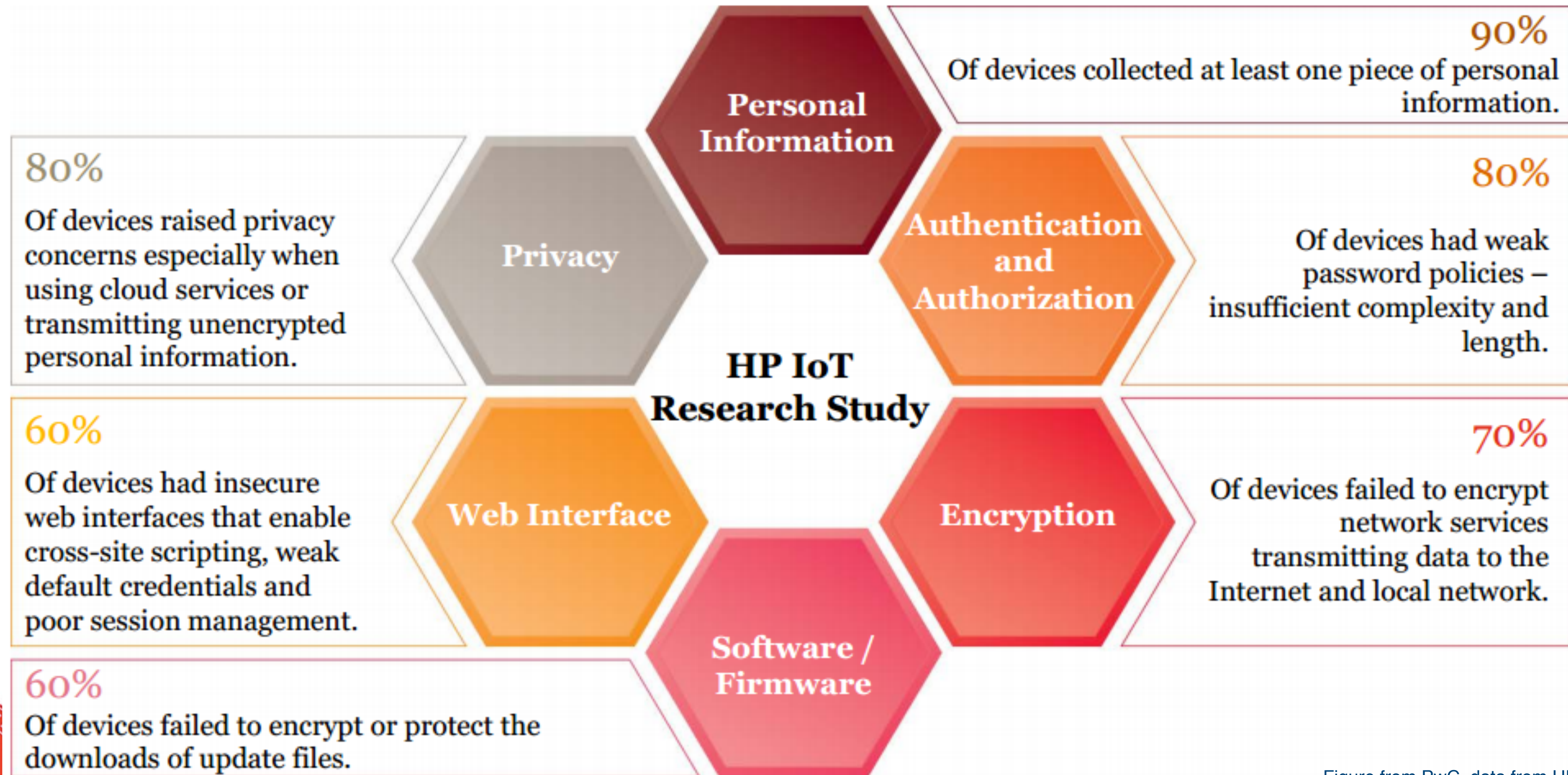
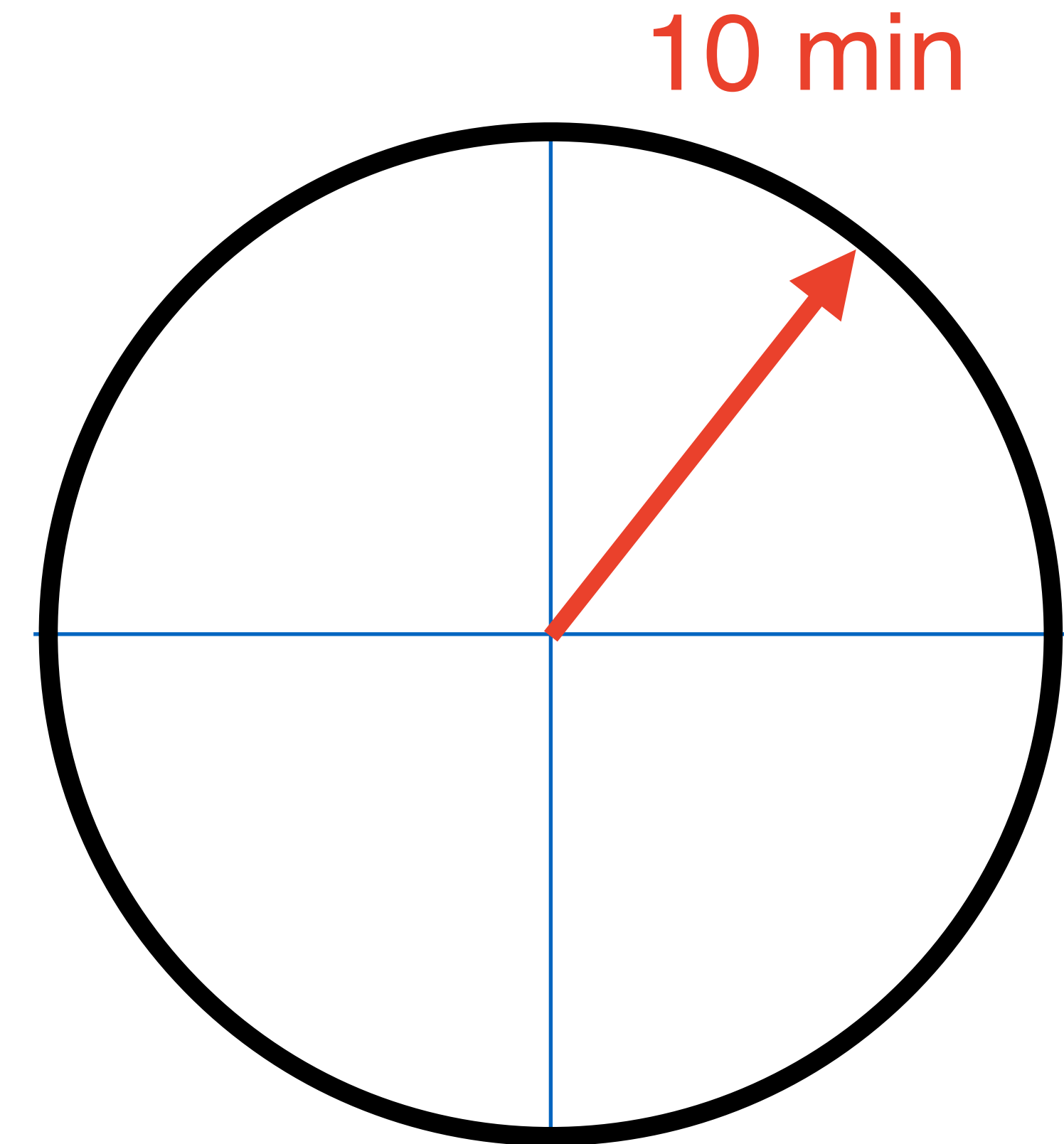


Figure from PwC, data from HP



## Security in IoT - discuss (10 min)

- Why is IoT difficult to secure?
- Create a top 5 ranking of device security (most to least important) - discuss - why
  - Examples: resources, communication, identity, firmware, tamper resistance, user identification, secure software execution, ...



# Measurable Security for the Internet of Things



## Overview

- Novel way of classifying systems
- Use case (application) SocialMobility
- Values for Security, Privacy
- Analyse the system of systems
- Identify Security, Privacy attributes and functionality for a sub-system
- Multi-Metrics analysis
- Future work



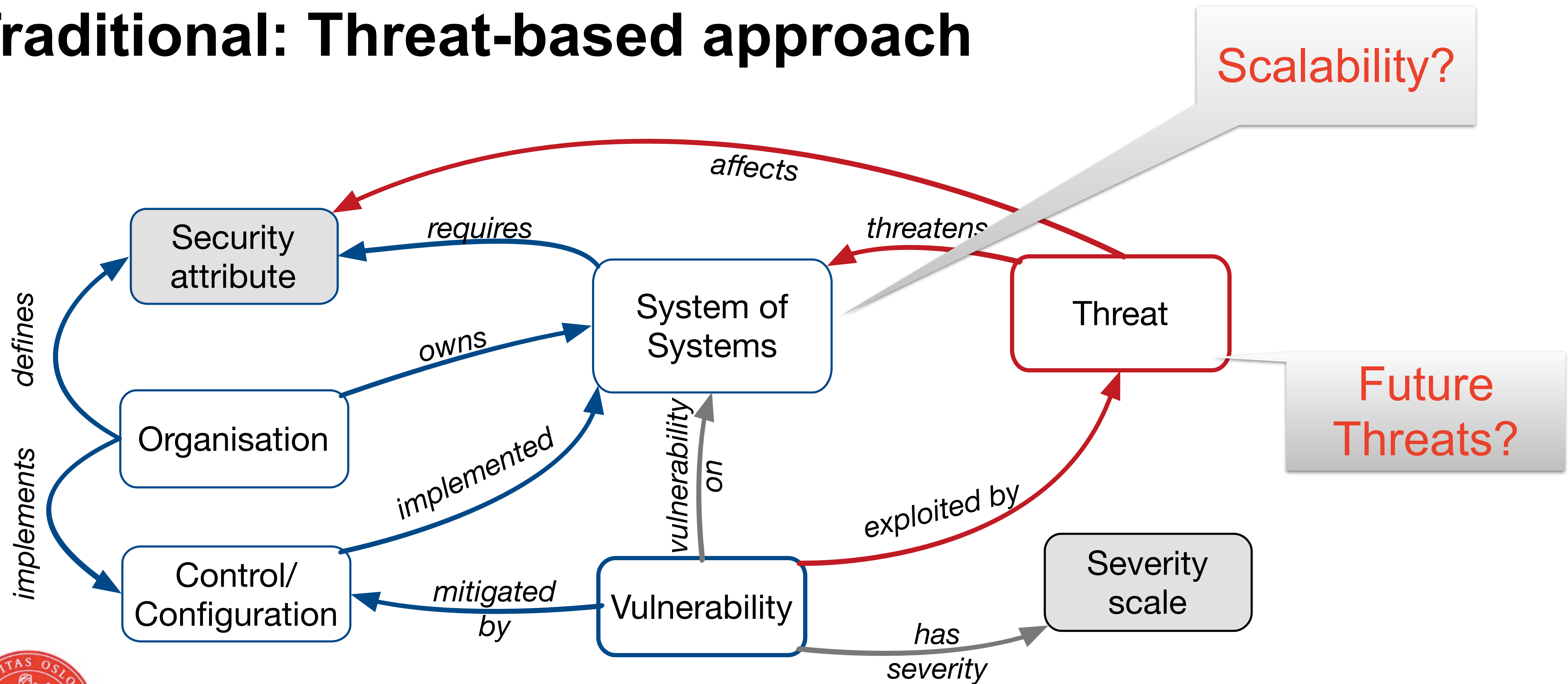
## Expected Learning outcomes

Having followed the lecture, you can

- establish a scenario/use case
- provide application examples
- provide reasons for the choice of s,p,d
- establish a system architecture with sub-systems and components
- explain the Multi-Metrics method
- (prepare for your own work)



# Traditional: Threat-based approach

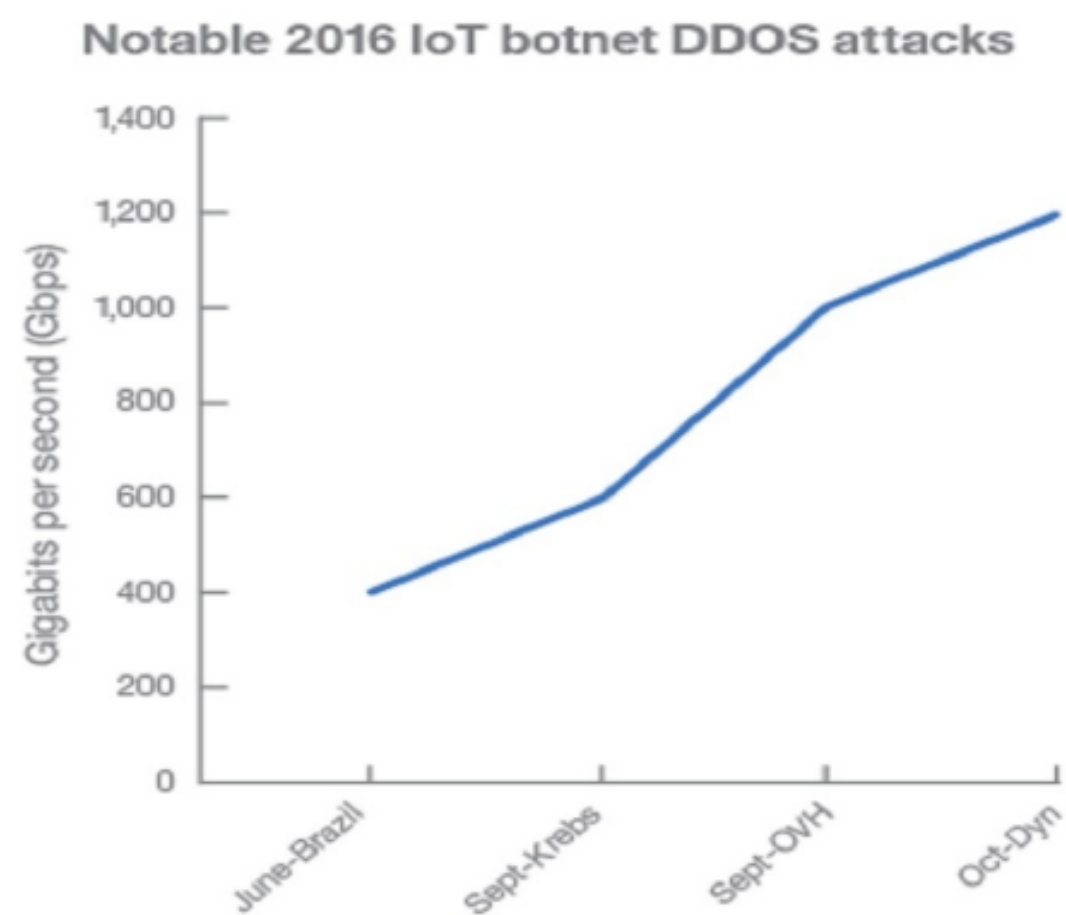


[source: <http://securityontology.sba-research.org/>]

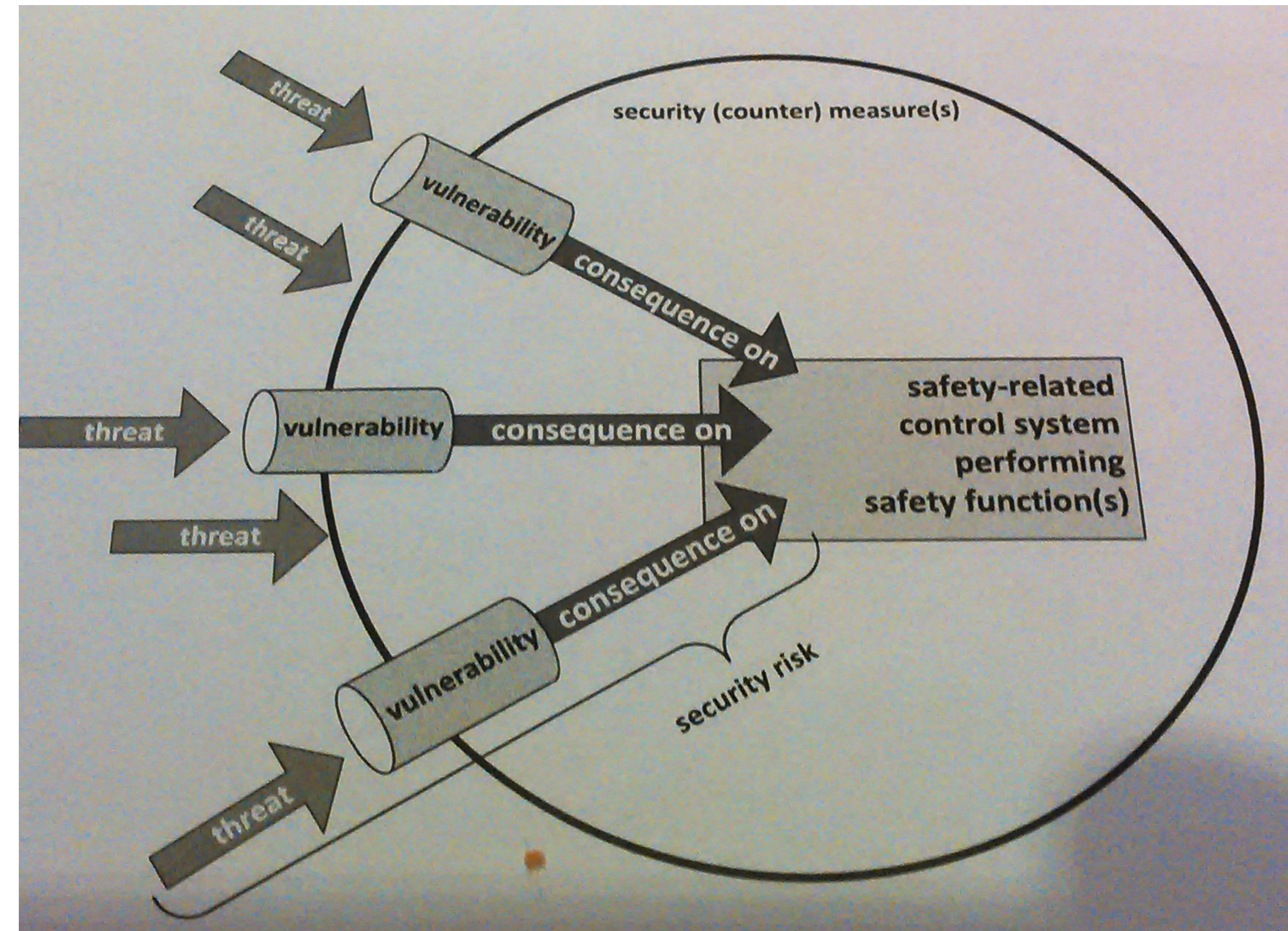


## Roadmap for a **more secure** and **privacy-aware** society

- “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



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

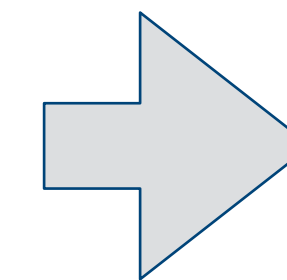
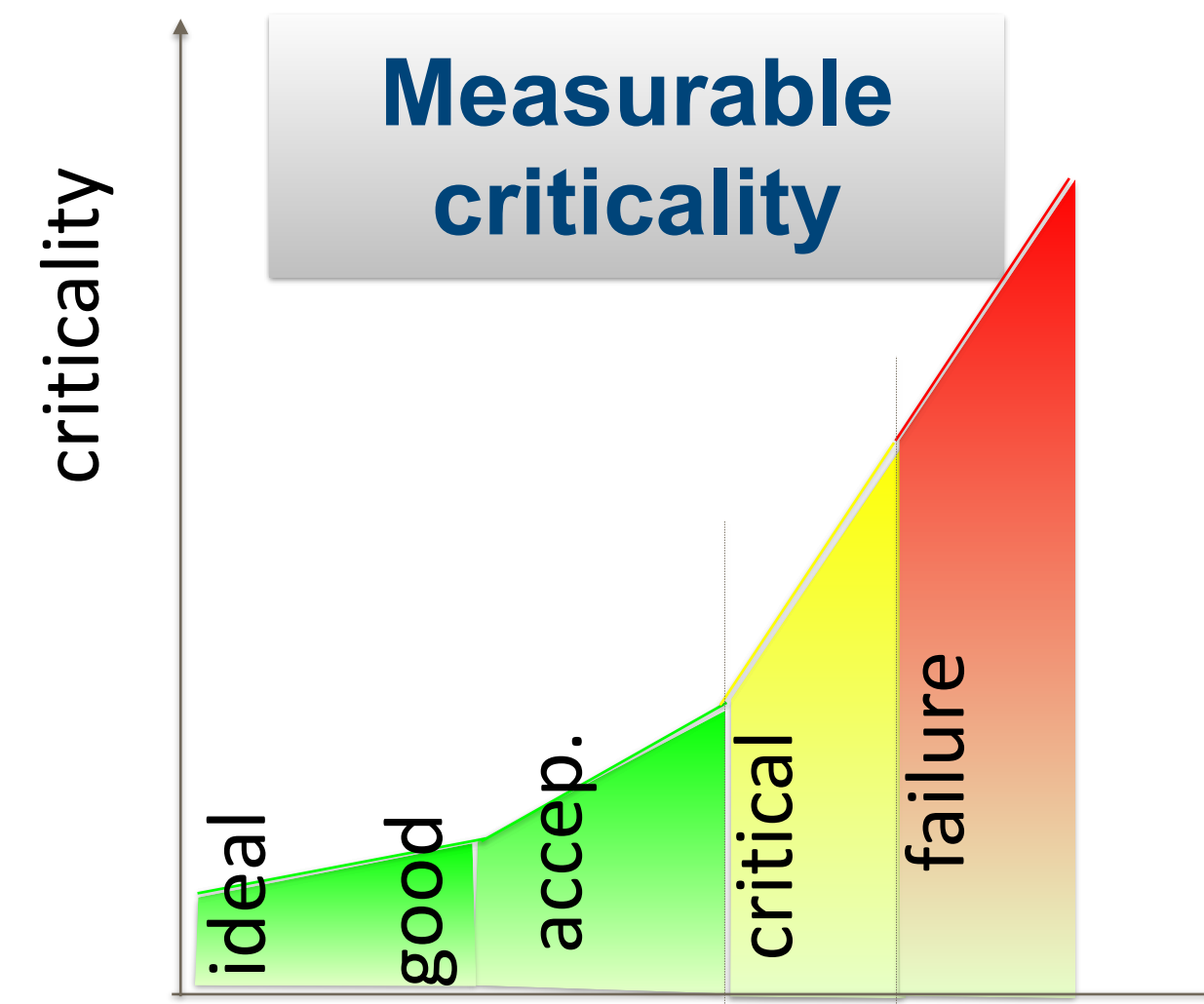
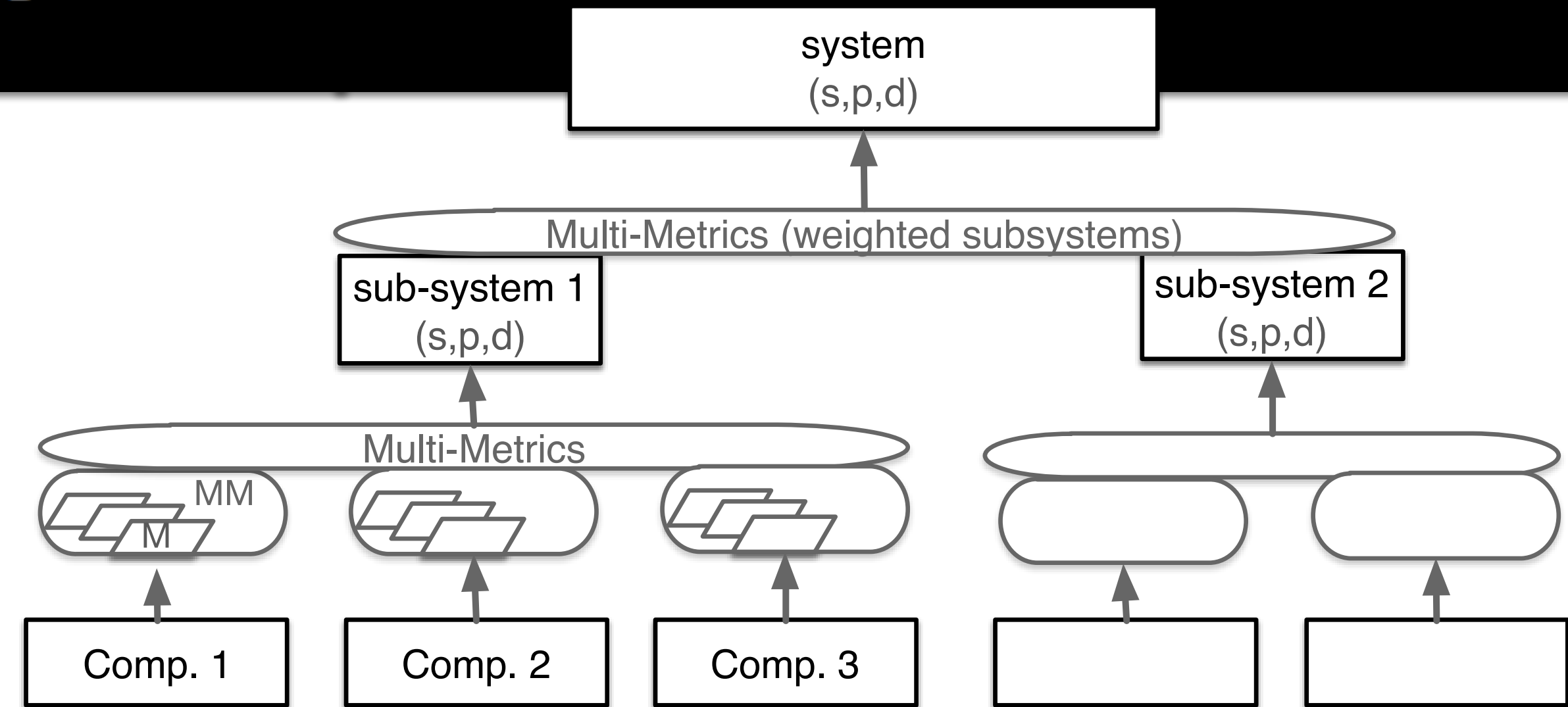


Thanks to our  
colleagues  
from SHIELD  
for the  
collaboration

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

## Accountable security

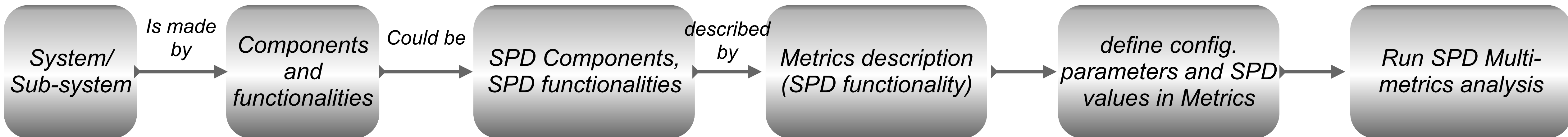
- Assessment
  - Comparison desired Class vs Calculated class
- Modelling
  - SPD Metrics, from criticality to SPD value
- Framework
  - Examples of applicability
- Measurable Security
  - Security is not 0/1



to measurable:  
security,  
privacy and  
dependability

SPD level	SPD vs SPD <sub>Goal</sub>
(67,61,47)	(●,●,●)
(67,61,47)	(●,●,●)
(31,33,63)	(●,●,●)

## Methodology: From System description to SPD level

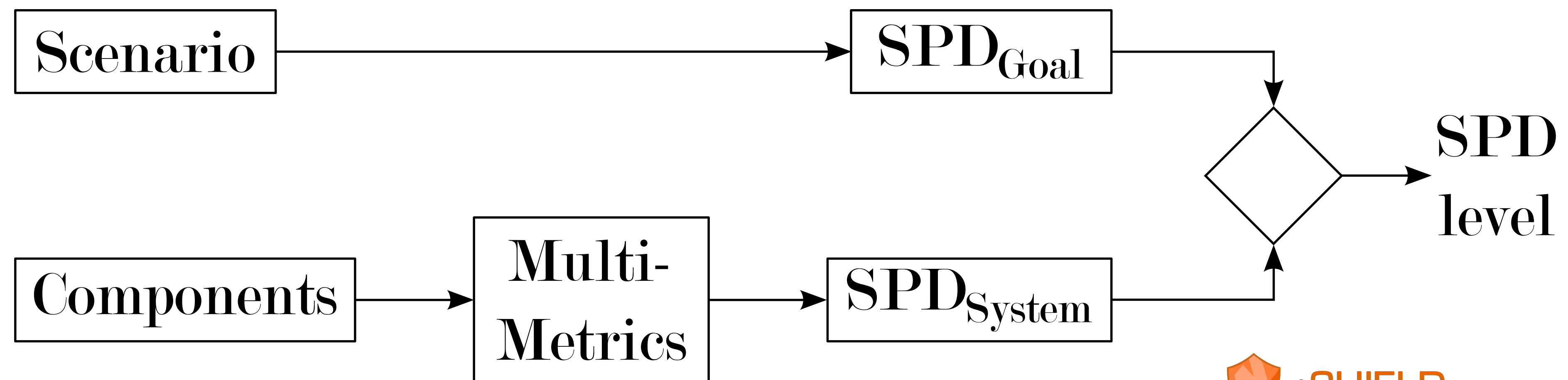


- System: Automatic Meter System (AMS) consists of reader (AMR), aggregator, communications, storage, user access
- Sub-systems: AMR consists of power monitor, processing unit, communication unit
- Component: AMR communication contains of a baseband processing, antenna, wireless link
- Configuration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



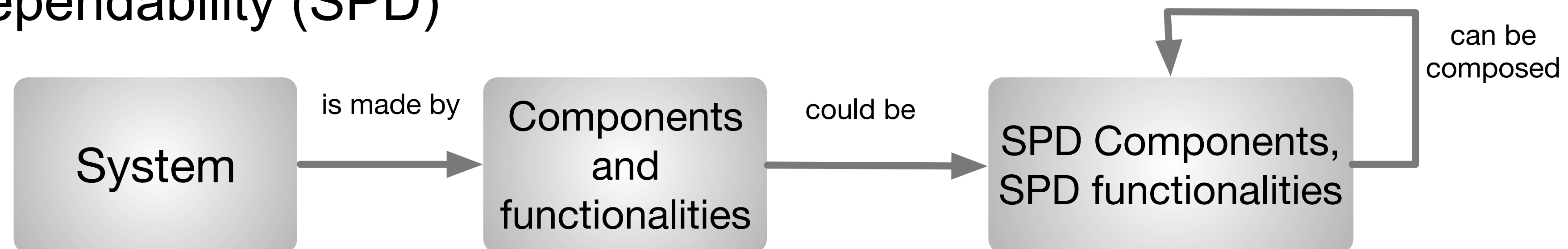
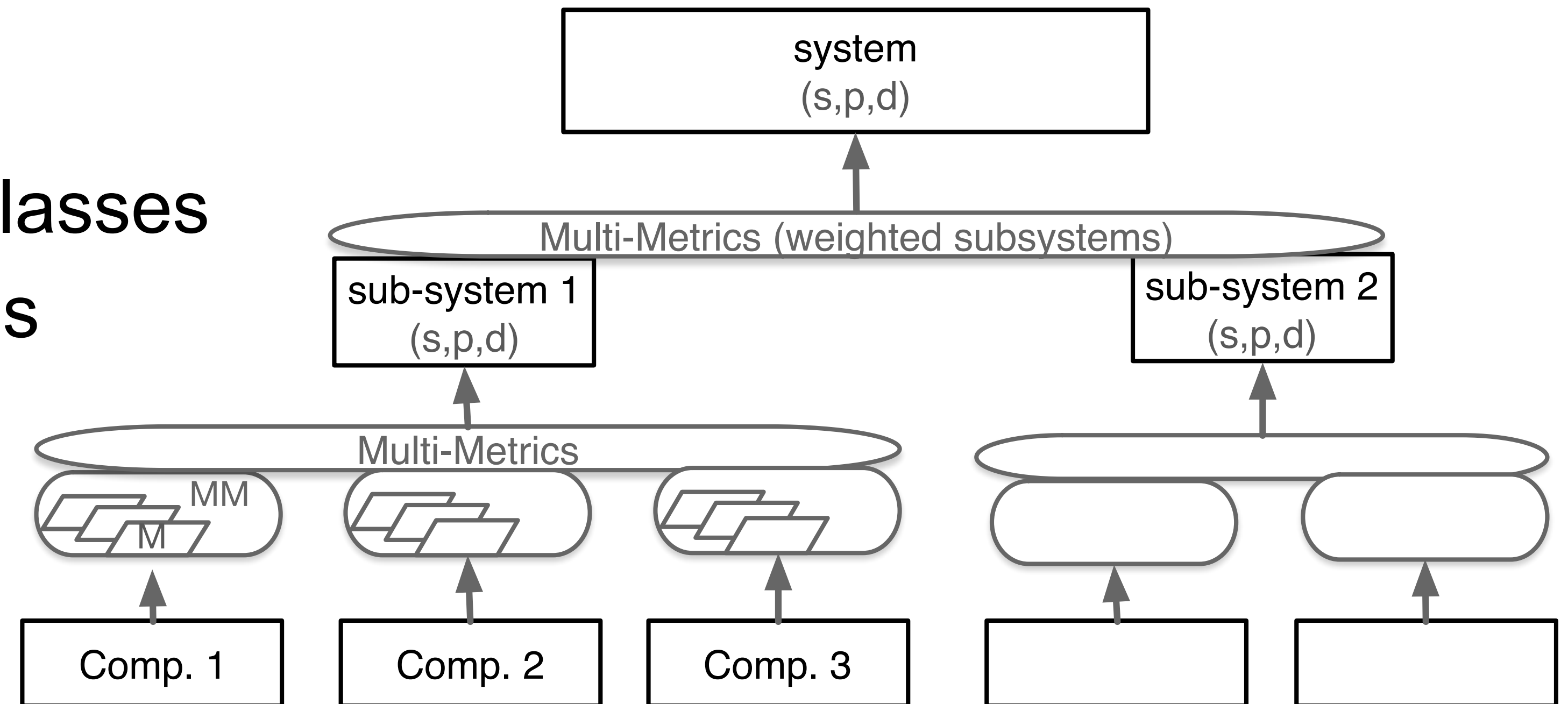
## Measurable Security, Privacy, Dependability (SPD)

- Focus on «entry the industrial market»
- Industry «needs security» - with entry models
- System Security, Privacy and Dependability is assessed
  - ➔ Application  $SPD_{Goal}$
  - ➔  $SPD_{System}$  assessment
  - ➔ 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



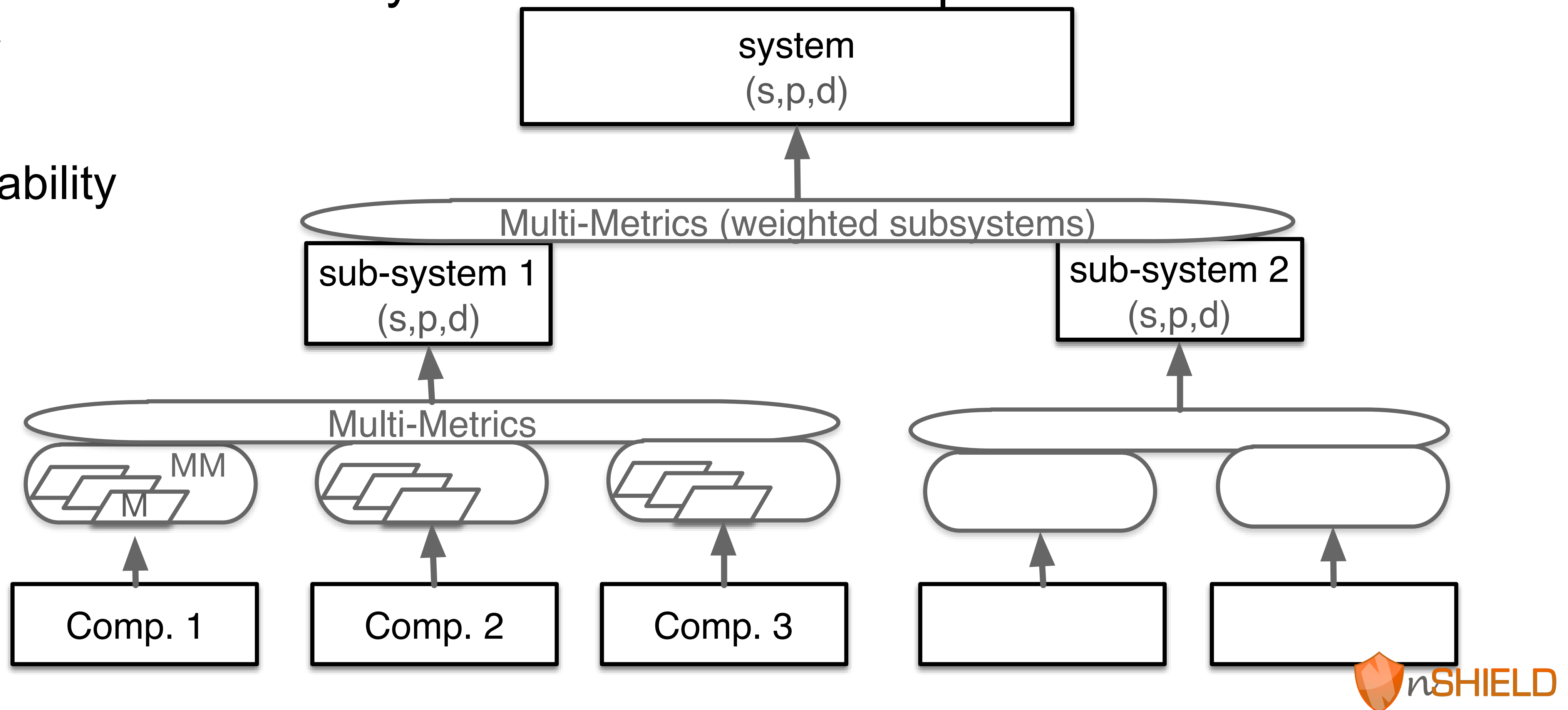
# Multi-Metrics - system composition

- System consists of sub-systems consists of components

→ security

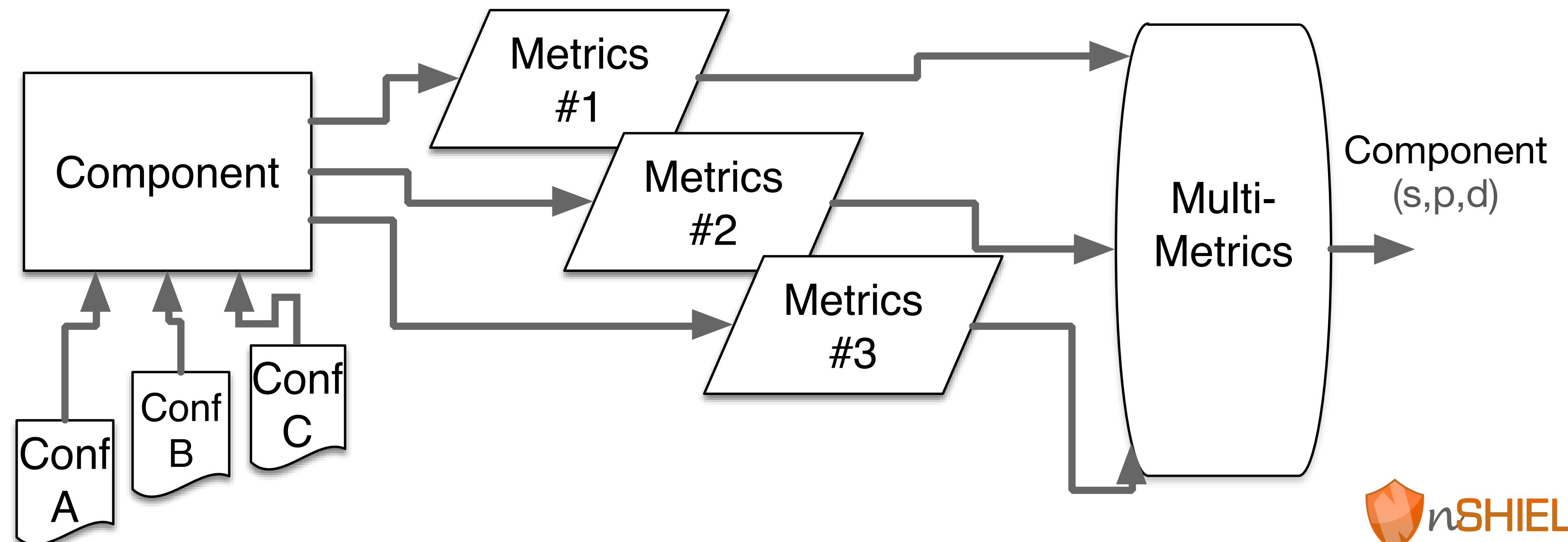
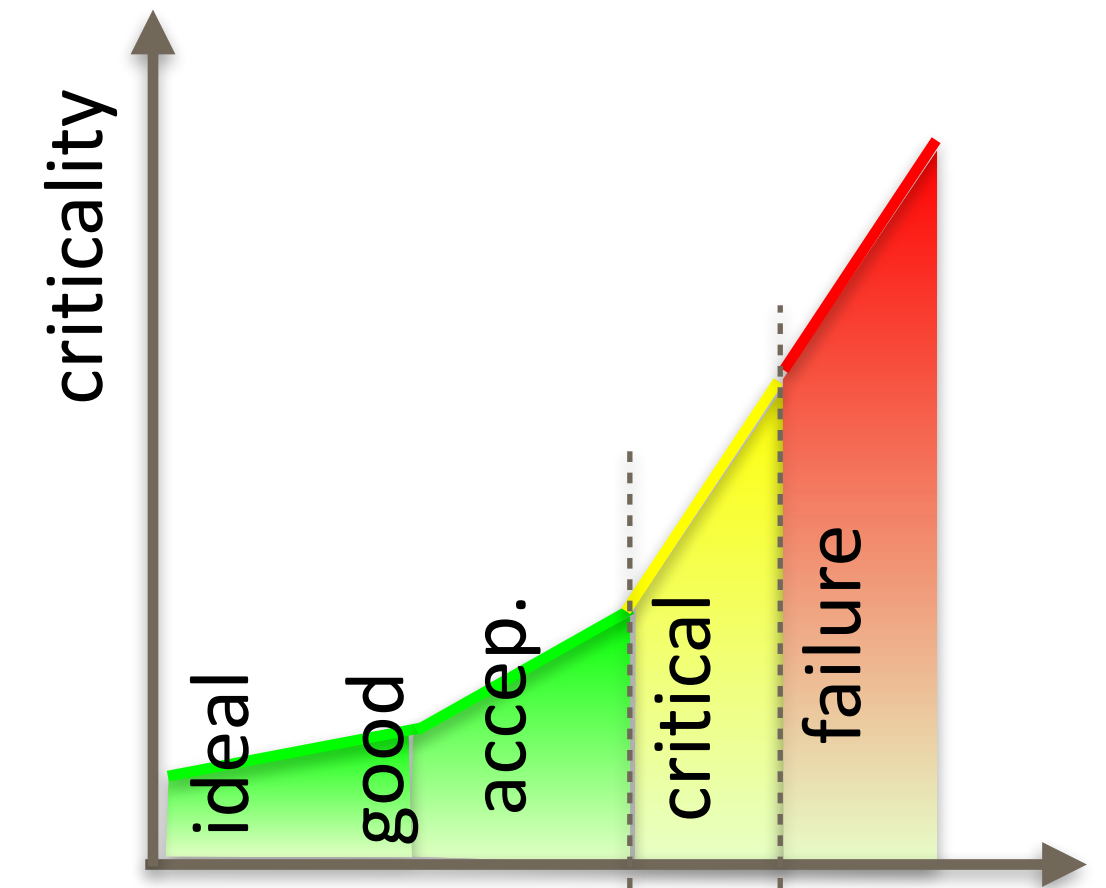
→ privacy

→ dependability



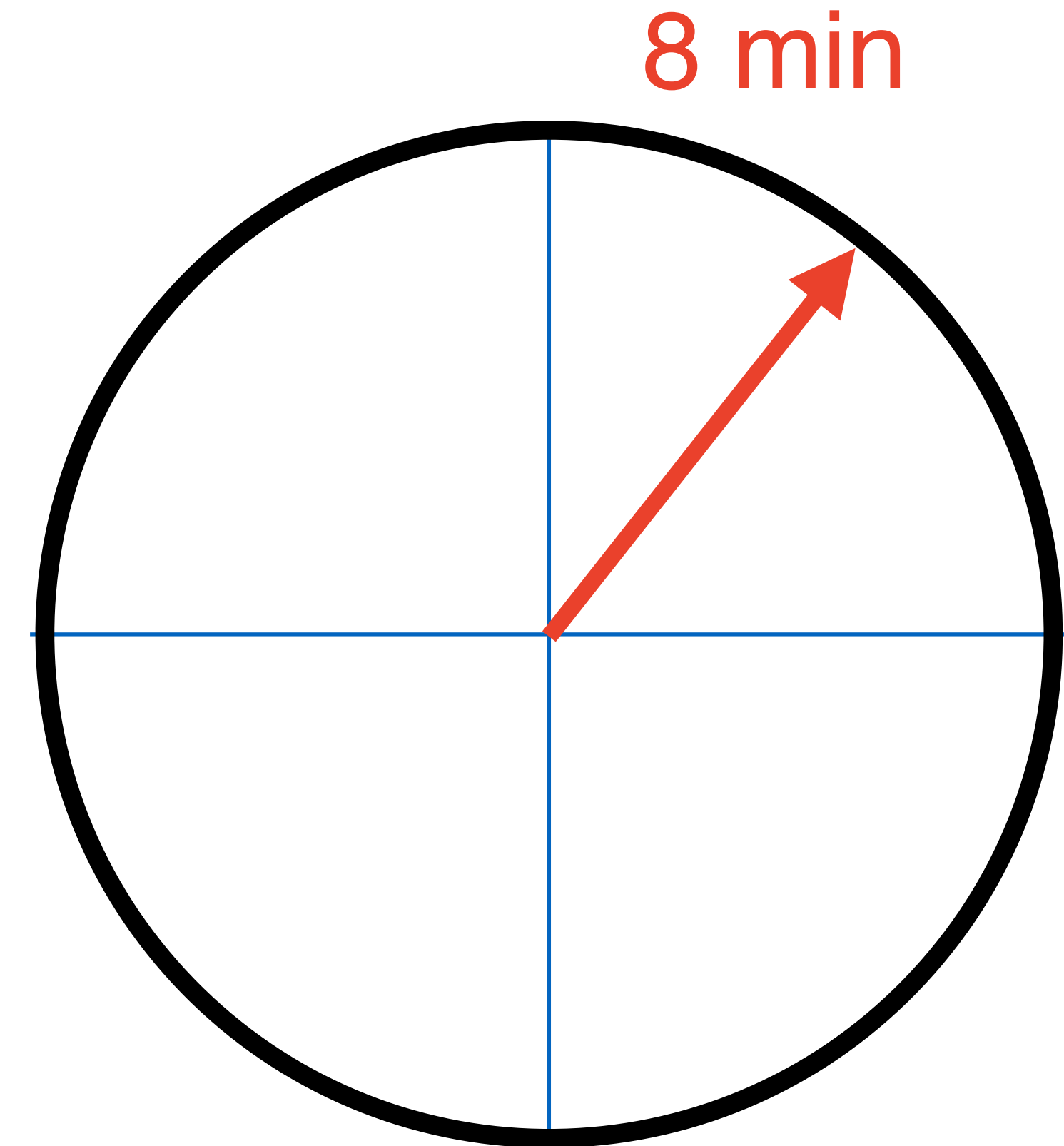
## Multi-Metrics components

- Components have a security, privacy and dependability factor.
- Metrics assess the components

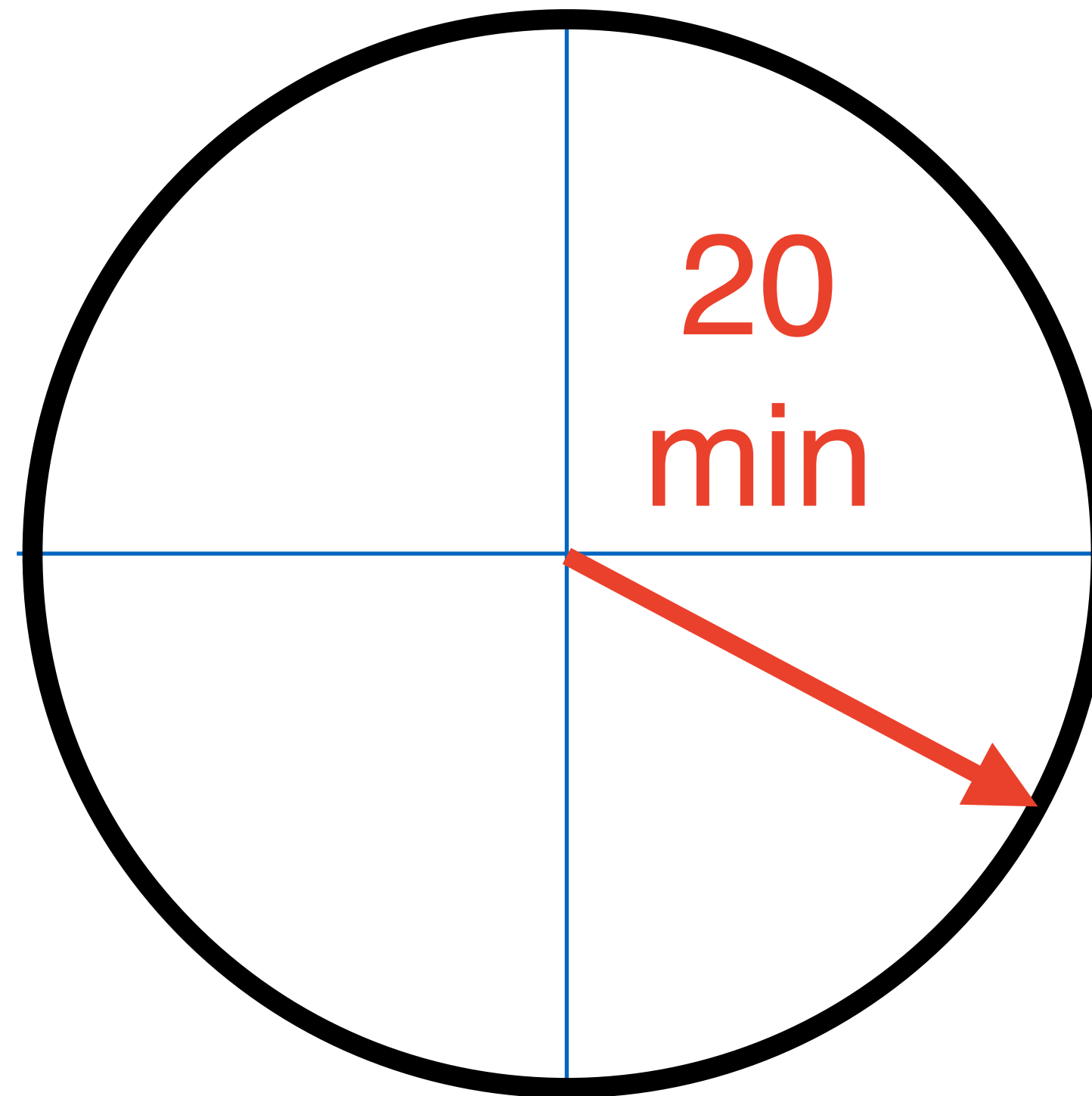


## Measurable security - discuss (8 min)

- ◉ A system of systems consists of ....
- ◉ SPD stands for ....
- ◉ SPD is accounted through
  - ➔ SPD functionality - provide 3-5 examples
  - ➔ SPD attributes - provide 3 examples



## Break - 20 min



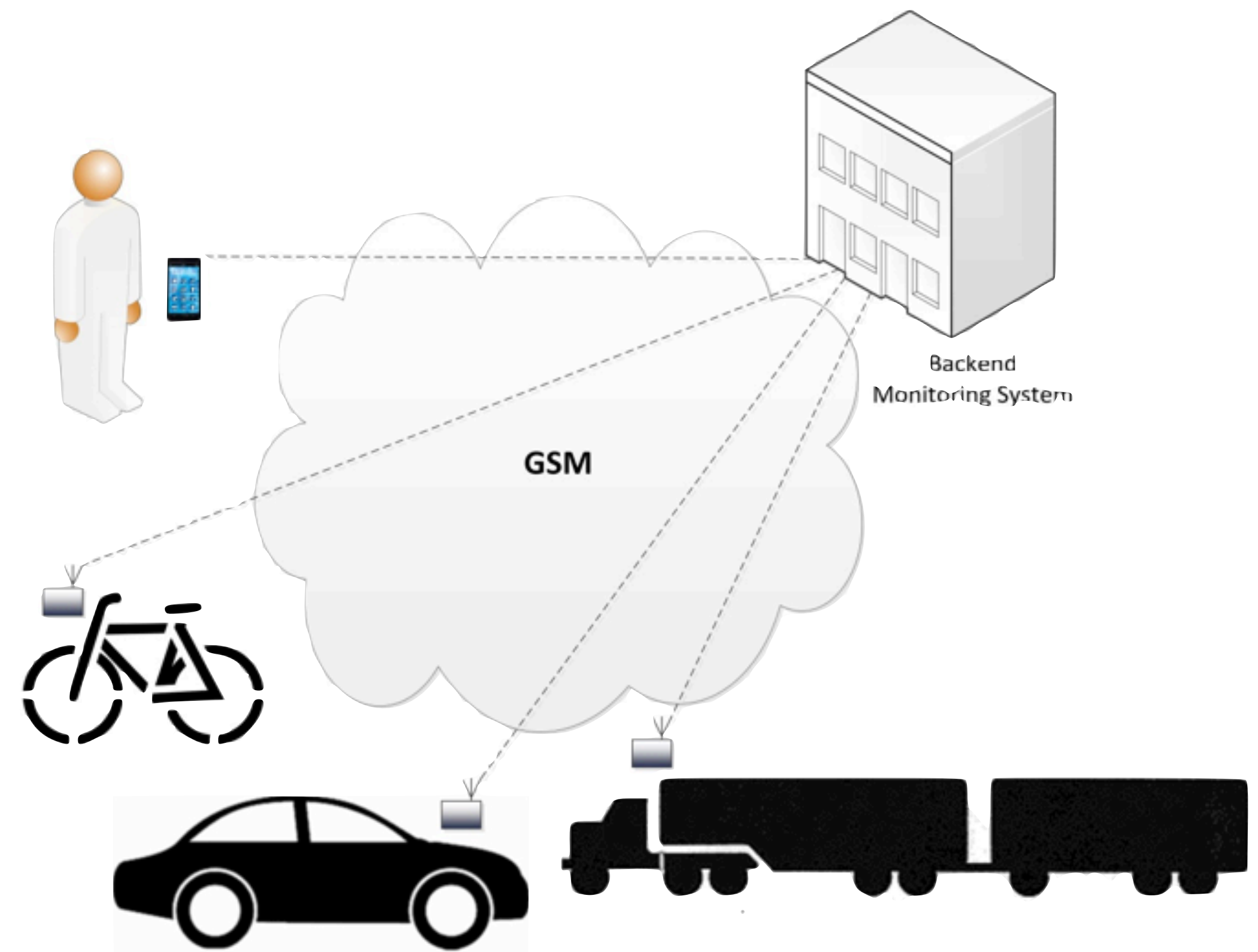
# Walk - through

## Measurable SPD for Personal Mobility



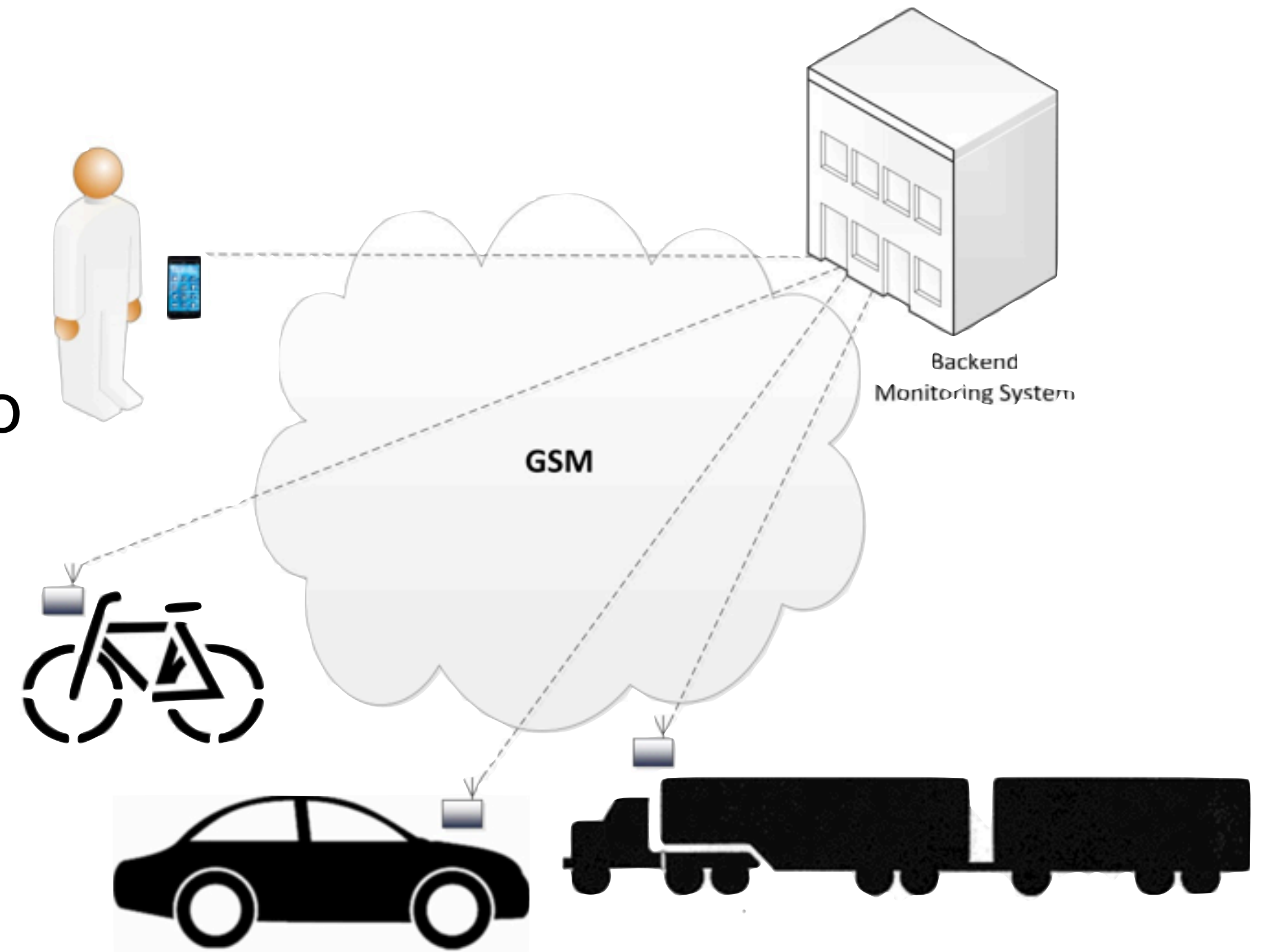
## Example: Privacy in a Social Mobility Use Case

- Social Mobility, including social networks, here: loan of vehicle
- Shall I monitor the user?



## 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

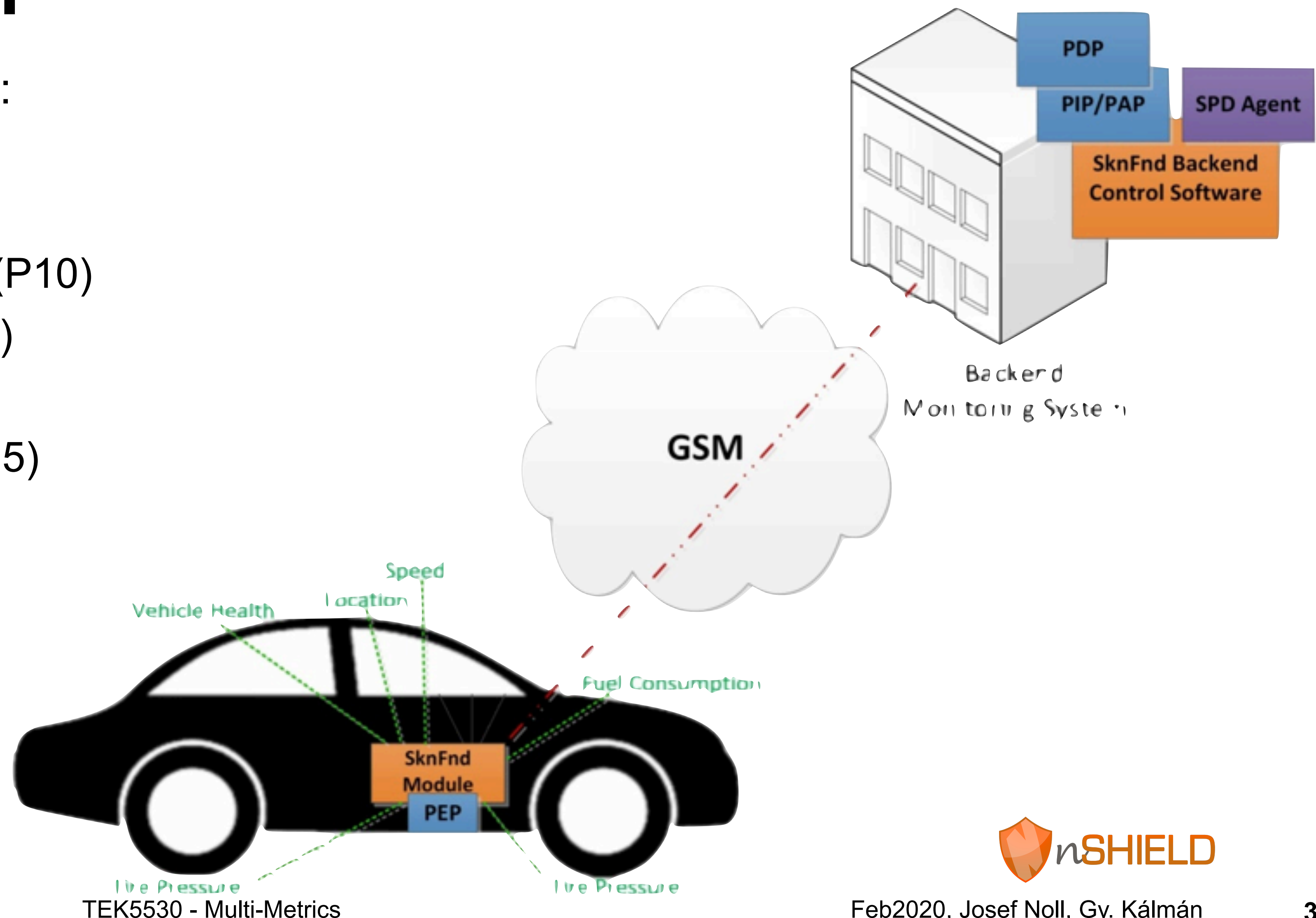


- Industrial applicability: Truck operation (Volvo), Autonomous operations on building places, add sensors (eye control)

## Social Mobility Components

SHIELD Components (Px) addressed:

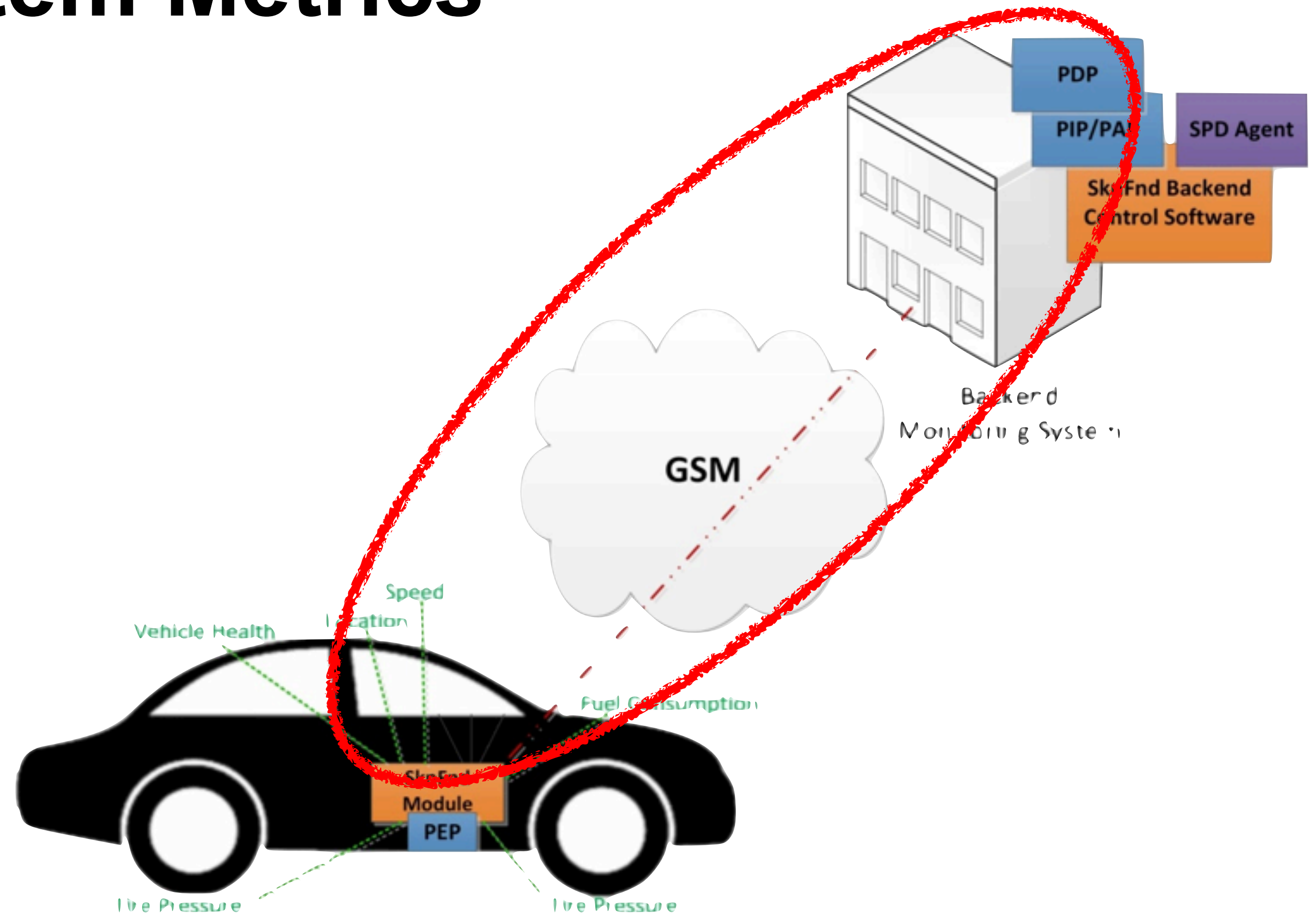
- 1- Lightweight Cyphering (P1)
- 2- Key exchange (P2)
- 3- Anonymity & Location Privacy (P10)
- 4- Automatic Access Control (P11)
- 5- Recognizing DoS Attack (P13)
- 6- Intrusion Detection System (P15)
- 7- Attack surface metrics (P28)
- 8- Embedded SIM, sensor (P38)
- 9- Multimetrics (P27)



## Communication Subsystem Metrics

### (SPD) Metrics

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



## Metrics & weight (only privacy)

1) Port metric, weight  $w_p=40$

	$C_p$	$SPD_p$
SNMP (UDP) 161 in the ES	40	60
SNMP trap (UDP) 162 in the BE	60	40
SSH (TCP) 23 in the ES	30	70
SMS	80	20

2) Communication channel metric, weight  $w_p=20$

	$C_p$	$SPD_p$
<i>GPRS with GEA/3</i>	20	80
<i>SMS over GSM with A5/1</i>	40	60

4) SMS message rate metric  $w_p=20$   
0,1, or 2 messages  $SPD_p=90-100$

5) Encryption metric  $w_p=60$

	$C_p$	$SPD_p$
<i>No encryption</i>	88	12
<i>Key 64 bits</i>	10	90
<i>Key 128 bits</i>	5	95
<i>Not applicable</i>	0	100

3) GPRS message rate metric  $w_p=80$

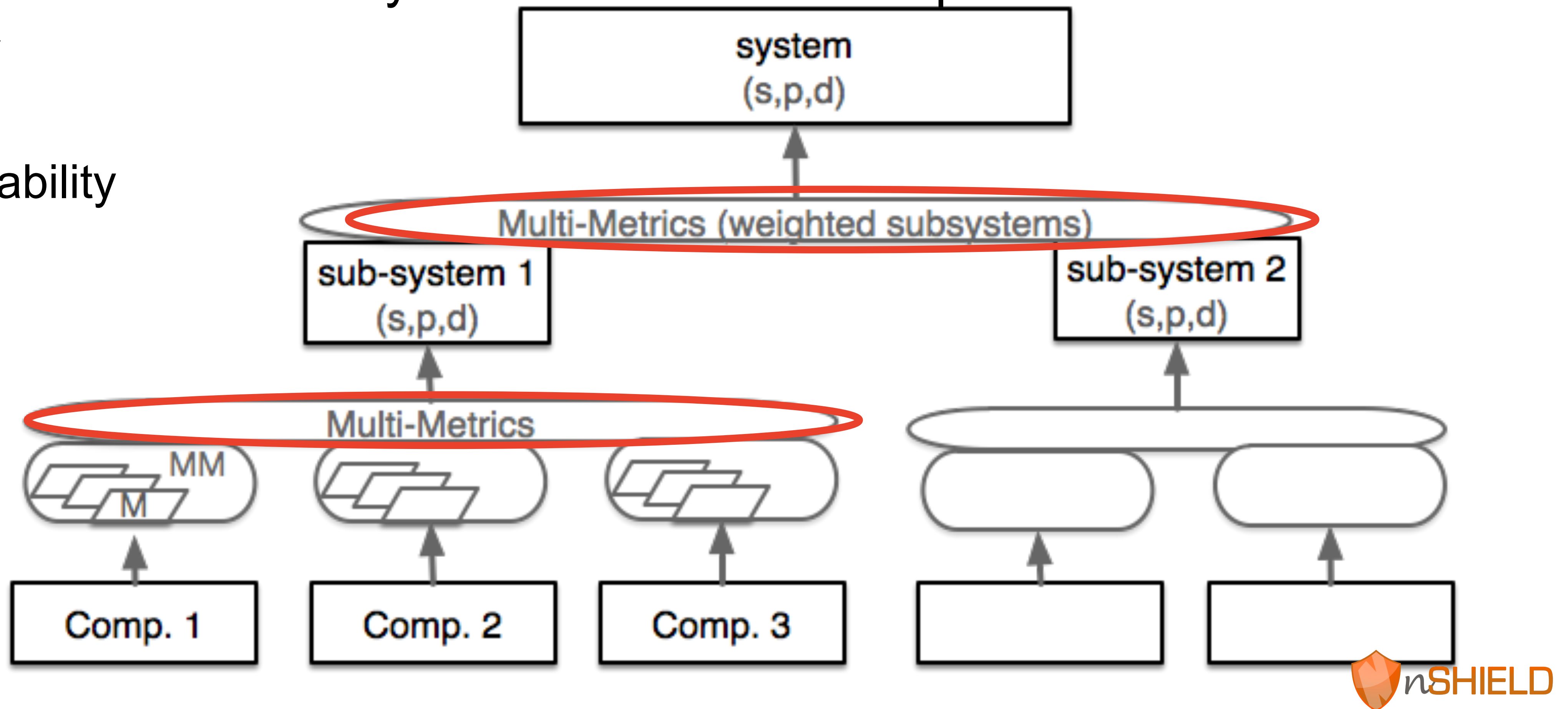
<i>message delay</i>	$C_p$	$SPD_p$
<i>0.5 sec</i>	80	20
<i>1 sec</i>	60	40
<i>2 sec</i>	45	65
<i>5 sec</i>	30	70
<i>10 sec</i>	20	80
<i>20 sec</i>	15	85
<i>60 sec</i>	10	90
<i>120 sec</i>	5	95
<i>No messages</i>	0	100



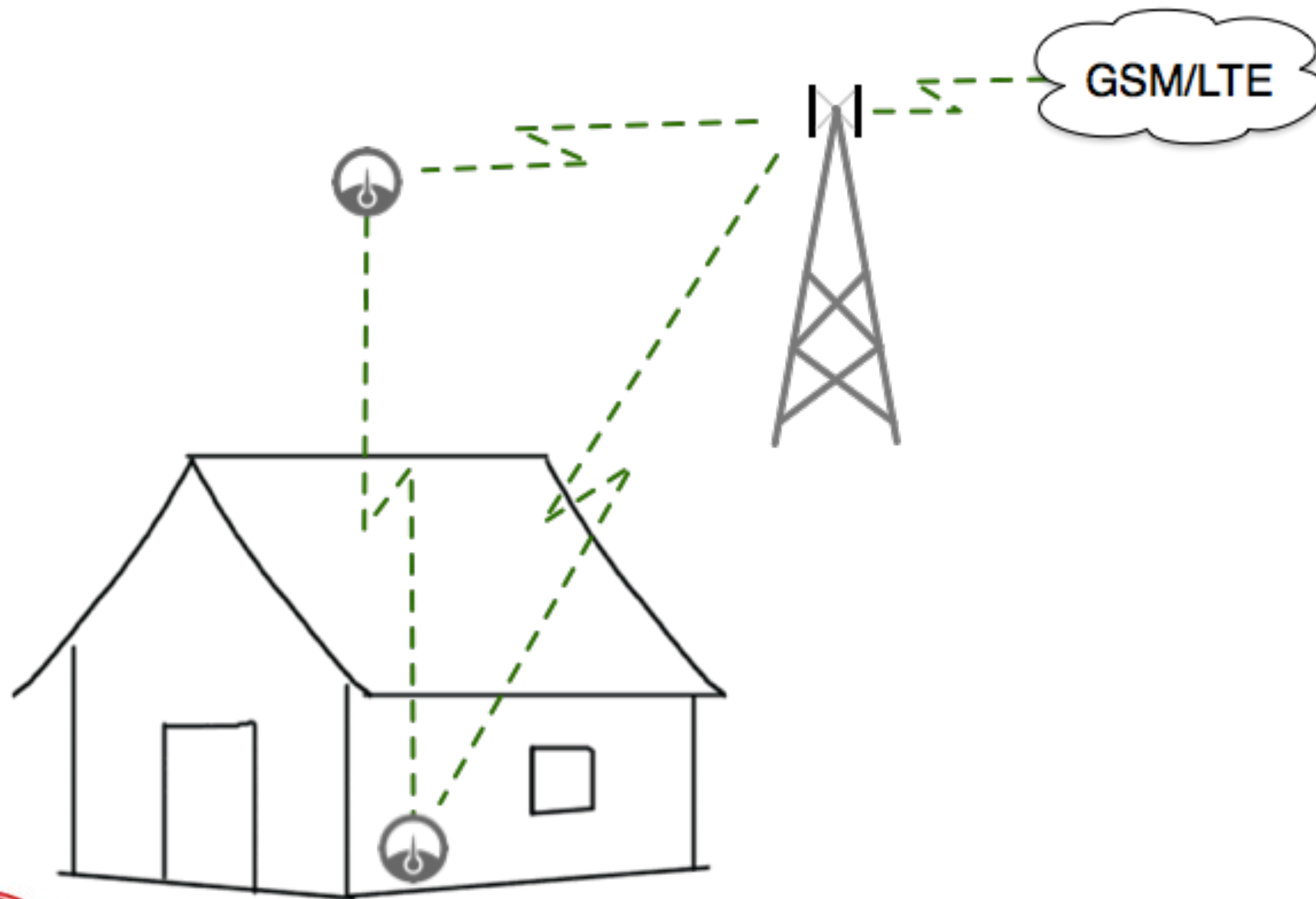
## Multi-Metrics<sub>v2</sub> - system composition

- System consists of sub-systems consists of components

- security
- privacy
- dependability



## Why weighting of sub-systems?



### 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 <sub>P</sub>			
	C1	C2	C3	C4	Sub-Sys.		Scen. 1	Scen. 2	Scen. 3
SPD <sub>Goal</sub>							(s,80,d)	(s,50,d)	(s,5,d)
Multi-Metrics Elements	M1	M2	M3 ∩ M4	M5	C1... ∩ ...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	●	●	●



## Privacy Scenarios - *to trigger your ideas*

- Loan of the car (normal operation, speeding, accident)
- The home medical equipment
  - ➔ Transmitting the data
  - ➔ Applications storing and handling the data
- Networked cameras and microphones
  - ➔ Privacy of persons captured
  - ➔ Who can access the data
- ➔ What kind of operations can be performed on the data
- Speaking & listening doll
  - ➔ Microphone recording everything in the room (children playing, grown-ups discussing)
- FitBit & Smart Watches
  - ➔ sleeping cycle
  - ➔ puls, fitness
- *your take ....*

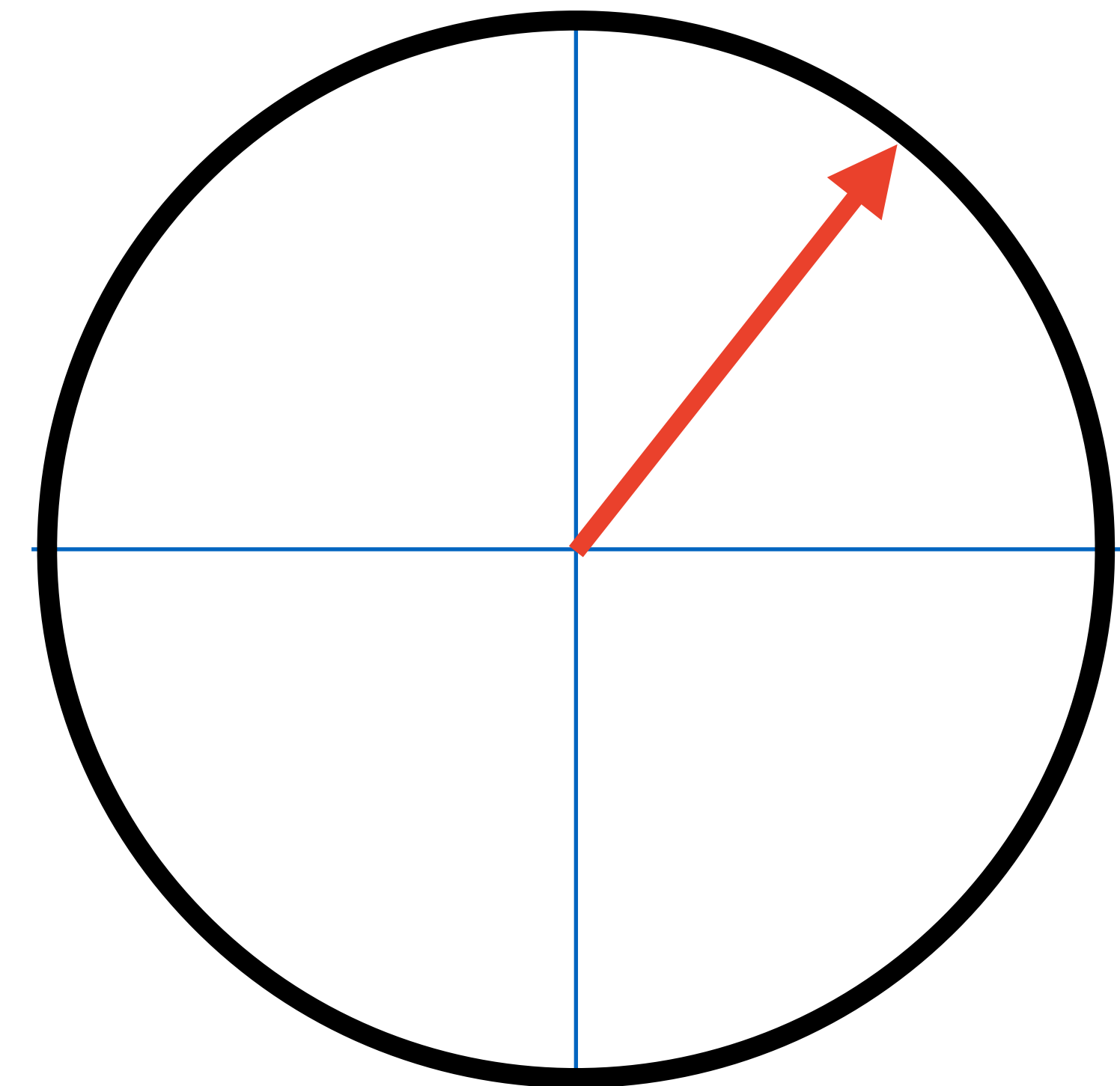


*thanks to Elahe Fazelkohrdi*

## Privacy-specific parameters - (discuss 8 min)

- Please discuss with your neighbours
  - ➔ a) other scenarios
  - ➔ b) what are the important privacy parameters
- Examples of privacy parameters
  - ➔ 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

8 min



# Run-Through Example

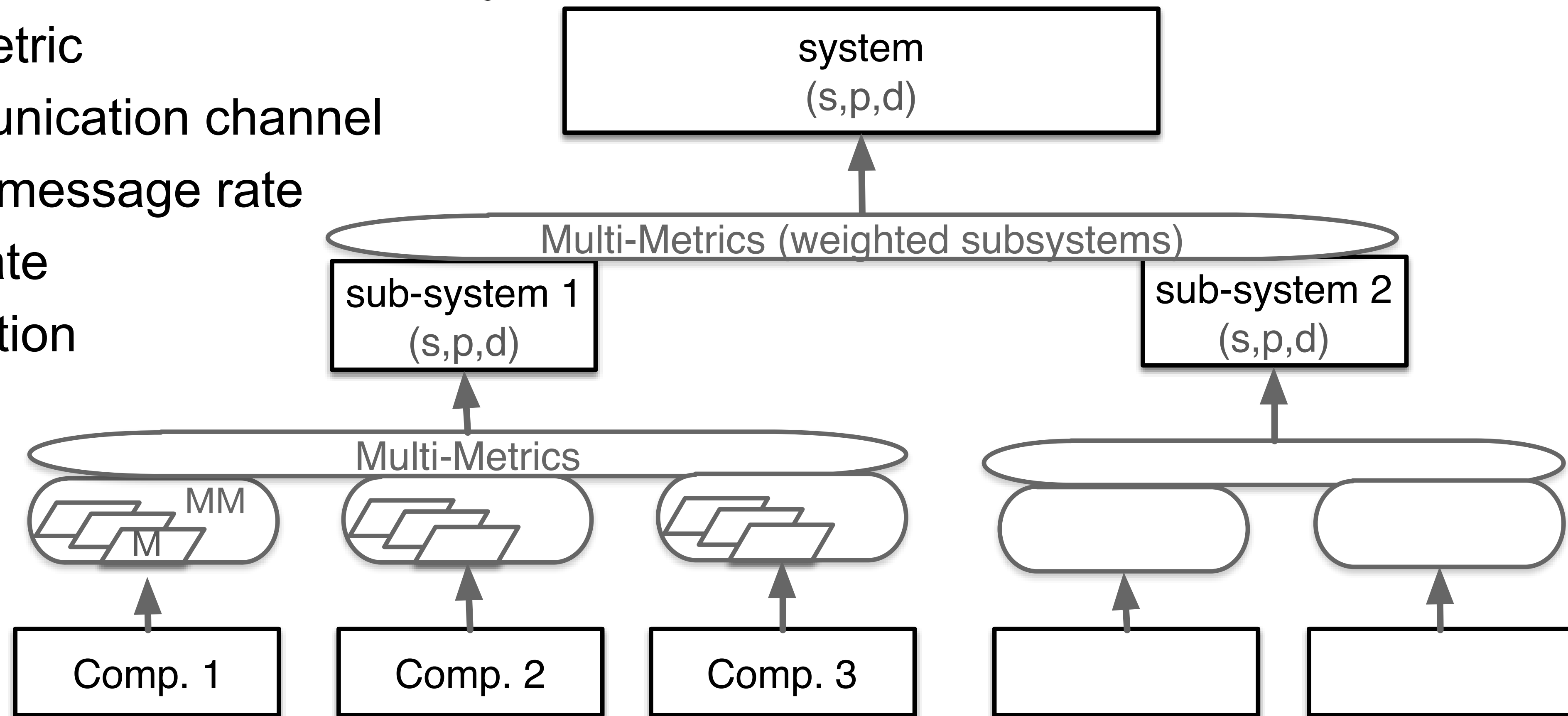
- Car loan, privacy considerations



# Multi-Metrics<sub>v2</sub> - system composition

- here: communication sub-system vehicle  $\leftrightarrow$  backend

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



## Social Mobility Configuration

- Conf. A: The ES does not send any SMS; GPRS data are encrypted with 128 bits key. The ES accepts remote configuration from the BE.
- Conf. B: same as above, except ES sends a keep alive message to the BE every 120 seconds.
- Conf. C: same as above, except BE sends messages to the ES and the last one replies every 60 seconds.
- Conf. D: The ES sends an SMS to parents; GPRS data to the BE are encrypted with 64 bits key. ES accepts remote configuration from the BE.
- Conf. E: same as above, except ES sends location and speed information to the BE every 10 seconds.
- Conf. F: same as above, except BE sends messages to the ES and the last one replies with location and speed information every 5 seconds.
- Conf. G: ES sends one SMS to parents, another to emergency services. Unencrypted data about the status of the MC are sent from the ES to the BE. ES accepts remote configuration from BE.
- Conf. H: same as above, except ES sends location and speed information to the BE every 2 seconds.
- Conf. I: same as above, except BE sends messages to the ES and the last one replies with location and speed information every 0.5 seconds.



## Metrics & weight (only privacy)

1) Port metric, weight  $w_p=40$

	$C_p$	$SPD_p$
SNMP (UDP) 161 in the ES	40	60
SNMP trap (UDP) 162 in the BE	60	40
SSH (TCP) 23 in the ES	30	70
SMS	80	20

2) Communication channel metric, weight  $w_p=20$

	$C_p$	$SPD_p$
<i>GPRS with GEA/3</i>	20	80
<i>SMS over GSM with A5/1</i>	40	60

4) SMS message rate metric  $w_p=20$   
0,1, or 2 messages  $SPD_p=90-100$

5) Encryption metric  $w_p=60$

	$C_p$	$SPD_p$
<i>No encryption</i>	88	12
<i>Key 64 bits</i>	10	90
<i>Key 128 bits</i>	5	95
<i>Not applicable</i>	0	100

3) GPRS message rate metric  $w_p=80$

<i>message delay</i>	$C_p$	$SPD_p$
<i>0.5 sec</i>	80	20
<i>1 sec</i>	60	40
<i>2 sec</i>	45	65
<i>5 sec</i>	30	70
<i>10 sec</i>	20	80
<i>20 sec</i>	15	85
<i>60 sec</i>	10	90
<i>120 sec</i>	5	95
<i>No messages</i>	0	100



## Metrics analysis

1. approach, using linear calculation  $X_i^2 * w_i / \text{SUM}(w_i)$

$30^2 * 40 / 155$

		Comp 1	Comp 2	Comp 3	Comp 4	Sum	$\text{SQRT}(\text{SUM})$ Cp	SPDp
Scenario 1 "privacy"	Conf. A	232	52	0	10	294	17	83
	Conf. B	960	52	4	10	1 025	32	68
	Conf. C	434	52	18	10	513	23	77
Scenario 2 "parents"	Conf. D	1 735	217	1	39	1 992	45	55
	Conf. E	1 735	217	73	39	2 064	45	55
	Conf. F	1 778	217	165	39	2 198	47	53
Scenario 3 "emergency"	Conf. G	1 735	228	4	2 998	4 964	70	30
	Conf. H	1 735	228	361	2 998	5 322	73	27
	Conf. I	1 778	228	1 171	2 998	6 174	79	21

sum of weight: 155



## Multi-Metrics subsystem evaluation

	Criticality					SPD <sub>P</sub>			
	C1	C2	C3	C4	Sub-Sys.		Scen. 1	Scen. 2	Scen. 3
SPD <sub>Goal</sub>							(s,80,d)	(s,50,d)	(s,5,d)
Multi-Metrics Elements	M1	M2	M3 ∩ M4	M5	C1... ∩ ...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	●	●	●



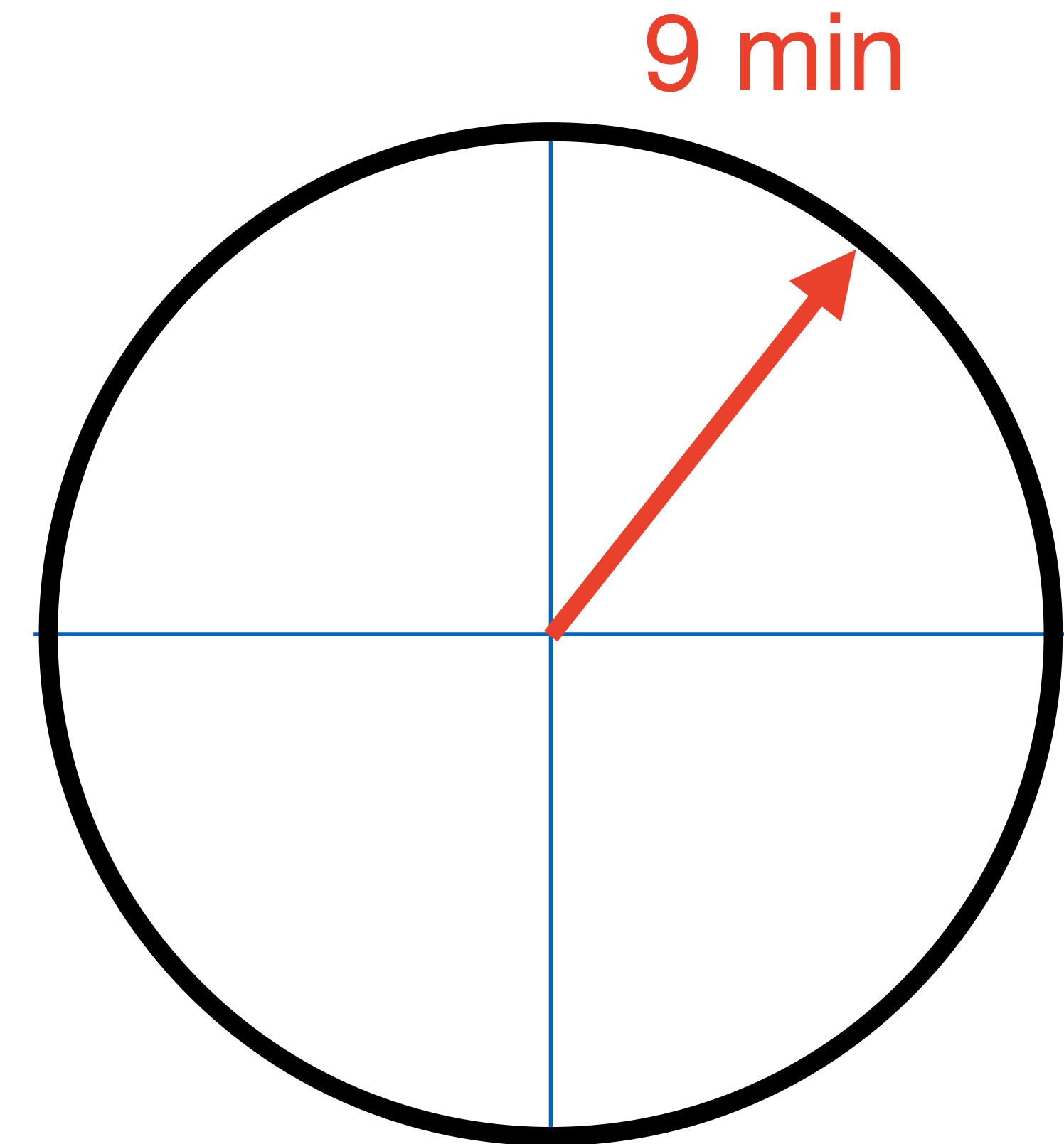
## Conclusions

- SHIELD is the security methodology developed through JU Artemis/ECSEL
- Security, Privacy, and Dependability (SPD) assessment
- Social Mobility Use-Case: loan a car
  - ➔ «behave» - full privacy awareness ->  $SPD_{goal} = (s, 80, d)$
  - ➔ «speeding» - limited privacy ->  $SPD_{goal} = (s, 50, d)$
  - ➔ «accident» - no privacy ->  $SPD_{goal} = (s, 5, d)$
- 11 configurations assessed
  - ➔ 2 satisfy «behave», 3 satisfy «speeding», 0 satisfies «accident»
- Goal: apply SHIELD methodology in various industrial domains



## Multi-metrics - (discuss 9 min)

- What is the outcome of a Multi-Metrics analysis?
- What determines the SPD\_Goal?
- Why do I need different configurations of my system?



## Run-Through Example

# Smart Meters - Use Cases

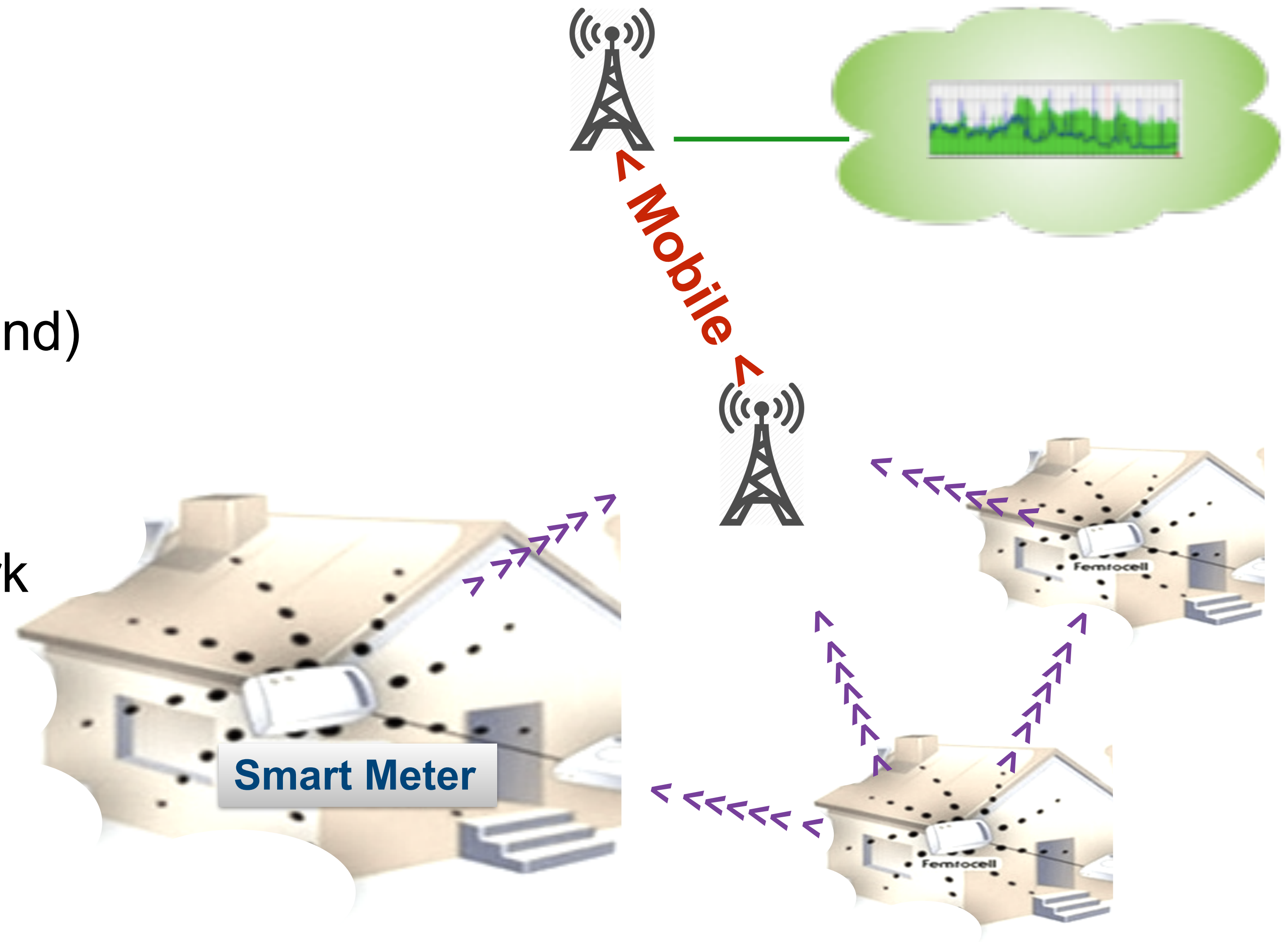


## Current Infrastructure

- Smart Meter (customer home)
  - connected via mesh or directly
  - proprietary solution (800 MHz band)
- Collector
  - collects measures
  - communicates via mobile network
- Mobile Network
  - as a transmission network
- Cloud (Provider)

entry point for remote access

Application platform



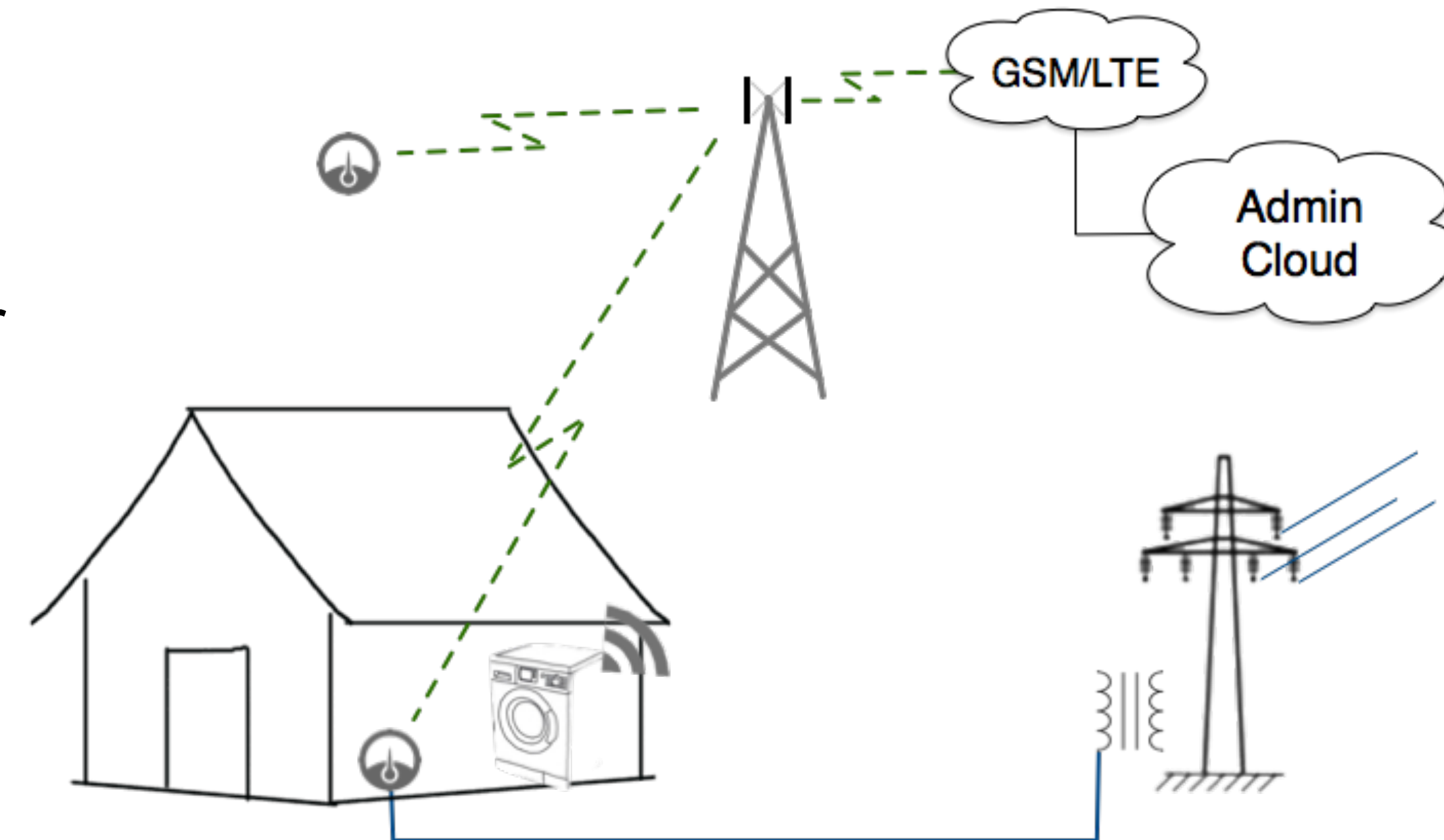
[source: [seminaronly.com](http://seminaronly.com)]



## Application Scenarios for Smart Meters

- ➔ Monitoring the grid to achieve a grid stability of at least 99,96%,
- ➔ Alarm functionality, addressing
  - failure of components in the grid,
  - alarms related to the Smart Home, e.g. burglary, fire, or water leakage,
- Intrusion detection, monitoring both hacking attempts to the home as well as the control center and any entity in between,
- Billing functionality, providing at least the total consumption every hour, or even providing information such as max usage,
- Remote home control, interacting with e.g. the heating system
- Fault tolerance and failure recovery, providing a quick recovery from a failure.
- Future services

Monitoring of activity at home, e.g. “virtual fall sensor”



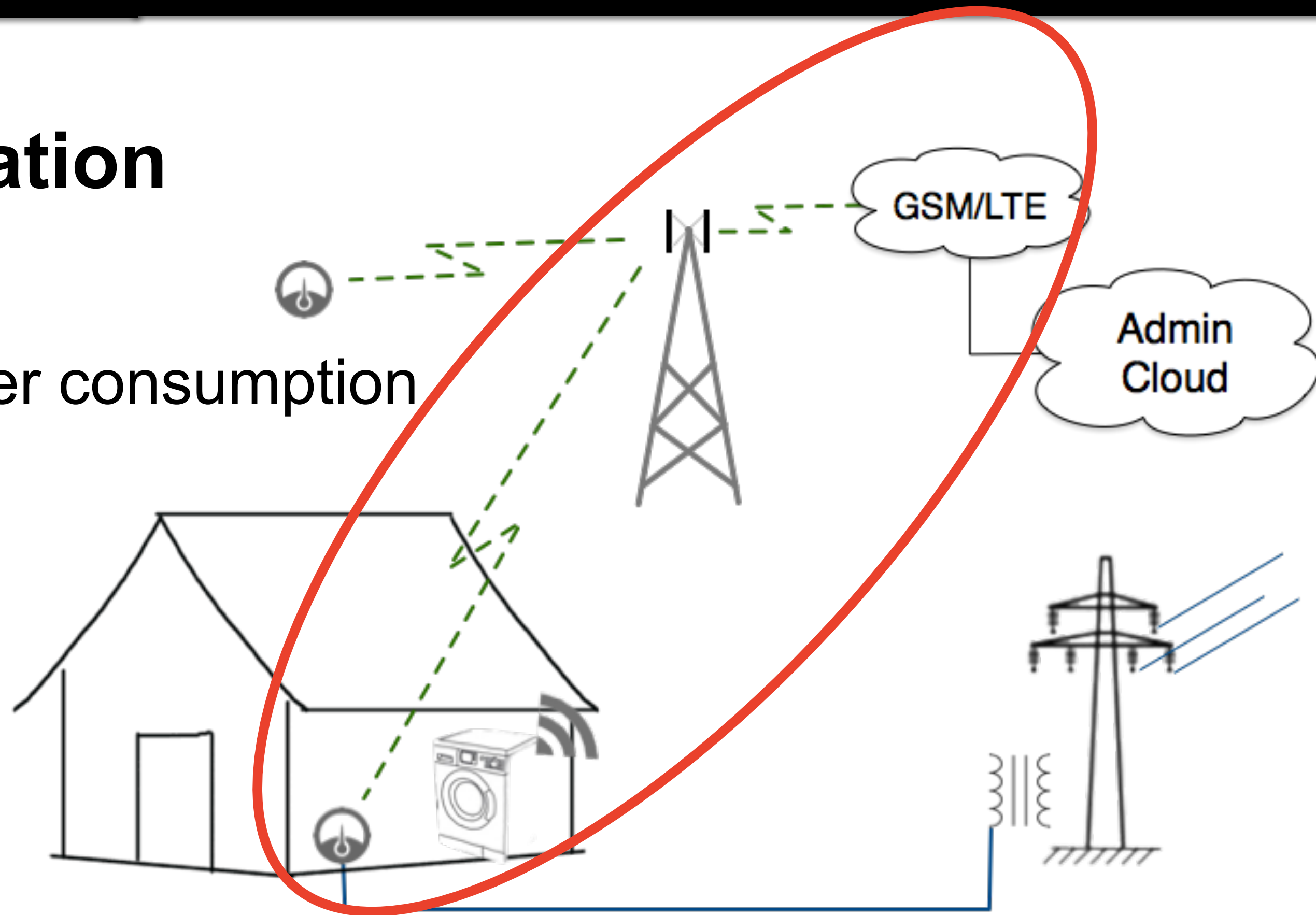
## Privacy measuring in Smart Grids and Energy metering

- Advanced Metering Infrastructures (AMI) and Smart Meters
- There are many Privacy Concerns around these:
  - How much Private information can be extracted from this data ?
  - How well is this data anonymized ?
  - How well can we measure the privacy implications of such Smart Systems ?



## Sub-system analysis Here: Smart Meter with Communication

- the Automatic Meter Reader (AMR)
  - AMR to measure, sense and control power consumption
- the Mesh radio link
  - direct communication to concentrator
  - or multi-hop through other AMR
- the Mobile link sub-systems
  - from collector to mobile operator
  - typical 2G/3G/4G data, or SMS

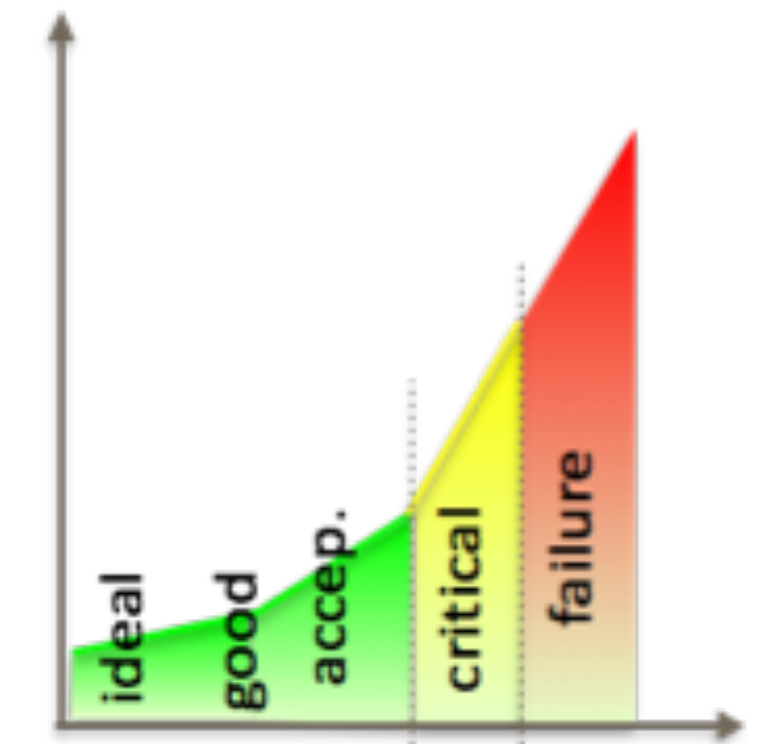
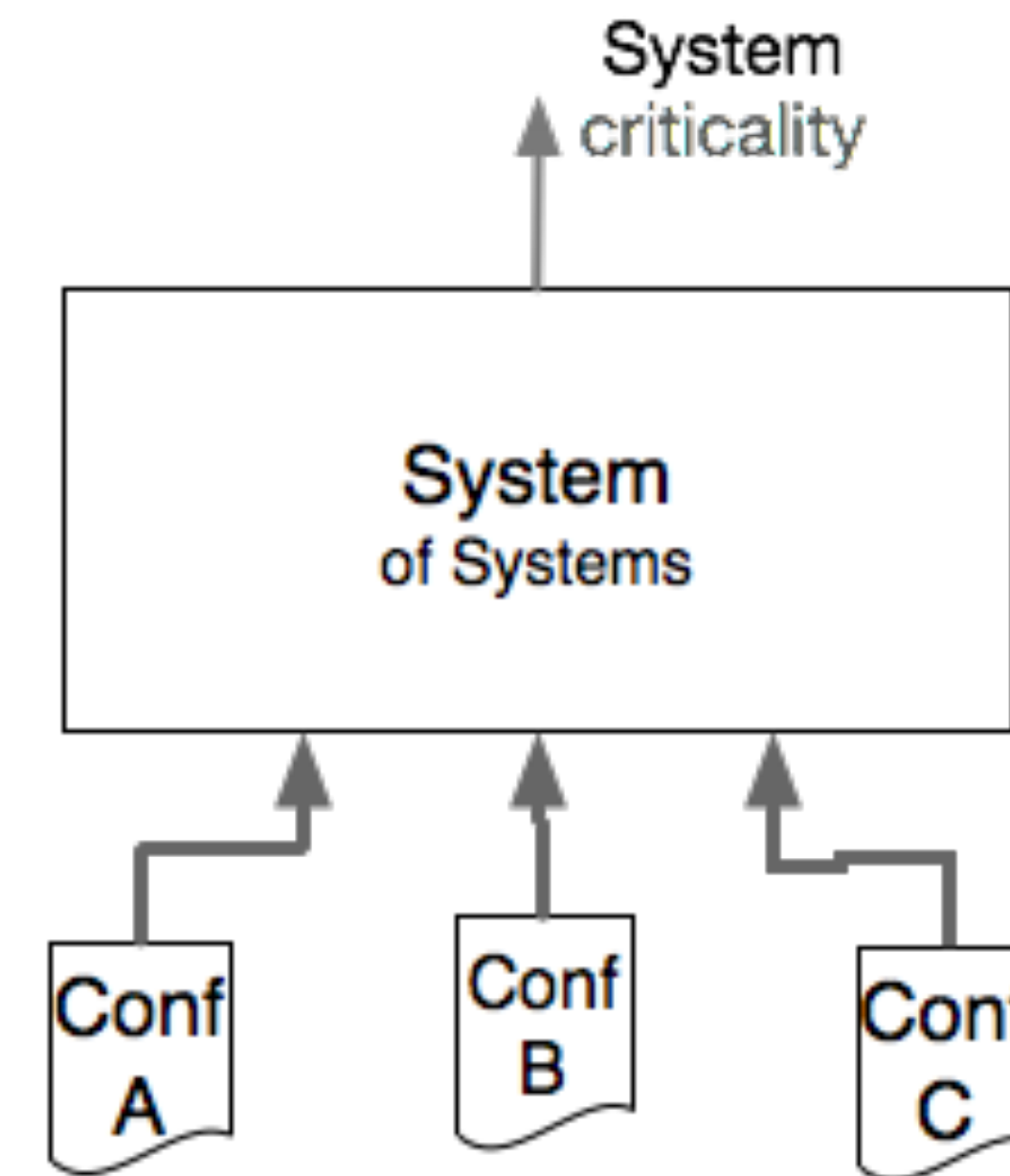


## Sub-system analysis Metrics for AMR

→ the Automatic Meter Reader (AMR)

- (1) remote access metric - (yes/no)
  - reading, or just controlling
- (2) authentication metric
  - everyone, or authenticated user
- (3) encryption metric (on, off)

$$(\bar{C}s, \bar{C}p, \bar{C}d) = (100, 100, 100) - (s, p, d).$$



### (1) remote access

Configuration	Cs	Cp
Remote Access ON	60	60
Remote Access OFF	10	20

### (2) authentication

Configuration	Cs	Cp
Authentication ON	10	30
Authentication OFF	80	70

### (3) encryption

Configuration	Cs	Cp
Encryption ON	10	10
Encryption OFF	80	80

## Sub-system analysis

## Metrics for Mesh Radio

→ the Mesh radio link

- (4) mesh
- (5) message rate
- (3) encryption

**(4) mesh**

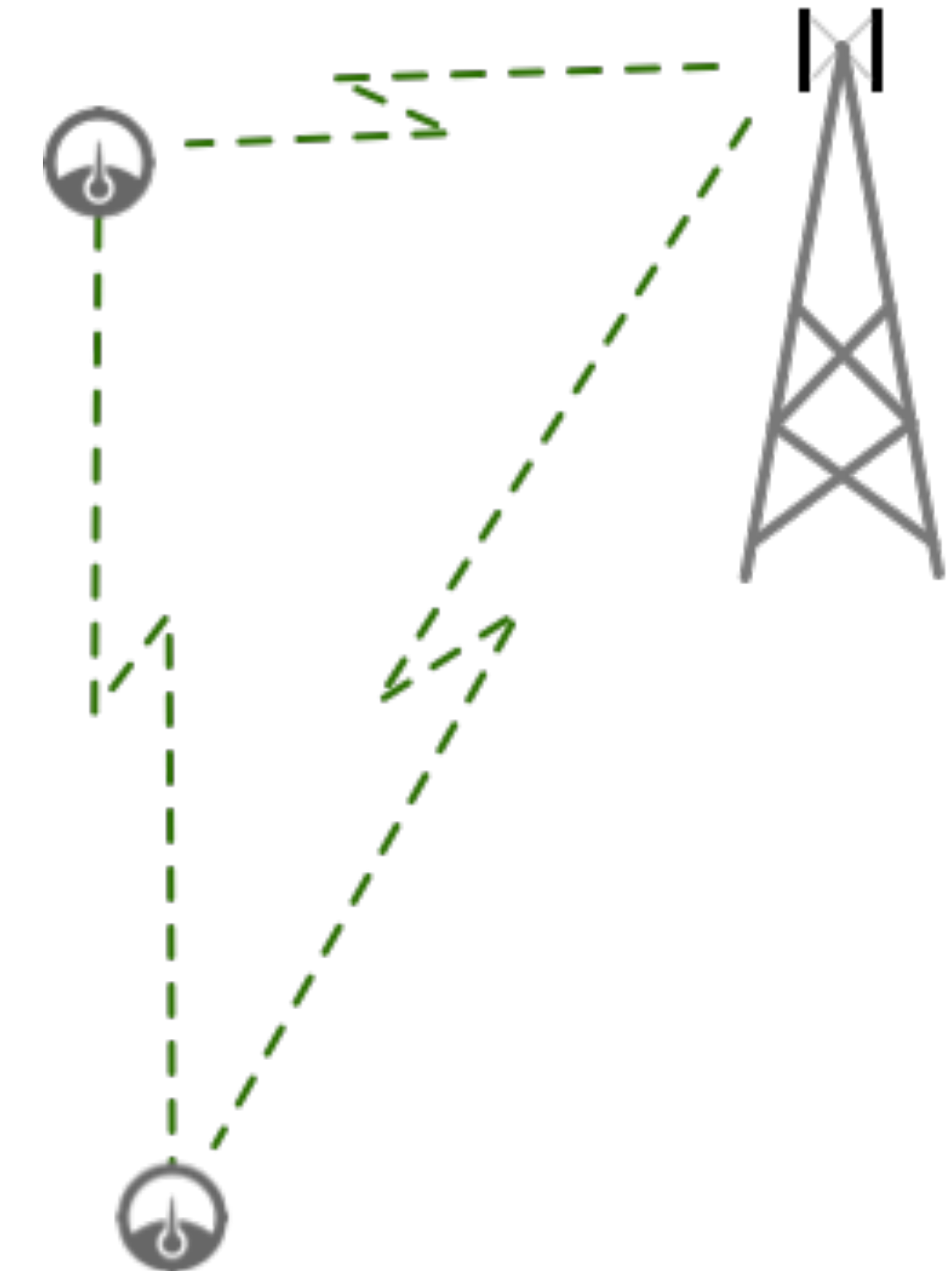
Configuration	Cs	Cp
Multi-path routing	60	60
Single-path routing	30	30

**(5) message rate**

Configuration	Cs	Cp
1 hour	20	20
20 min	25	30
1 min	40	50
5 sec	50	70

**(3) encryption**

Configuration	Cs	Cp
Encryption ON	10	10
Encryption OFF	80	80

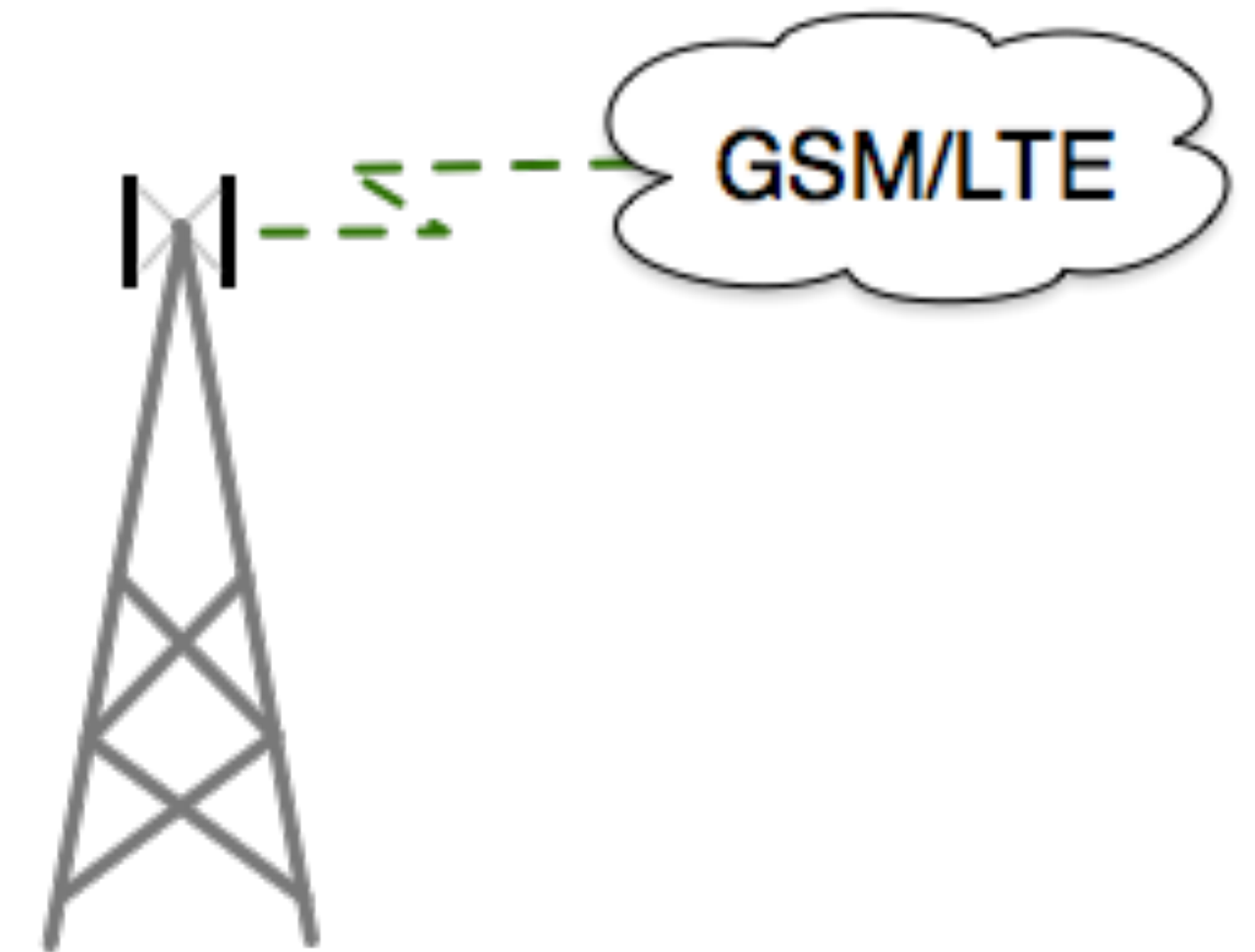


## Sub-system analysis

## Metrics for mobile link sub-system

→ the Mobile link sub-systems

- (6) mobile channel (2G or SMS)
- (6+) 3G/4G, IP, powerline
- (3) encryption



### *(3) encryption*

Configuration	Cs	Cp
Encryption ON	10	10
Encryption OFF	80	80

### *(6) mobile channel*

Configuration	Cs	Cp
GPRS	60	70
SMS	40	50



## AMR sub-system analysis Summary of Metrics for functionality

### → the Automatic Meter Reader (AMR)

- (1) remote access metric
- (2) authentication metric
- (3) encryption metric

### → the Mesh radio link

- (4) mesh
- (5) message rate
- (3) encryption

### → the Mobile link sub-systems

(6) mobile channel (2G or SMS)

(3) encryption

(1)

Configuration	Cs	Cp
Remote Access ON	60	60
Remote Access OFF	10	20

(3)

Configuration	Cs	Cp
Encryption ON	10	10
Encryption OFF	80	80

(2)

Configuration	Cs	Cp
Authentication ON	10	30
Authentication OFF	80	70

(4)

Configuration	Cs	Cp
Multi-path routing	60	60
Single-path routing	30	30

(5)

Configuration	Cs	Cp
1 hour	20	20
20 min	25	30
1 min	40	50
5 sec	50	70

(6)

Configuration	Cs	Cp
GPRS	60	70
SMS	40	50



## Sub-system weighting

- Component criticality from metrics
- sub-system criticality from evaluation of components
- system criticality from evaluation of sub-systems
- Criticality  $C$  through root mean square weight
- Actual criticality  $x_i$  for component or (sub-)system
- Weight  $w_i$  for each metric,
- Result will maximise the impact of high criticalities

$$C = \sqrt{\sum_i \left( \frac{x_i^2 W_i}{\sum_i^n W_i} \right)} \quad W_i = \left( \frac{w_i}{100} \right)^2$$

Table 8 Sub-systems and components weights

Sub-system	Sub-sys. Weight	Component	Comp. Weight
AMS	80	Remote Access	70
		Authentication	80
		Encryption	80
Radio link	50	Mesh	60
		Message Rate	80
		Encryption	40
Mobile link	20	Mobile link	70
		Encryption	40



## s,p-goal versus system-s,p

- 11 possible configurations
  - selected as combinations of “states”
- highest SPD element dominates the outcome of the metrics
  - Billing & Home Control: security
  - Alarm: dependability
- Sensitivity Analysis:
  - max security:  $s=84$
  - same config:  $p=77$
  - satisfies billing
  - satisfies home control



Table 1  $SPD_{Goal}$  of ea

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

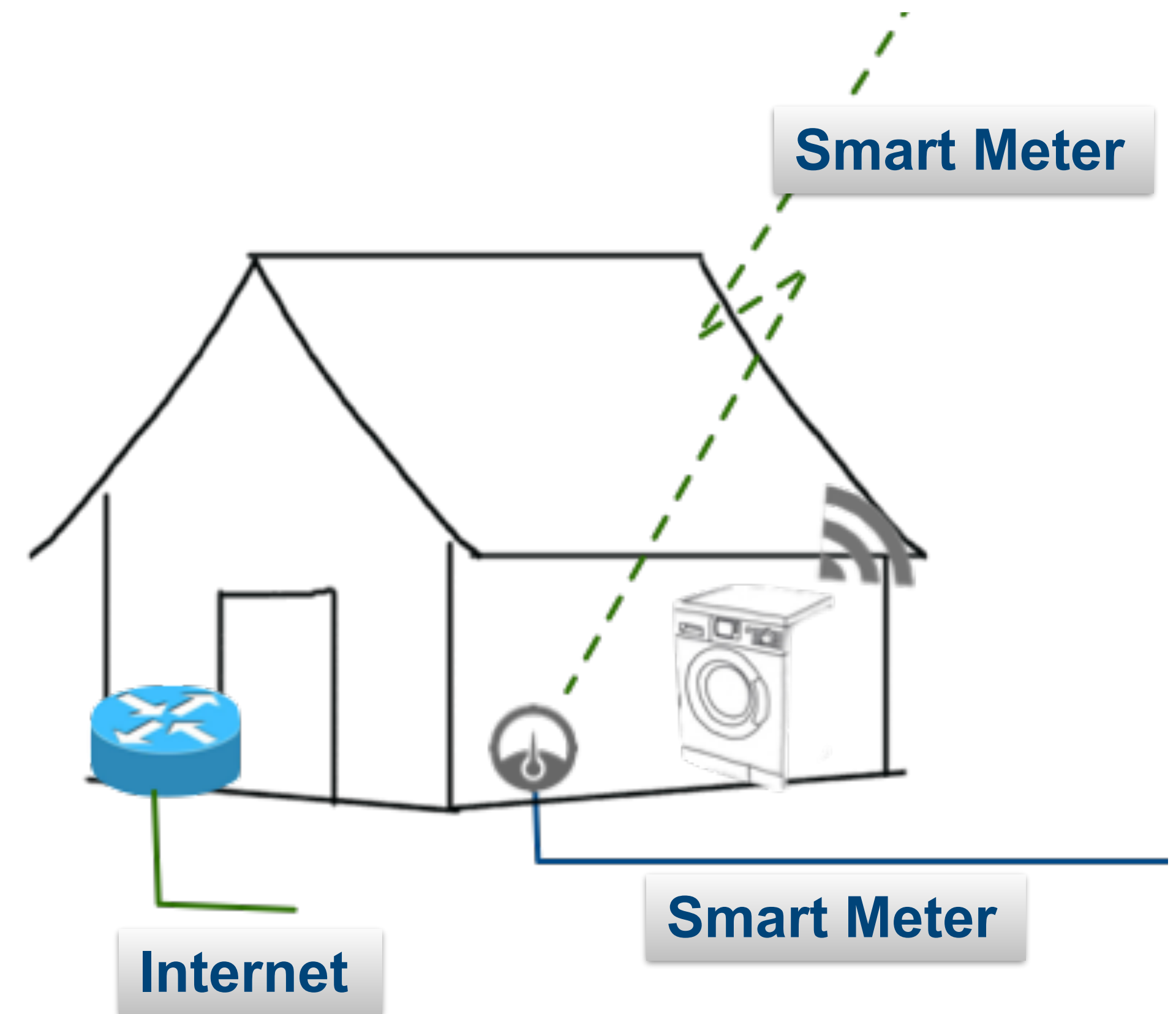
Table 9 Selected configuration SPD level for each use case

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)	(●, ●, ●)



## Upcoming Infrastructure

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



[source: [seminaronly.com](http://seminaronly.com)]



## Conclusions - Smart Meter

- Security and Privacy methodology applied for Smart Grid
- Sub-system Meter Reader, Mesh communication, Mobile Communication assessed
- Weighting, see example
- 11 configurations assessed, best result providing (s,p,d) = (84,77,42)

Table 8 Sub-systems and components weights

Sub-system	Sub-sys. Weight	Component	Comp. Weight
AMS	80	Remote Access	70
		Authentication	80
		Encryption	80
Radio link	50	Mesh	60
		Message Rate	80
		Encryption	40
Mobile link	20	Mobile link	70
		Encryption	40



## Questions to be answered

