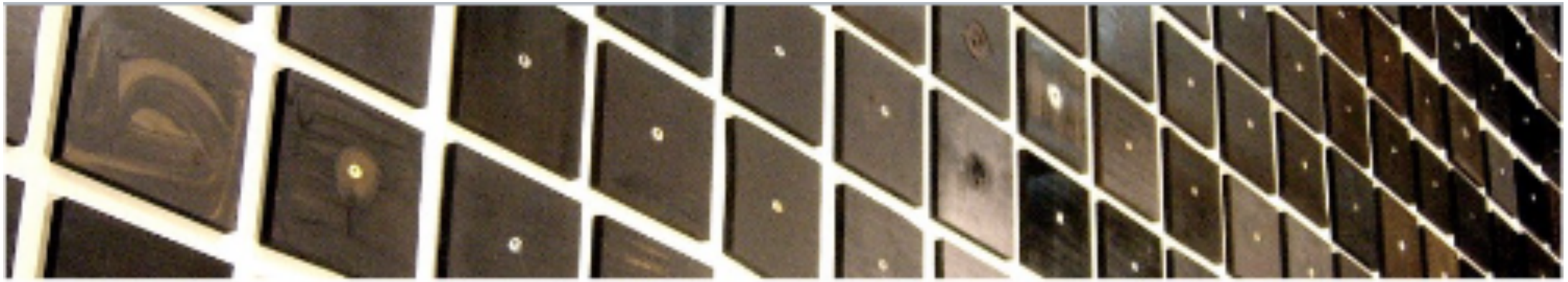


UiO : Universitetet i Oslo

MANTIS Industrial Workshop, May 2017, Helsinki

Measurable Security for the Autonomous Operation of Systems of Systems

Josef Noll

josef@jnoll.net, @josefnoll, m: +47 9083 8066

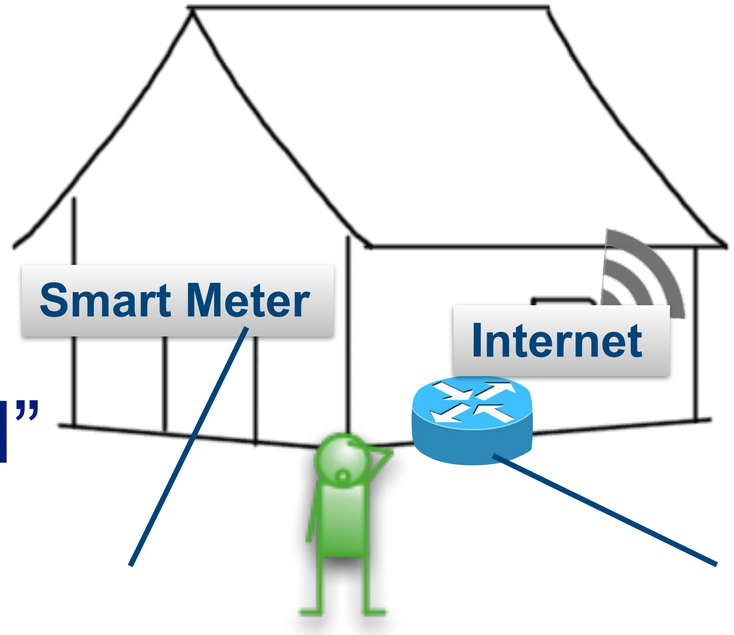
Professor at University of Oslo, Department of Technology Systems

Co-Founder and Secretary General at Basic Internet Foundation

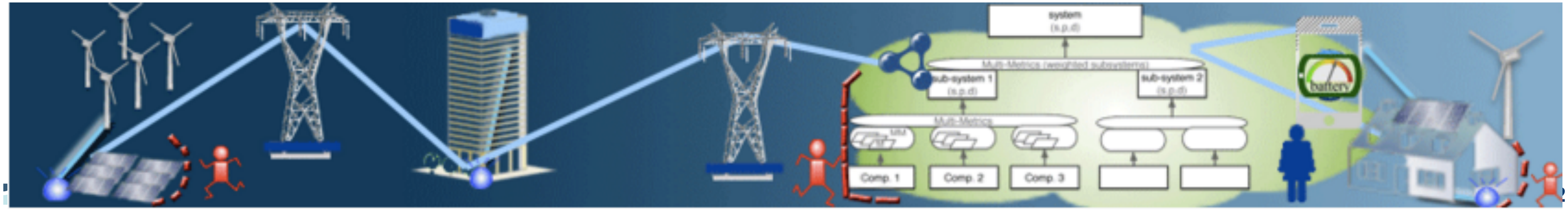
“Security in IoT for Smart Grids”

IoTSec.no

“Research on IoT security”
with
“The national Security Centre for Smart Grid”



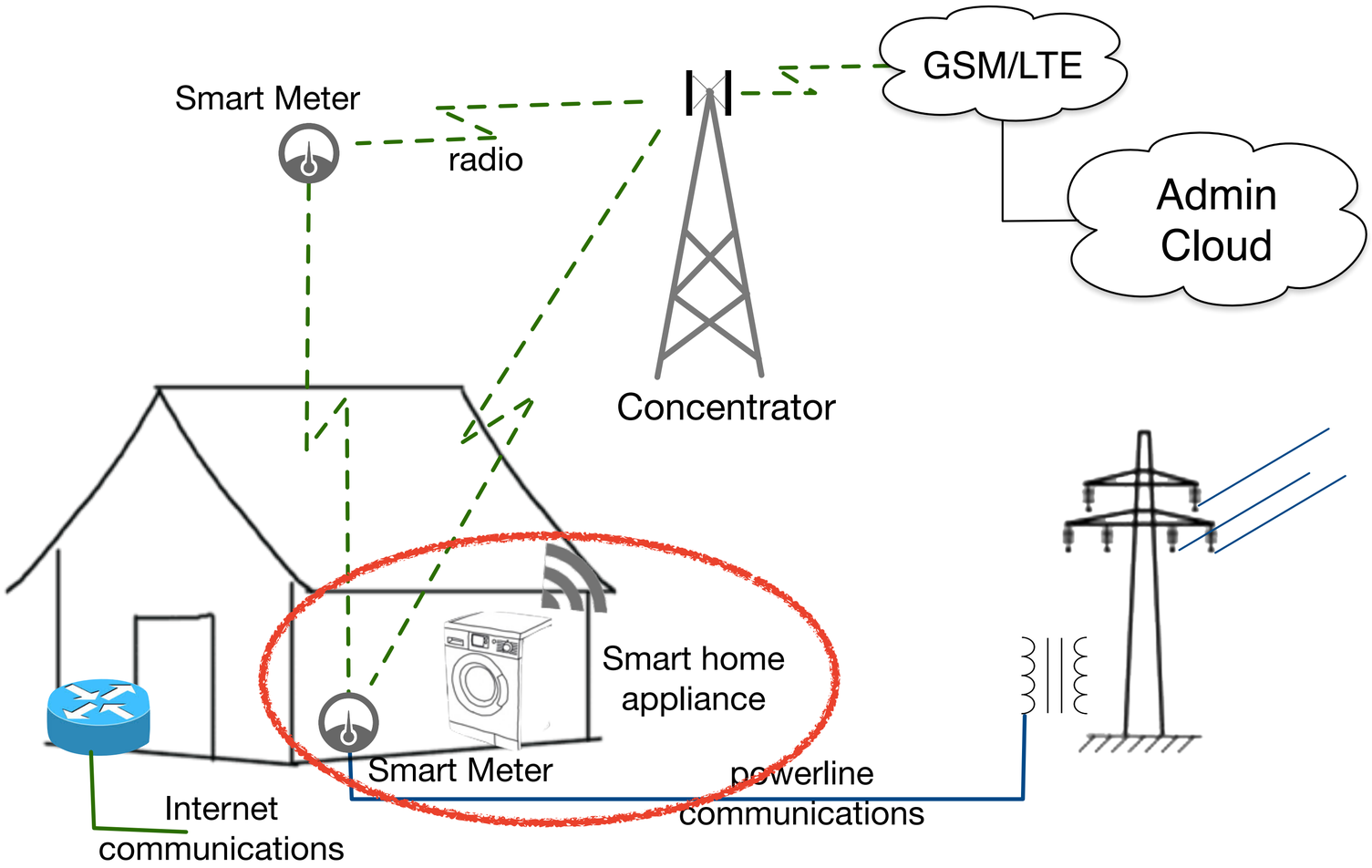
NFR funded Research Initiative, 2015-2020
20 partners med 5 x Academia (UiO, NTNU, Simula, NR, UiA),
industry and public authorities (Datatilsynet, Forbrukerrådet)



SMARTGRID
SECURITY CENTER

We help the Utility Companies achieve their smart grid goals with higher resiliency and quicker response times against security threats.

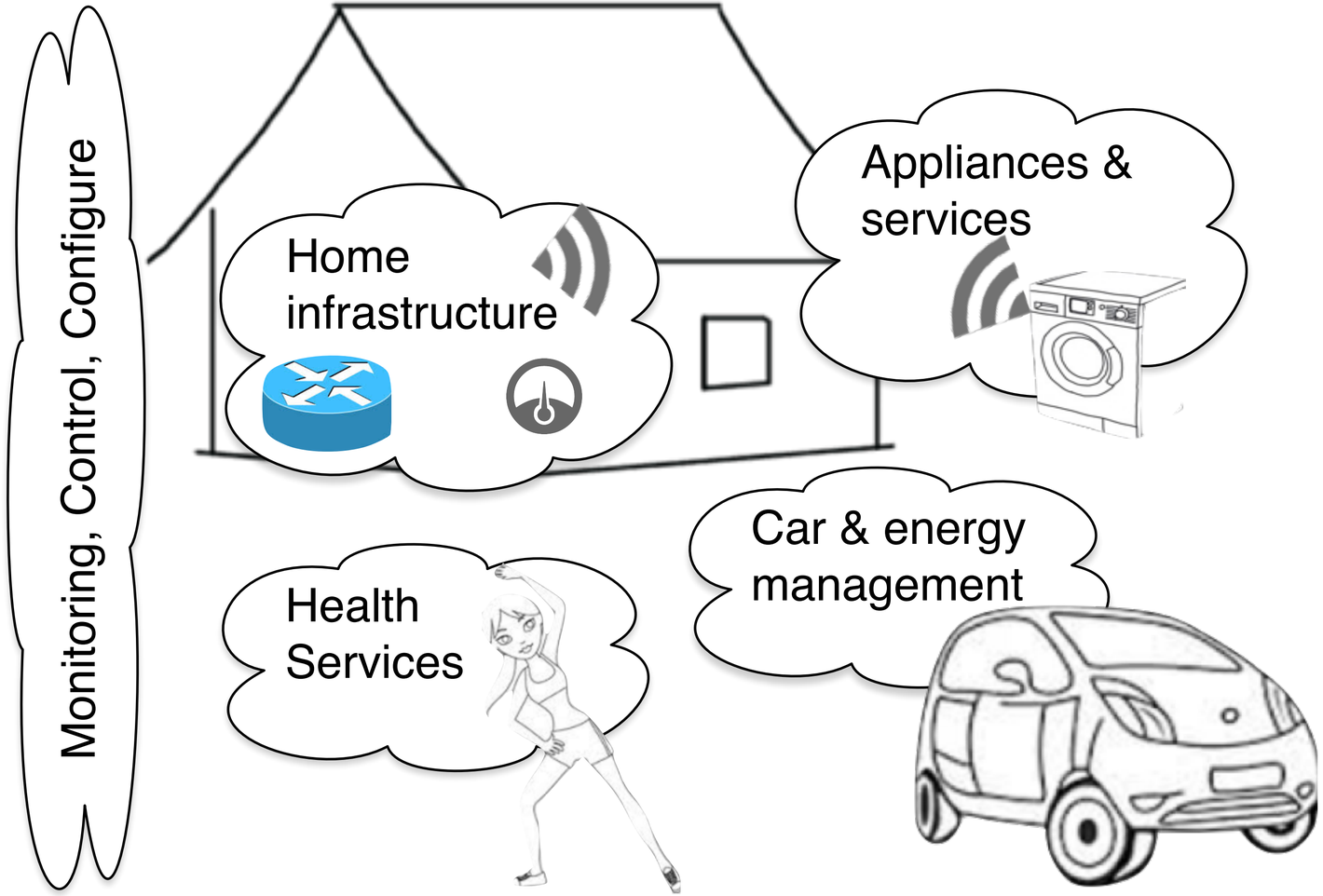
Who is going to manage the home?



Considerations

- A variety of services
- Security and Privacy requirements

- Novel trends, flexibility
- My Home is everywhere

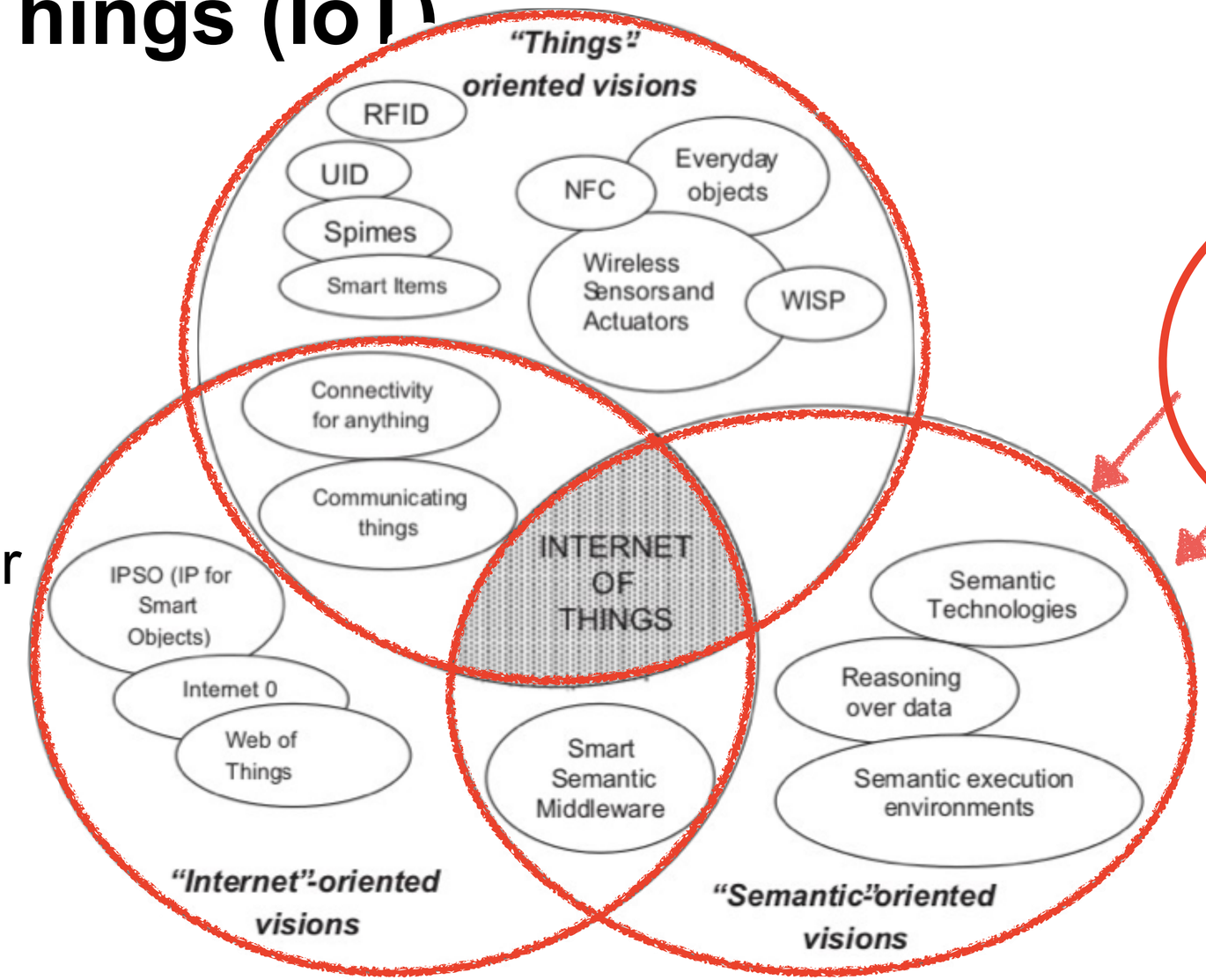


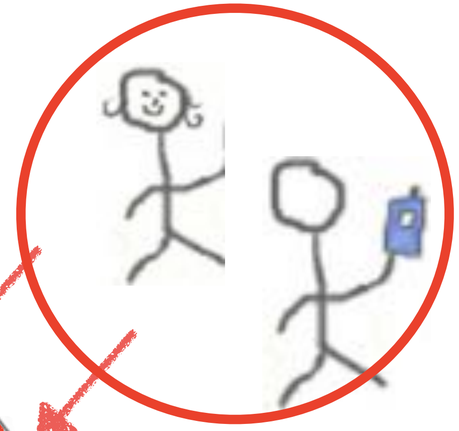
Source: L. Atzori et al., The Internet of Things: A survey, Comput. Netw. (2010), doi:10.1016/

The Internet of Things (IoT)

- IoT =
  - Internet +
  - Semantics +
  - Things

- Tingene som snakker
  - med en datamaskin,
  - som forstår hva det dreier seg om,
  - og tar selvstendige beslutninger



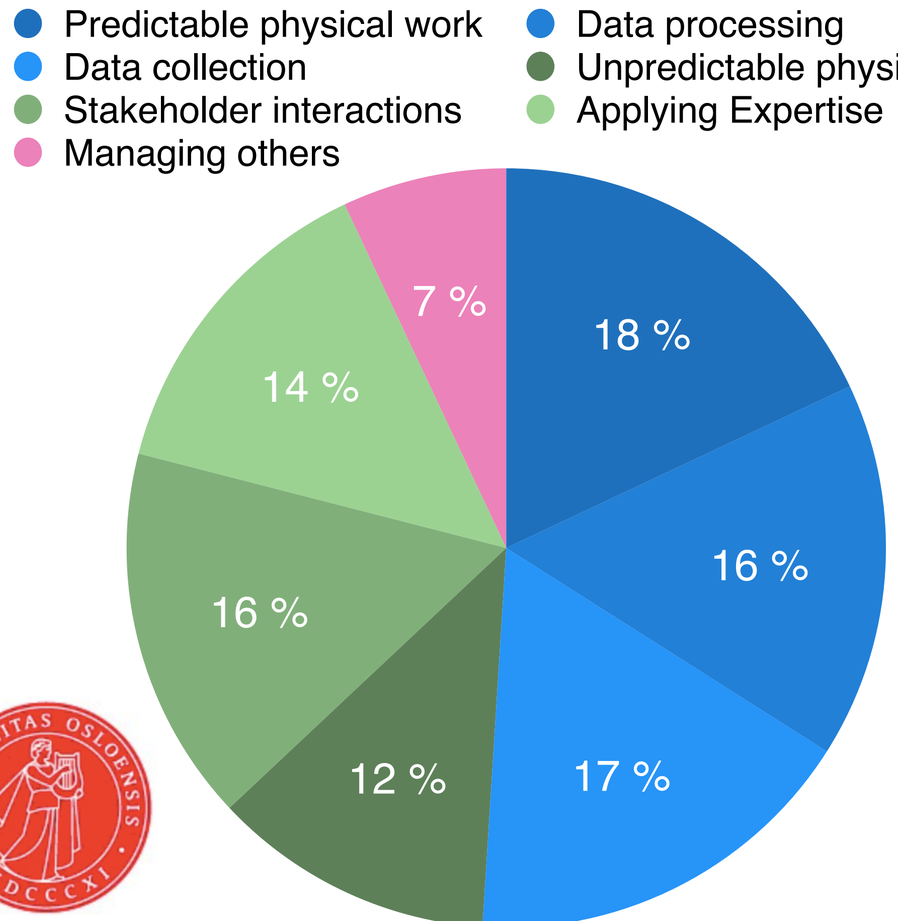


* security
* privacy
* dependability
* context-aware
* personalised

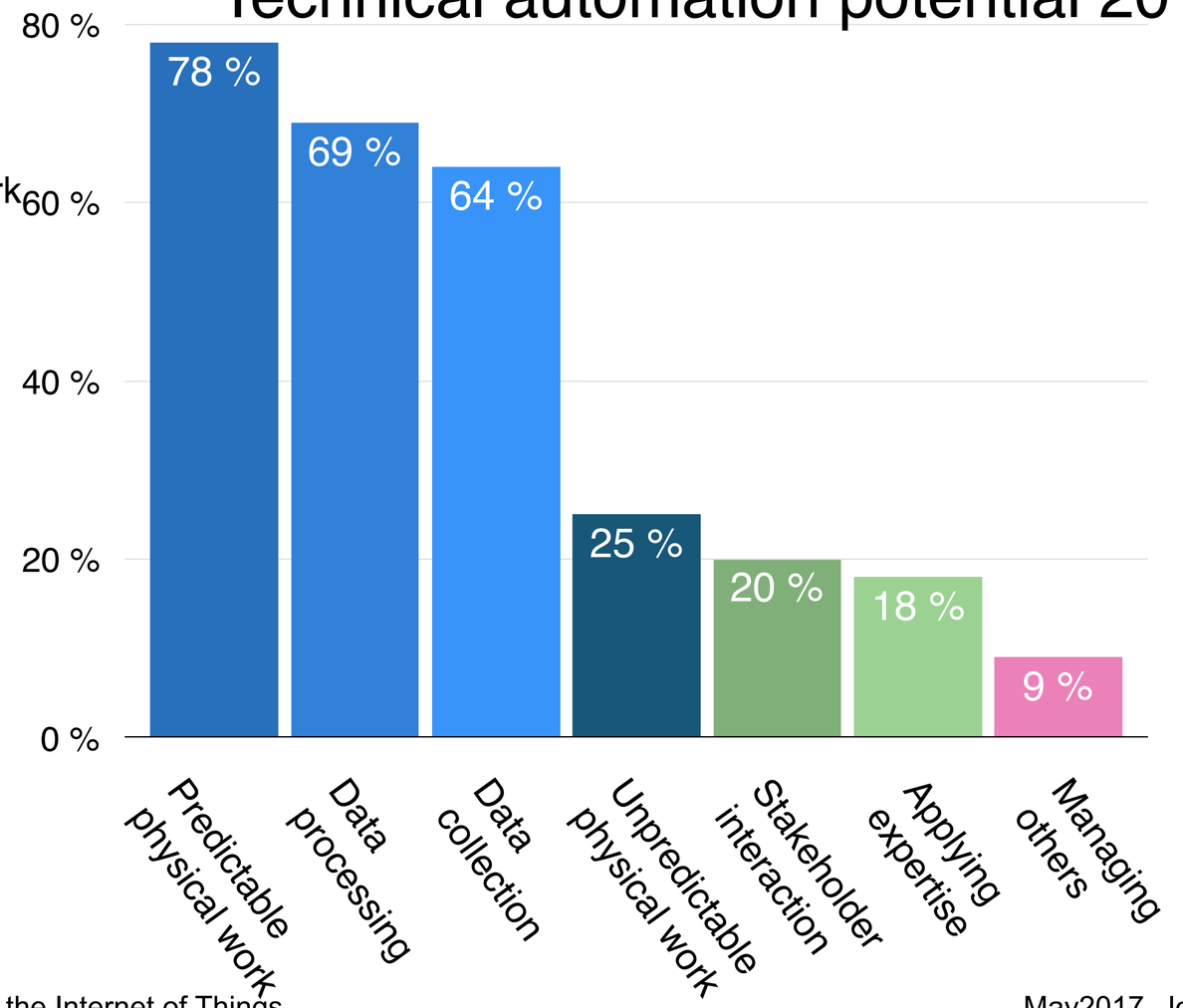
Fig. 1. "Internet of Things" paradigm as a result of the convergence of different visions.

The challenge from automation

USA work force time spent [%]



Technical automation potential 2016 [%]



“When I look at MANTIS”

- Complex system of systems
- Good architecture of cloud and edge based components
- Artifacts = Agents(?)
- centralised decision making

Challenges

- Security overlay
- Company Privacy (=Confidentiality)
- “Authorization”
- Non-secure IoT devices

IoT threats

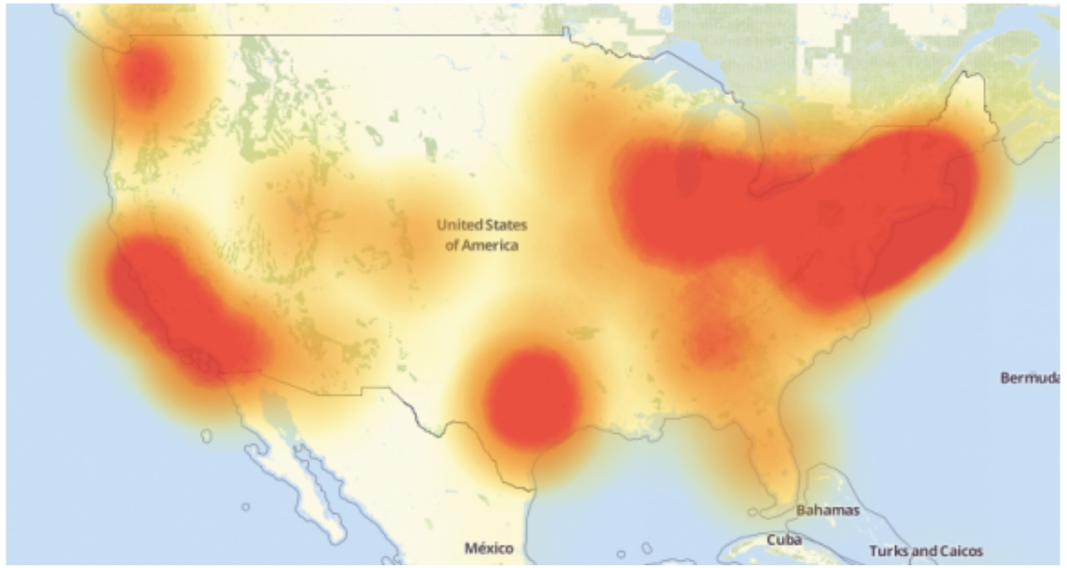
- First massive attack from IoT devices
  - 16Oct2016 IoT botnet attack on Dyn
  - Camera (CCTV), video recorder, TV,…
  - 1.2 Gbps Denial-of-Service attack

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

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

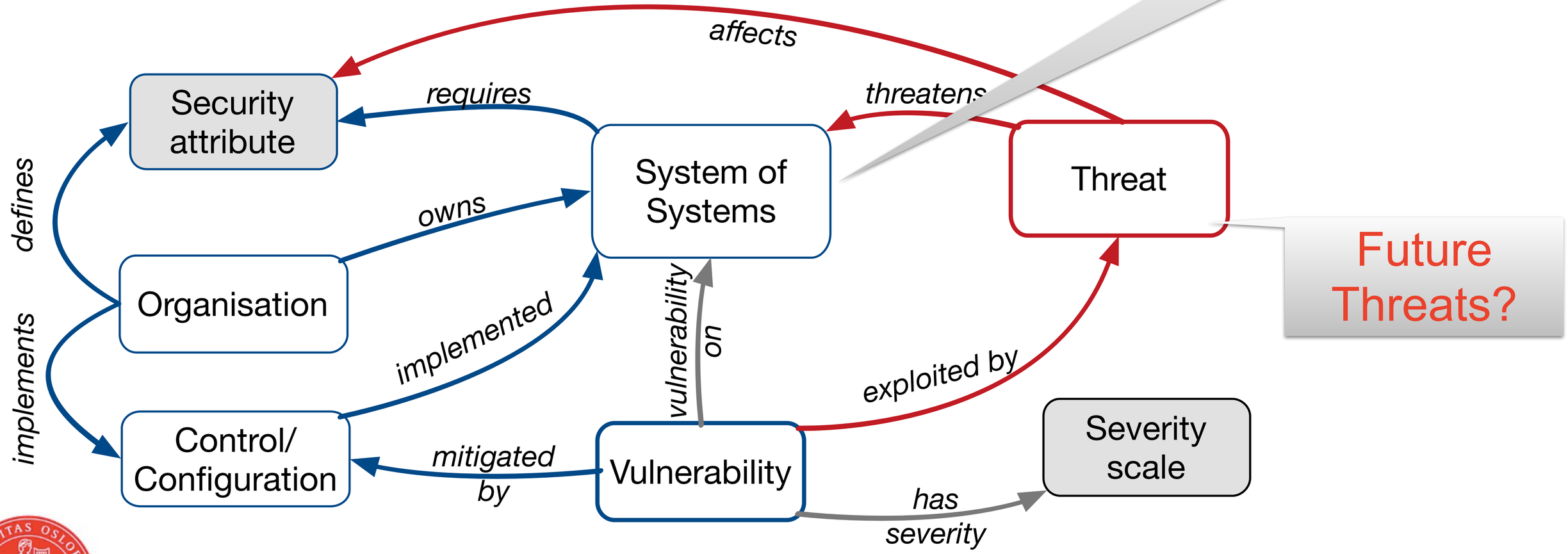
A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked “Internet of Things” (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

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

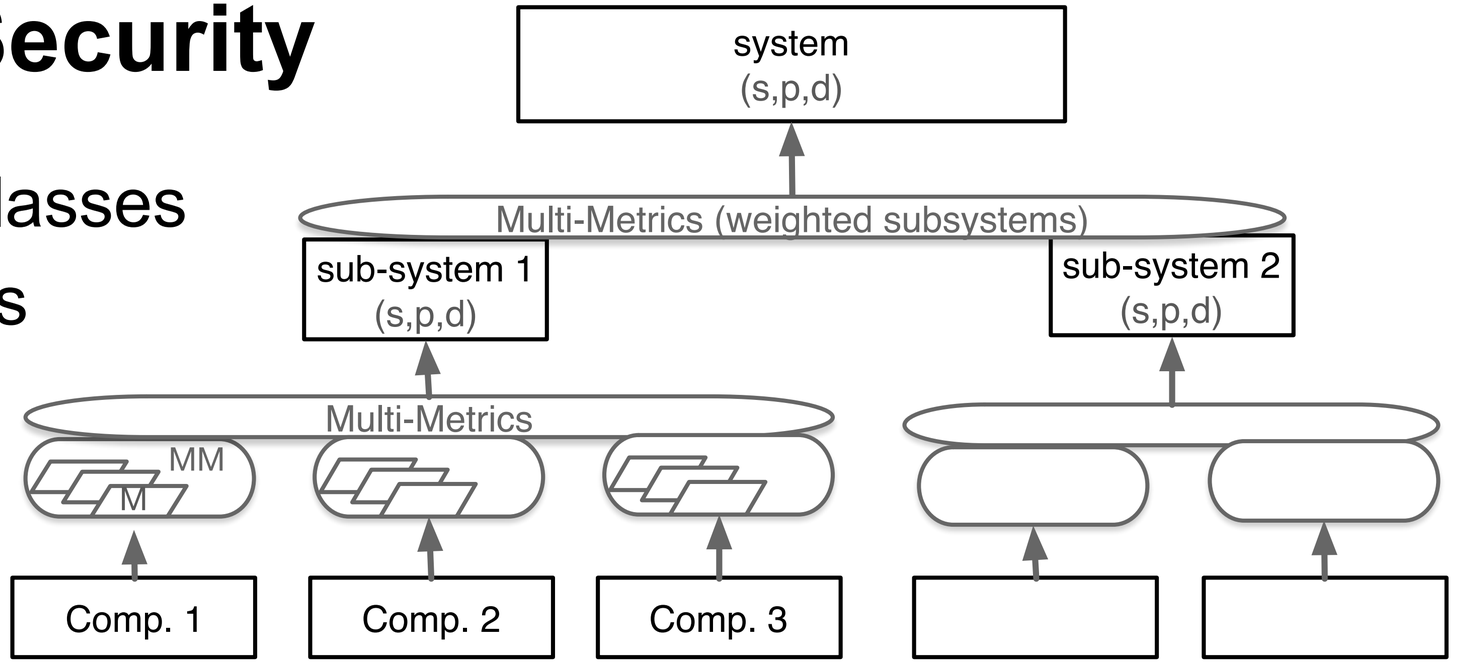
Traditional: Threat-based approach



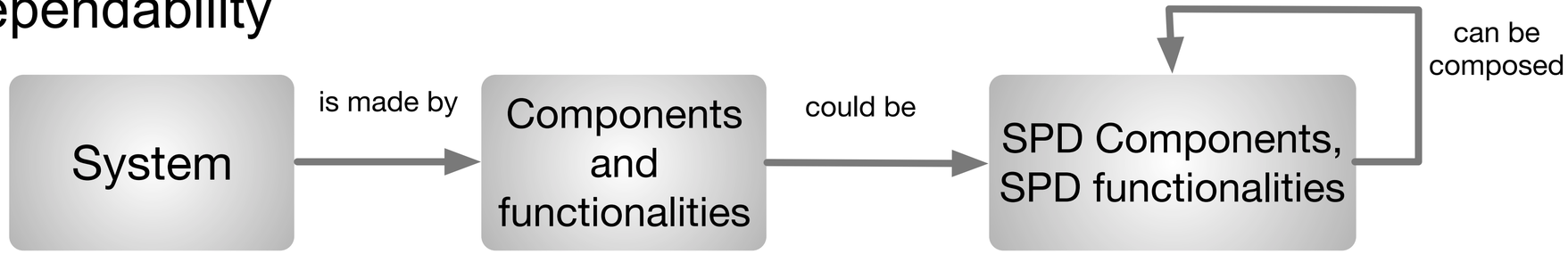
[source: http://securityontology.sba-research.org/]

Example: Measurable Security

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

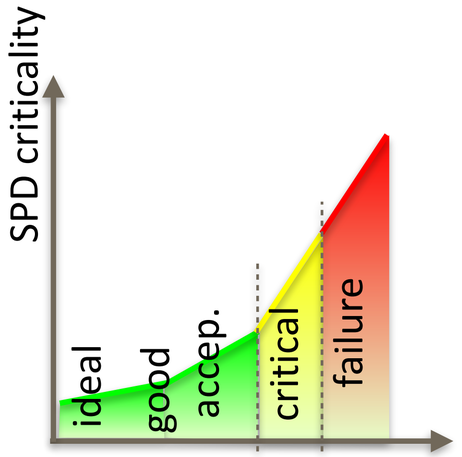


- based on
  - ➡ security, privacy and dependability functionalities

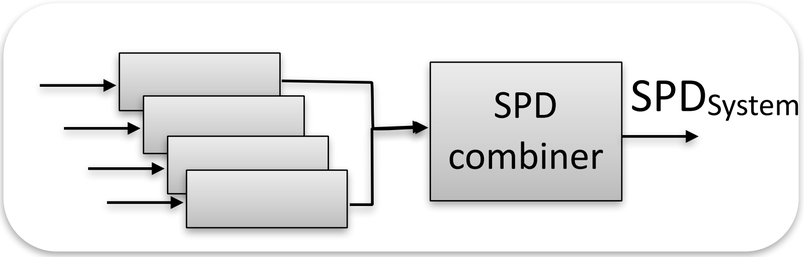


Multi Metrics Assessment

- Metrics to Security, Privacy, Dependability (SPD) conversion
  - » Parametrisation of system parameters, e.g. latency -> [ms]
  - » SPD regression: «SPD value and importance for the system»
    - » parameter into S,P,D value range, e.g. latency=50ms :=> (ideal, good, acceptable, critical, failure)

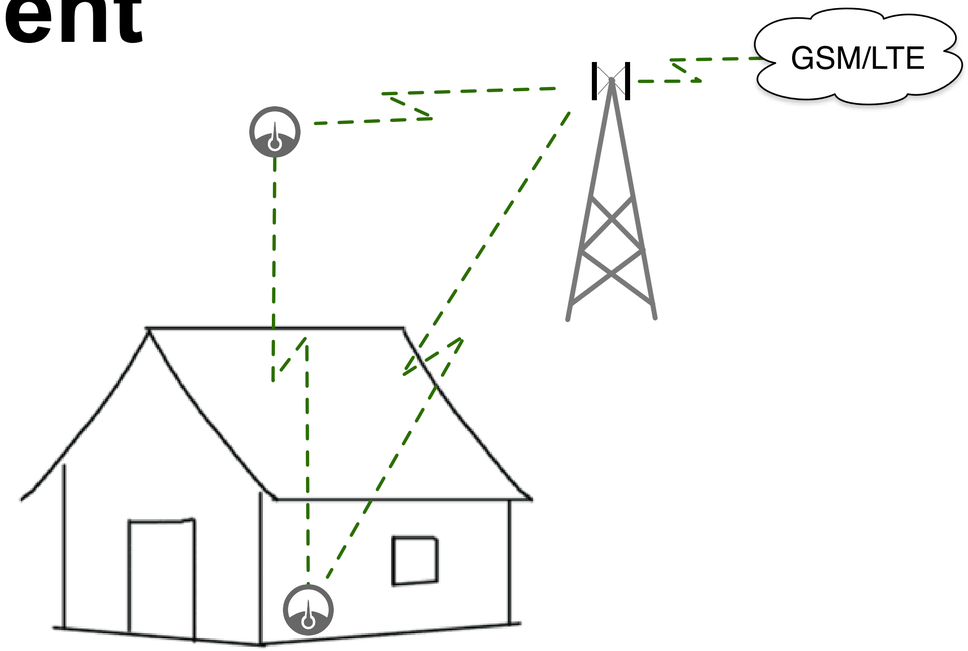


- Metrics combination to provide SPD_{System}: (60, 30, 70)
  - » Mathematical combination, e.g. $S_{System}=100 - SQRT(S_1^2+S_2^2+\ldots S_x^2)$



From System to Security Assessment

- System described through
  - Security functionality
  - Security attributes
  - Metrics converting security into [0…100]



- Automatic Meter Reader (AMR)
  - (1) remote access metric - (yes/no)
    - reading, or just controlling
  - (2) authentication metric
    - everyone, or authenticated user

(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

SPD_{Goal} versus System-SPD_{Level}

- Application-based security goals
- Automated assessment

- Visualisation of “operating envelopes”
  - Security good enough?
  - Too high Security

- Critical component/sub-system assessment

Table 1 SPD_{Goal} of ea

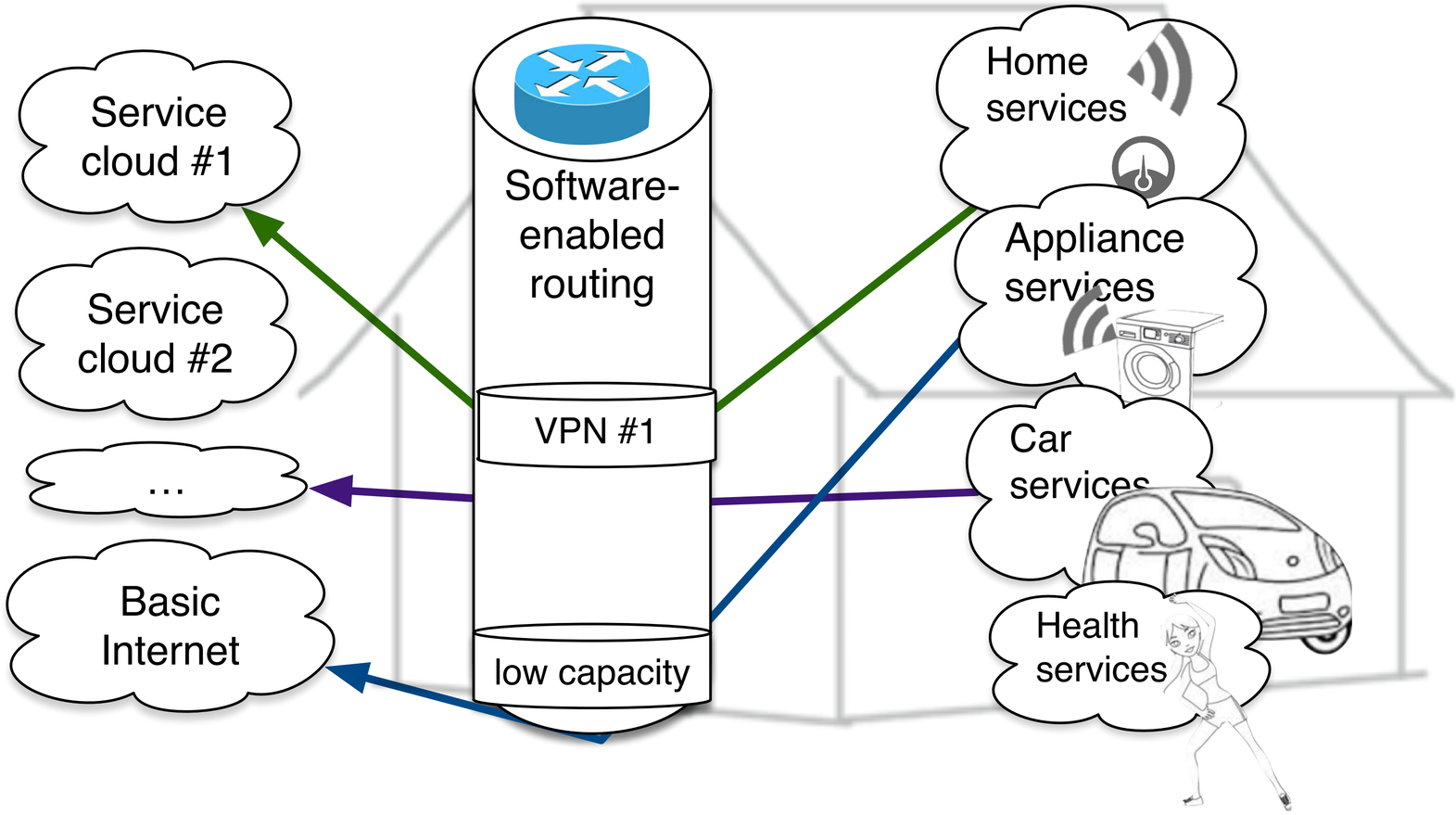
Use Case	Security	Privacy
Billing	90	80
Home Control	90	80
Alarm	60	40

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)	(🔴,🟡,🟡)

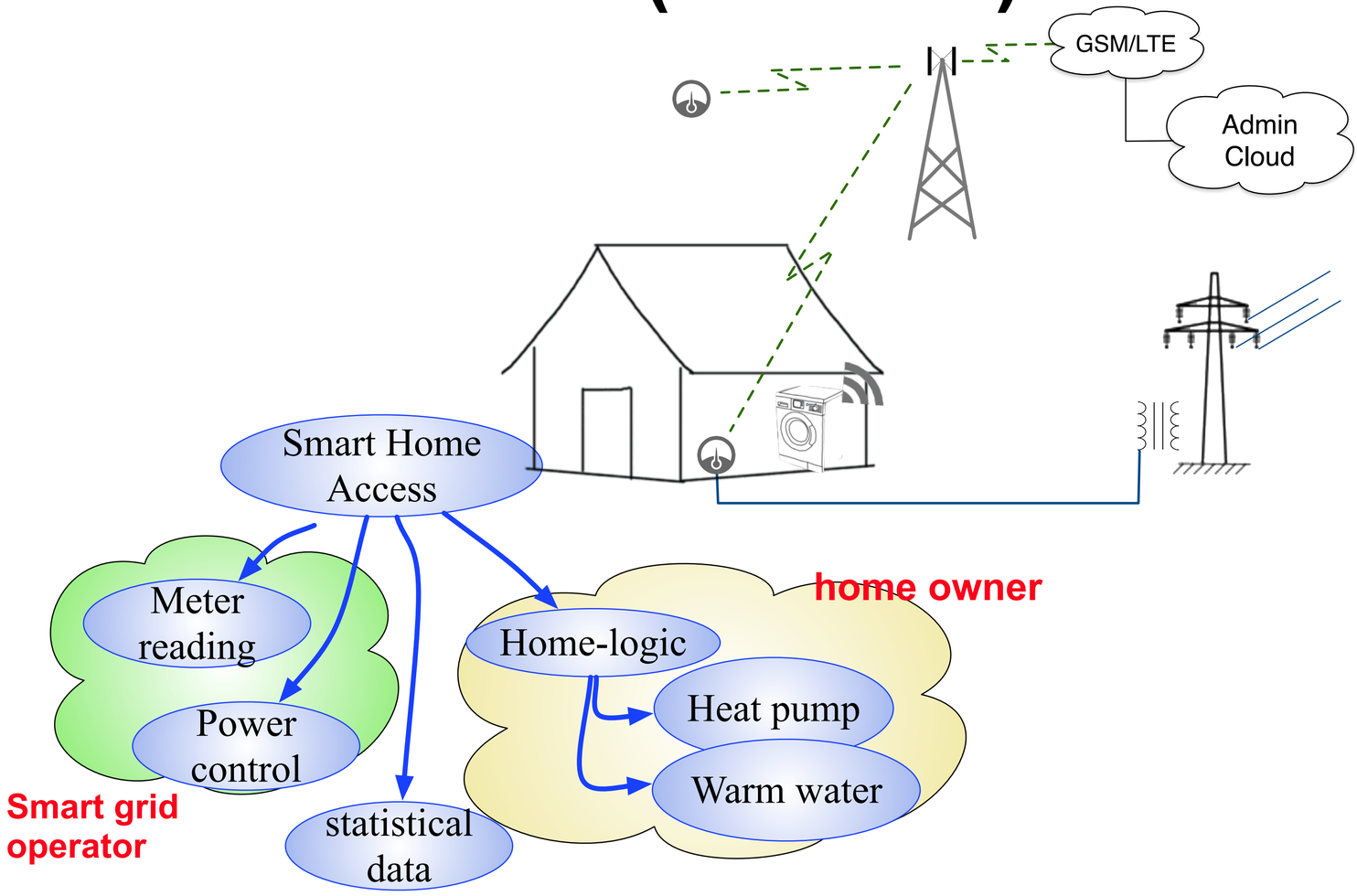
Learn from Industrial Automation and Mobile Networks

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



Semantic attribute based access control (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

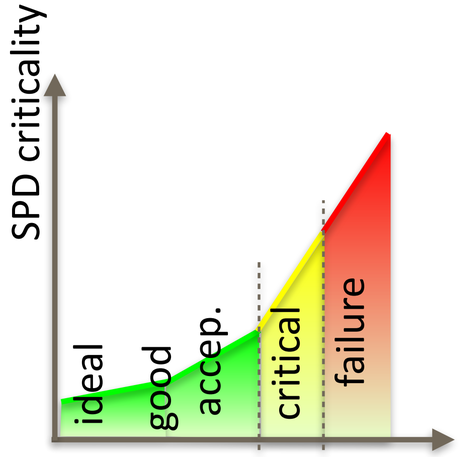


Attributes: roles, access, device, reputation, behaviour, ...

Conclusions

- Things (IoT) are driving the digital societies
- Common challenges
  - Internet + Semantics + Things = IoT
  - Insecure devices
  - Measurable Security and Privacy
  - Autonomous Decisions

- IoT Security and privacy
  - automated privacy/security through Multi-Metrics
  - Semantic-Attribute Based Access Control



Other Topics

Privacy labelling

IoT trust /IOTA.org

17 PARTNERSHIPS FOR THE GOALS

Global perspective
UNO SDG 2030