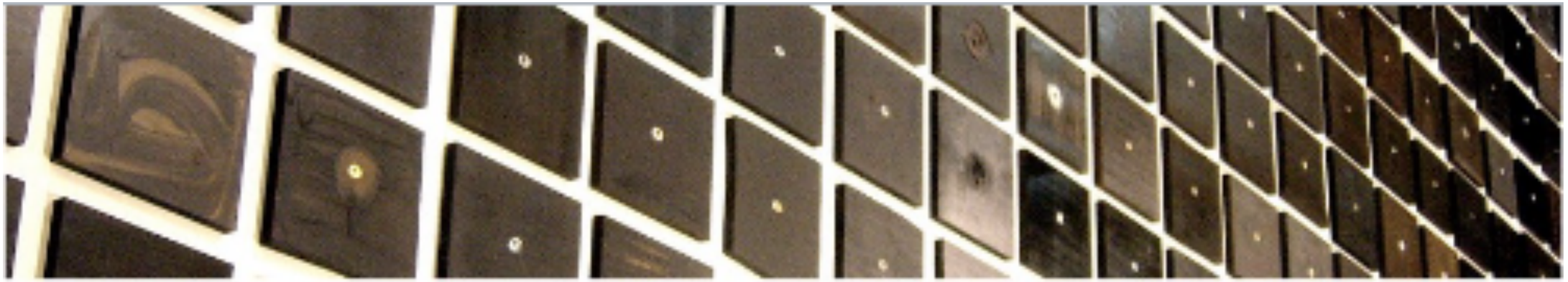


UiO : Universitetet i Oslo

Smartgridkonferansen 2016, 13-14Sep2016, Fornebu

Security and privacy-aware ecosystem for the Internet of Things in Smartgrids

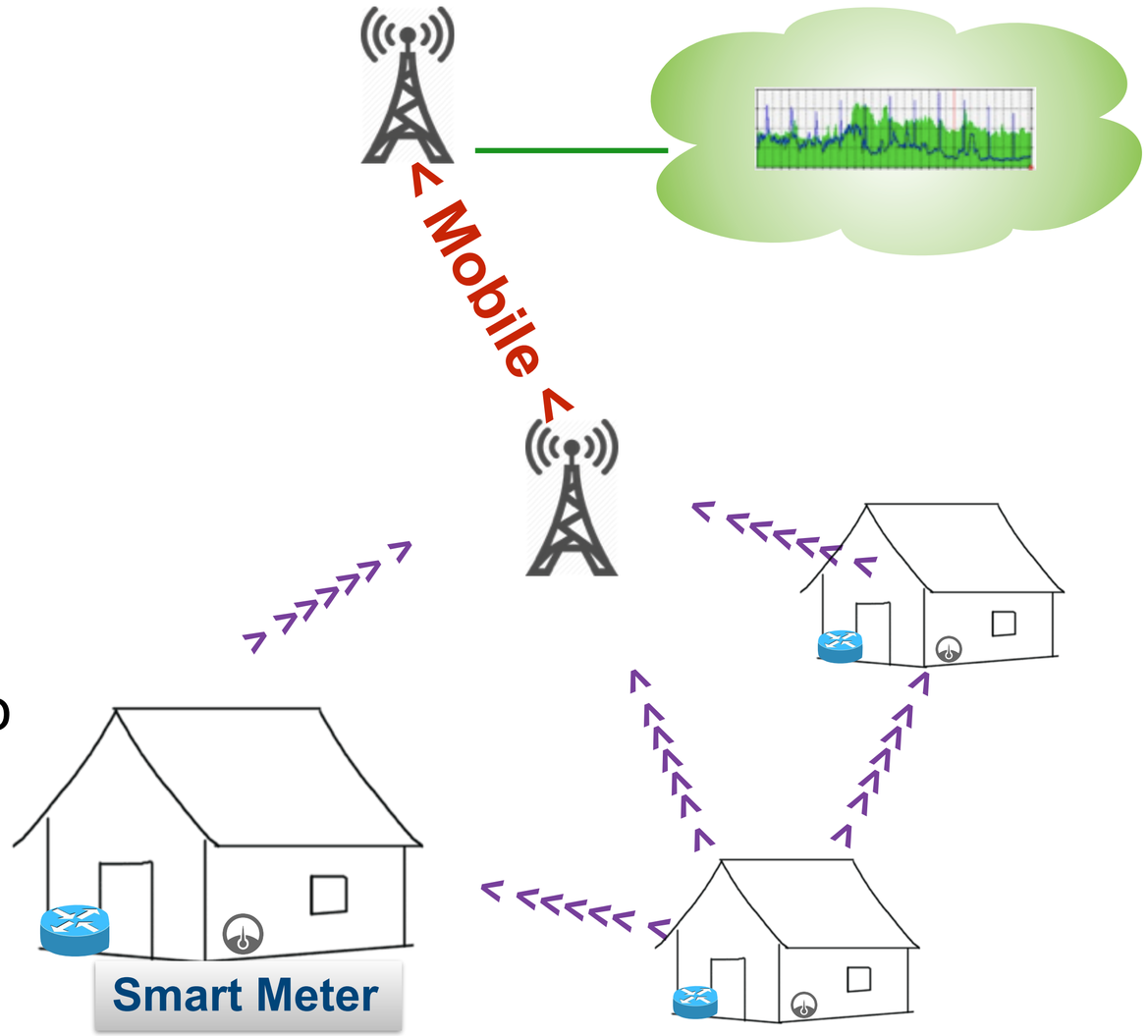
Josef Noll

Co Founder and Visionary at Basic Internet Foundation
Prof. at University Graduate Studies (UNIK), University of Oslo (UiO)
Head of Research at Movation AS
Norway

"Our Journey of Today"

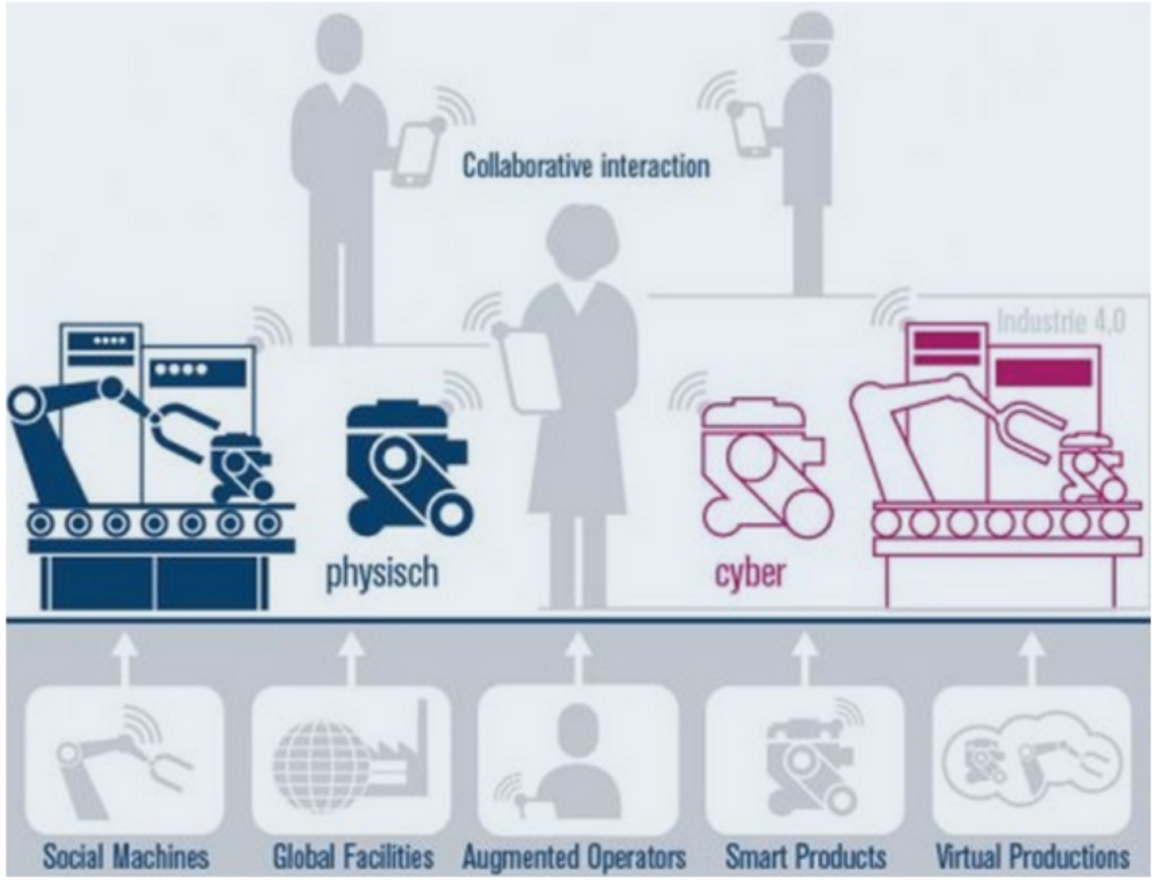
- Digitalisation of the Society
  - IoT, Big Data, Analytics
  - The Internet of Things (IoT) challenges
- Smart Grid, Smart Homes, Smart Infrastructures
  - Scalability in IoT
  - Measurable Security & Privacy - IoTSec.no
  - Logic, Cloud,
- "*Some meat for discussion*"

  Privacy labelling



Background: Digitalisation of Industry

- EU has introduced[1] Industrie4.0
  - digital innovation hubs,
  - leadership in digital platforms,
  - closing the digital divide gap
  - providing framework conditions
- Norwegian Government has established[2] "Klyngene som omstillingsmotorer" (Sep2015)
  - NCE Smart Energy Markets on "**Digitalisation of Industry**"
  - NCE Systems Engineering på Kongsberg og NCE Raufoss on Productivity and Innovation



Source: Trumpf / Forschungsunion Wirtschaft & Wissenschaft

[1] http://europa.eu/rapid/press-release_SPEECH-15-4772_en.htm

[2] http://abelia.no/innovasjon/klyngene-skal-omstille-norge-article3563-135.html Sec.no

Future Smart Grid operation, § 4-2 functional requirements

"Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv."

1. Store measured values, registration frequency max 60 min, can configure to min 15 min.
2. **Standardised interface (API) for communication with external equipment using open standards**
3. Can connect to and communicate with other type of measurement units
4. Ensures that stored data are not lost in case of power failure
5. **Can stop and reduce power consumption in every measurement point** (exception transformator)
6. Can send and receive information on electricity prices and tariffs. Can transmit steering information and ground faults
7. Can provide security against miss-use of data and non-wished access to control-functions
8. Register flow of active and re-active power flow in both directions

§ 4-2. *Funksjonskrav*

AMS skal:

a) lagre måleverdier med en registreringsfrekvens på maksimalt 60 minutter, og kunne stilles om til en registreringsfrekvens på minimum 15 minutter,

b) ha et standardisert grensesnitt som legger til rette for kommunikasjon med eksternt utstyr basert på åpne standarder,

c) kunne tilknyttes og kommunisere med andre typer målere,

d) sikre at lagrede data ikke går tapt ved spenningsavbrudd,

e) kunne bryte og begrense effektuttaket i det enkelte målepunkt, unntatt trafomålte anlegg,

f) kunne sende og motta informasjon om kraftpriser og tariffer samt kunne overføre styrings- og jordfeilsignal,

g) gi sikkerhet mot misbruk av data og uønsket tilgang til styrefunksjoner og

h) registrere flyt av aktiv og reaktiv effekt i begge retninger.

Norges vassdrags- og energidirektorat kan etter søknad i særlige tilfeller gi dispensasjon fra enkelte funksjonskrav.

0 Tilføyd ved forskrift 16 jan 2012 nr. 75 (i kraft 20 jan 2012).

https://lovdata.no/dokument/SF/forskrift/1999-03-11-301

Mobile Security => IoT Security

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

So lässt sich das UMTS-Netz knacken

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

[source:

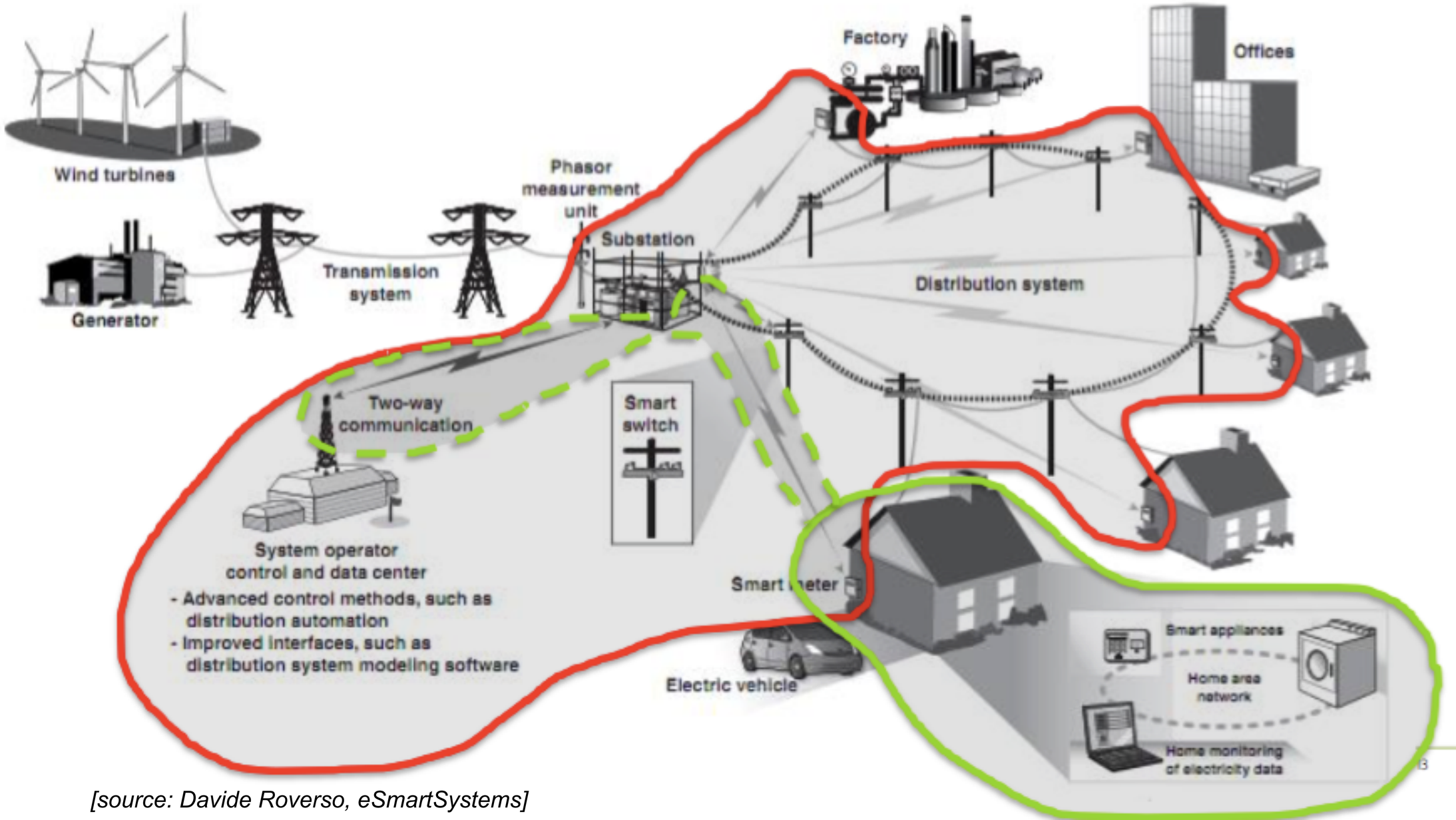
www.aftenposten.no

Hard kritikk mot justisministeren i mobilspionasje-saken:

-Dette er forklaringer som ikke holder vann

LES OGSÅ: Spionjegere avfeier Anundsens nye mobilforklaring

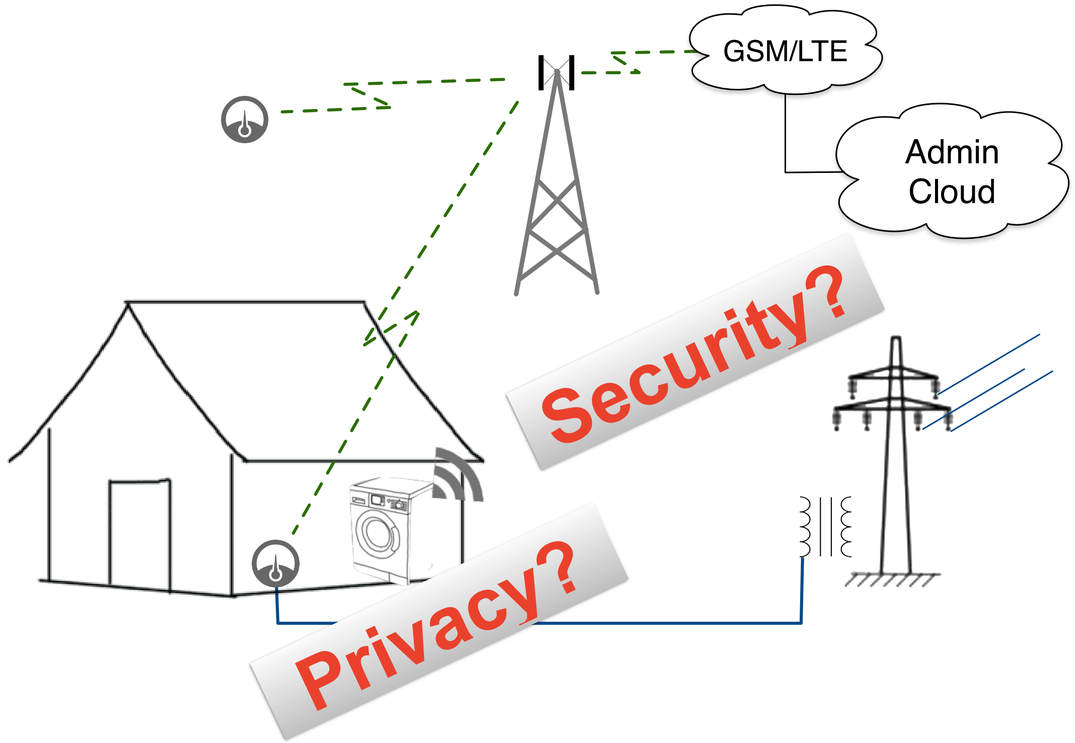
Smart Home vs Smart (Distribution) Grid focus



[source: Davide Roverso, eSmartSystems]

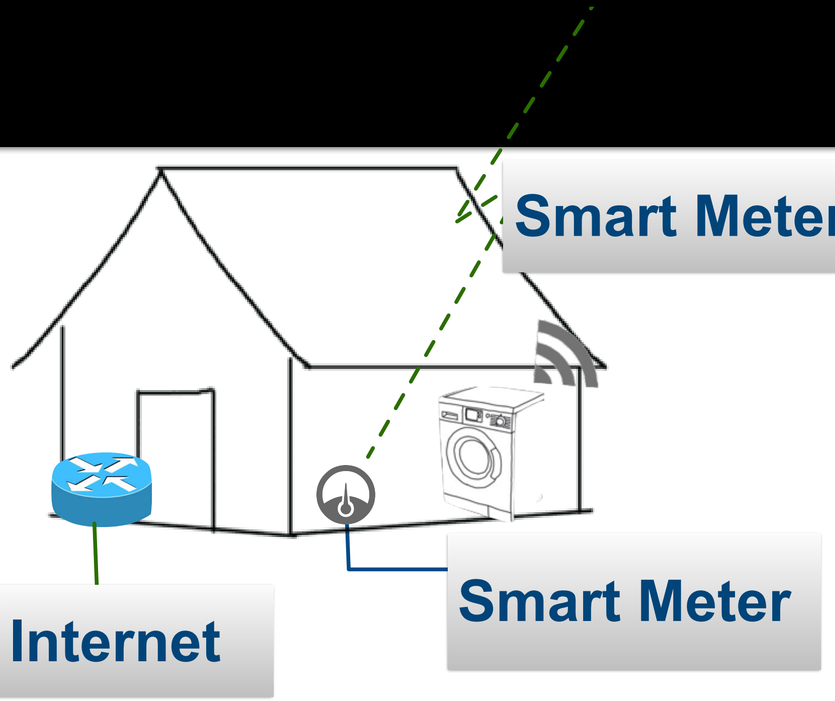
Ecosystem - Application Scenarios for Smart Meters

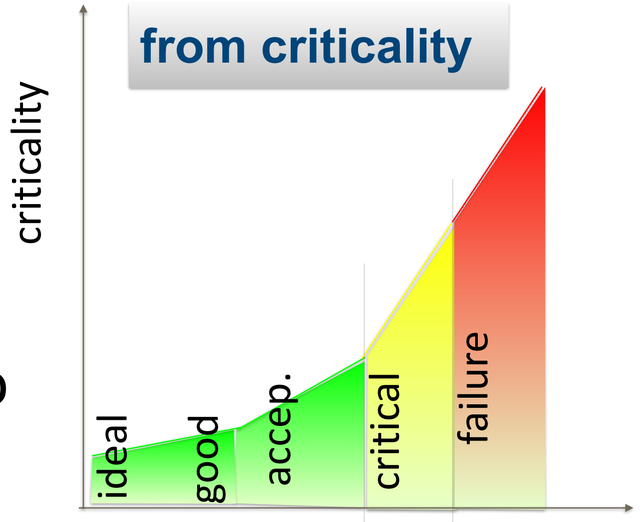
- Monitoring the grid to achieve a grid stability of at least 99,96%,
- Alarm functionality, addressing
  - ➡ failure of components in the grid,
  - ➡ alarms related to the Smart Home, e.g. burglary, fire, or water leakage,
- Intrusion detection, monitoring both hacking attempts to the home as well as 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”



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

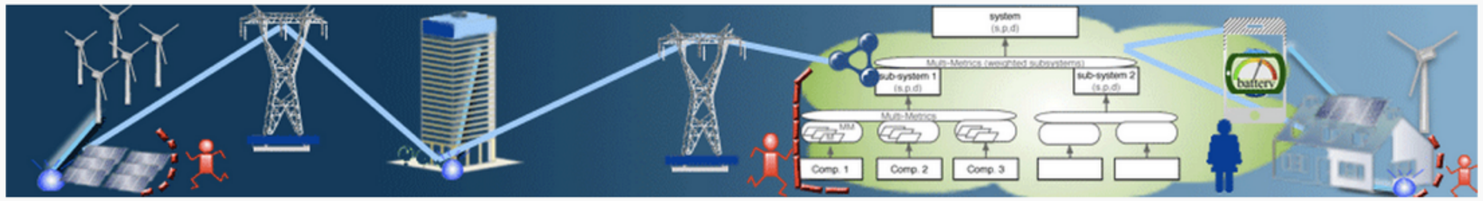
SPD level	SPD vs SPD_{Goal}
(67,61,47)	(●,●,●)
(67,61,47)	(●,●,●)
(31,33,63)	(●,●,●)

UiO : Department of Informatics
The Faculty of Mathematics and Natural Sciences

National initiative for a more secure future in IoT

IoTSec.no - Security for IoT for Smart Grids

Home | Research Areas | Security Centre | Publications | About us



The **IoTSec - Security in IoT for Smart Grids** initiative was established in 2015 to promote the development of a safe and secure Internet-of-Things (IoT)-enabled smart power grid infrastructure. The Research Project received funding from the Research Council of Norway (RCN) to contribute to a safe information society.

IoTSec addresses the basic needs for a reliable and efficient, uninterrupted power network with dynamic configuration and security properties. It addresses in addition the needs of businesses and end users of additional IoT services by exploring use cases for value-added services with the intent to design the building blocks for future services that consider the necessary security and privacy preconditions of successfully deployed large-scale services. IoTSec will apply the research in the envisaged Security Centre for Smart Grids, co-located with the Norwegian Centre of Excel… (NCE Smart).

About

The IoTSec initiatives drives Research for secure IoT and Smart Grids

#iotsecno

Josef Noll @josefnoll Nov

NCE Smart Partnerkonferanse… @KristinHalvorsen og Nasjona… …er for Sikkerhet i SmartGrid #IoT… pic.twitter.com/FLLua94…

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

Partners and Collaborations

Academia
- UiO
- UNIK
- NR
- Simula
- NTNU

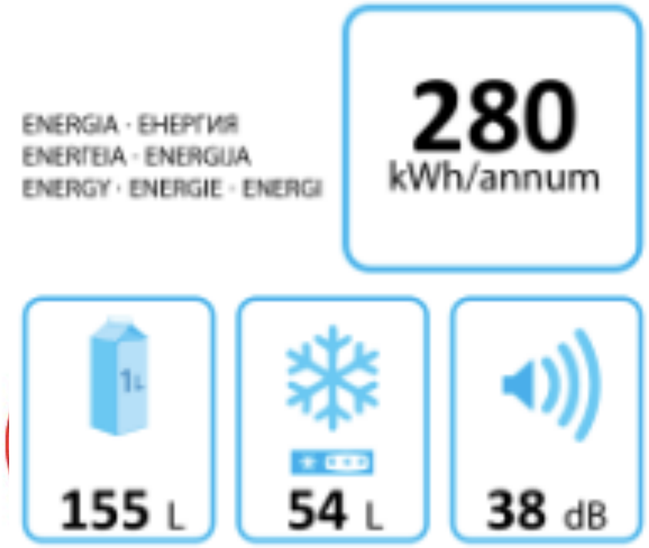
Industry
- Smart Innovation Østfold
- eSmart Systems
- Fredrikstad Energi
- EB Nett
- Movation

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

Towards Measurable Privacy - Privacy Labelling



- "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

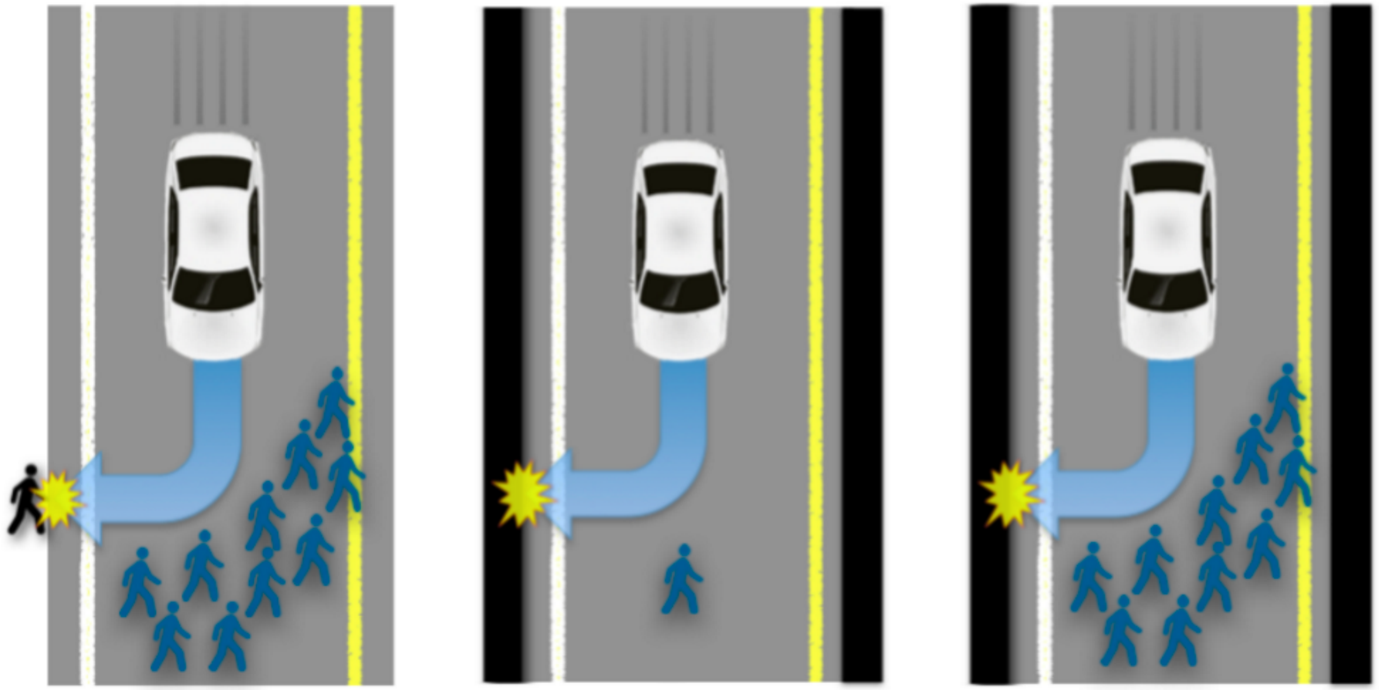
The Norwegian Consumer Council analysed the terms of 20 mobile apps. The purpose is to uncover potential threats to consumer protection hidden in the end-user terms and privacy policies of apps.

IoT challenges - “programmed to kill”

Why Self-Driving Cars Must Be Programmed to Kill

Self-driving cars are already cruising the streets. But before they can become widespread, carmakers must solve an impossible ethical dilemma of algorithmic morality.

October 22, 2015



https://www.technologyreview.com/s/542626/why-self-driving-cars-must-be-programmed-to-kill/

Change in Business Models due to IoT

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

Teri Robinson, Associate Editor

Follow @TeriRnNY

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

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

13 Oct 2015 at 06:04, OUT-LAW.COM

68 22 78

Volvo will "accept full liability" for collisions involving its autonomous vehicles, the company has confirmed.

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]

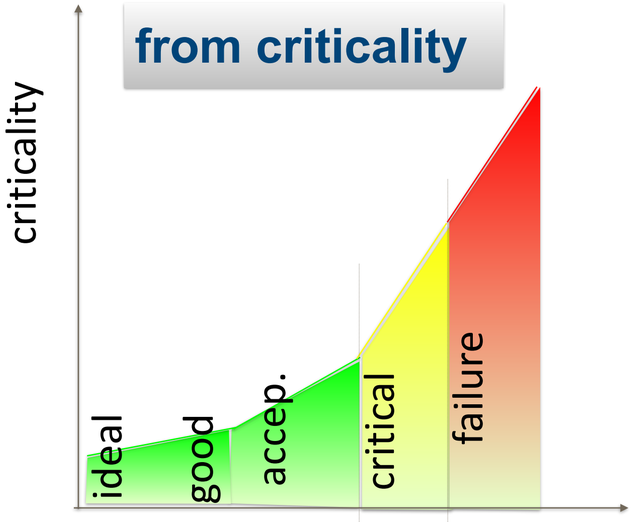
Conclusions

- Internet of Things (IoT) is a game changer
  - Everything is wireless: Smart Infrastructures
  - Autonomous systems, Critical Infrastructure
- 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
  - IoTSec.no - Security for Smart Grid
  - Industrial impact: Security Centre for Smart Grid
  - Privacy labelling for apps and devices

Innovation ecosystem for the IoT

Reducing the digital gap

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)	(●,●,●)