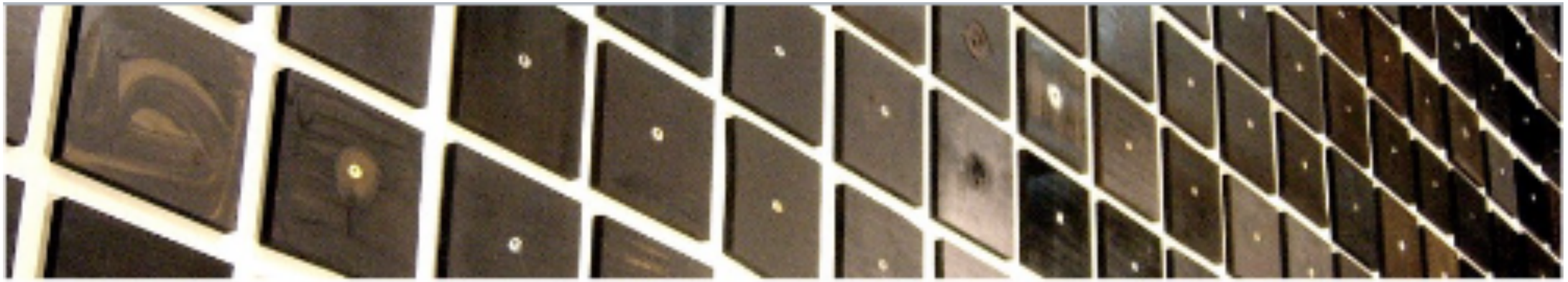


UiO : Universitetet i Oslo

Energi Norge, 18Nov2016

Security and Privacy in Energy

Josef Noll,
Prof. at University of Oslo/UNIK
Project leader IoTSec.no
josef@jnoll.net

DNV report 2013, DNV GL report 2014

Technology Outlook 2020 / Transformative Technologies

- Technology applications in Maritime, Renewables & Electricity, Health Care, Oil & Gas and Food & Water industries
  - ➡ sensors will drive automated data management
  - ➡ from passive data to automated decisions
  - ➡ **automated decision tools by 2020**

- Maritime: «policy driven»
- Health care: «trust» on sensor and mobile apps

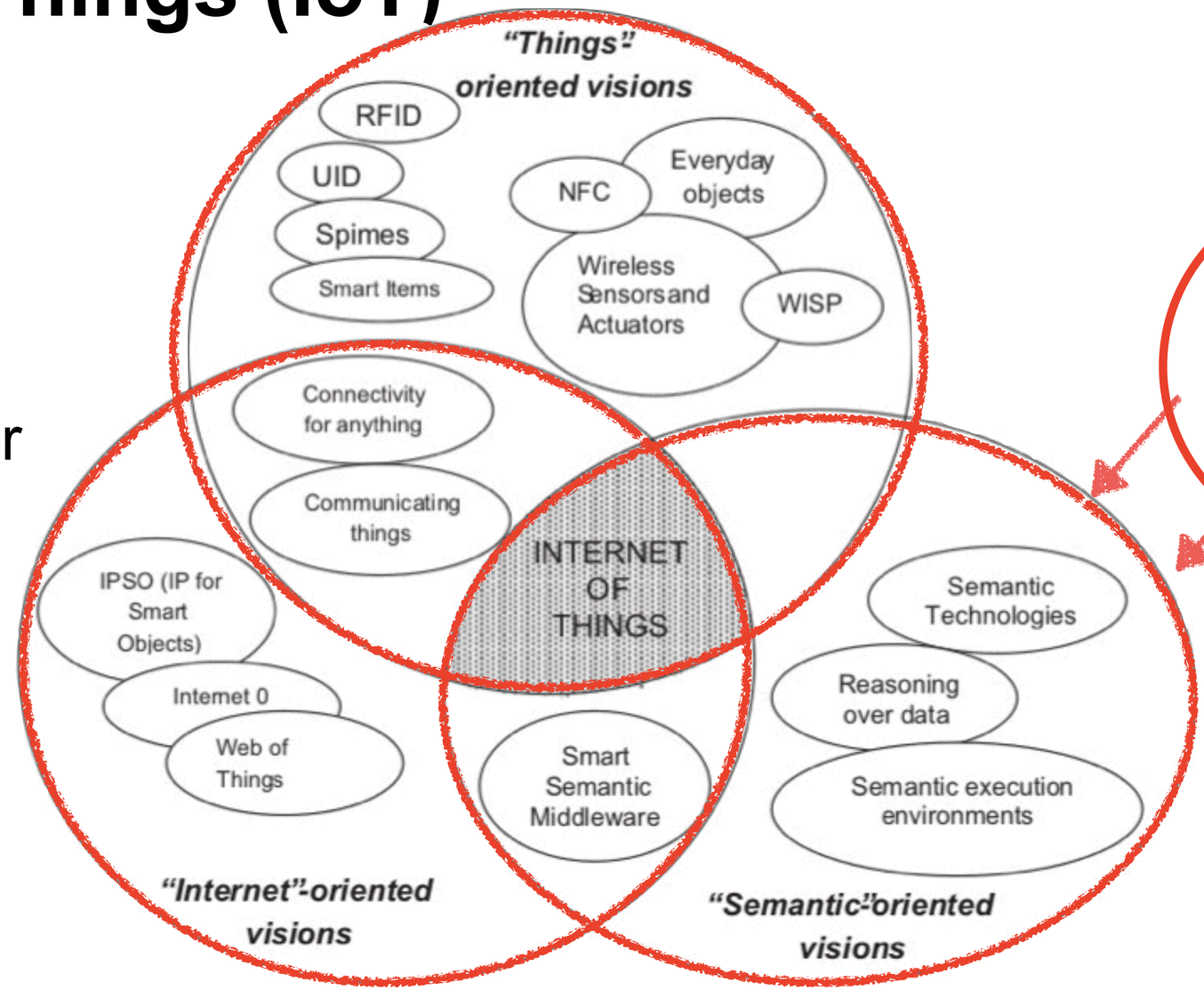
"Only 59% of the public trust the energy industry," (Edelman Trust Barometer 2013)

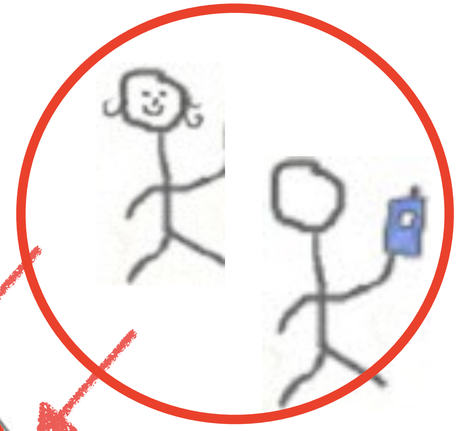
"In any change management process, the challenge is communicating risk," (Peter Bjerager, DNV GL)

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
- 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. The "Internet of Things" paradigm as a result of the convergence of different visions.

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.

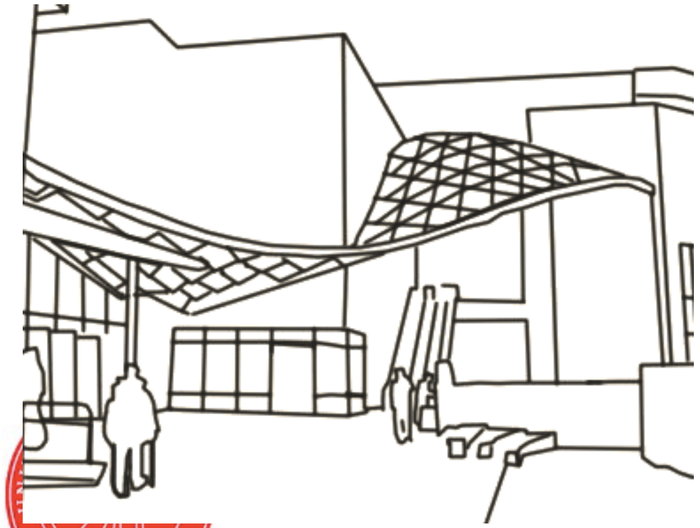
Digitalisation of the Society

Source: EU commission,
https://www.youtube.com/watch?v=BK-UuUnQaIM&feature=youtu.be

Addressing the challenges of IoT connectivity

Device ownership

- who owns the device
- which data are going to whom
  - ➡ maintenance

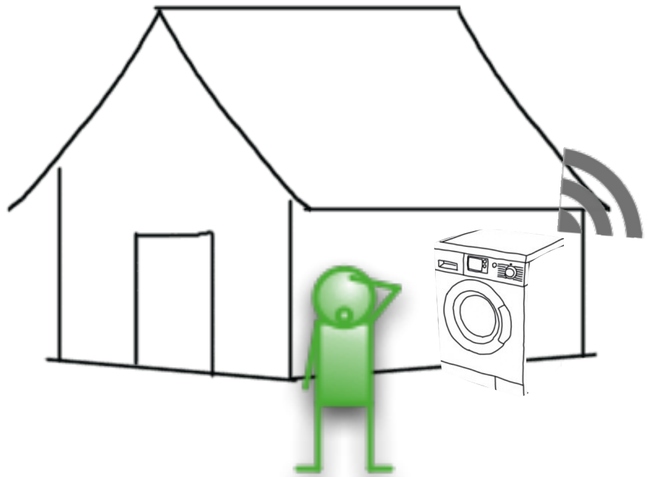


Easyness Setup

- 1. step ownership
- take control

Scalability

- business model for SIM/device not scalable
- free wireless for IoT data



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.rediff.com]

www.aftenposten.no

Hard kritikk mot justisministeren i mobilspionasje-saken:

- Dette er forklaringer som ikke holder vann

LES OGSÅ: Spionjegere avfeier Anundsens nye mobilforklaring

IoT Security - IoTSec.no

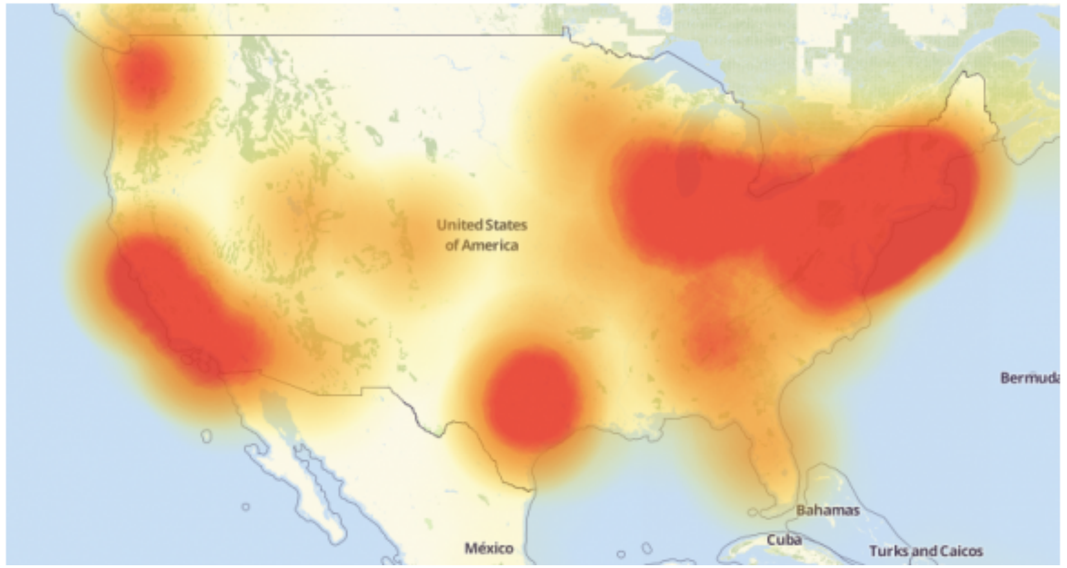
- First massive attack from IoT devices
  - 16Oct2016 IoT botnet attack on Dyn
  - Camera (CCTV), video recorder, TV,…
- Norway: Only one project on IoT Security
  - IoTSec.no - Focus on Research
  - Outcome: Smart Grid Security Centre (SGSC)
- Academic research versus industrial viewpoint
  - “language missmatch”
  - Academic: long term, open available information, e.g. Smart Home focus
  - Industry: current challenges, e.g. focus on grid

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

OCT 16

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.

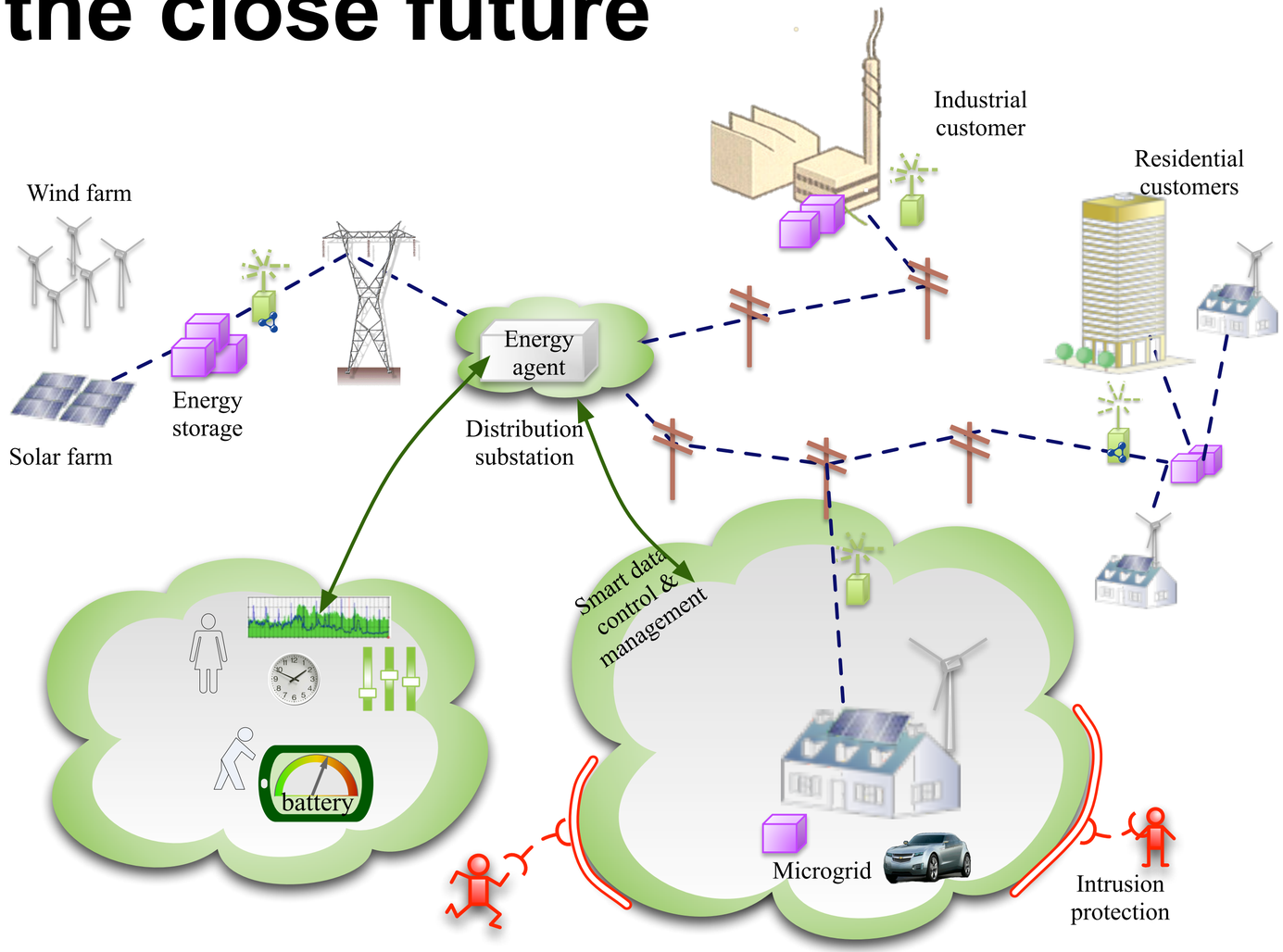
Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet’s top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.



[Source: https://krebsonsecurity.com/2016

The Smart Grid in the close future

- Smart grid with prosumers
  - ➡ various control mechanisms
  - ➡ attack scenarios
  - ➡ critical infrastructure



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.

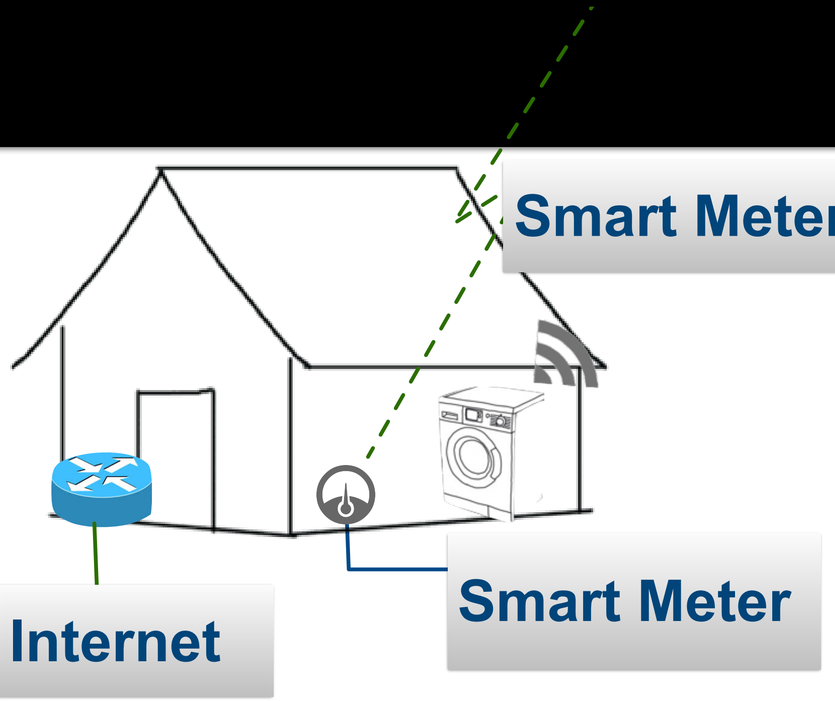
Norges vassdrags- og energidirektorat kan etter søknad i særlige tilfeller gi dispensasjon fra enkelte funksjonskrav.

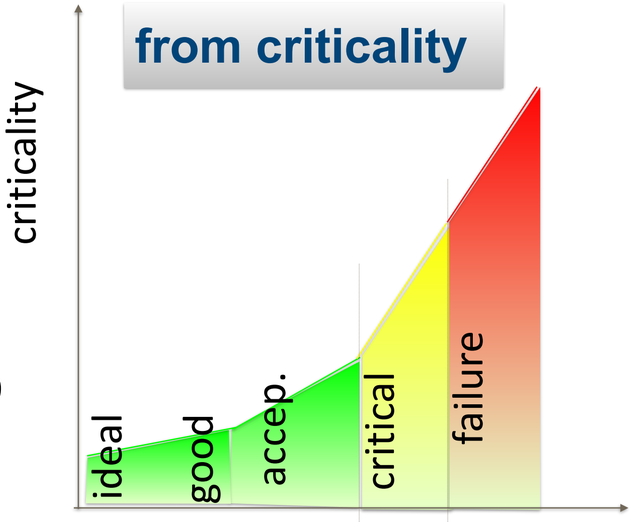
0 Tilføyd ved forskrift 16 jan 2012 nr. 75 (i kraft 20 jan 2012).

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

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

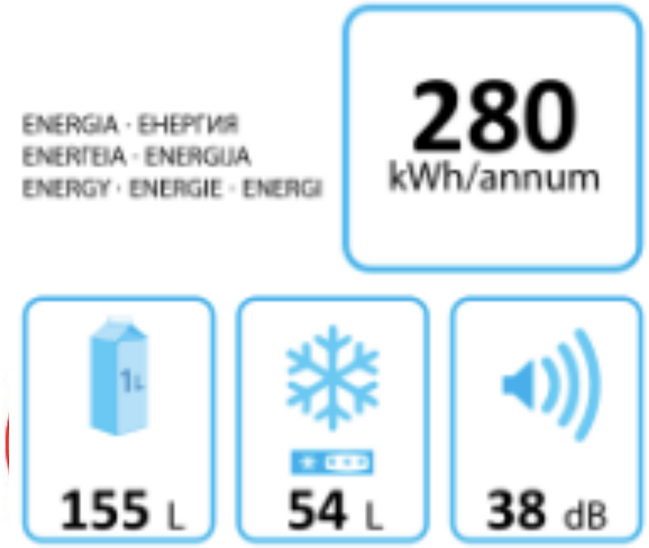




to measurable: security, privacy and dependability

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

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.

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

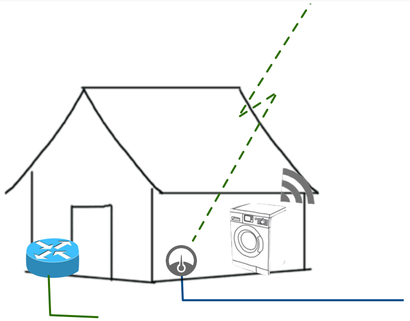
Prosumer bidding and scheduling in electricity markets

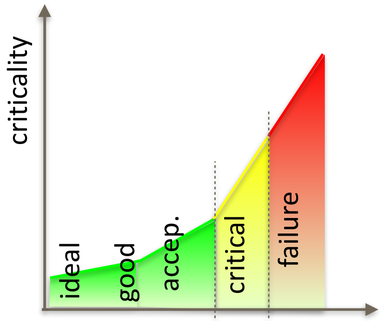
12. January 2016 Ukategorisert Administrator

[Source: eSmartSystems.com]

Conclusions

- Things (IoT) are driving the digital societies
- Automated services/Industrie4.0
  - skilled people
  - privacy/security
  - Digitisation of the Society
- IoT Security and privacy
  - Need for measurable security
  - Privacy label (A++, A+…D)
- Free access to basic information: InfoInternet
  - addressing the UN Sustainable Development Goals (SDG 2030)





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