IoTSec Status Meeting, 20Nov2016, Halden

High level view on IoTSec

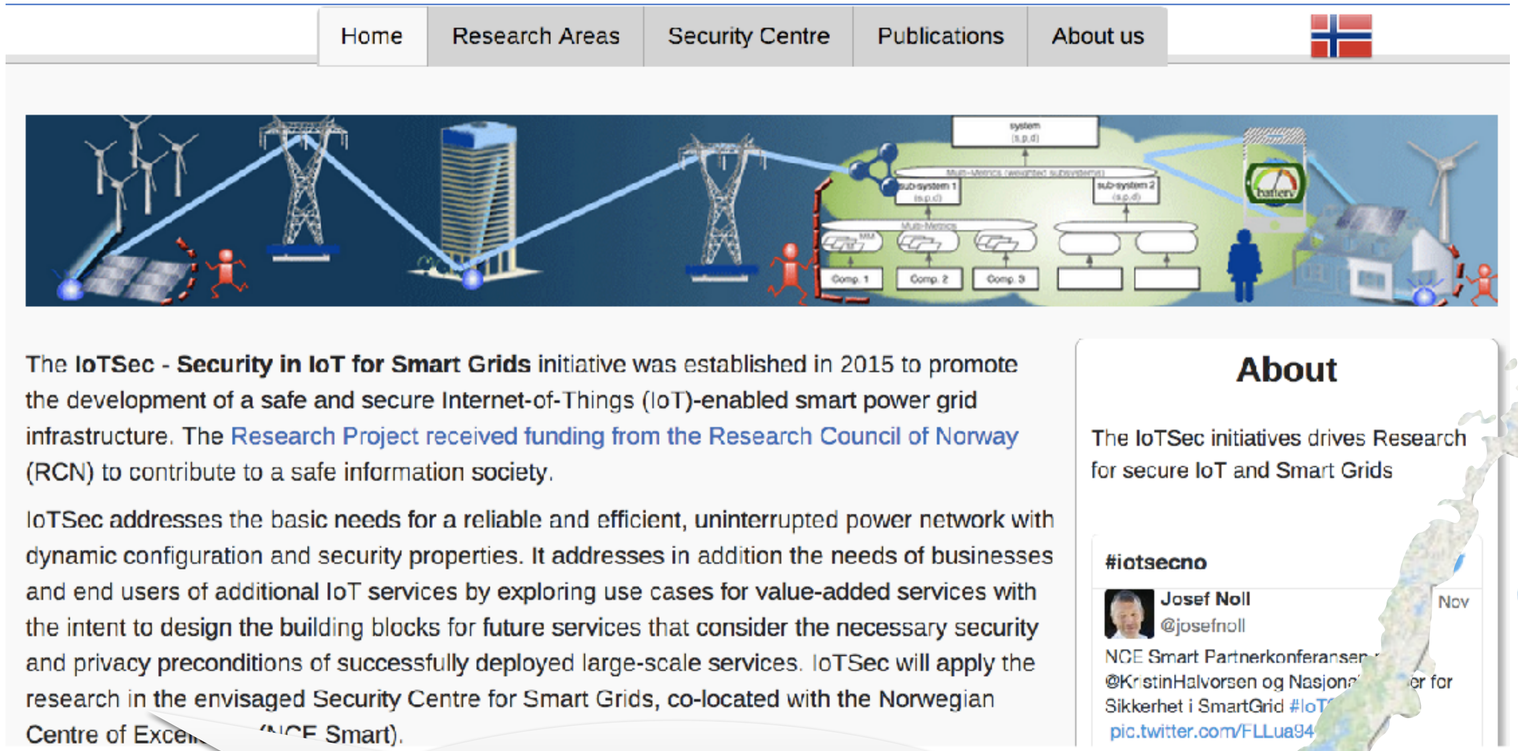
Christian Johansen
Ifi & ITS, UiO
christi@ifi.uio.no

Josef Noll
ITS, UiO
josef@unik.no

#IoTSec, #IoTSecNO

National initiative for a more secure future in IoT

IoTSec.no - Security for IoT for Smart Grid



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

Partners and Collaborations

Academia
- UiO
- UNIK
- NR
- Simula
- NTNU

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

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

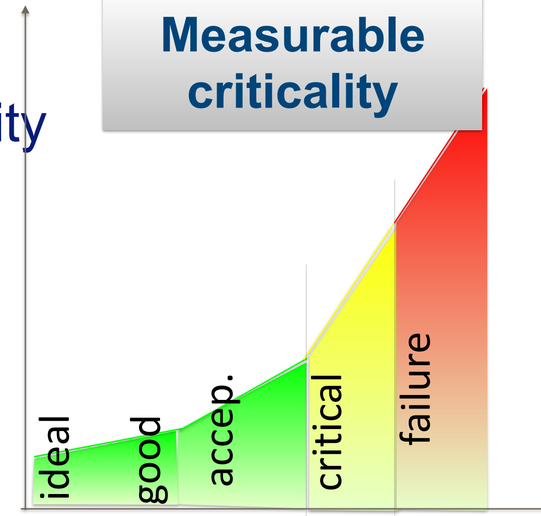
Industry
- EyeSaaS
- mnemonic

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

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

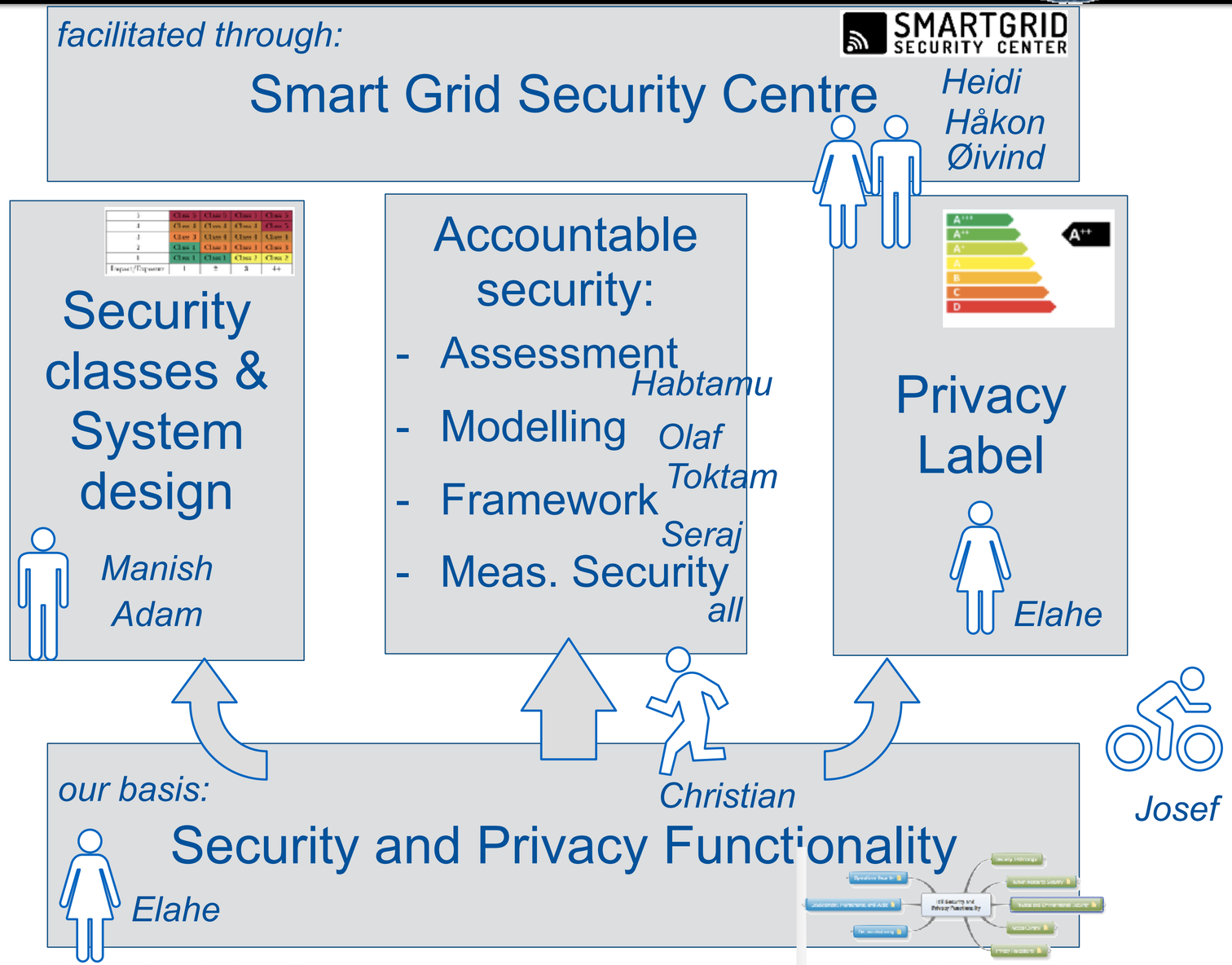


to measurable: security, privacy and dependability

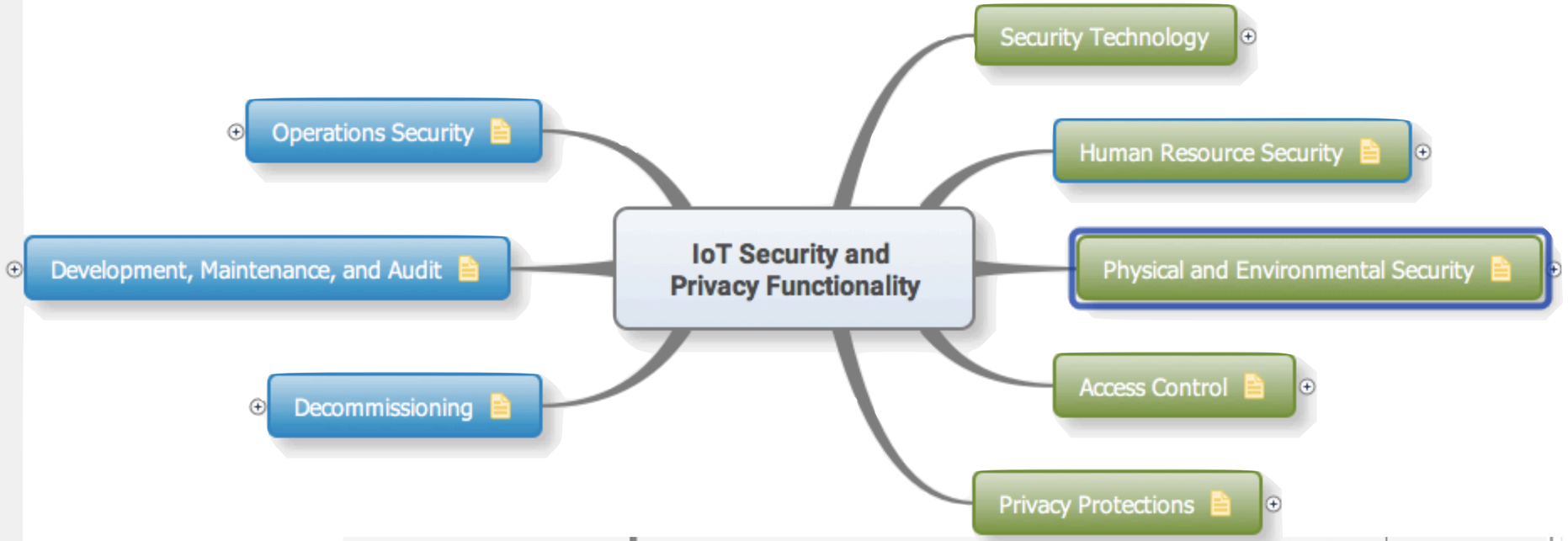
SPD level	SPD vs SPD_{Goal}
(67,61,47)	(●,●,●)
(67,61,47)	(●,●,●)
(31,33,63)	(●,●,●)

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

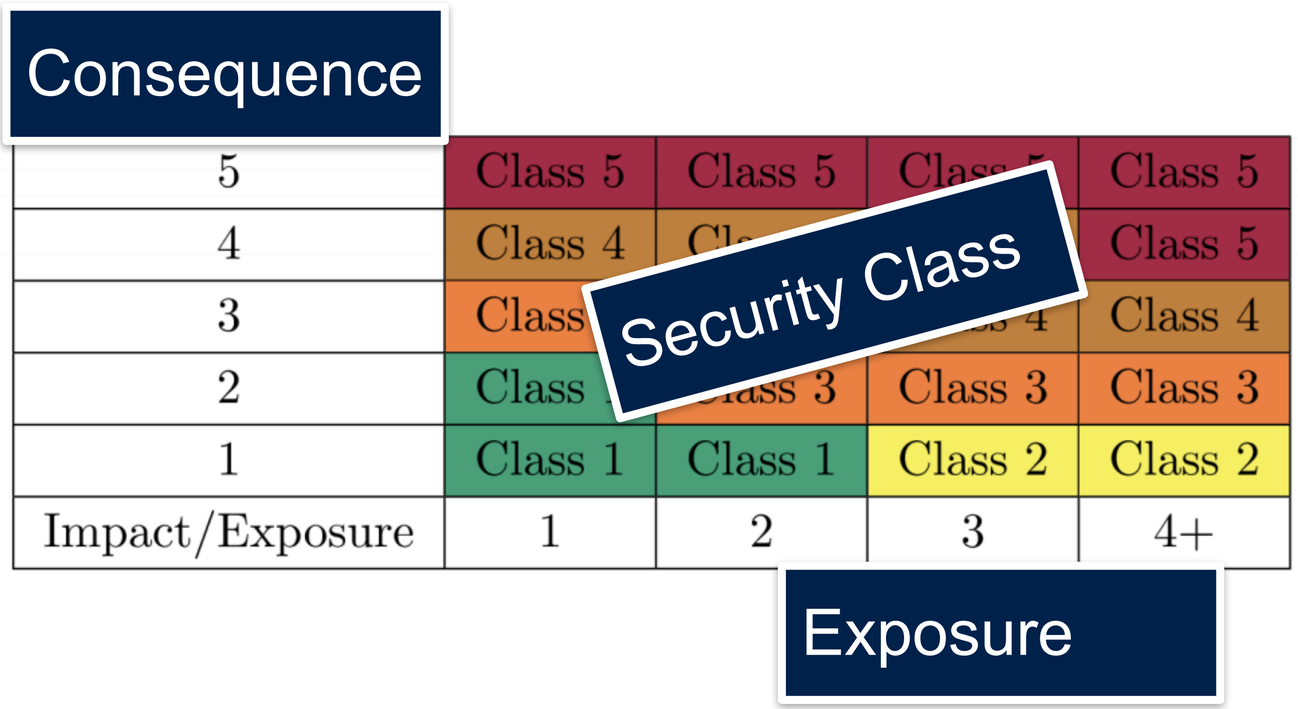
Industrial Internet of Things Volume G4: Security Framework, 2016

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

Security Classes and System design

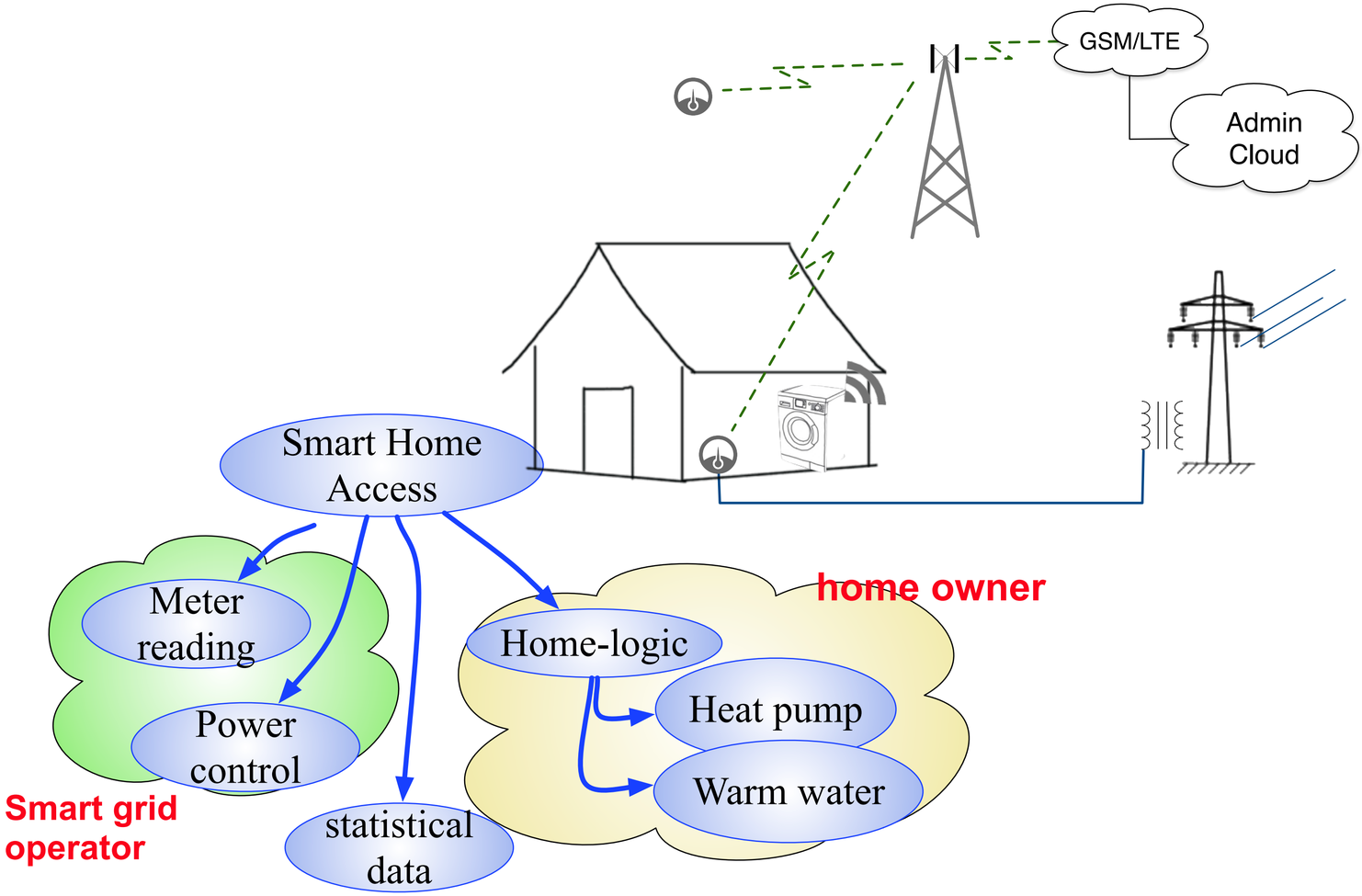
- Security Class in IoT
  - ➡ Consequence
  - ➡ Exposure
- Consequence
  - ➡ as in risk map
- Exposure
  - ➡ Physical exposure
    - people, building, physical ports,…
  - ➡ IT exposure
    - ports, firewall, connectivity
- Used to assess the security class of Systems, sub-systems and components

New postulate of security class



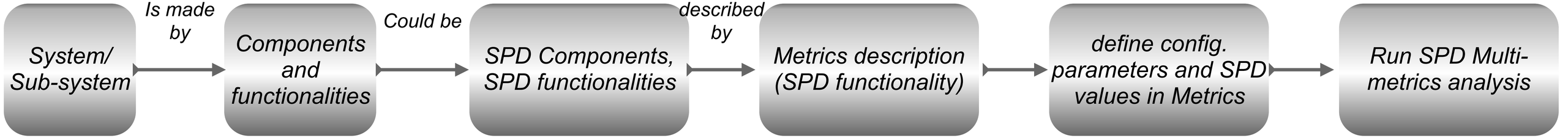
Semantic attribute based access control (S-ABAC)

- 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, ...

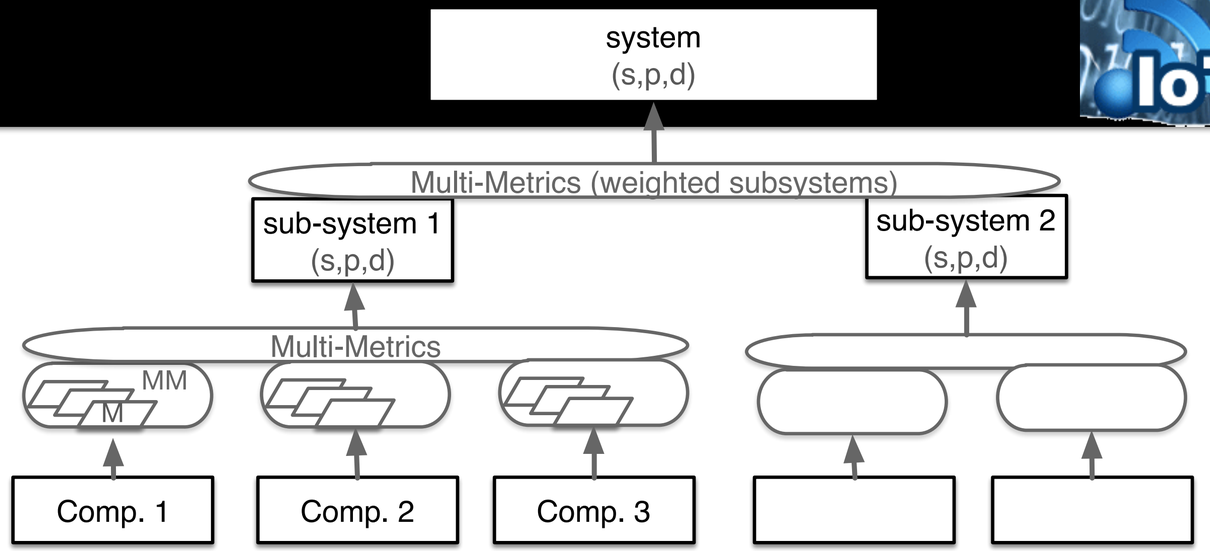
Methodology:
From System description to SPD level

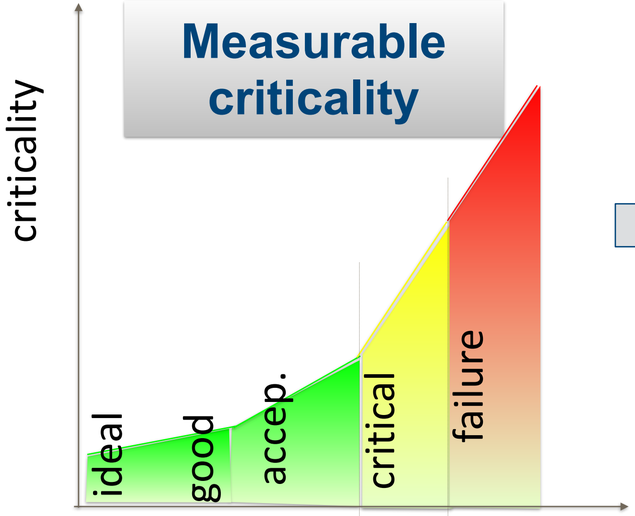


- System: Automatic Meter System (AMS) consists of reader (AMR), aggregator, communications, storage, user access
- Sub-systems: AMR consists of power monitor, processing unit, communication unit
- Component: AMR communication contains of a baseband processing, antenna, wireless link
- Configuration 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

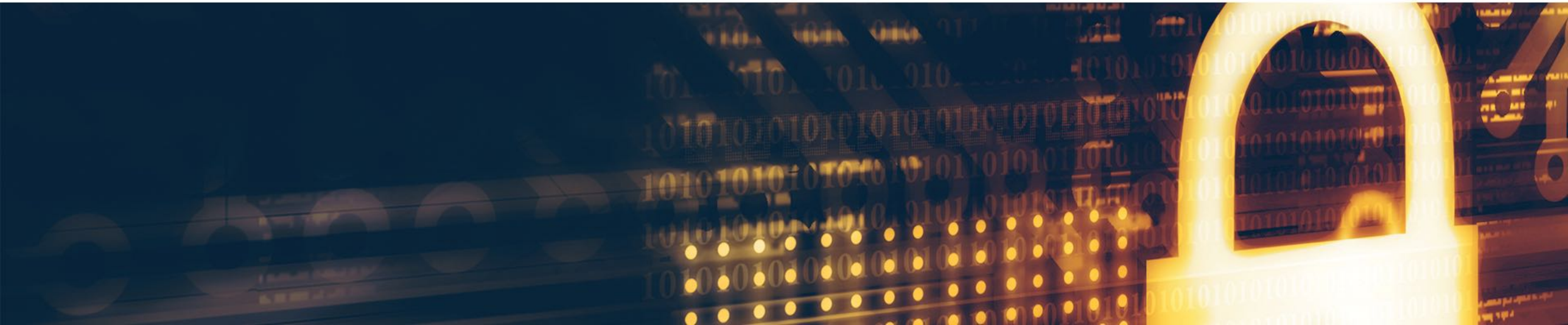




to measurable: security, privacy and dependability

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

SMARTGRID SECURITY CENTER



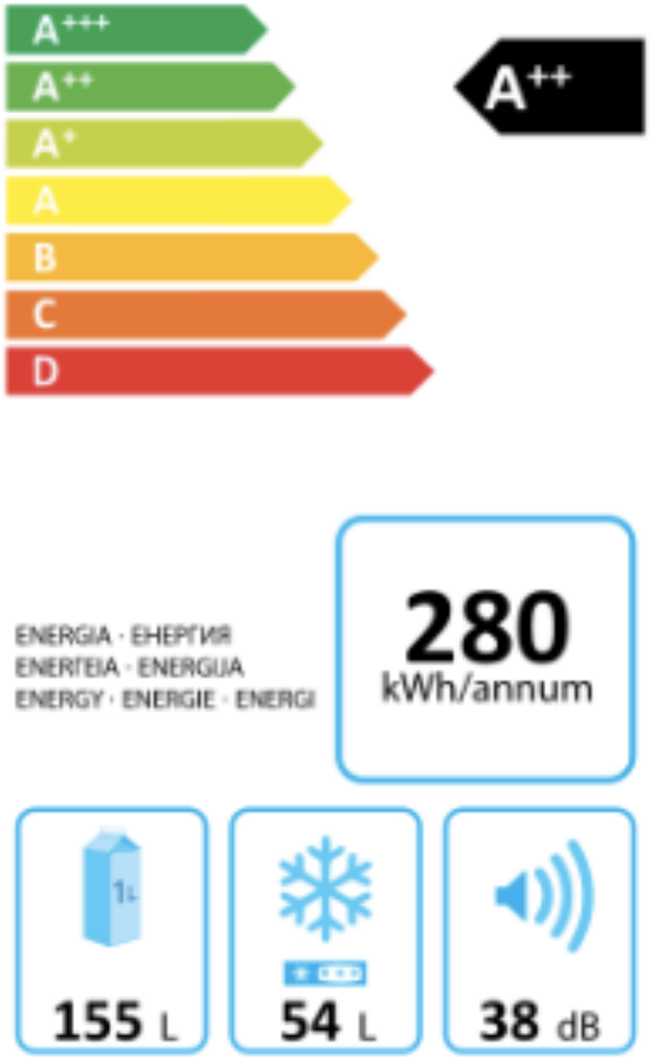
Mission Statement

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

In collaboration with Consumer Services (Forbrukerrådet)
- Paul Chaffey (Statssekretær) support
- Finn Myrstad (Forbrukerrådet) -> EU

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.

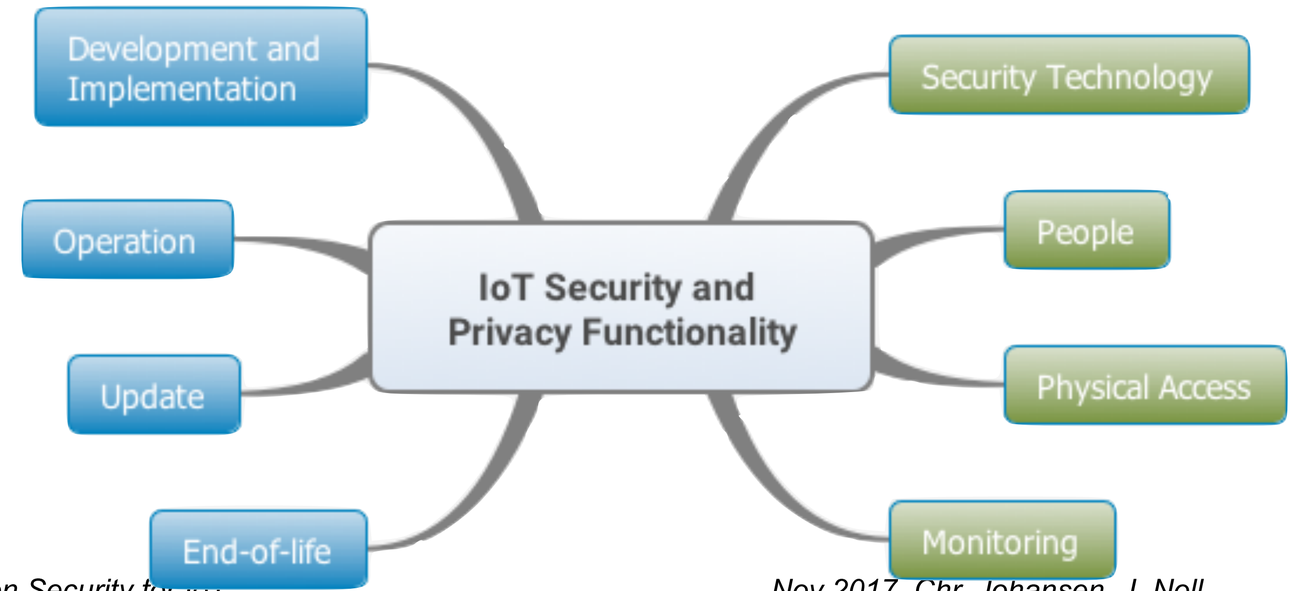
SCOTT contribution: privacy label?

IoTSec - Conclusions

- IoTSec from a helicopter perspective
  - ➡ overall vision broken down into activities
  - ➡ measurable achievements
- Example Smart Home
  - ➡ positive surveillance
  - ➡ privacy-aware
  - ➡ including neighbours, family, friends
- Impact
  - ➡ more secure IoT
    - security classes
    - security and privacy ontology
  - ➡ competitive advantage e.g.:
    - privacy label

New postulate of security class

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+



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”

Home About Visit esmartsystems.com

Prosumer bidding and scheduling in electricity markets

12. January 2016 Ukategorisert Administrator

[Source: eSmartSystems.com]