UNIK4750 - Measurable Security for the Internet of Things

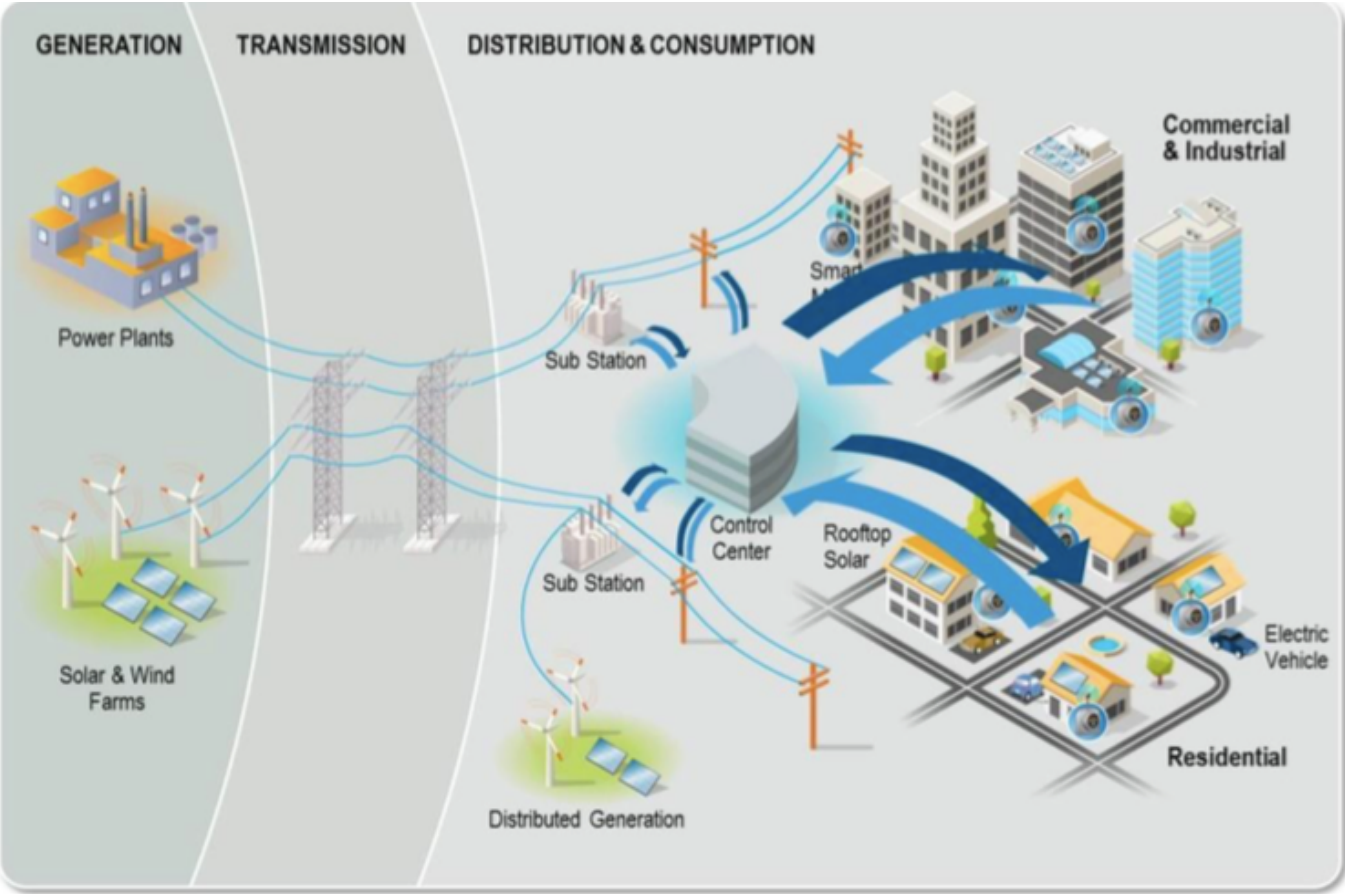
L14 - IoTSec infrastructure challenges

György Kálmán,
Mnemonic/CCIS/UNIK
gyorgy@unik.no

Josef Noll
UiO/UNIK
josef@unik.no

Overview

- Learning outcomes L14
- Use case
  - ➡ Power grid provider
  - ➡ Home infrastructure
- Infrastructures, sub-system and components
- Vulnerability analysis
- Examples of security analysis
- State-of-the-art in literature
- Future work



[Source: Davide Roverso, eSmart Systems]

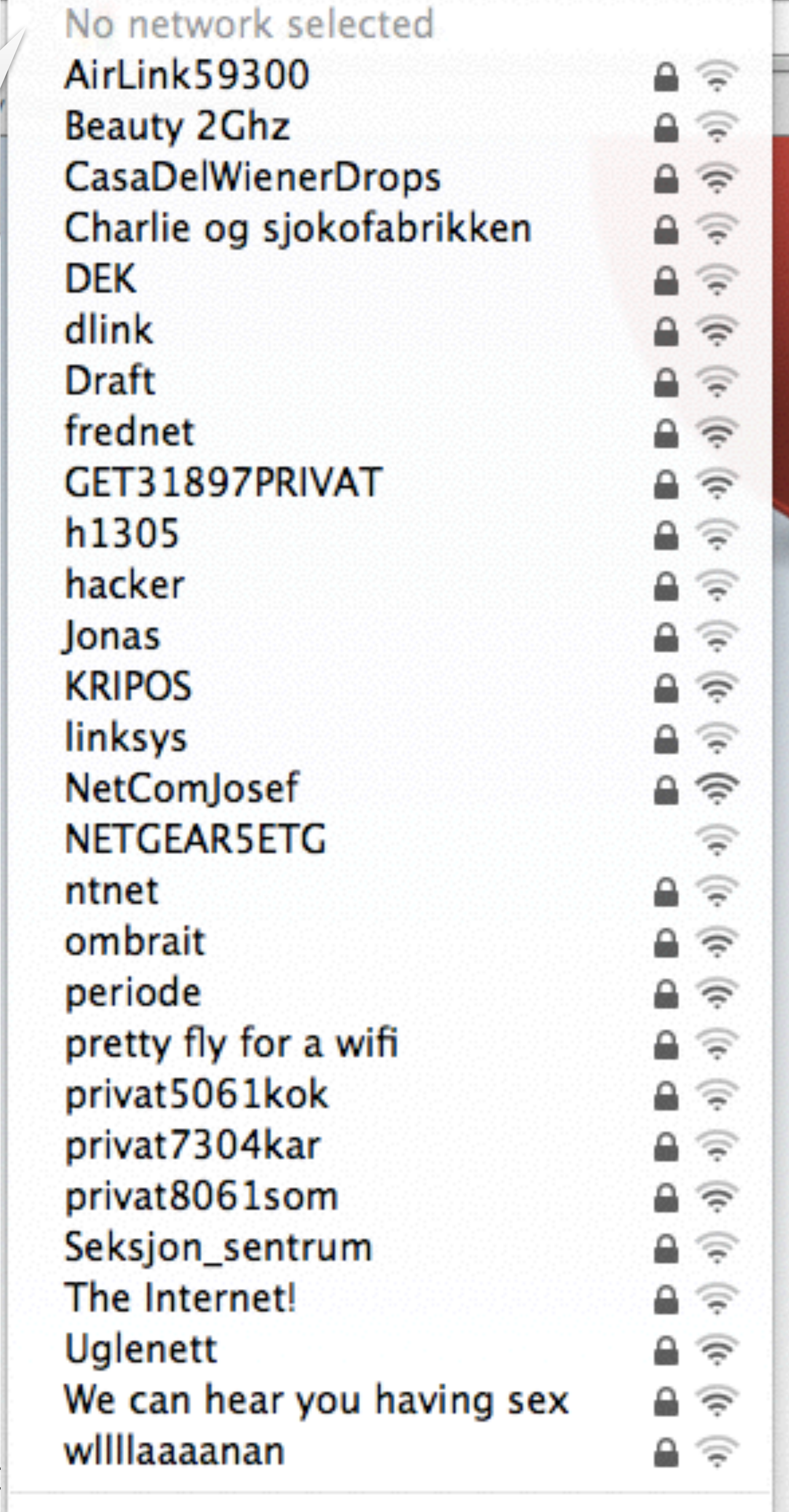
Background:

IoTSec.no - Security in IoT for Smart Grids

The world of 2016

- Interference-limited Wifi
  - ➡ increased demand on customer services
  - ➡ “meaningless discussions” on “Wifi”
- Operators in the need of becoming “Digital Companies”
  - ➡ Revenue, Investors?
  - ➡ Digital Ecosystem: Identity, Federation
- 5G dilemma
  - ➡ revenue versus costs
  - ➡ network infrastructure (core vs access network costs)
- Societal challenges
  - ➡ Energy, Health, “Internet for all”
  - ➡ Security, Privacy, “Digital Societies”

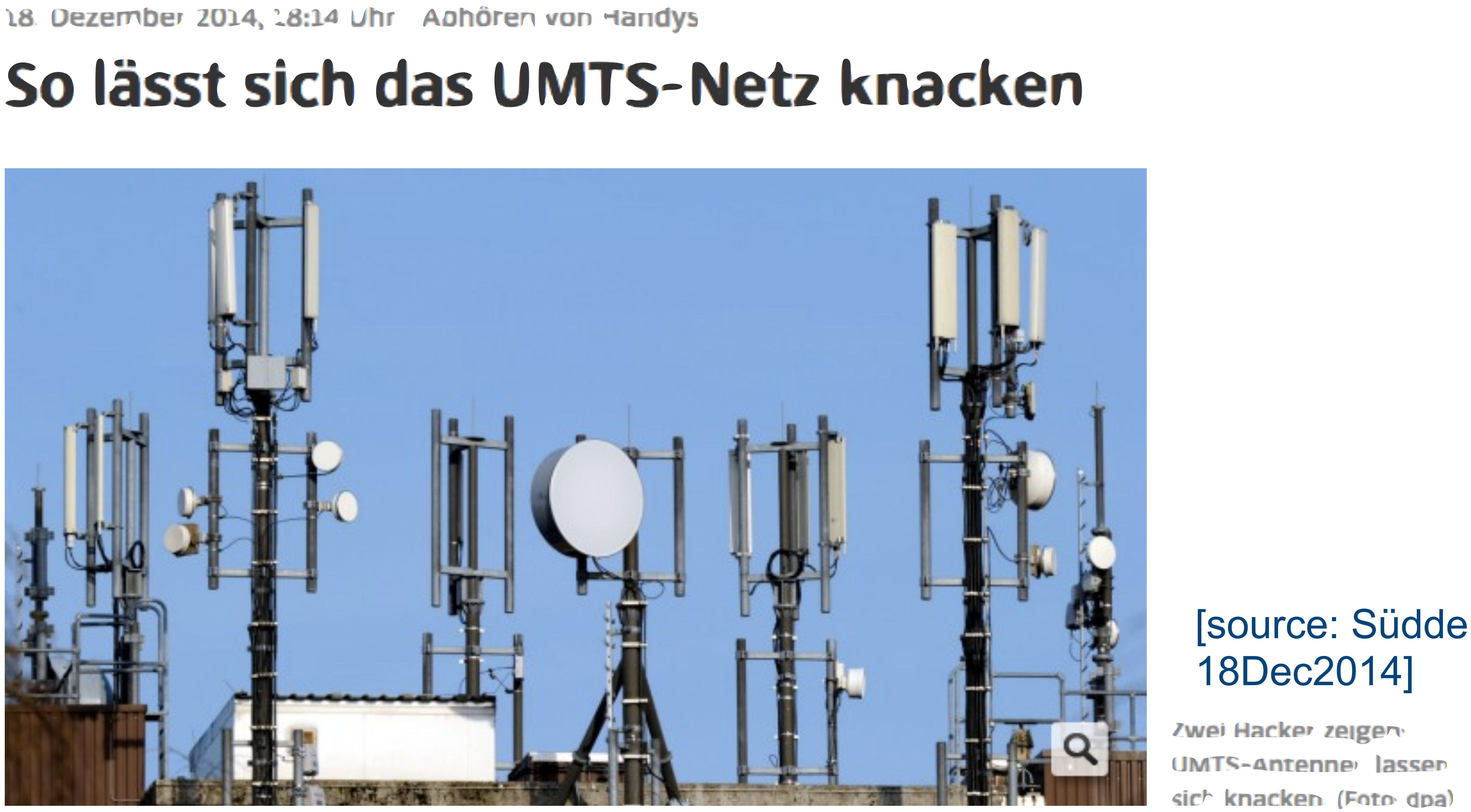
Wifi at “Legevakten” Feb2011



No network selected
AirLink59300
Beauty 2Ghz
CasaDelWienerDrops
Charlie og sjokofabrikken
DEK
dlink
Draft
frednet
GET31897PRIVAT
h1305
hacker
Jonas
KRIPOS
linksys
NetComJosef
NETGEAR5ETG
ntnet
ombrait
periode
pretty fly for a wifi
privat5061kok
privat7304kar
privat8061som
Seksjon_sentrum
The Internet!
Uglenett
We can hear you having sex
wllllaaaanan

Addressing the Threat Dimension for IoT

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



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

So lässt sich das UMTS-Netz knacken

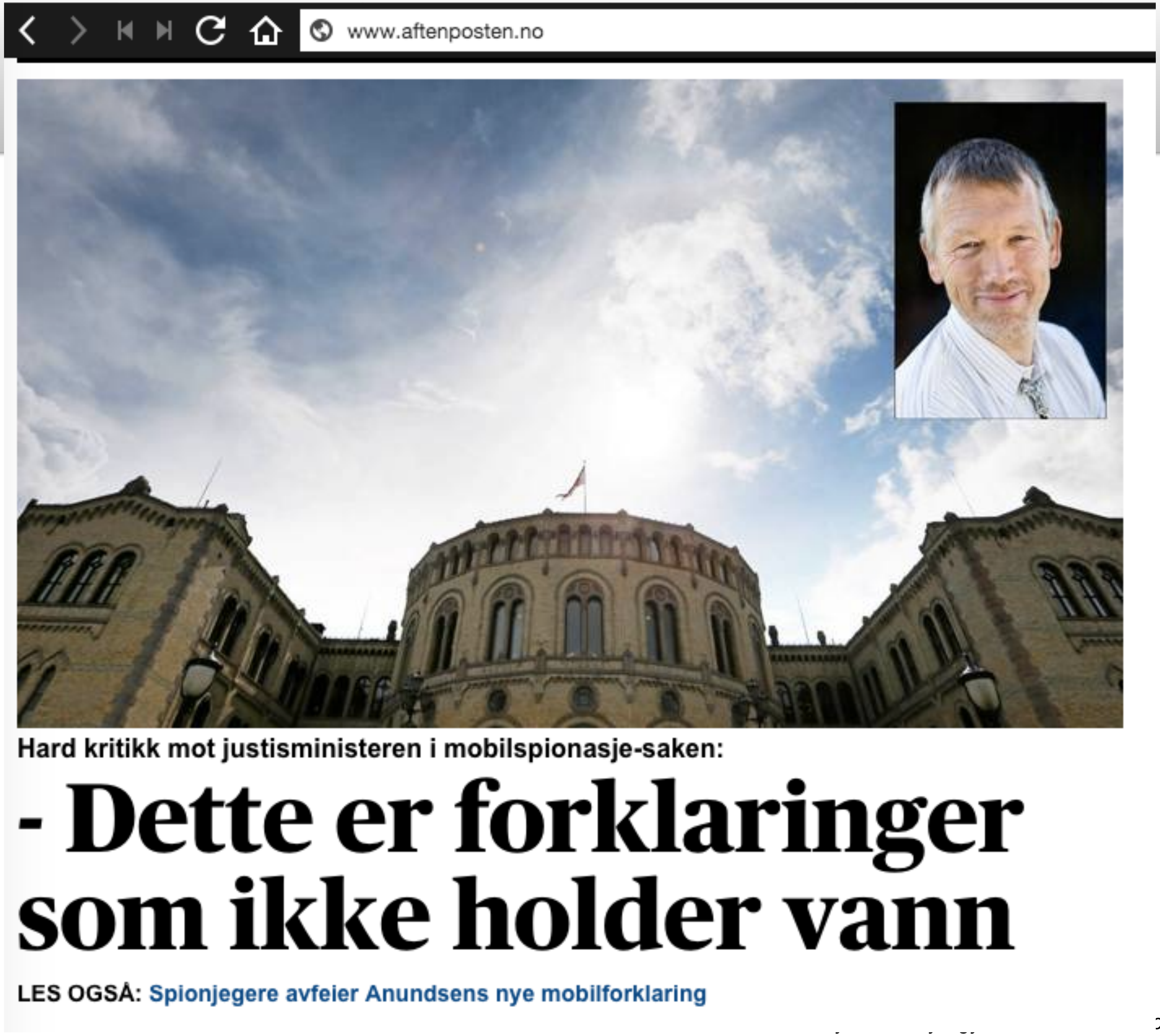
Zwei Hacker zeigen: UMTS-Antennen lassen sich knacken. (Foto: dpa)

[source: Süddeutsche Zeitung, 18Dec2014]

[source: www.rediff.com]

7Mar2015

- Aftenposten online



Hard kritikk mot justisministeren i mobilspionasje-saken:

- Dette er forklaringer som ikke holder vann

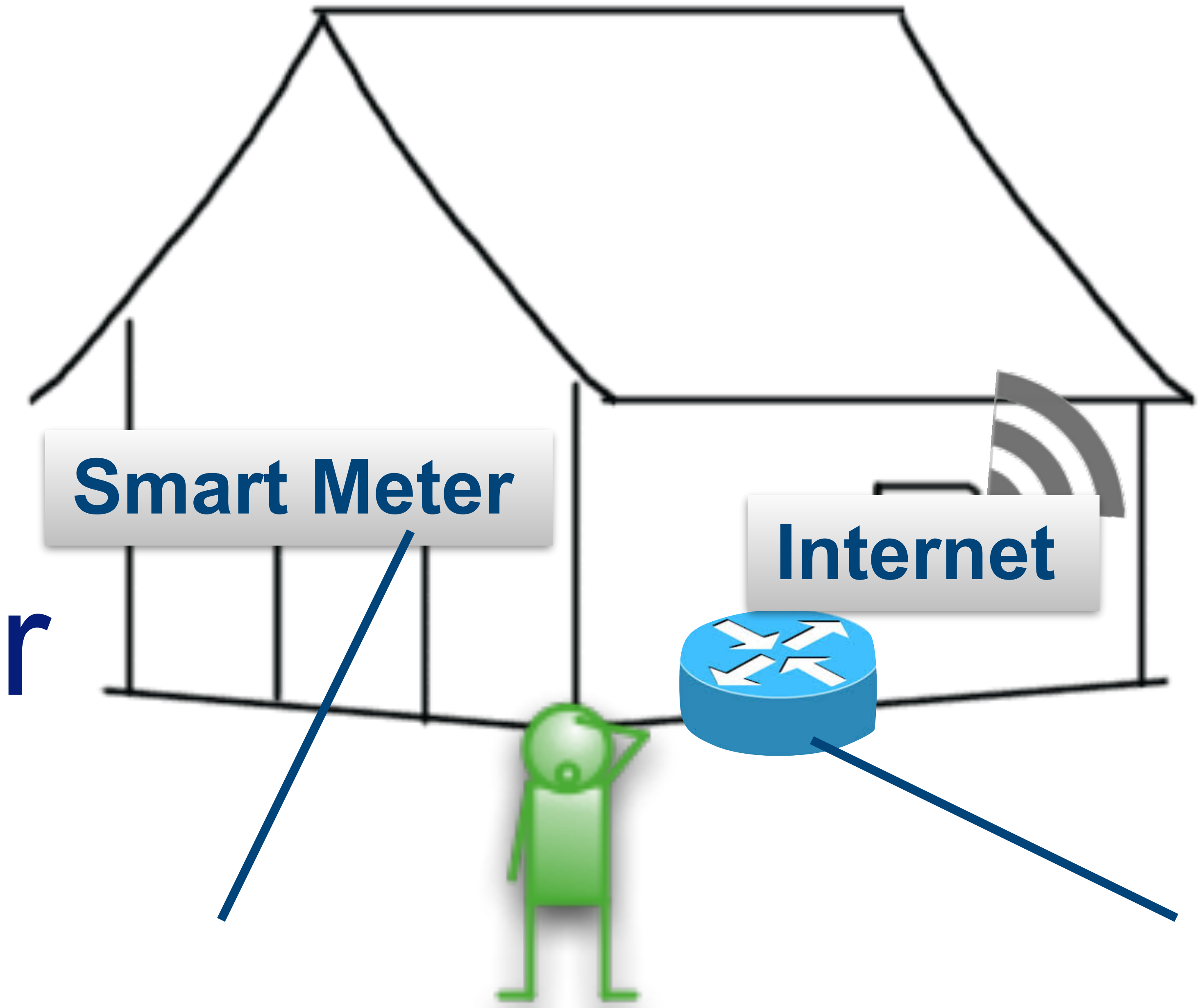
LES OGSÅ: Spionjegere avfeier Anundsens nye mobilforklaring

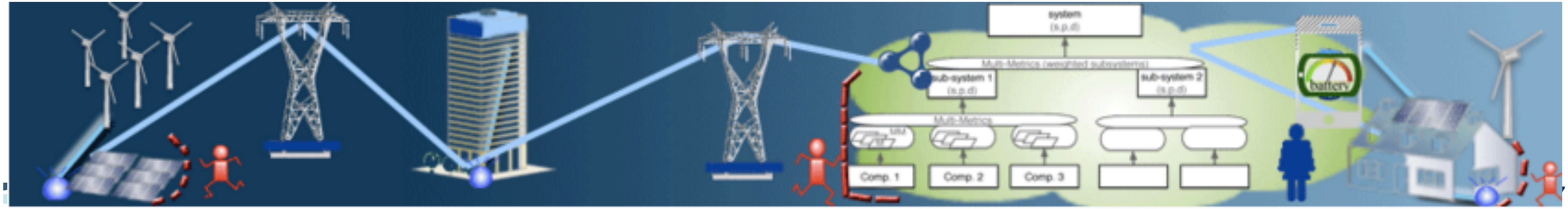
Communication & IoT for society

IoTSec.no

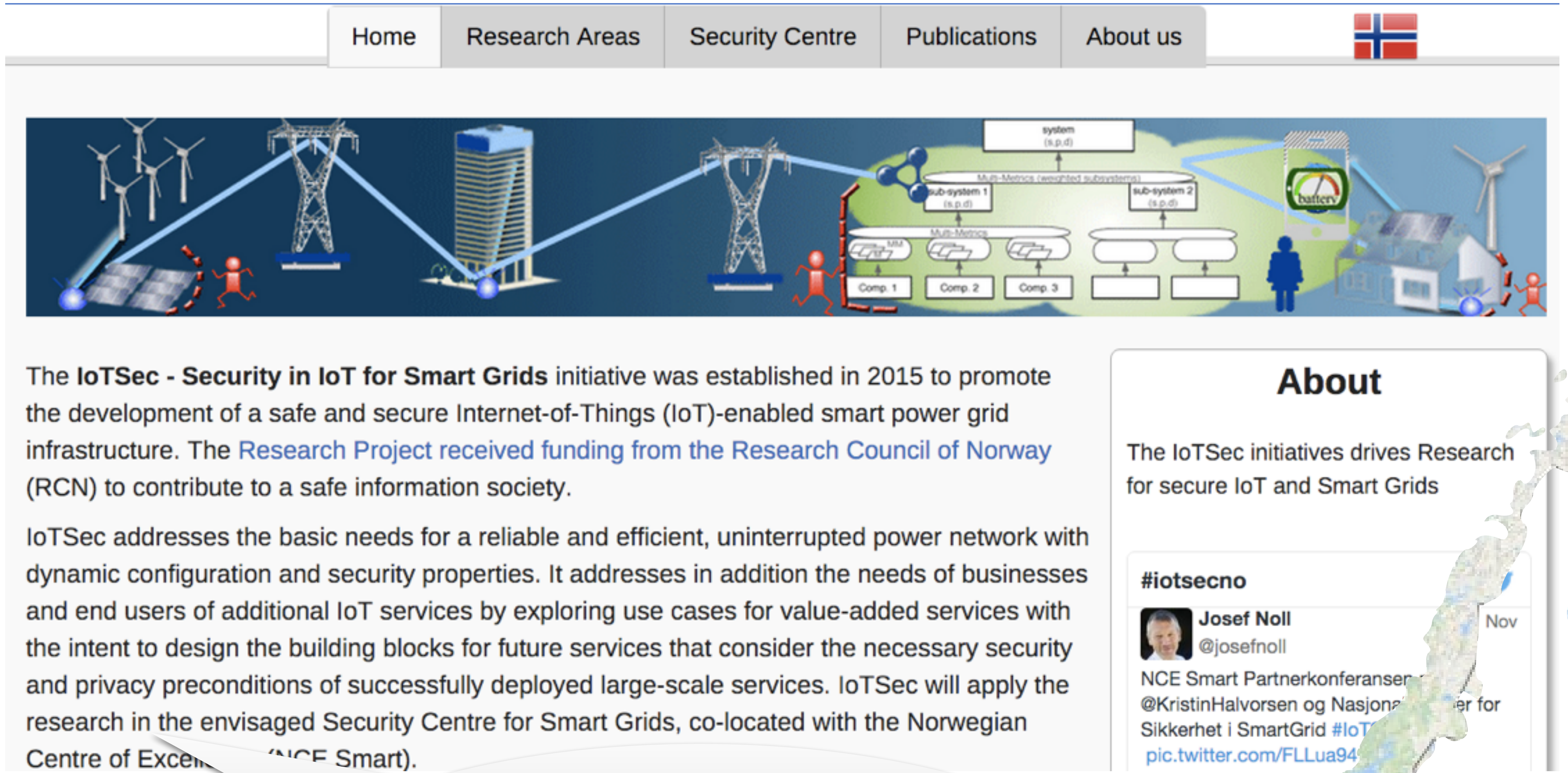
“Research on IoT security”
“Building the national Security Centre for Smart Grid”

http://IoTSec.no





Knowledge and collaboration space
IoTSec.no #IoTSecNO



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 Exce (NCE Smart).

About

The IoTSec initiatives drives Research for secure IoT and Smart Grids

#iotsecno

Josef Noll @josefnoll Nov

NCE Smart Partnerkonferansen @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

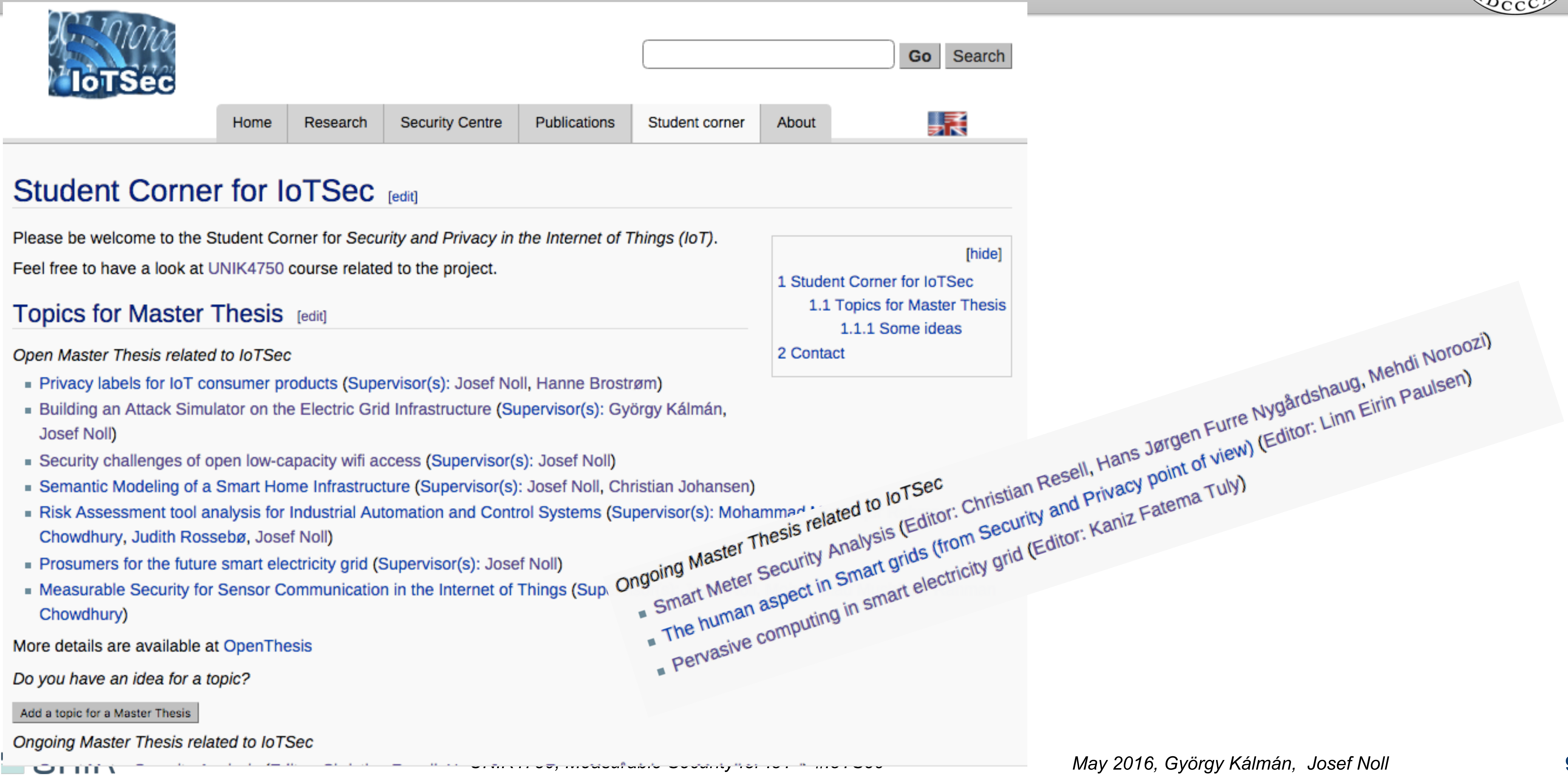
Industry
- Smart Innovation Østfold
- eSmart Systems
- Fredrikstad Energi
- EB Nett
- Movation

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

Special Focus - IoTSec: Student Corner



Student Corner for IoTSec [edit]

Please be welcome to the Student Corner for *Security and Privacy in the Internet of Things (IoT)*.

Feel free to have a look at UNIK4750 course related to the project.

Topics for Master Thesis [edit]

Open Master Thesis related to IoTSec

- Privacy labels for IoT consumer products (Supervisor(s): Josef Noll, Hanne Brostrøm)
- Building an Attack Simulator on the Electric Grid Infrastructure (Supervisor(s): György Kálmán, Josef Noll)
- Security challenges of open low-capacity wifi access (Supervisor(s): Josef Noll)
- Semantic Modeling of a Smart Home Infrastructure (Supervisor(s): Josef Noll, Christian Johansen)
- Risk Assessment tool analysis for Industrial Automation and Control Systems (Supervisor(s): Mohammad Chowdhury, Judith Rossebø, Josef Noll)
- Prosumers for the future smart electricity grid (Supervisor(s): Josef Noll)
- Measurable Security for Sensor Communication in the Internet of Things (Sup Chowdhury)

More details are available at OpenThesis

Do you have an idea for a topic?

Ongoing Master Thesis related to IoTSec

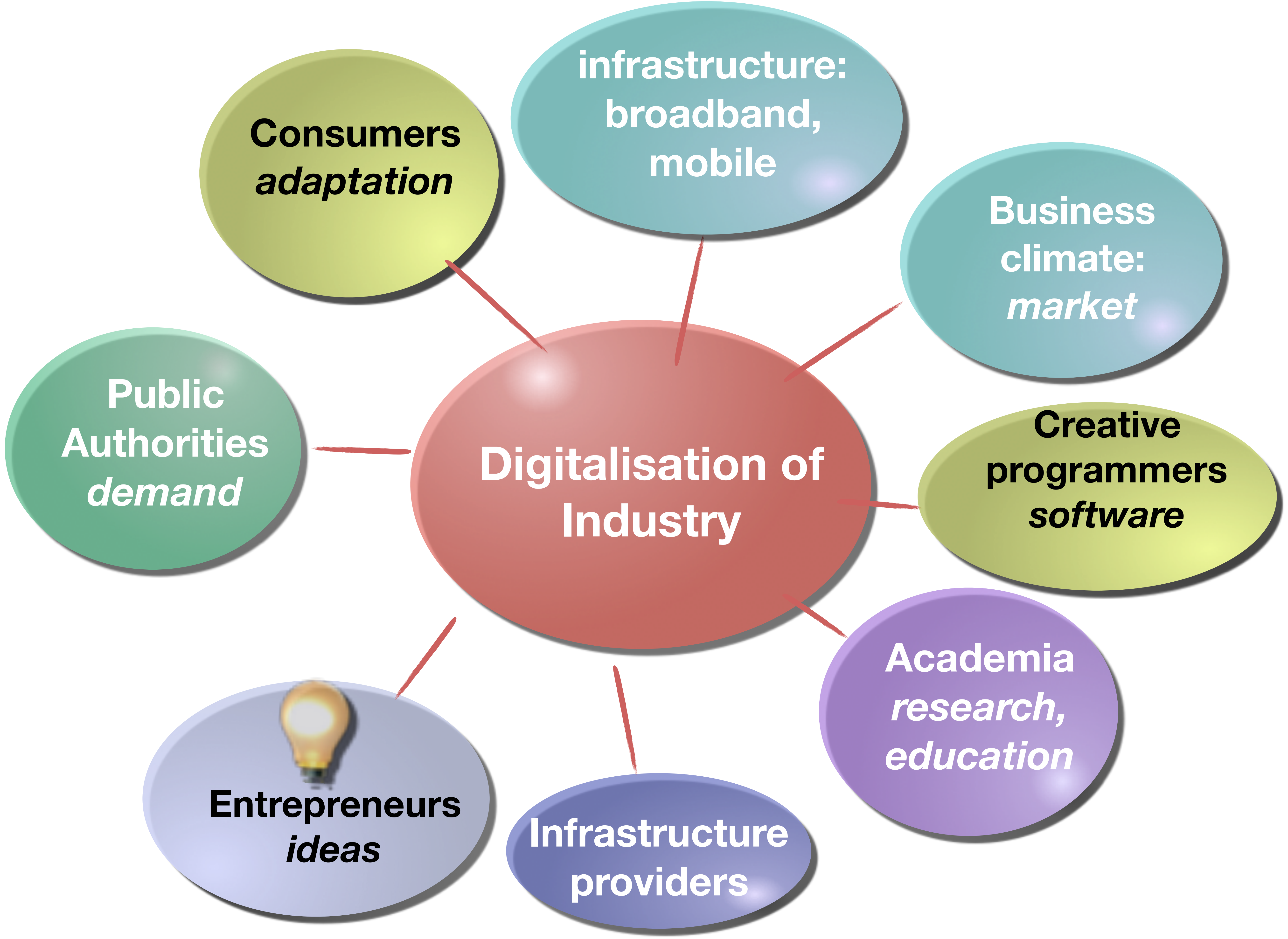
Ongoing Master Thesis related to IoTSec

- Smart Meter Security Analysis (Editor: Christian Resell, Hans Jørgen Furre Nygårdshaug, Mehdi Noroozi)
- The human aspect in Smart grids (from Security and Privacy point of view) (Editor: Linn Eirin Paulsen)
- Pervasive computing in smart electricity grid (Editor: Kaniz Fatema Tuly)

Focus of IoTSec

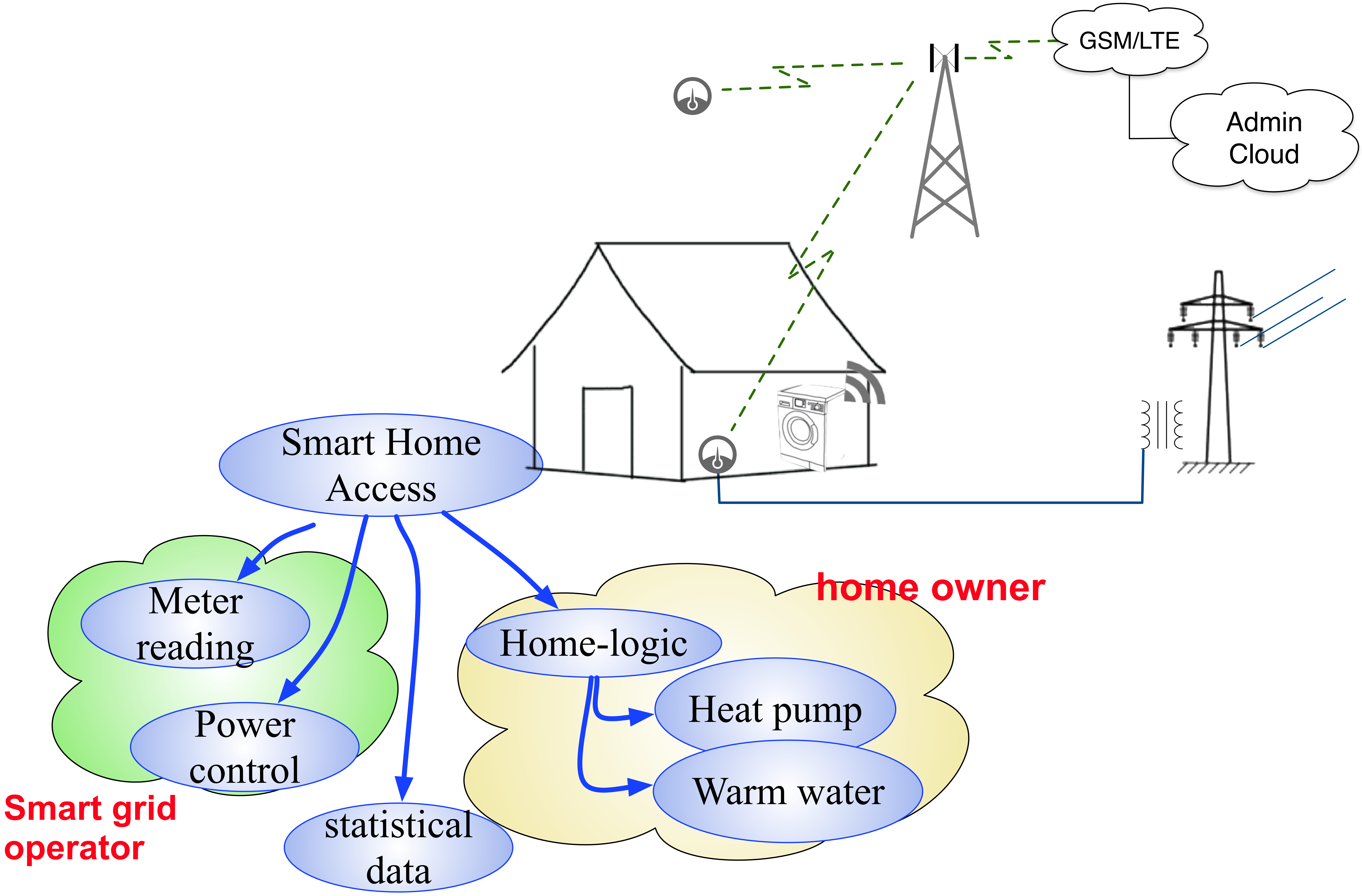
- *“we are building the Security Centre for Smart Grid”*
- Smart Grid infrastructure
  - ➡ towards Smart Homes, Smart Cities
  - ➡ towards Autonomous systems
- Security & Robustness of Industrie4.0
- Model System of Systems
- Networked Autonomous Systems
- Smart Grid enabled Distributed Systems

based on: security & privacy for systems of systems


Digitalisation of Industry
Consumers *adaptation*
infrastructure: broadband, mobile
Business climate: *market*
Creative programmers *software*
Academia *research, education*
Infrastructure providers
Entrepreneurs *ideas*
Public Authorities *demand*

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, ...

Home infrastructure Communications and Insight

- Distributed equipment
  - ➡ router, TV, mobile,…
  - ➡ authentication
  - ➡ traffic routing
  - ➡ service logics (where, what)
- Collaborative services
  - ➡ owner information
  - ➡ service data
  - ➡ statistics, e.g. urban,…
- Local decisions
  - ➡ knowledge cloud
  - ➡ fog computing

Challenges: Set-up, Connectivity

Addressing the challenges of IoT connectivity

Device ownership

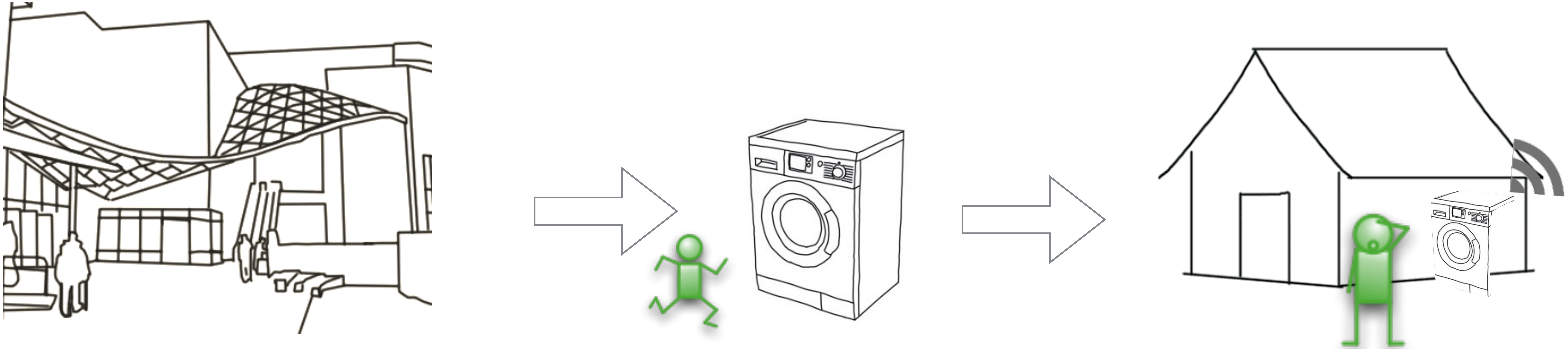
- who owns the device
- which data are going to whom
  - ➡ maintenance
  - ➡ usage

Easyness Setup

- 1. step ownership
- take control

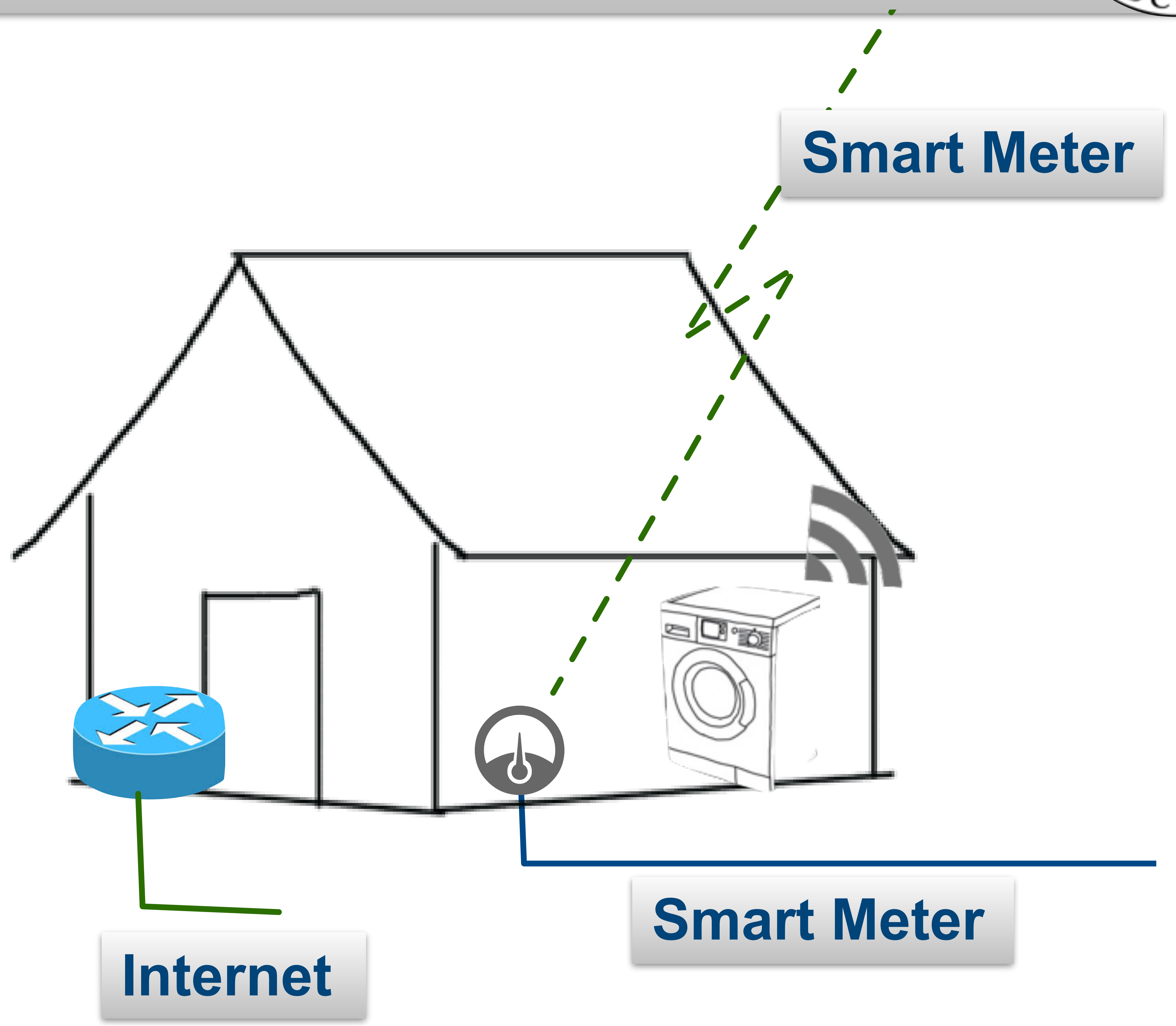
Scalability

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



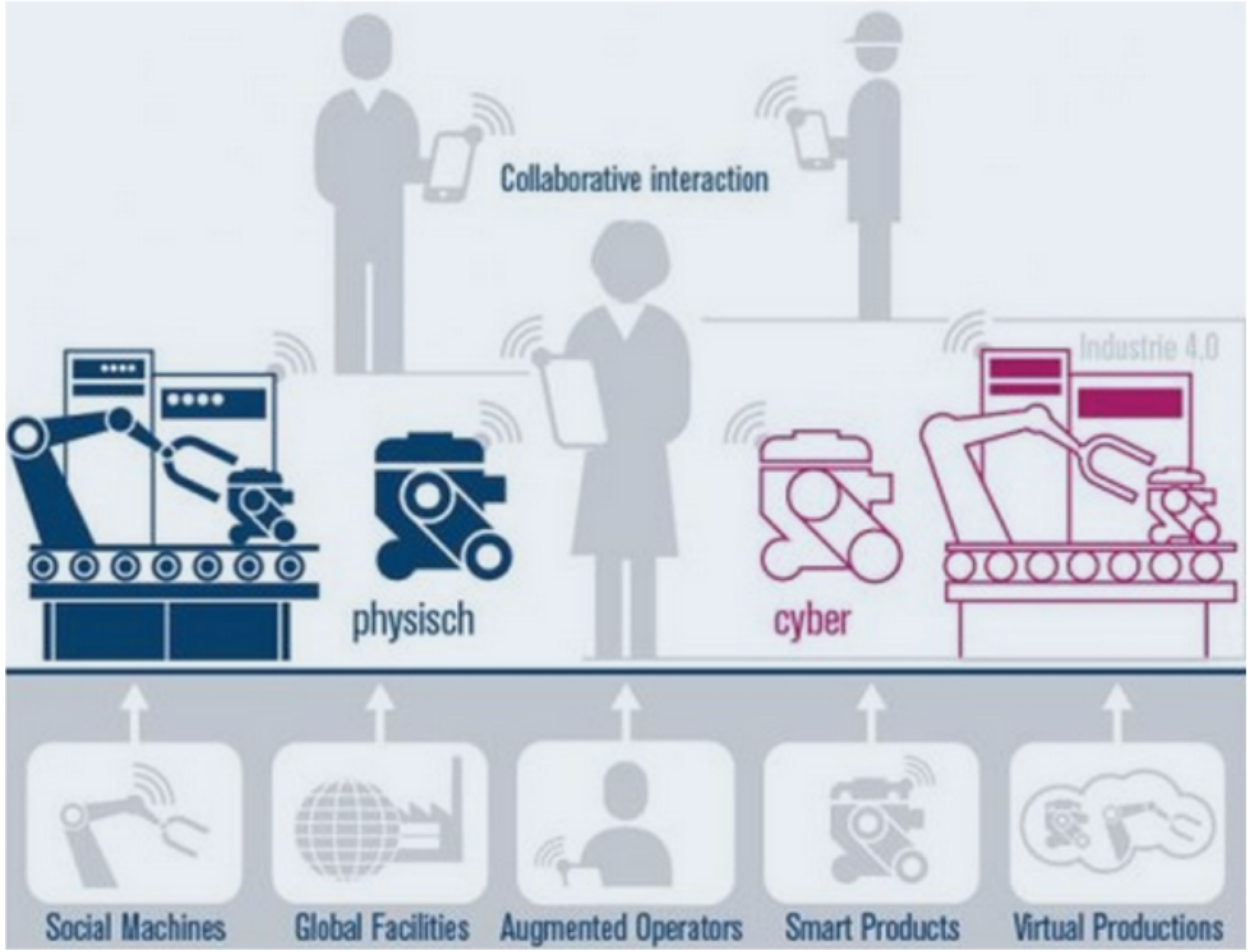
Upcoming Infrastructure

- 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



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

IoTSec.no

Specific Challenges

Source: Davide Roverso, eSmart Systems

Smart Grid Actors

TSO: Transmission System Operator

- The TSO perspective – IoT in the Smart Transmission Grid
  - ➡ IoT security of the Smart Grid critical infrastructure (devices/communication/...) at the transmission network level

DSO: Distribution System Operator

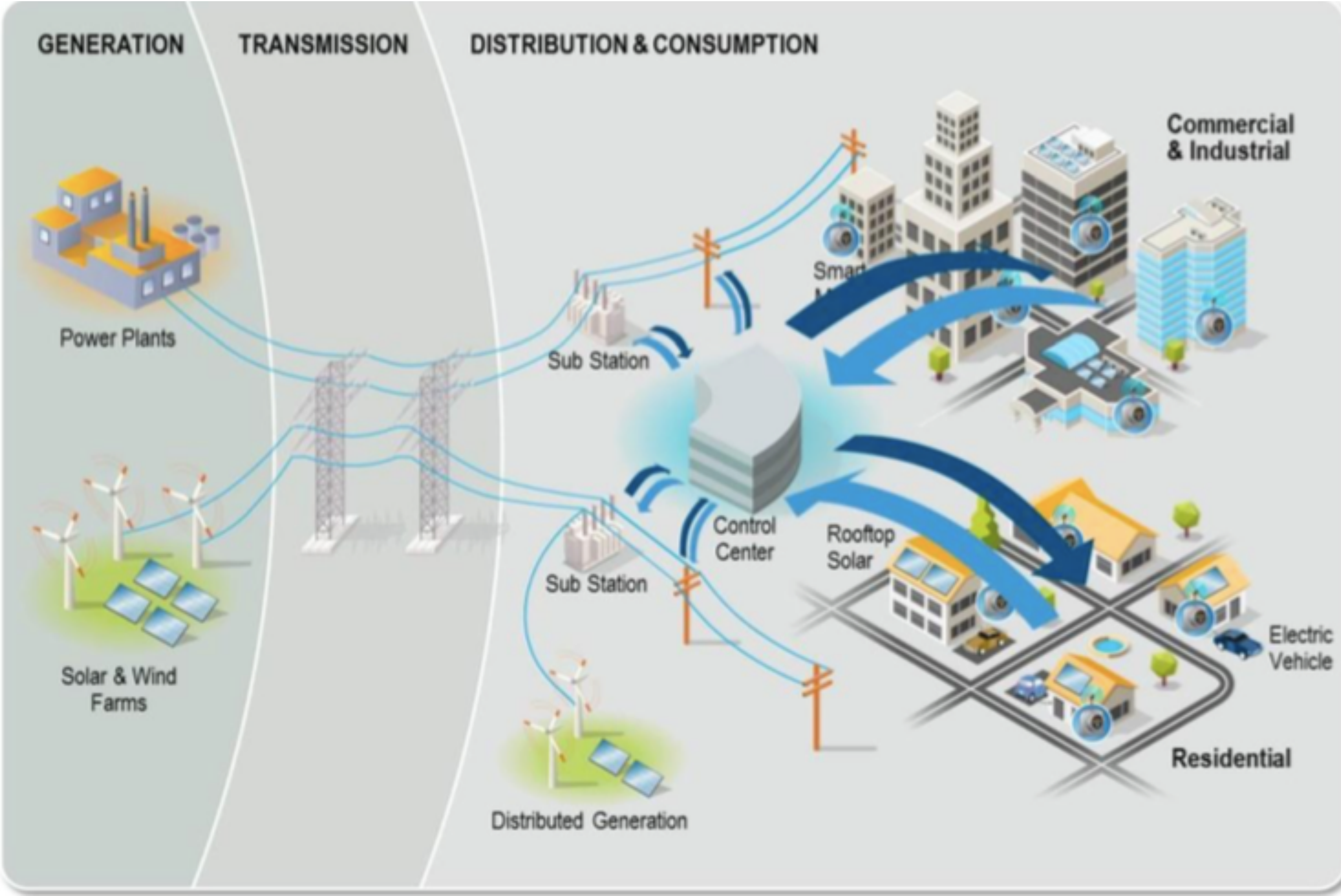
- The DSO Perspective – IoT in the Smart Distribution Grid
  - ➡ IoT security of the Smart Grid critical infrastructure (devices/communication/...) at the distribution network level,
  - ➡ included privacy issues
  - ➡ Smart Meters, Concentrators, Automated Substations, ...
- The end-user perspective – IoT in the Smart Home
  - ➡ IoT security of Smart Home related devices/communication, mainly related to home automation and its relation
  - ➡ with smart metering infrastructure, including privacy issues
- Other perspectives - Service Provider, Producer, Prosumer, Aggregator, ...

Specific challenges of the DSO

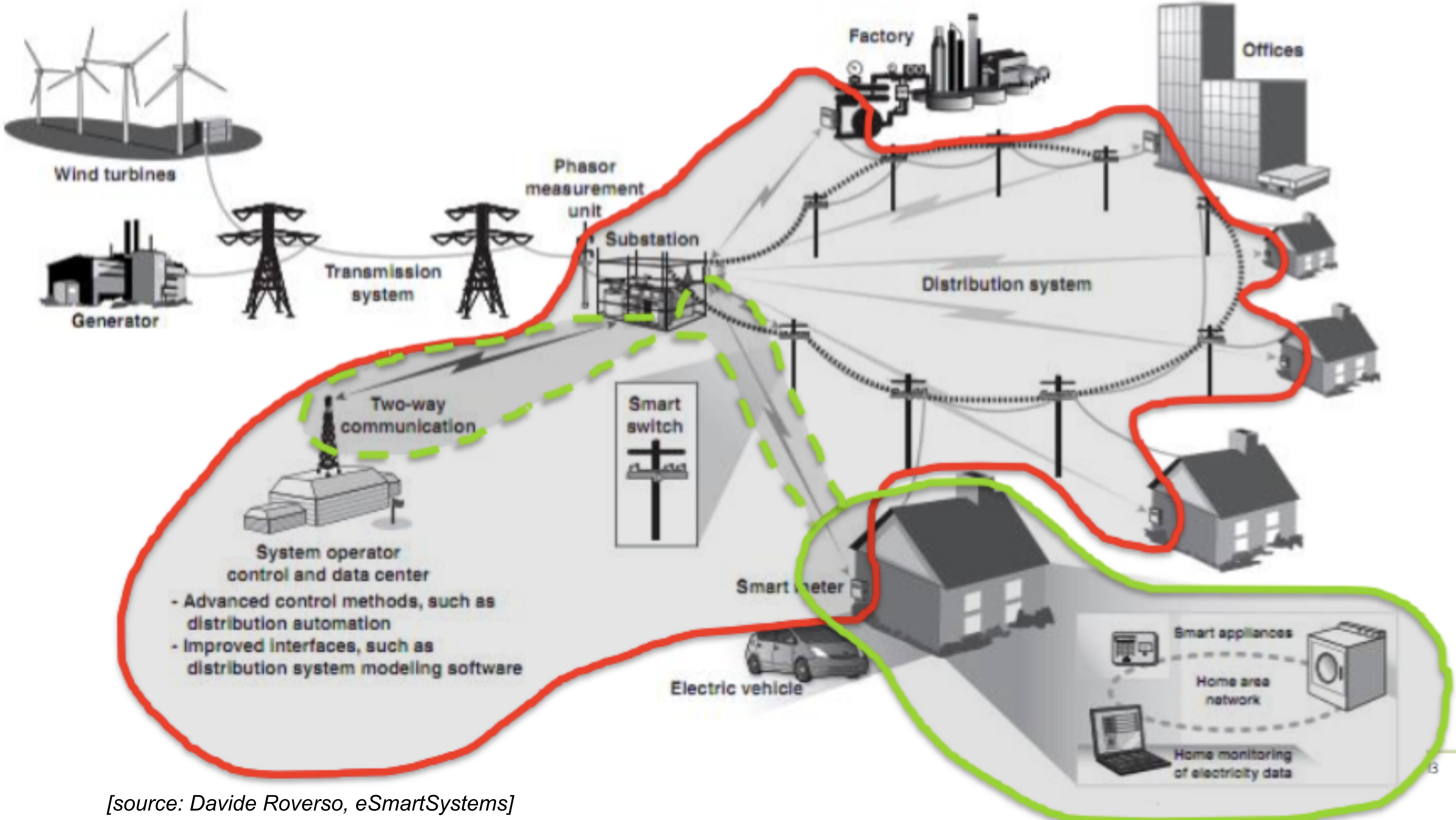
Powered by penalties of not-delivered energy

- Quality-adjusted income for non-delivered energy//Kvalitetsjusterte inntektsrammer ved ikke levert energi (KILE)

- short-time (< 3 min) and long-time (> 3 min) disturbances, both planned and not planned (U > 1kV)
- Total amount ca 800 MNOK/år in Norway
- Costs related to societal costs
- Related to build, operate, maintain the distribution grid in an economic-optimal way for the society



Smart Home vs Smart (Distribution) Grid focus



Wind turbines
Generator
Transmission system
Phasor measurement unit
Substation
Factory
Offices
Distribution system
Two-way communication
Smart switch
System operator control and data center
- Advanced control methods, such as distribution automation
- Improved interfaces, such as distribution system modeling software
Smart meter
Electric vehicle
Smart appliances
Home area network
Home monitoring of electricity data

[source: Davide Roverso, eSmartSystems]

Information exchange between TSO and DSO

TFO: Transformer Operator

- ownership of TSO?
- overload of interface between transport and distribution network

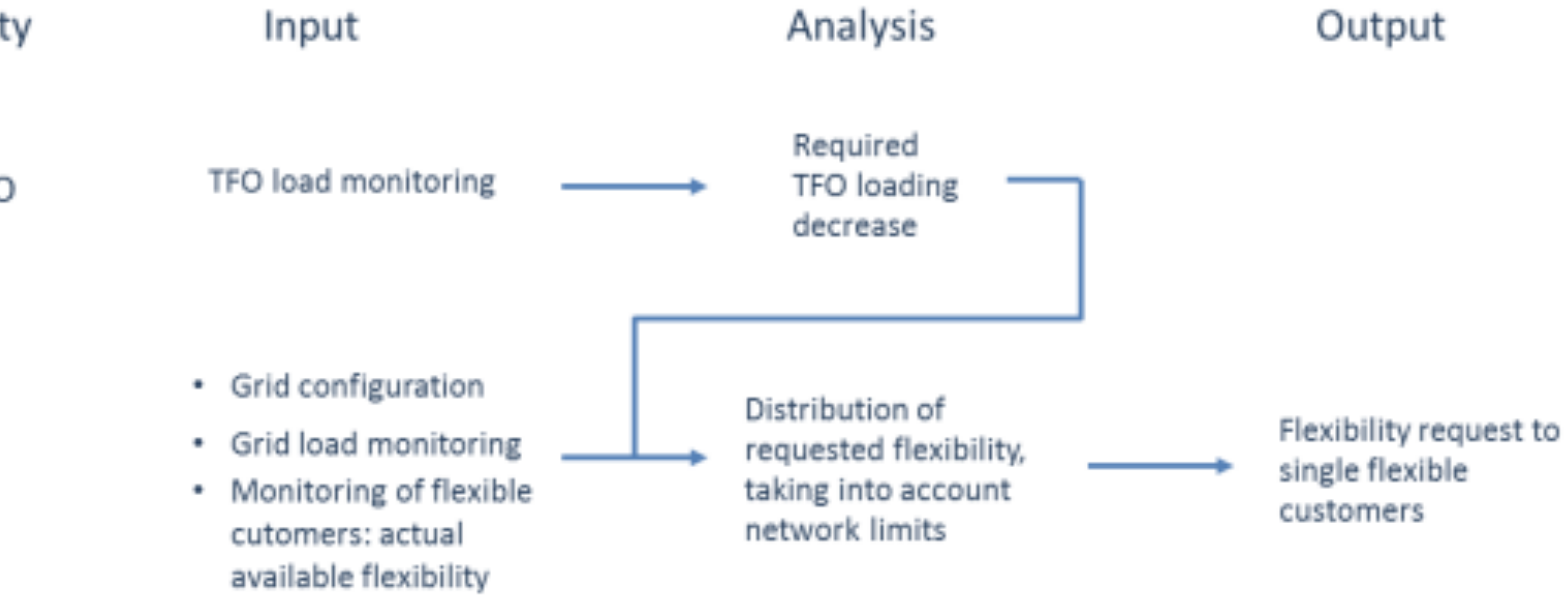

Party
Input
Analysis
Output
TSO
TFO load monitoring
Required TFO loading decrease
• Grid configuration
• Grid load monitoring
• Monitoring of flexible cutomers: actual available flexibility
Distribution of requested flexibility, taking into account network limits
Flexibility request to single flexible customers

Figure 3 - Process proposal to avoid TFO congestion using flexibility on distribution grid

[Source: http://smartgrids.no/wp-content/uploads/sites/4/2016/01/ISGAN-TSO-DSO-interaction.pdf]

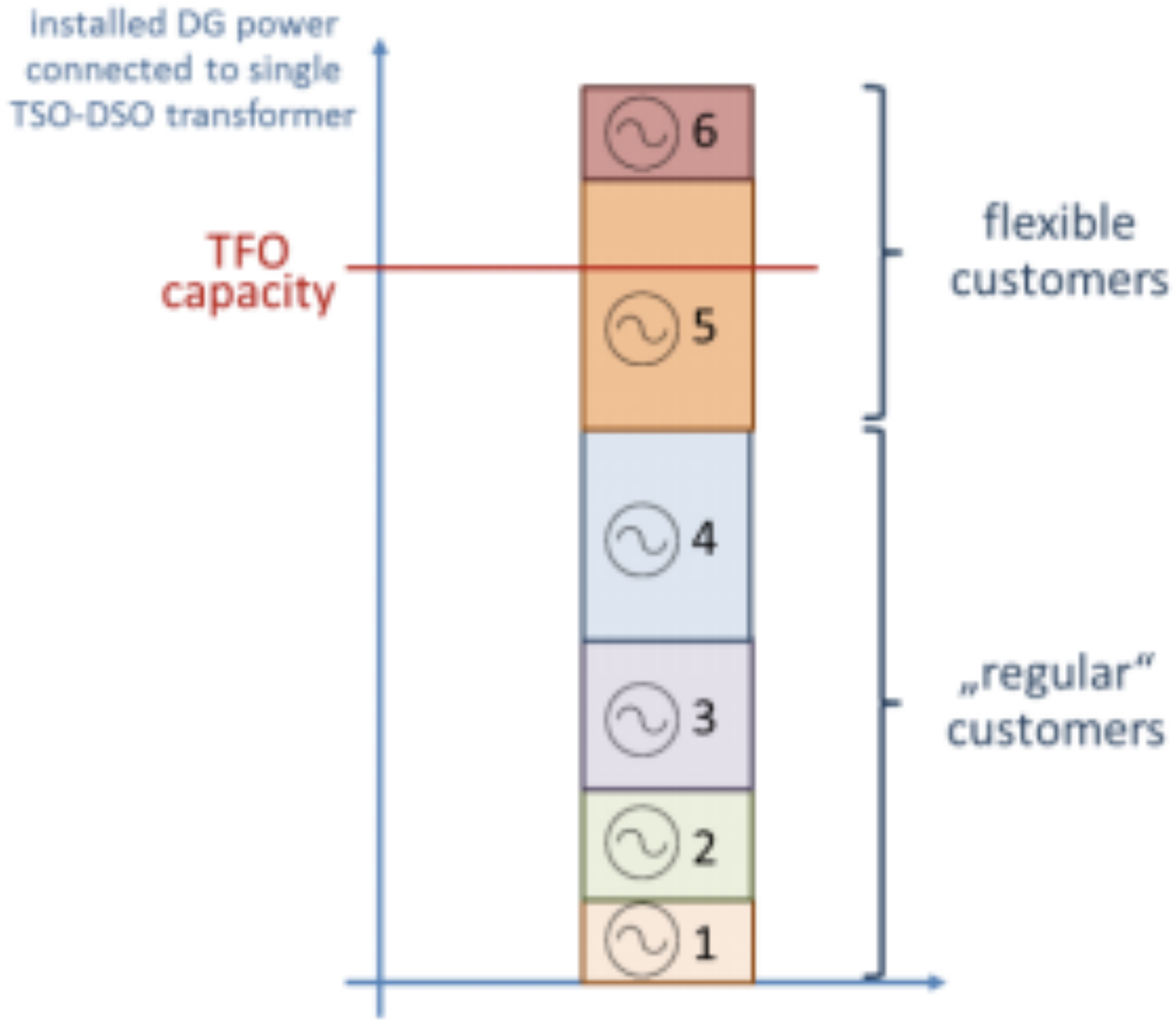


Figure 4 - Illustration of regular and flexible customers

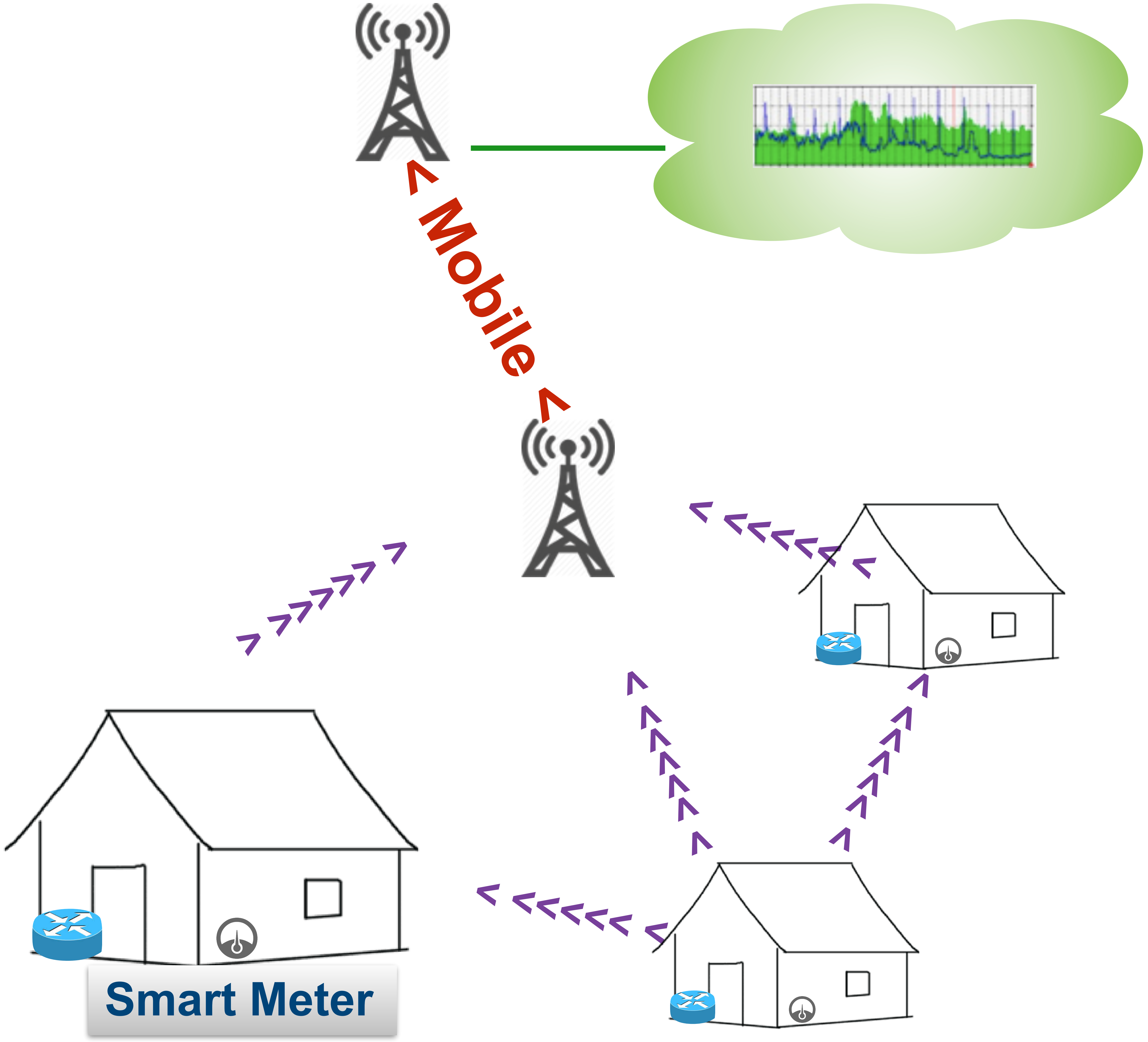
Example: TFO challenges

- TFO overload
  - ➡ More grid monitoring and intensified data exchange would allow using flexibility on the distribution grid to reduce transformer loading when necessary.
  - ➡ A request could be sent from the TSO to the DSO to decrease the transformer loading. The DSO could translate this request to use-of-flexibility requests to flexible customers connected to the distribution grid.
- Line congestions
  - ➡ The use of flexibility on the distribution grid to manage transmission line loading.
  - ➡ DSO could provide information about available flexibility on the distribution grid, aggregated per TSO-DSO point of connection. The TSO could use this information and his own grid monitoring to calculate the required use of flexibility. Resulting requests for flexibility could be sent to the DSO and to flexible customers connected to the transmission grid.
  - ➡ Some mechanism has to be implemented to decide between the flexibility of transmission customers and distribution customers.
- Voltage support
- Balancing
- Island operation
- Co-ordinated protection

[Source: http://smartgrids.no/wp-content/uploads/sites/4/2016/01/ISGAN-TSO-DSO-interaction.pdf]

Current Infrastructure

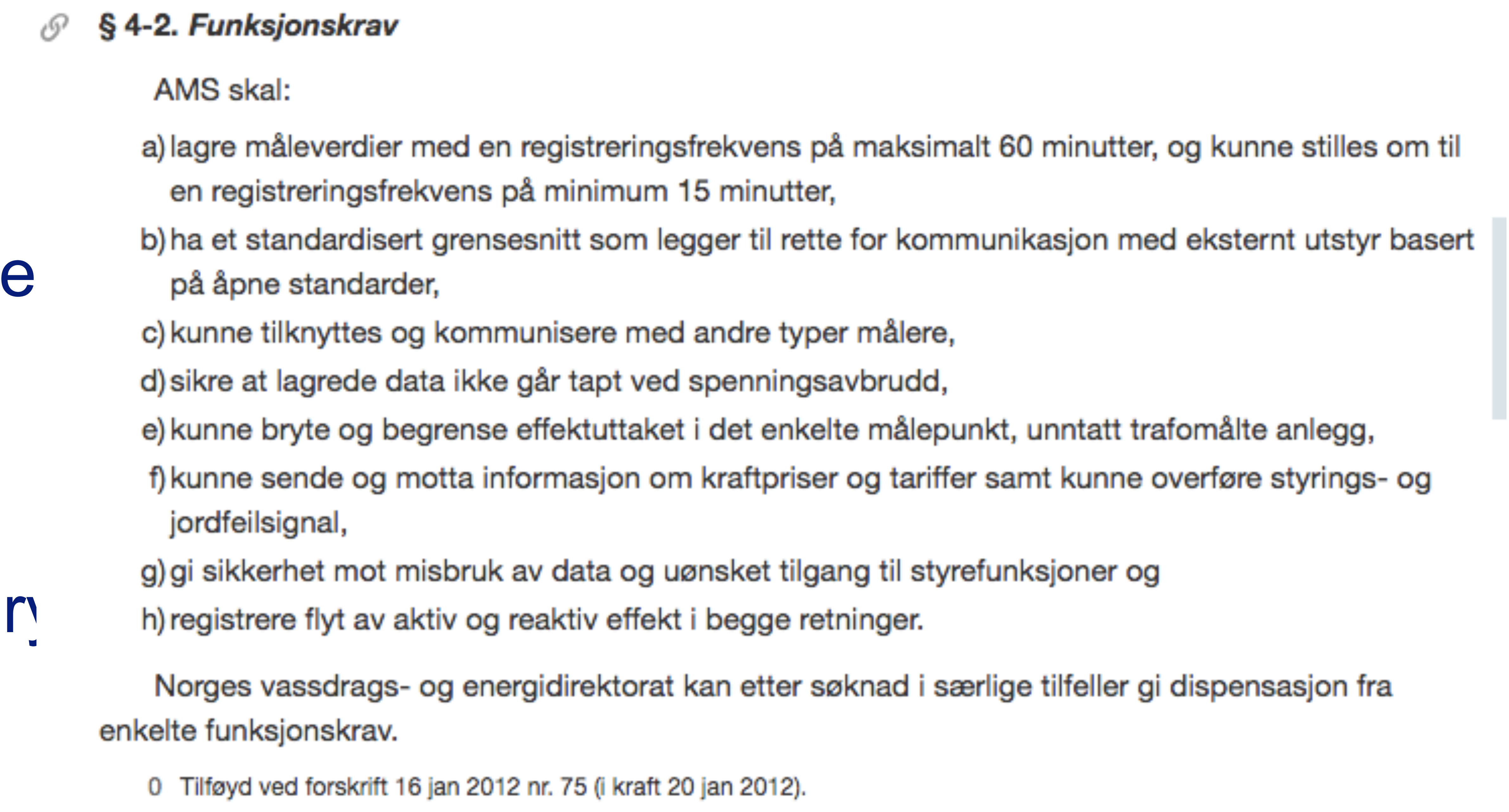
- Smart Meter (customer home)
  - ➡ connected via mesh or directly
  - ➡ proprietary solution (433, 800 MHz band, power line)
- Collector
  - ➡ collects measures
  - ➡ communicates via mobile network
- Mobile Network
  - ➡ as a transmission network
- Cloud (Provider)
  - ➡ entry point for remote access
  - ➡ Application platform



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 ever 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.

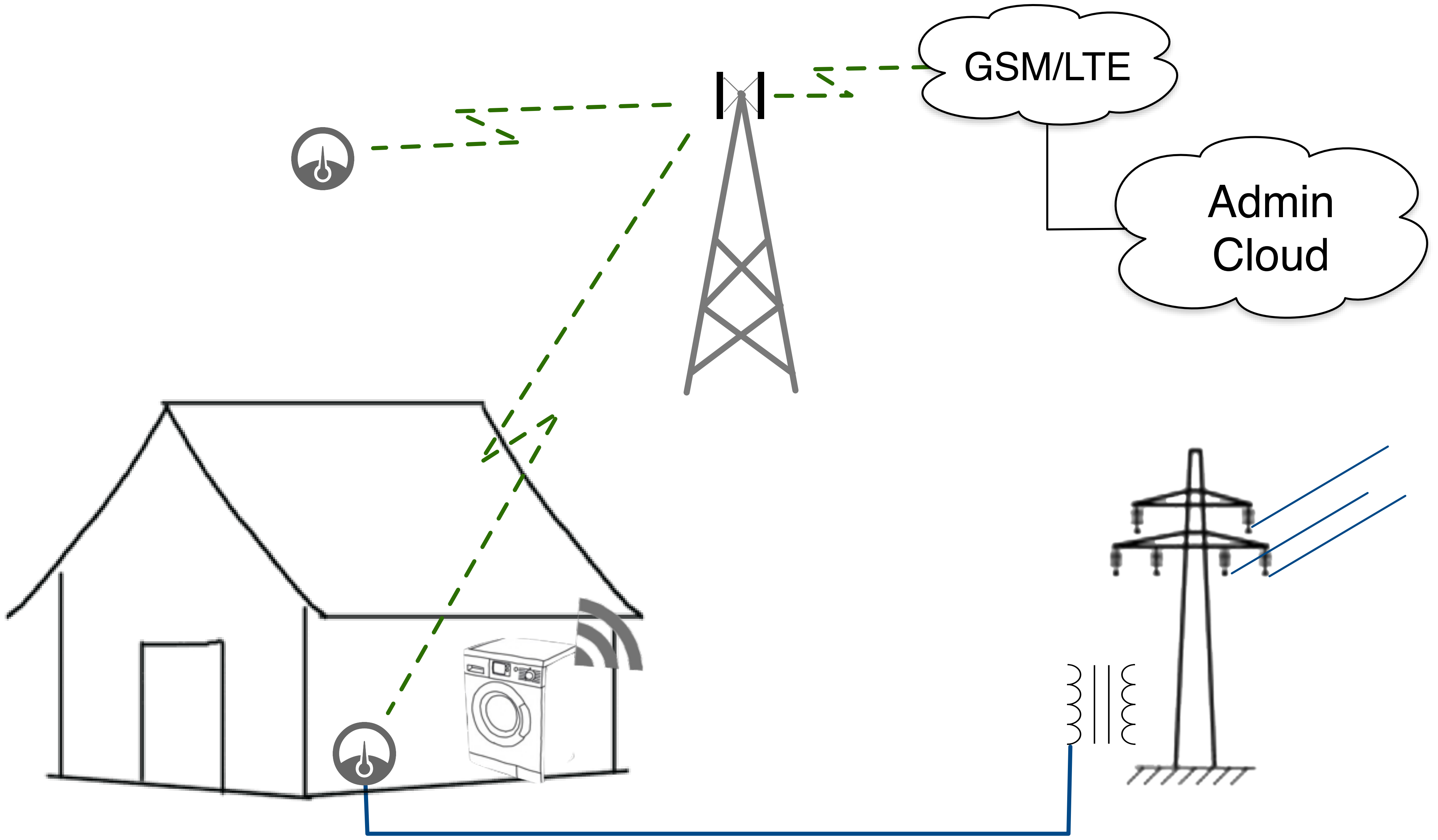
Norges vassdrags- og energidirektorat kan etter søknad i særlige tilfeller gi dispensasjon fra enkelte funksjonskrav.

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

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

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”



Instead of conclusions…

DISCUSSION

Expected Learning outcomes

Having followed the lecture, you can

- name the actors in a smart grid networks
- identify their responsibilities
- reason over security challenges
- provide applications and discuss their security requirements