UiO : Department of Technology Systems
University of Oslo

NEKs Ekomkonferanse 21Nov2017, Oslo

The Internet of Things - The Need for Standardisation

Josef Noll
Department of Technology Systems, University of Oslo
m: +47 9083 8066, e: josef.noll@its.uio.no

IoTSec.no - SCOTT.IoTSec.no

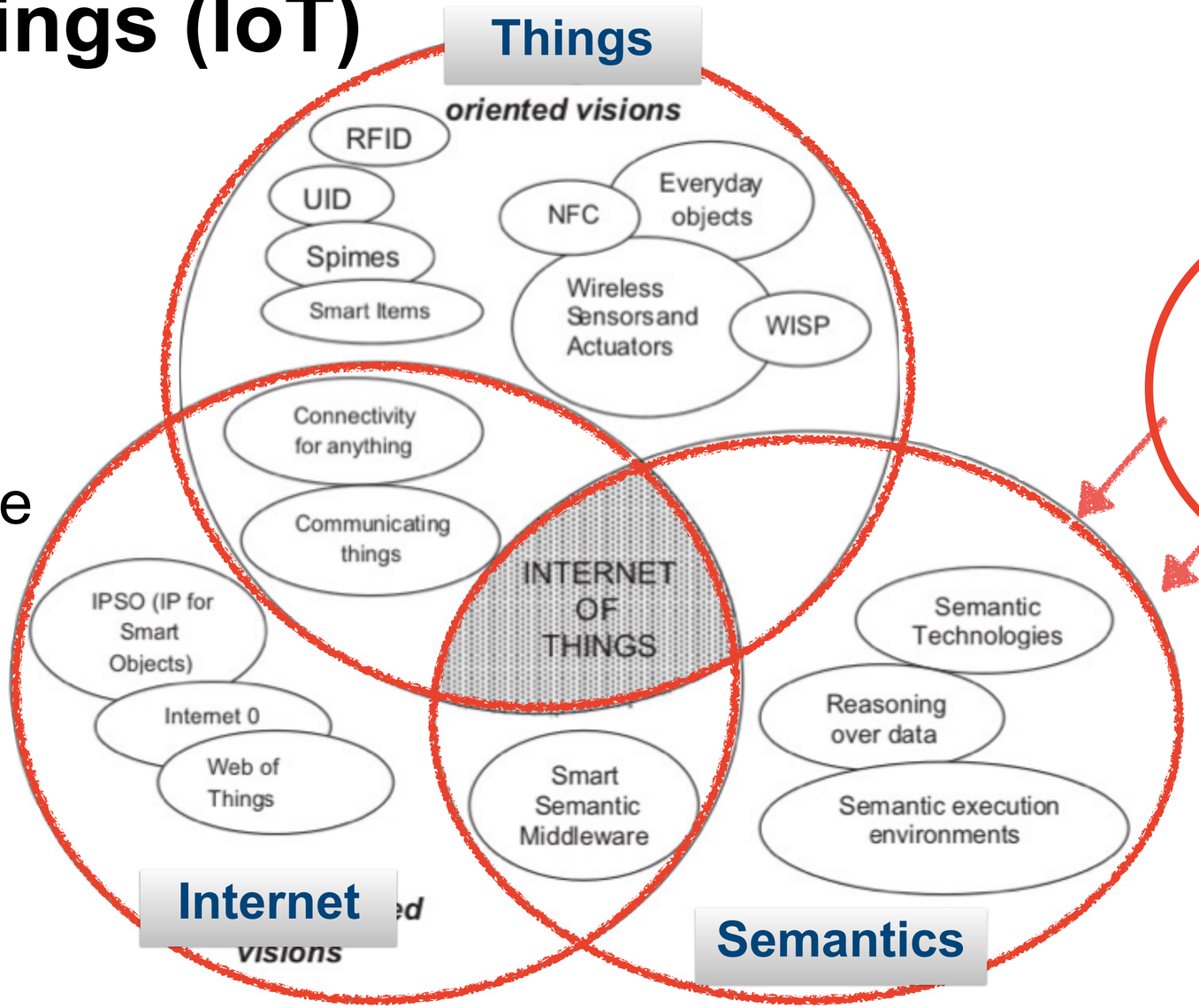
"The last time I was connected by wire was at birth" - our when Internet of Things (IoT) meets people

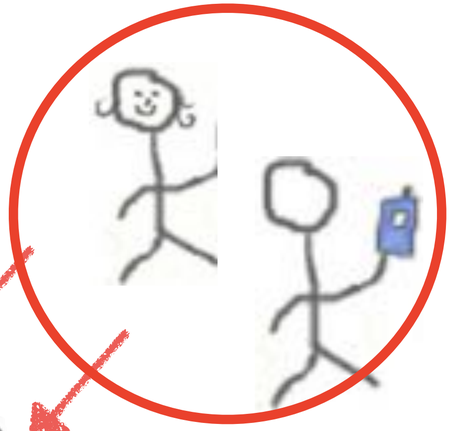
- The changing role of security in HMS -> HMSS
- Internet has changed, IoT will accelerate
  - ➡ the ecosystem of making business
  - ➡ automated processes
- Security in IoT
  - ➡ "teach our sensors to talk Norwegian"
- Standardisation
  - ➡ new paradigm: measurable security
  - ➡ security classes "design"
- related to projects:
  - ➡ Security in IoT for Smart Grids: IoTSec.no
  - Secure Trusted IoT: SCOTT.IoTSec.no,
  - Diversity in IoT Security: DiversIoT.IoTSec.no

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

The Internet of Things (IoT)

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





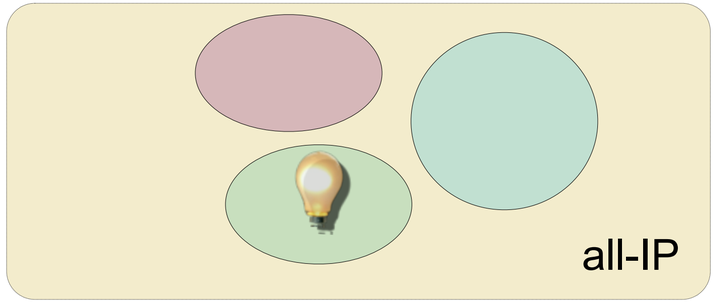
* security
* privacy
* dependability
* context-aware
* personalised

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

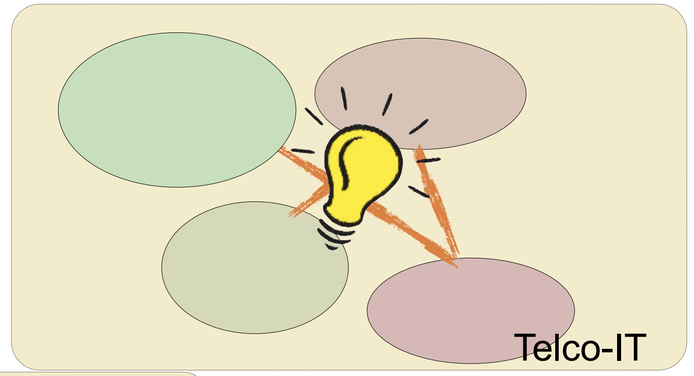
IoT - 3rd wave of convergence

"By 2020, business is dominated by automated processes" [DNV-GL 2013]

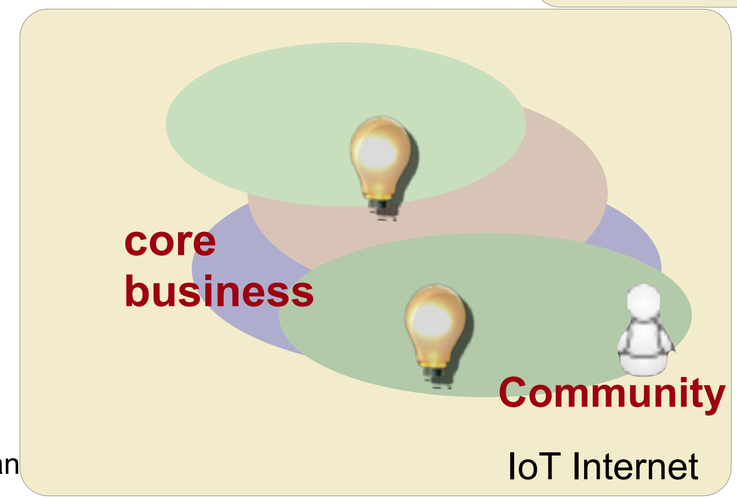
- 1. wave: All-IP
  - flat world, global business



- 2. wave: Telecom - IT - Broadcast
  - from fixed to mobile and quadruple play
  - Telecom = mobile



- 3. wave: IoT Internet
  - The business merger



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

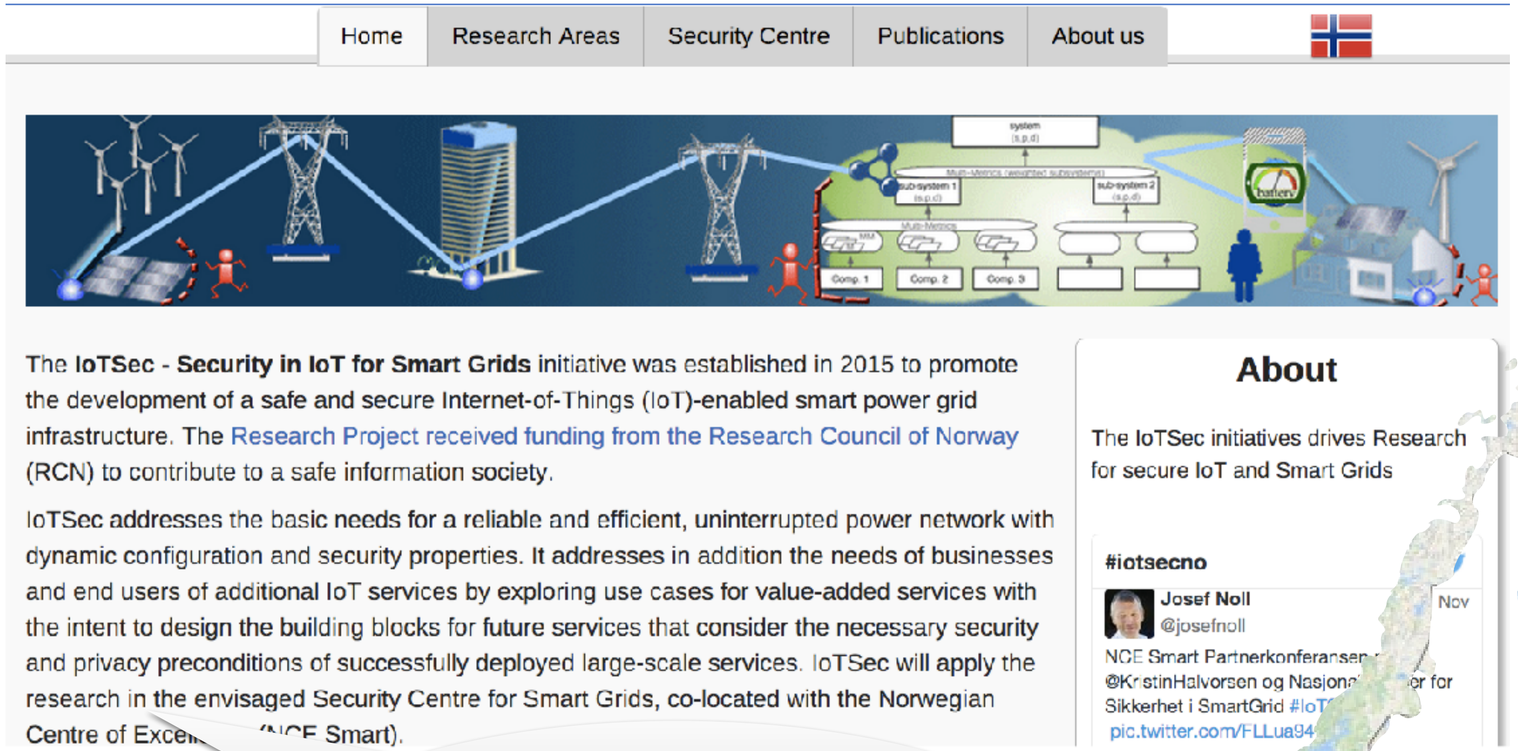
But decide on rules so we can make the dang vehicles

)UT-LAW.COM 68 22 78

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

National initiative for a more secure future in IoT

IoTSec.no - Security in IoT for Smart Grids



«Open World Approach»
everything that is not declared closed is open

Partners and Collaborations

- UiO
- UNIK
- NR
- Simula
- NTNU

Academia

- Smart Innovation Østfold
- eSmart Systems
- Fredrikstad Energi
- EB Nett
- Movation

Industry

- Smartgrid Centre
- Norw. Data Protection Auth.
- Forbrukerrådet

Interest Org.

- EyeSaaS
- mnemonic

Industry

- Mondragon Unibersitatea
- University of Victoria
- Universidad Carlos III
- La Sapienza
- COINS Research School
- Nimbeo
- H2020 and ECSEL projects

International

Addressing the Threat Dimension for IoT

- Hollande (FR), Merkel (DE) had their mobile being monitored
- «and we believe it is not happening in Norway?

[source: www.rediff.com]

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

So lässt sich das UMTS-Netz knacken

[source: Süddeutsche Zeitung, 18Dec2014]

Zwei Hacker zeigen
(UMTS-Antenne lassen
sich knacken (Foto dpa)

Significance

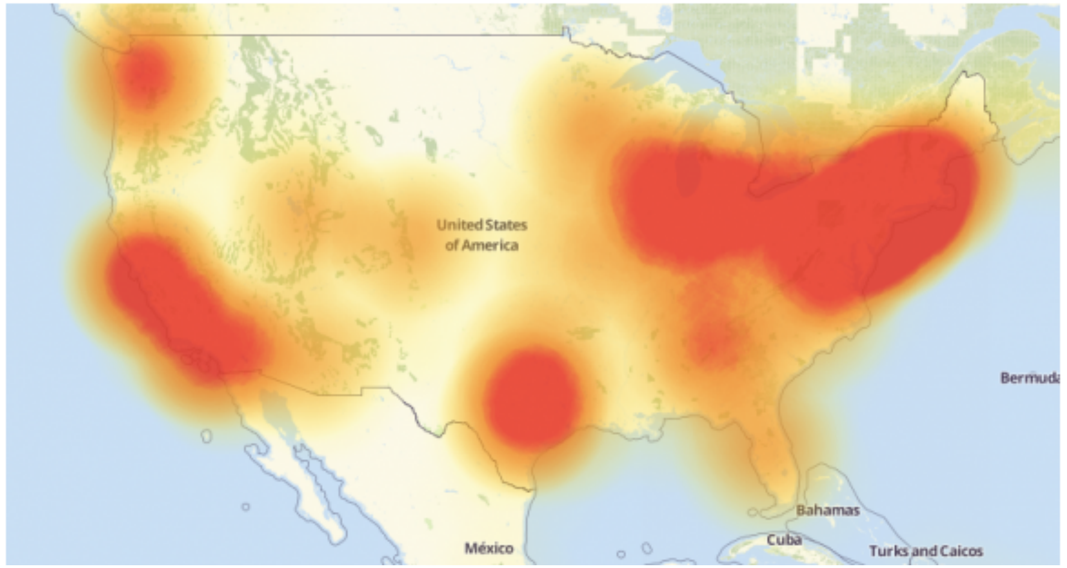
IoT security challenges

- Mirai attack
  - ➡ “security by obscurity”
  - ➡ different security viewpoint
- “it is just the beginning”

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

Communication & IoT for society

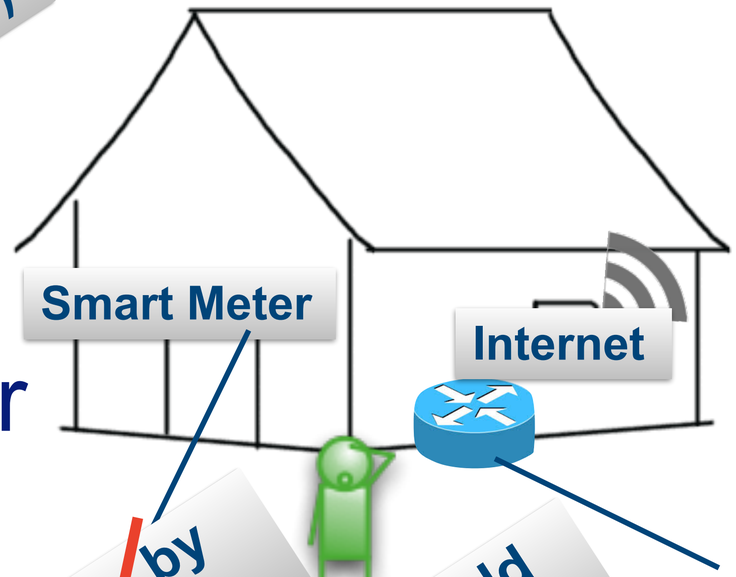
2015-2020 project

IoTSec.no

>20 partners (5 academics)

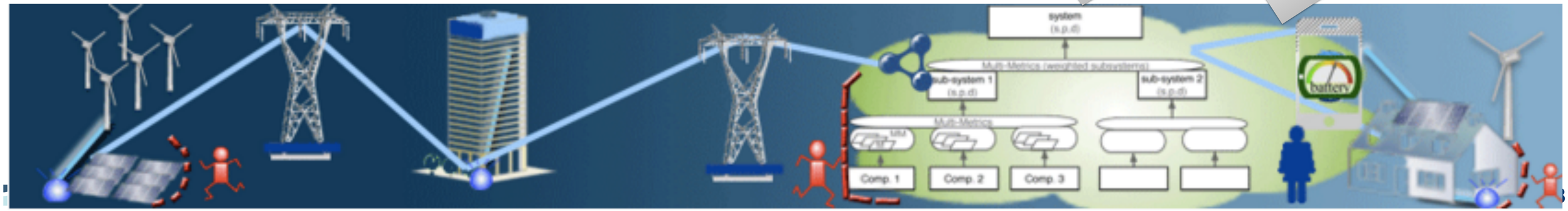
"Research on IoT security"
"Building the national Security Centre for Smart Grid"

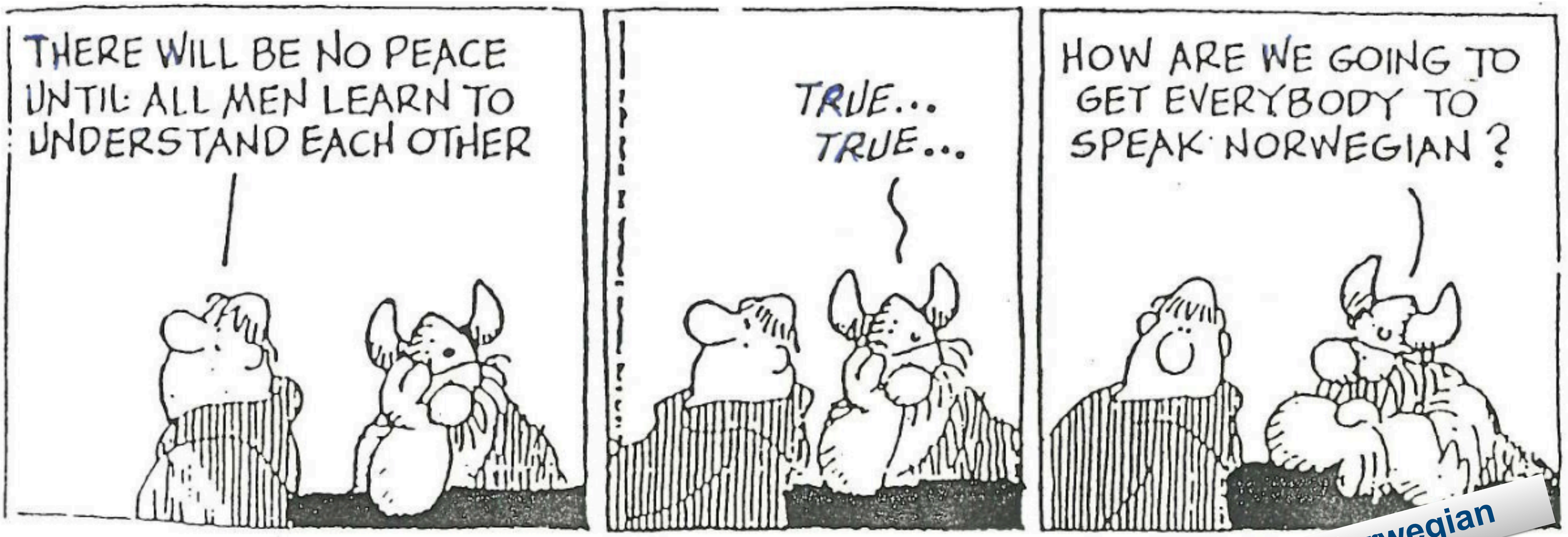
http://IoTSec.no



~~Security by obscurity~~

Open World Approach





teach our sensors to talk Norwegian

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

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

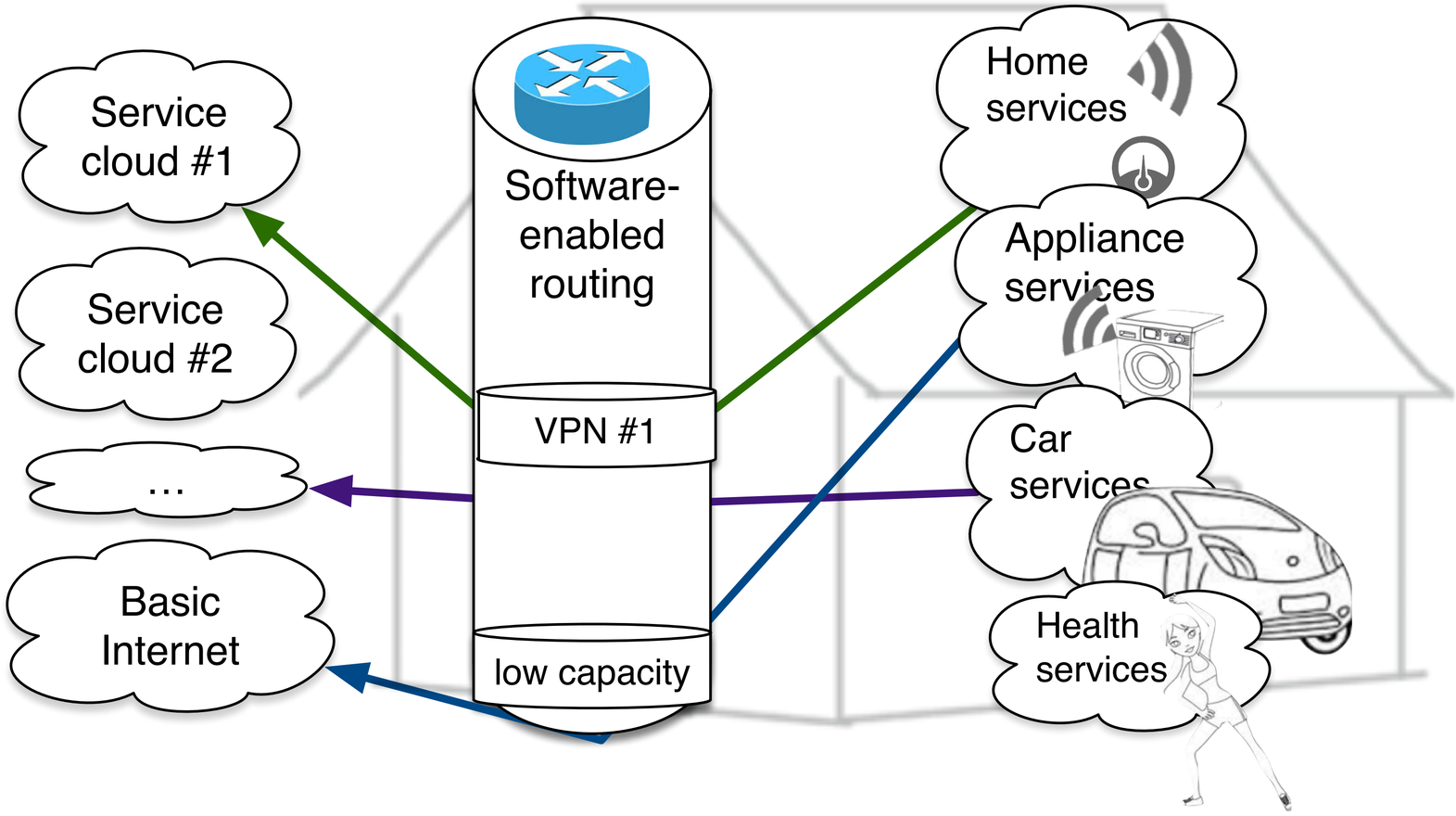
http://SCOTT.IoTSec.no

http://SCOTT-project.eu

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

Learn from Industrial Automation and Mobile Networks

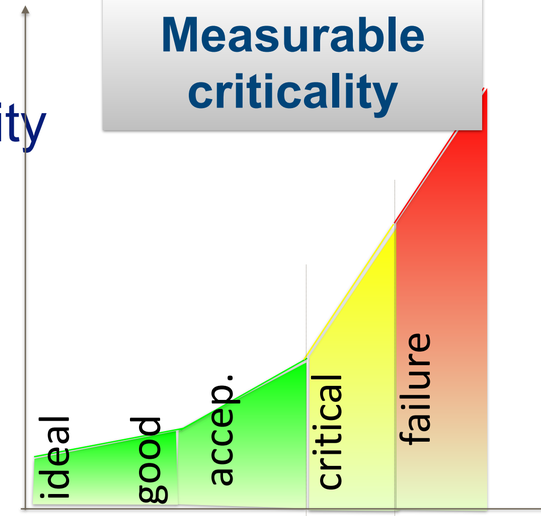
- "What to secure?"
- Network segregation
  - ➡ *Network slicing*
- From Confidentiality, Integrity, Availability (CIA)
- to Availability, Integrity, Confidentiality (AIC)



Security in IoT - our promises

- Semantic system description
  - ➡ Understanding the system and describing security through security functionality
  - ➡ Measurable security - the novel security concept
- Security modelling
  - ➡ Development of privacy-aware models and measures
  - ➡ Adopting and enhancing adaptive security for system of systems
  - ➡ Formal languages for semantically proving signalling
- System versus Goal analysis
  - ➡ Application-specific security/privacy, e.g. billing vs
  - ➡ Human/technical interface, security usability
- Operational security for IoT-based critical infrastructure
  - ➡ IoTSec ecosystem -> extended network
  - ➡ Roadmap for Smart Grid Security Centre (SGSC)
  - ➡ (Gap Analysis of security methods for critical infrastructures)

Measurable criticality



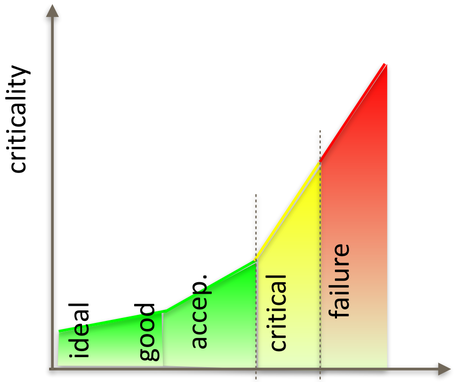
to measurable: security, privacy and dependability

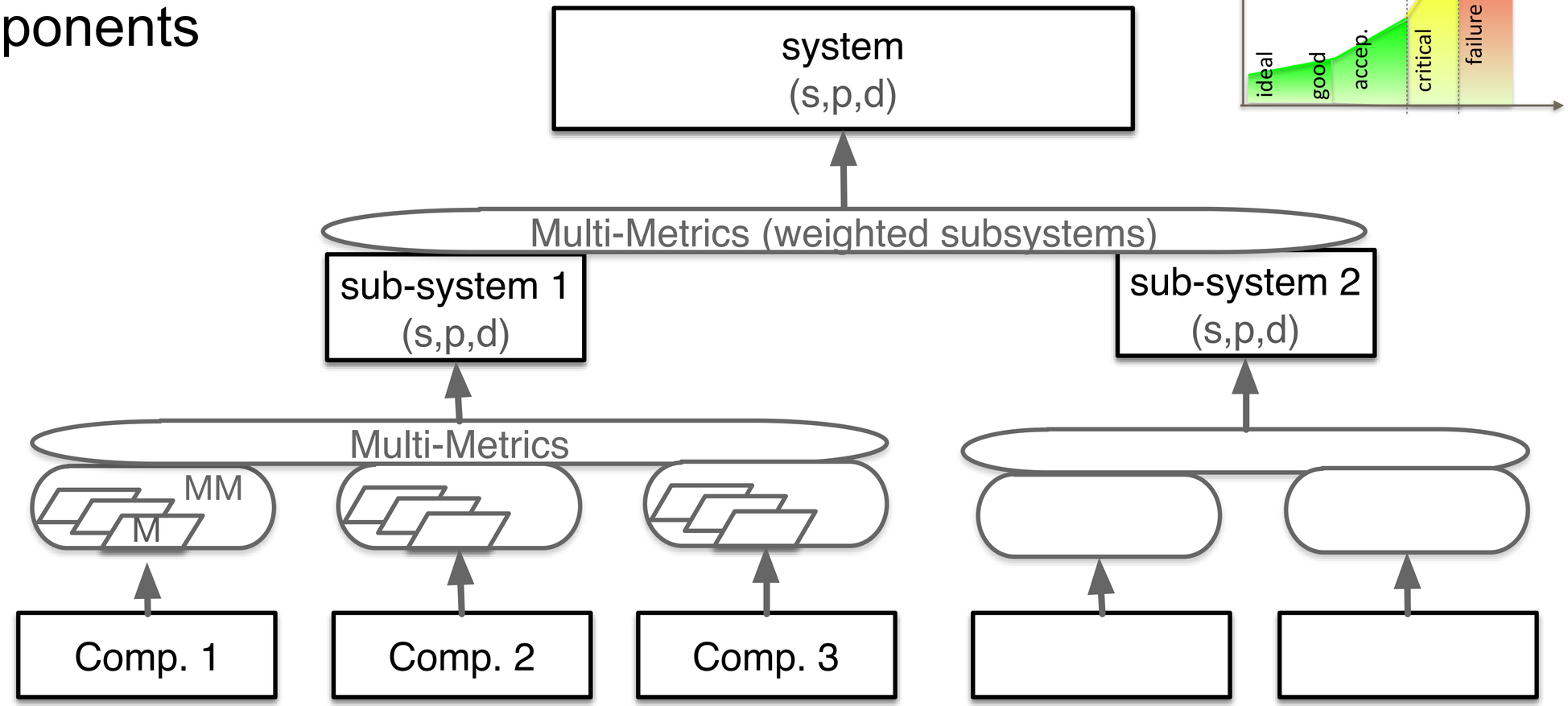
SPD level	SPD vs SPD_{Goal}
(67,61,47)	(●,●,●)
(67,61,47)	(●,●,●)
(31,33,63)	(●,●,●)

Example of Research:

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

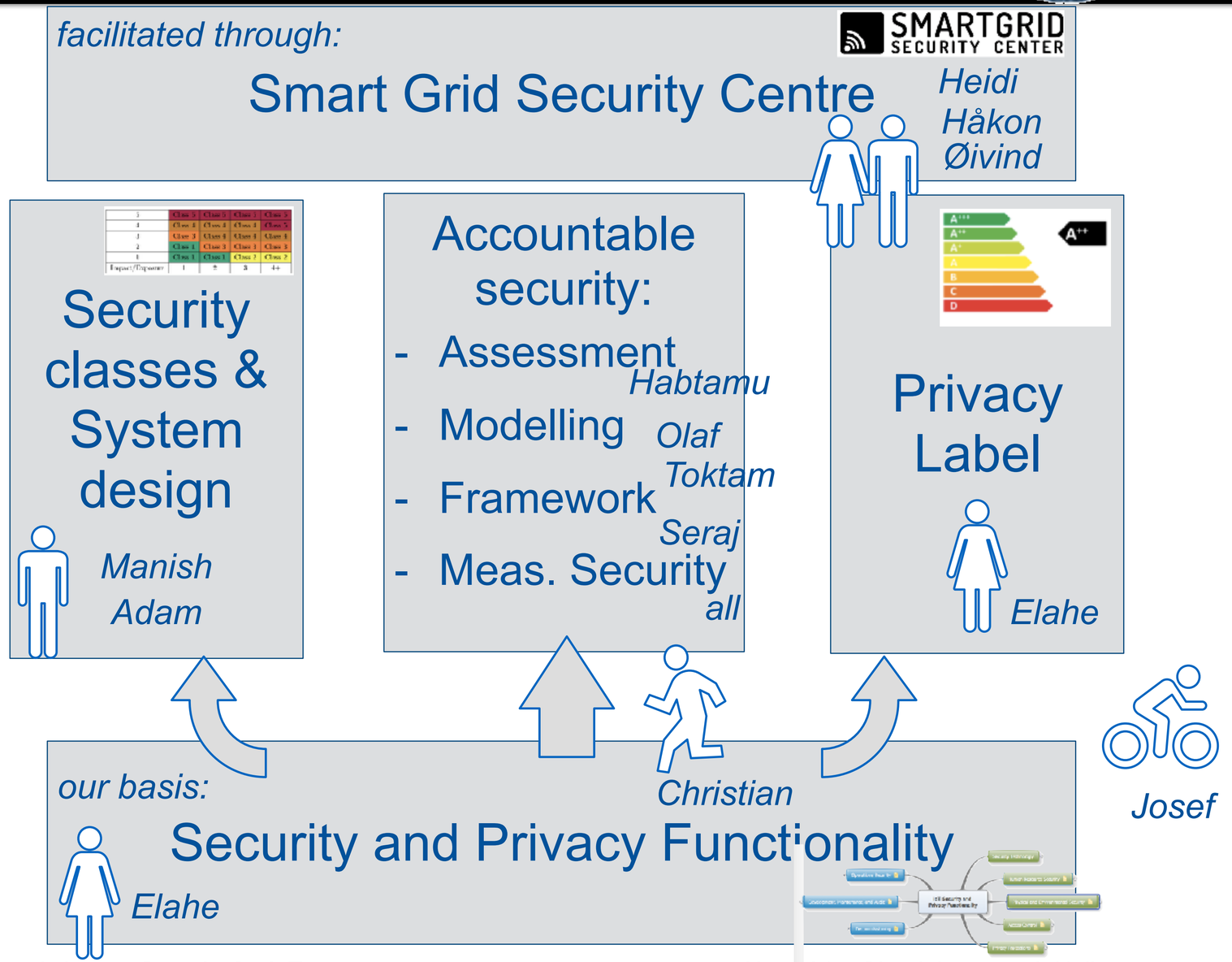
- System consists of sub-systems consists of components
  - security
  - privacy
  - dependability



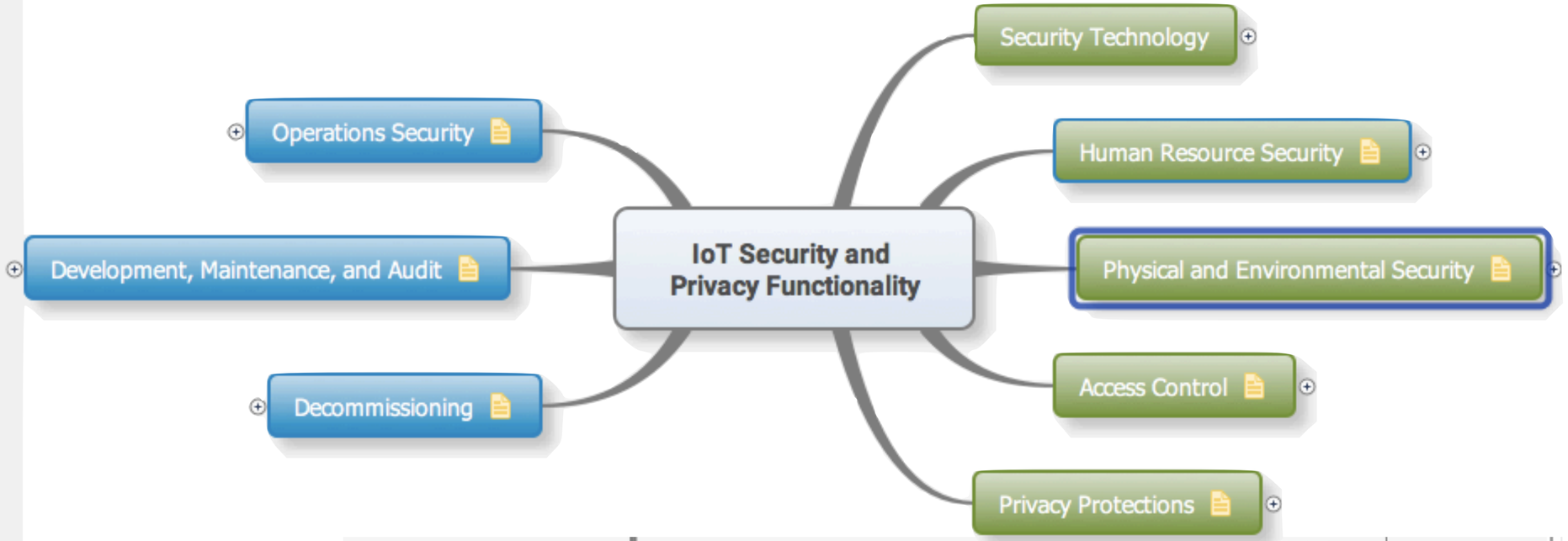


High level view of Security in IoT

- Goal
- Provide the means for IoT security
  - ➡ from todays attack to tomorrows design
  - ➡ security thinking in organisations
- Trust in Things
  - ➡ Privacy label
- Smart Grid Security Centre



Security and Privacy Functionality



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

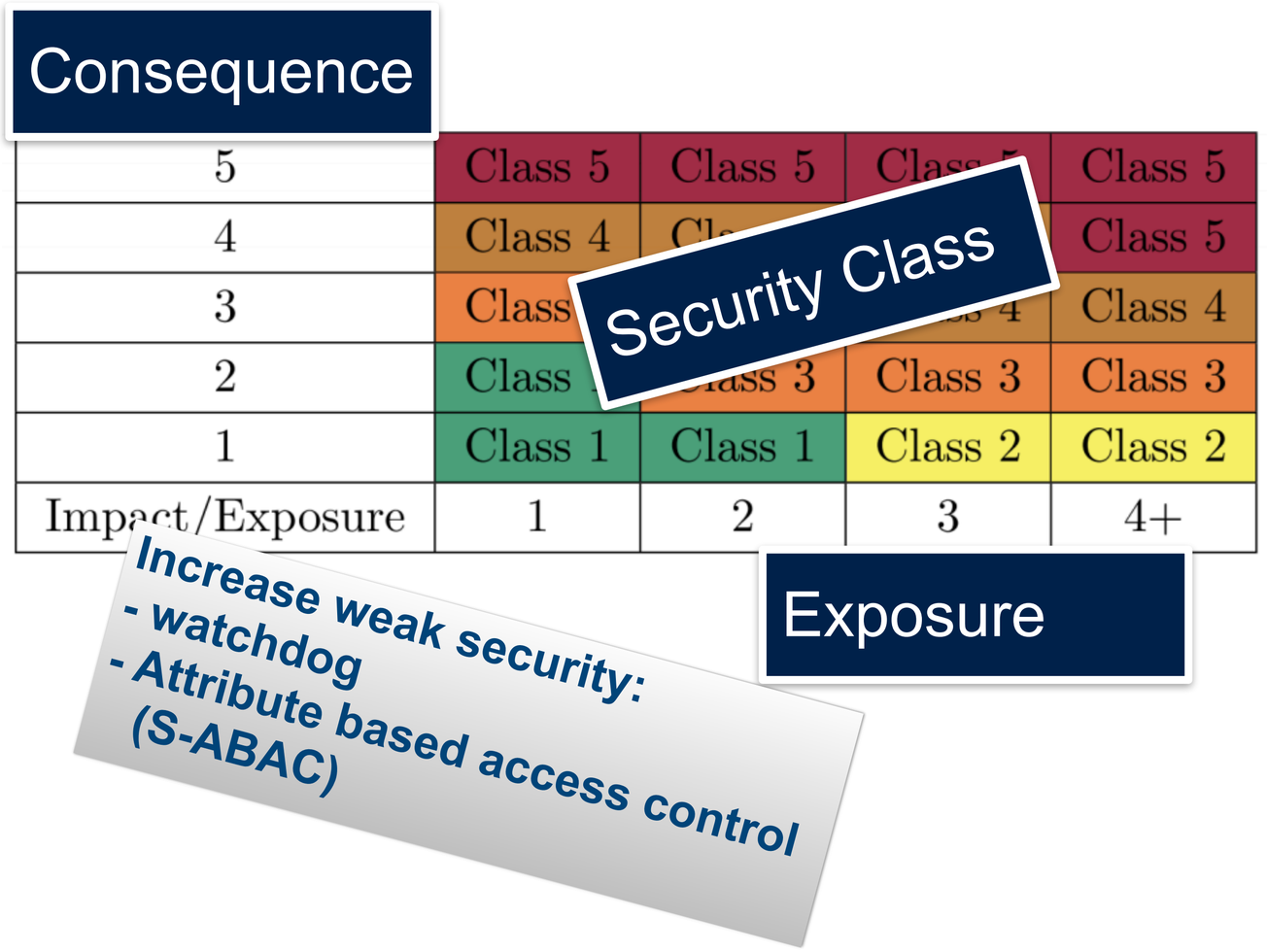
Industrial Internet of Things Volume G4: Security Framework, 2016

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

Security Classes and System design

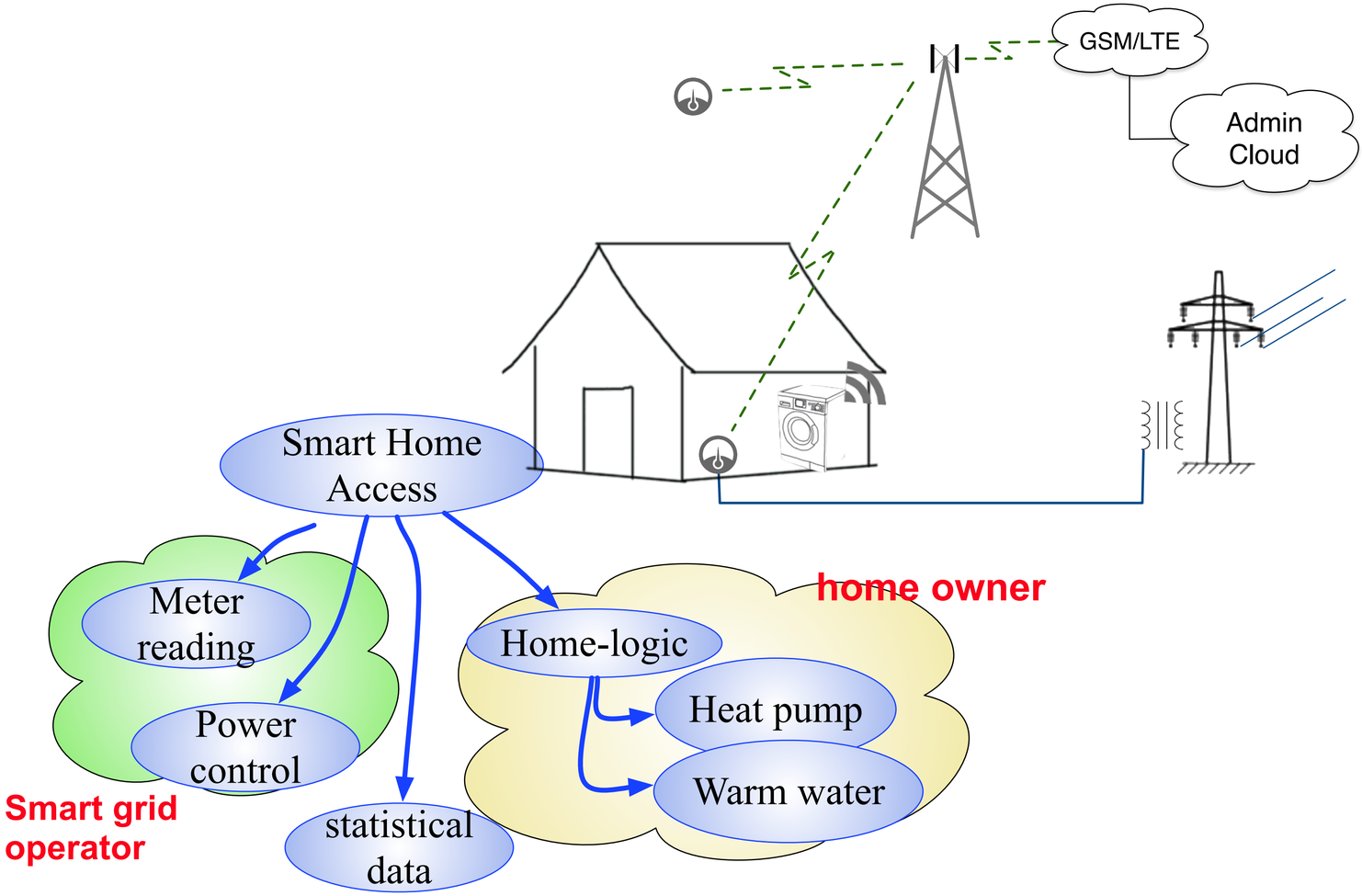
- Security Classes in IoT
  - ➡ Consequence
  - ➡ Exposure
- Consequence
  - ➡ as in risk map
- Exposure
  - ➡ Physical exposure
    - people, building, physical ports,…
  - ➡ IT exposure
    - ports, firewall, connectivity
- Used to assess the security class of Systems, sub-systems and components

New postulate of security class



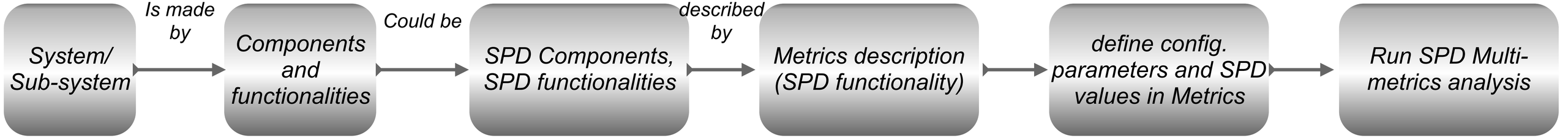
Semantic attribute based access control (S-ABAC)

- 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, ...

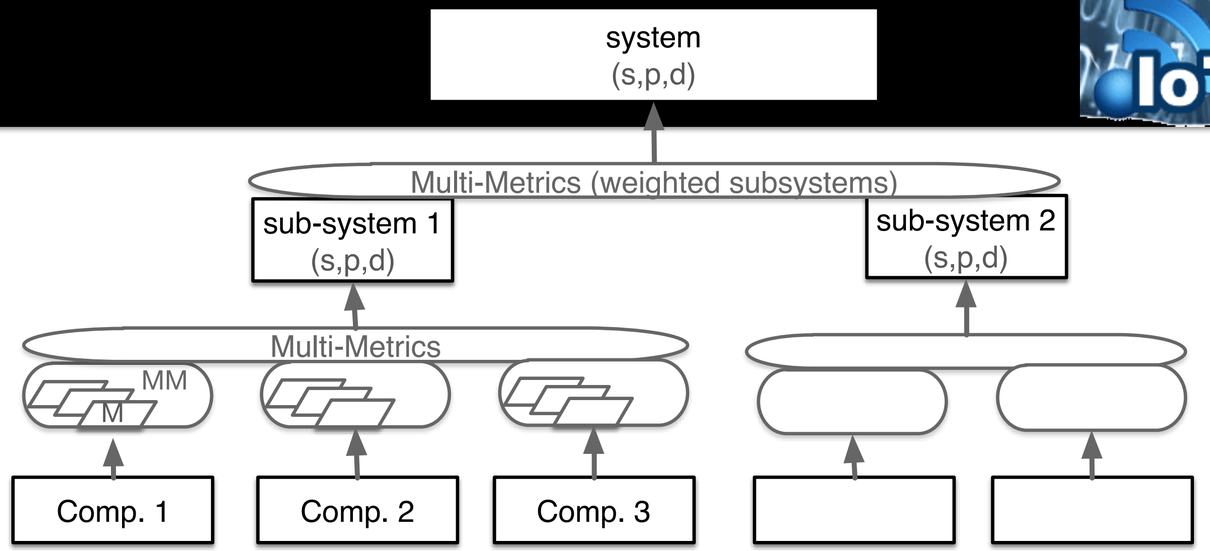
Methodology:
From System description to SPD level

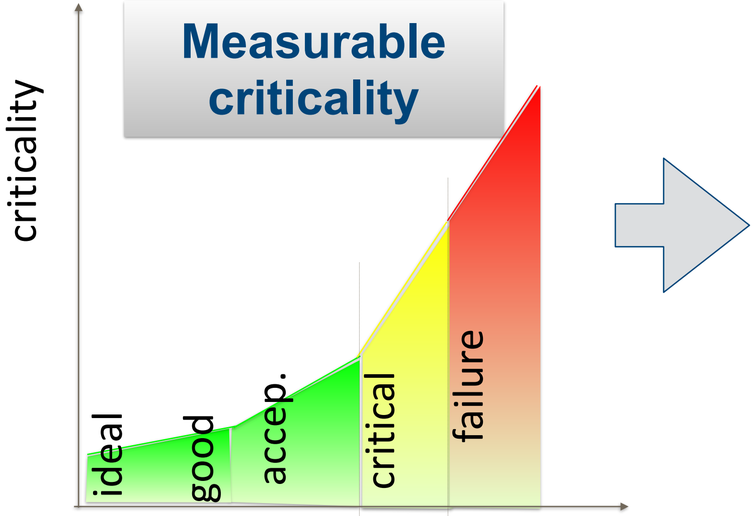


- System: Automatic Meter System (AMS) consists of reader (AMR), aggregator, communications, storage, user access
- Sub-systems: AMR consists of power monitor, processing unit, communication unit
- Component: AMR communication contains of a baseband processing, antenna, wireless link
- Configuration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

Accountable security

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

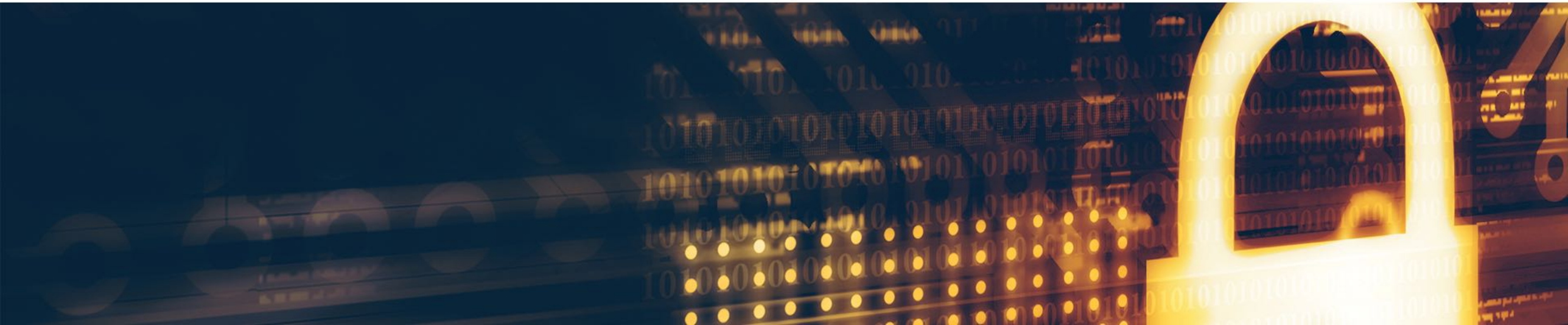




to measurable: security, privacy and dependability

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

SMARTGRID SECURITY CENTER



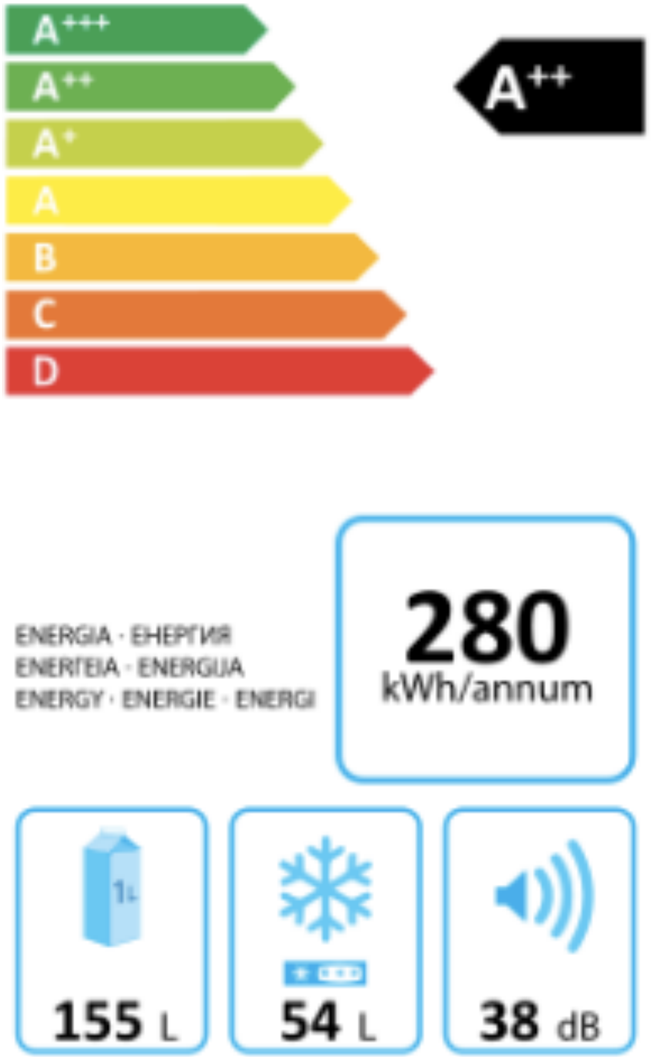
Mission Statement

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

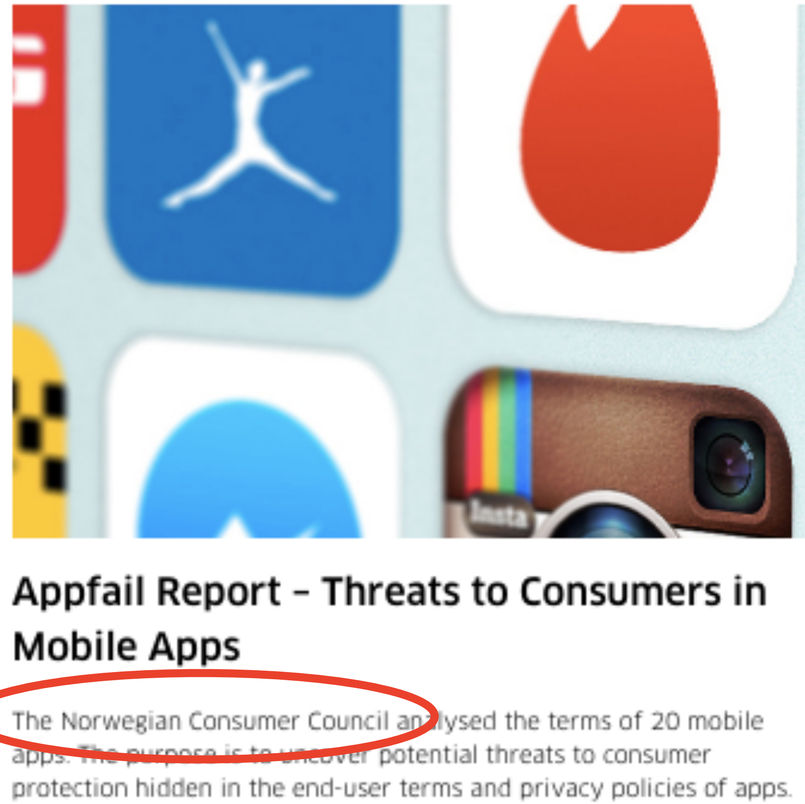
SMARTGRID
SECURITY CENTER

Privacy Labelling

http://PrivacyLabel.IoTSec.no



- "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.

Answer the Challenges a

D

DIGITALEUROPE's views on Cybersecurity Certification and Labelling Schemes

Brussels, 23 March 2017

RECENT EU PROPOSALS ON CYBERSECURITY CERTIFICATION AND LABELLING

In the course of 2016 the European Commission announced two initiatives for further assessment in the field of certification and labelling: 1) a security **certification framework for ICT products** and 2) a **"Trusted IoT label"** giving information about different levels of privacy and security and, where relevant, demonstrating compliance with the NIS Directive.

2. Trusted IoT Label

In its July 2016 Communication, the European Commission also brought forward the idea of a European label for trust/security of ICT products. This has since been further elaborated in policy discussions in the context of the Internet of Things ("IoT") and has been suggested as a potential item for a Trust in the Digital Single Market package in the Spring 2017.

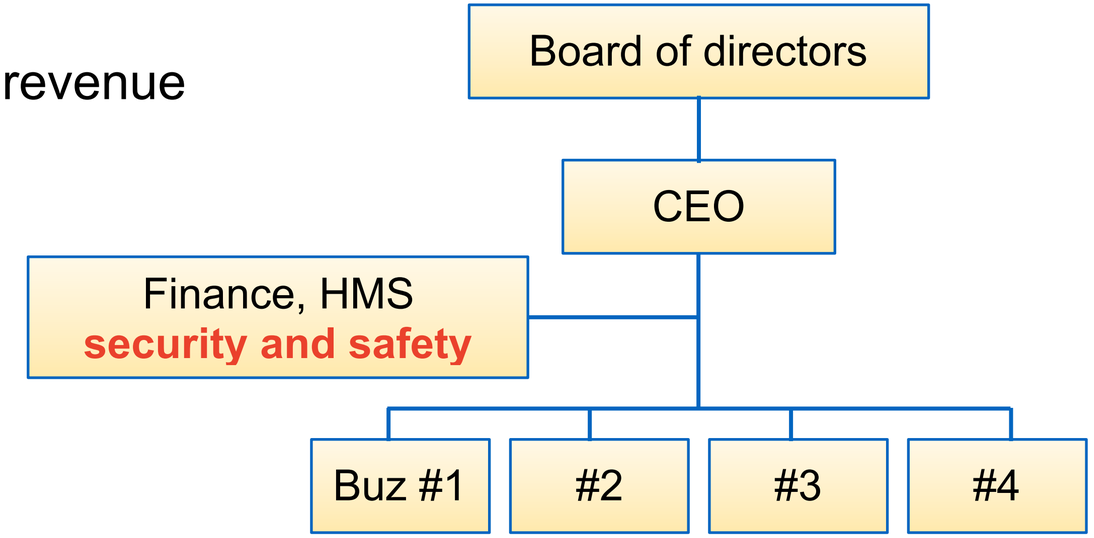
SCOTT contribution: privacy label?

Helse, Miljø og Sikkerhet

? *safety*

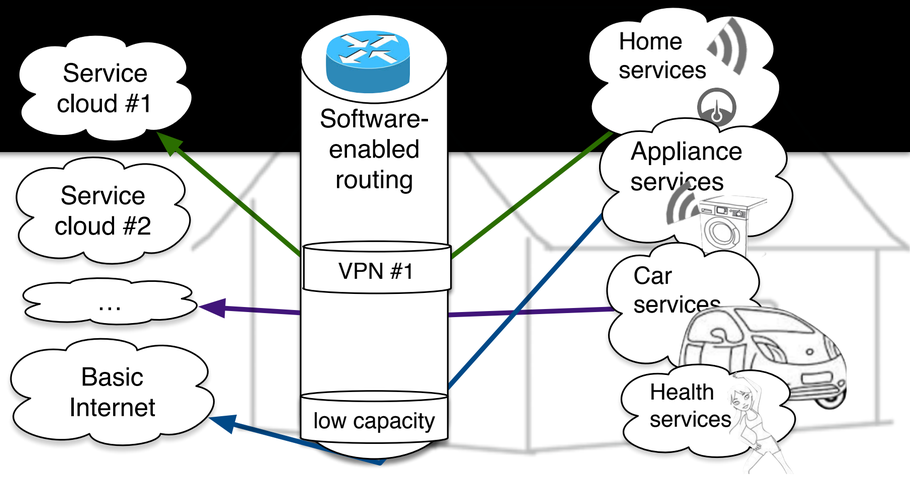
- Security affects safety
  - ➡ IoT attack -> car crashes
- Security affects core business
  - ➡ company confidential information
  - ➡ Customer information
    - Privacy regulative (GDPR May2018): 4% of revenue

➡IoT is corporate governance



Conclusions

- Things (IoT) are driving the digital societies
- IoT: Business merger
  - Internet + Semantics + Things = IoT
  - Digitisation of the Society
- IoT Security and privacy
  - new security paradigm
  - Security classes, accountable security
  - security and privacy ontology
- competitive advantage e.g.:
  - Privacy label (A++, A+…D)



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+