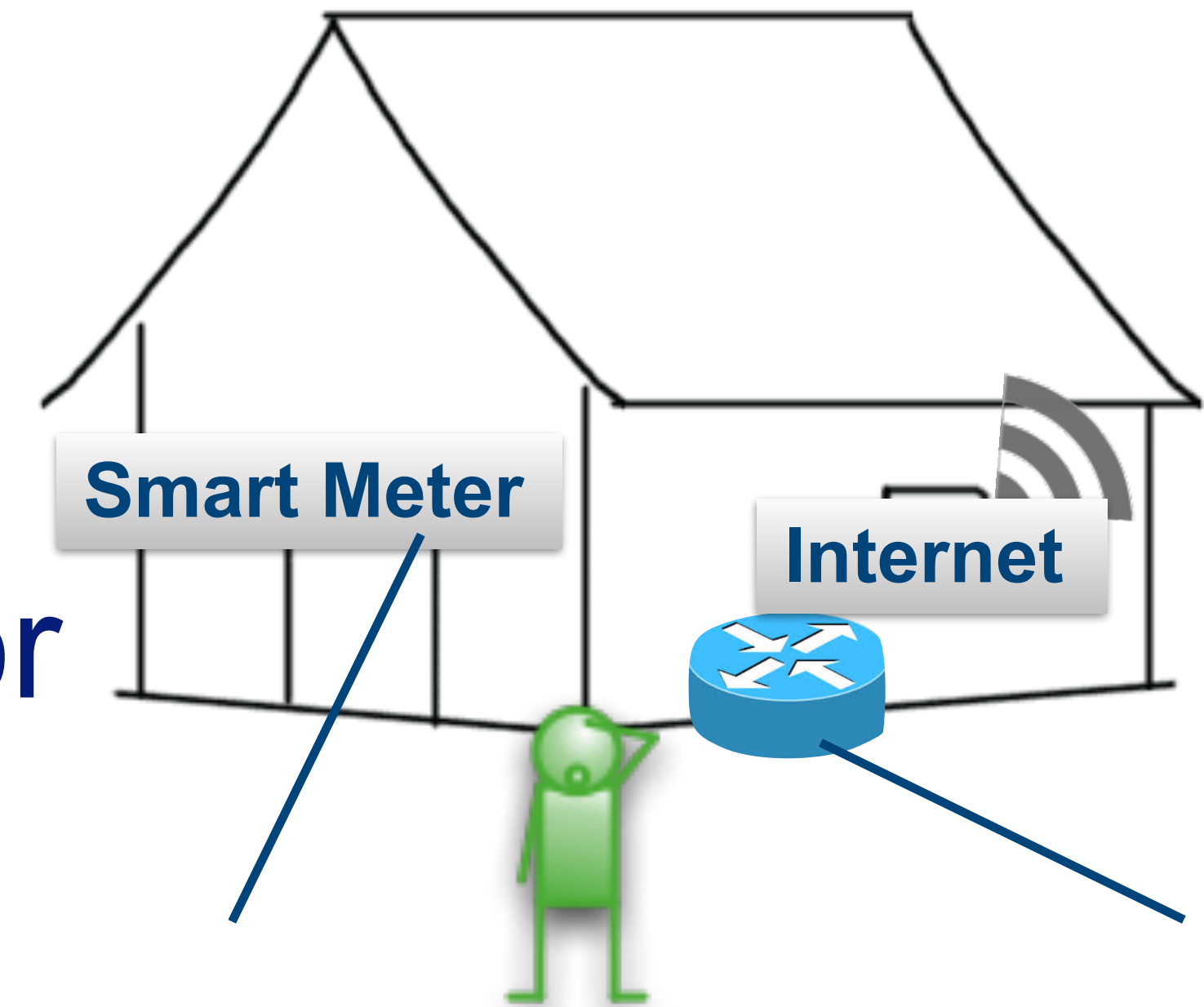
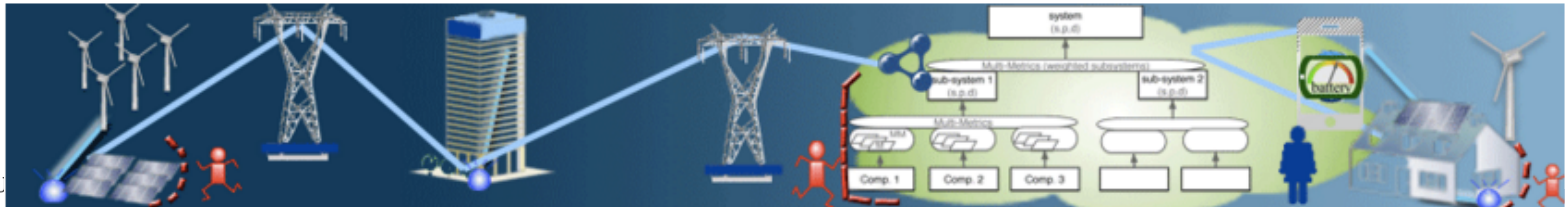


IoTSec.no

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



<http://IoTSec.no>

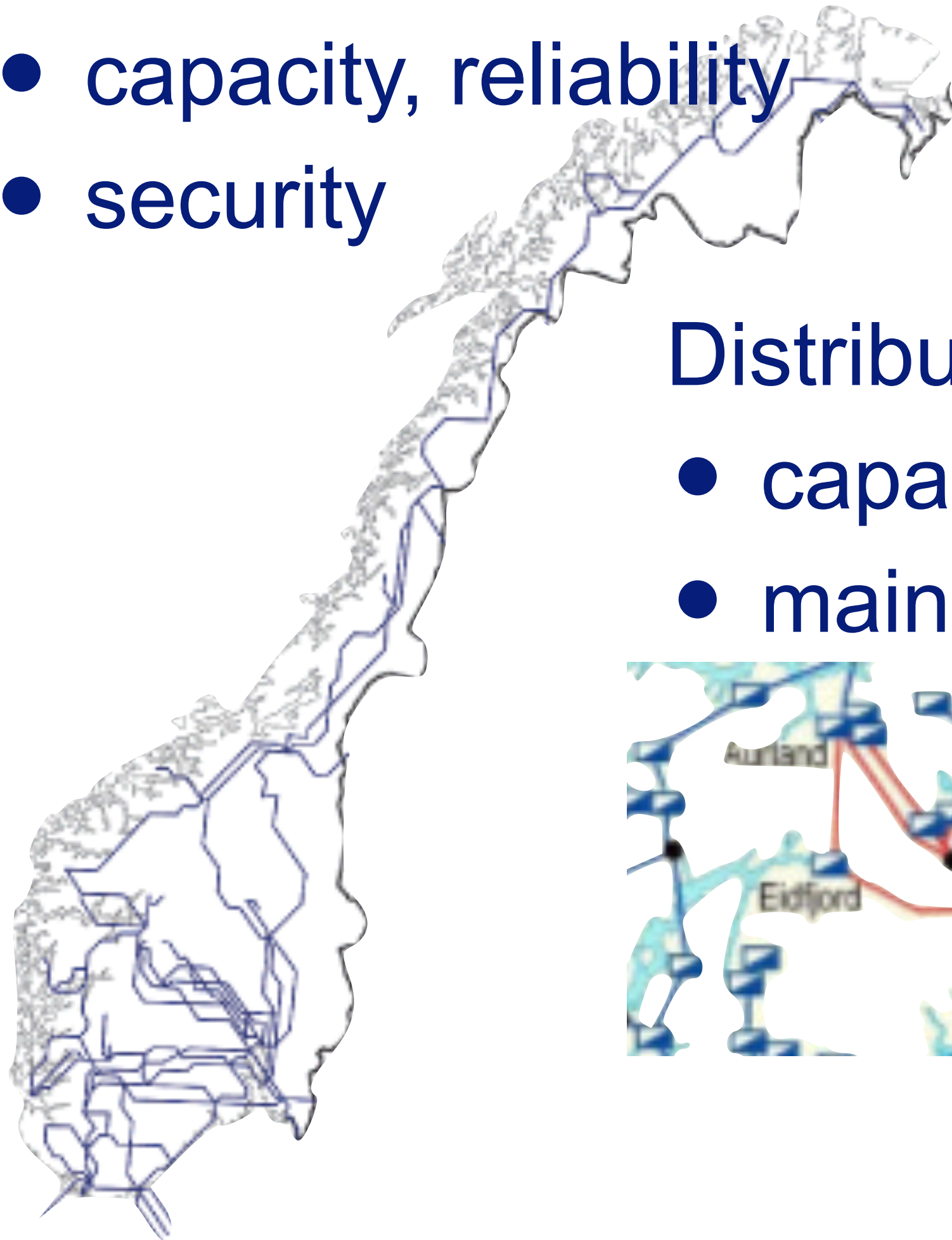


From power lines to Smart Meter Infrastructure & Services



Transmission Grid

- capacity, reliability
- security

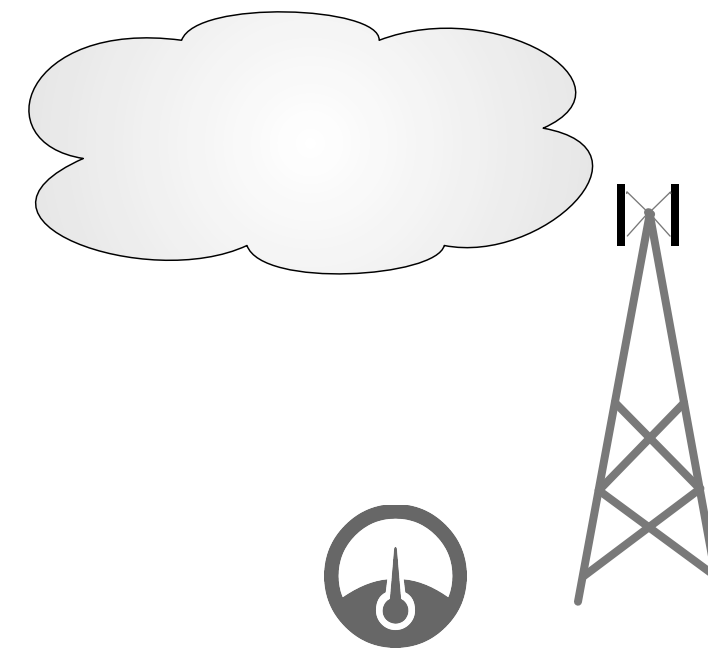
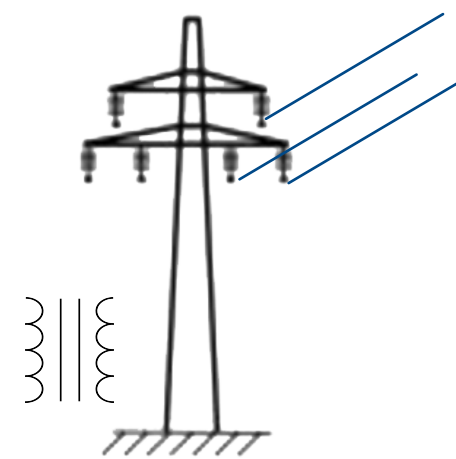
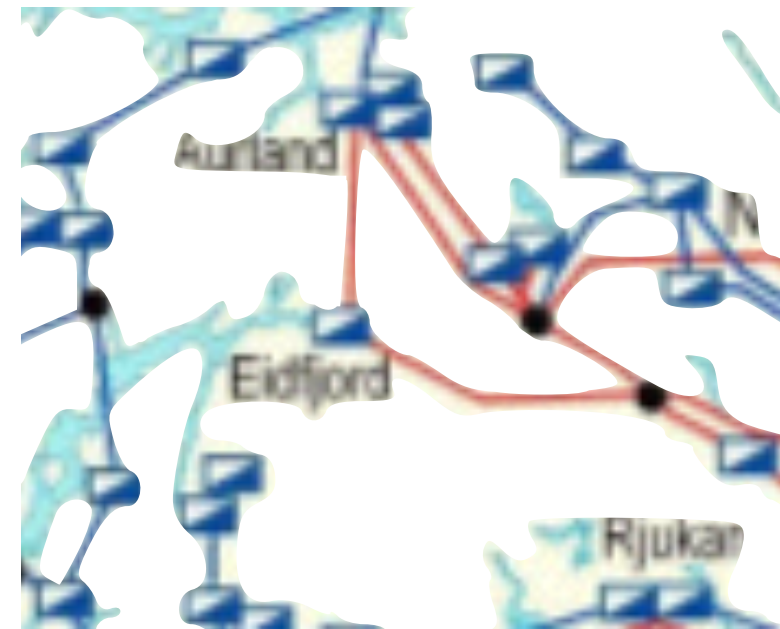


Smart Grid Infrastructure

- smart meter
- security

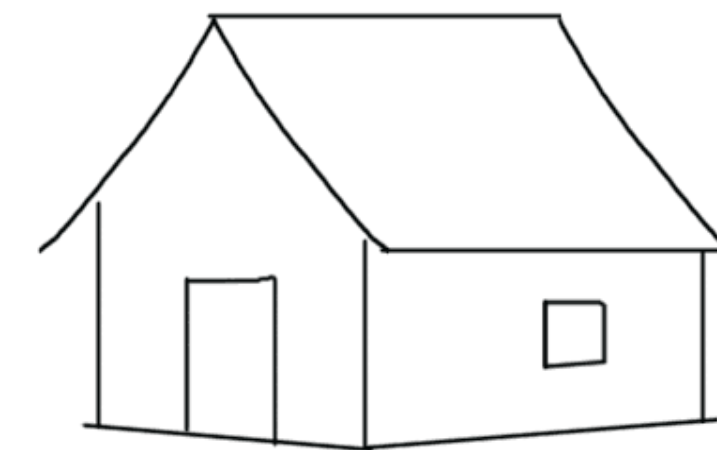
Distribution Grid

- capacity
- maintainability



Smart Home

- privacy, security
- societal challenges



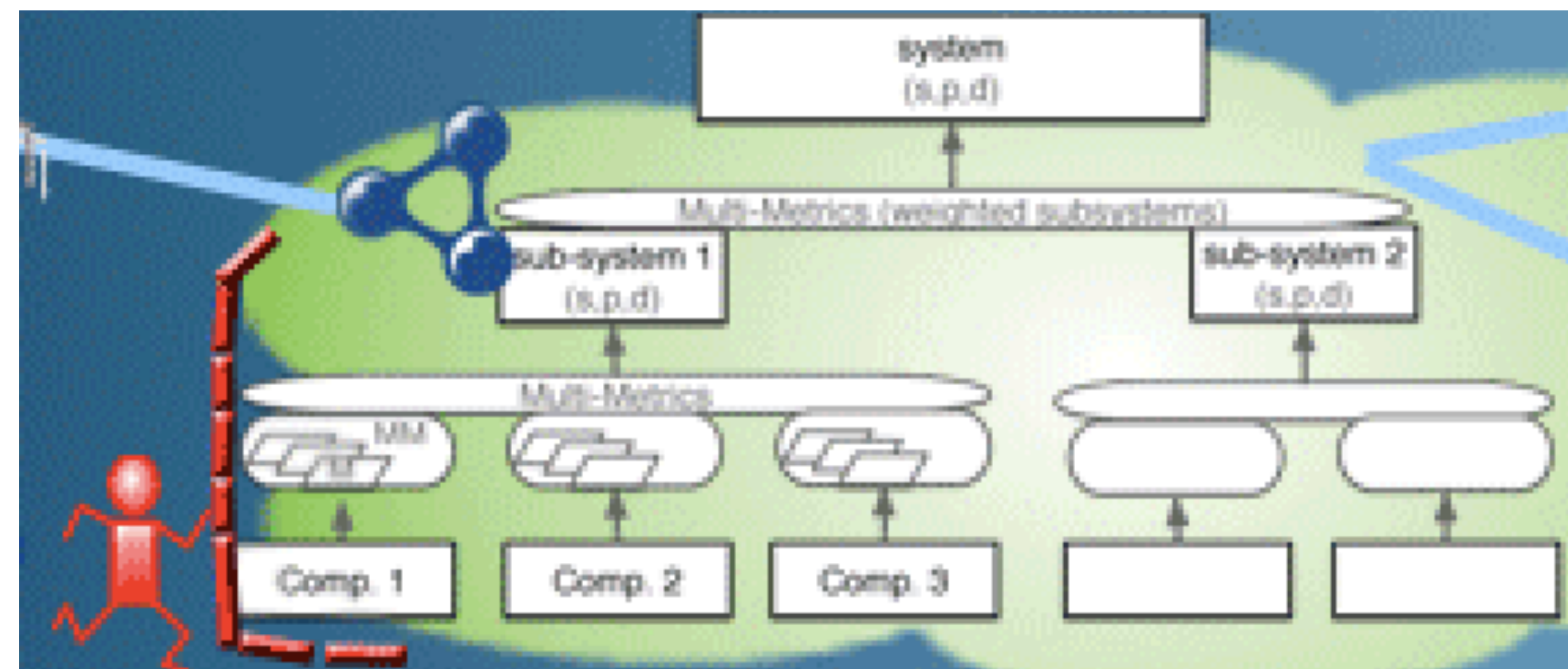
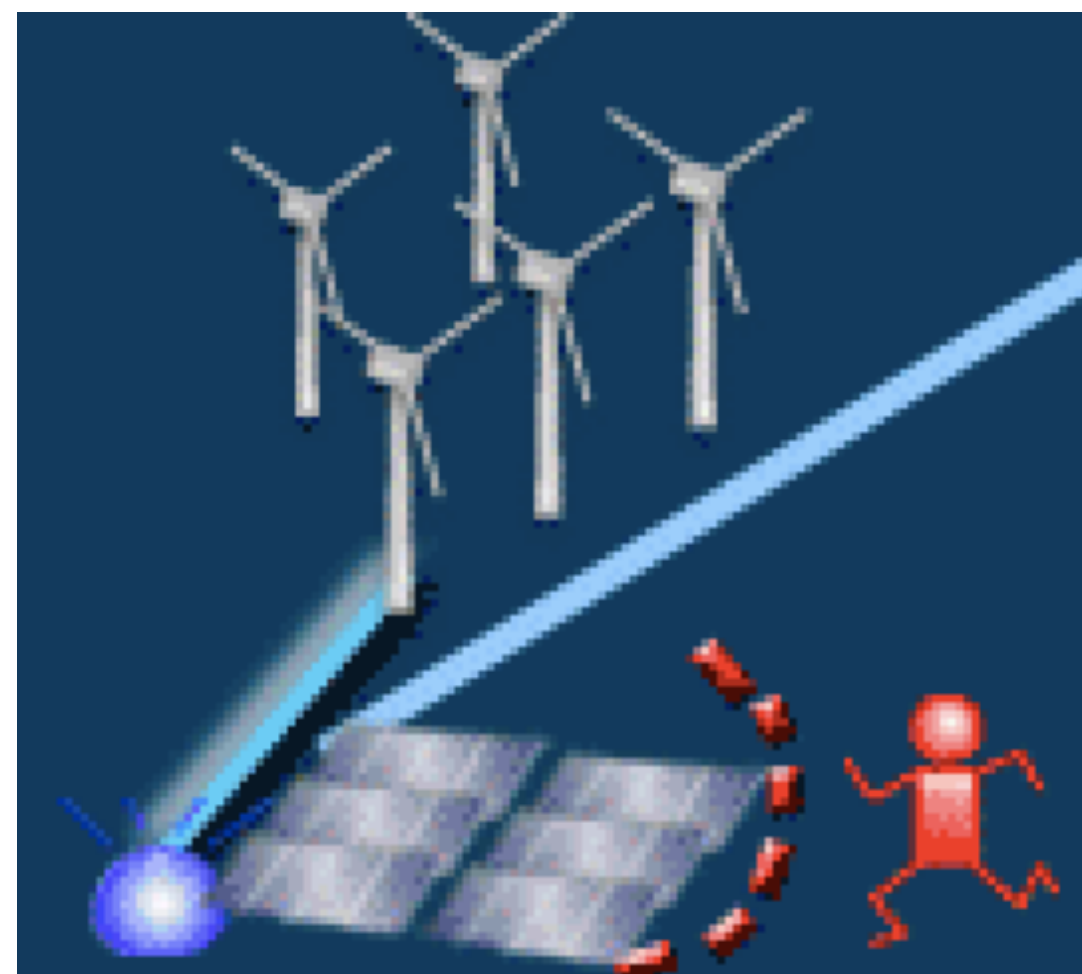
Future infrastructure/ services

- digitisation/Home4.0
- alarm, "green"



“Building the national Security Centre for Smart Grid”

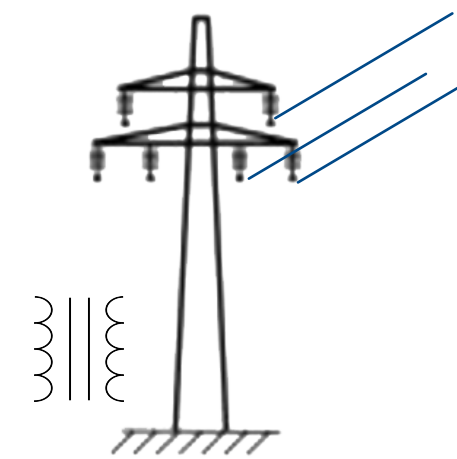
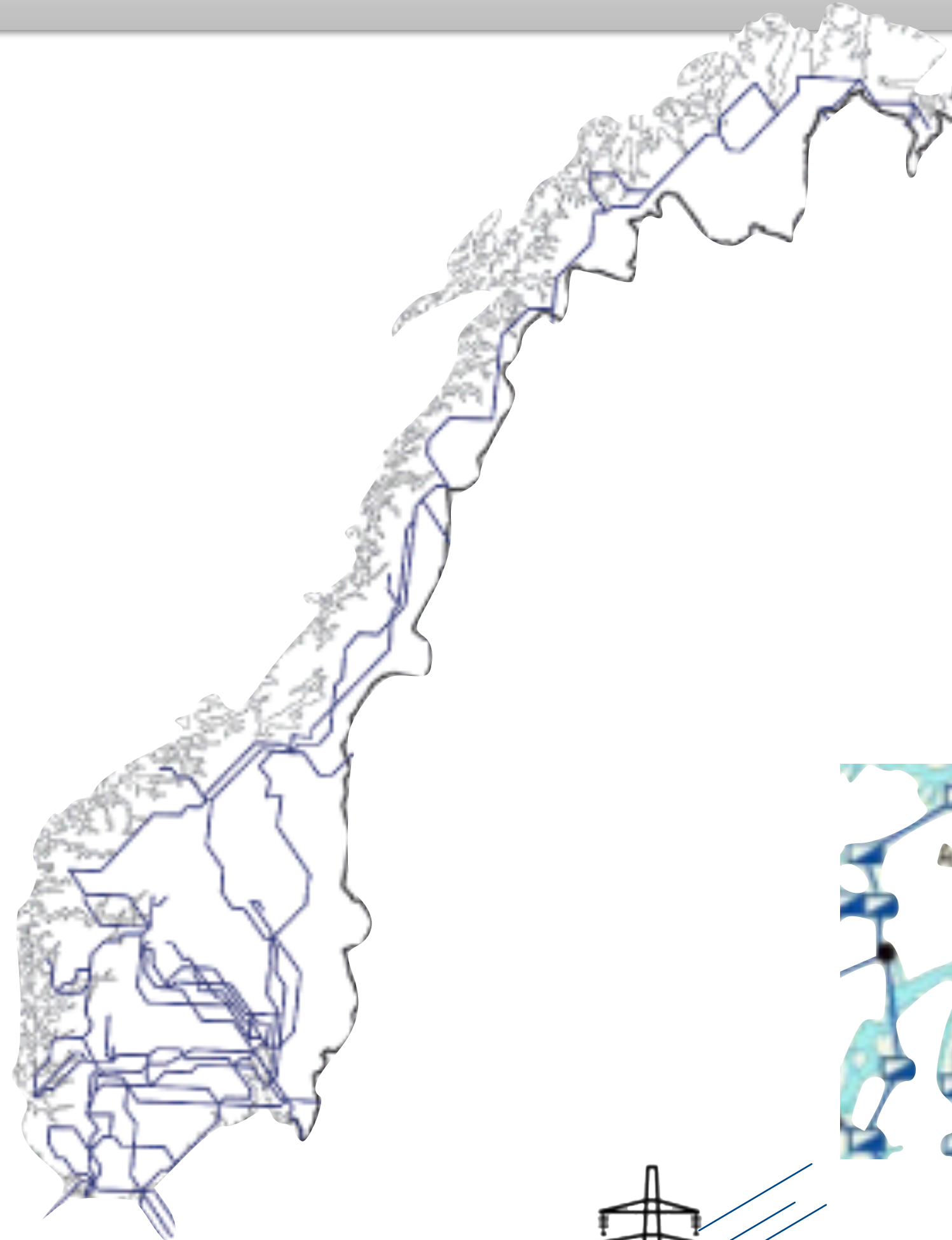
<http://IoTSec.no>



The Open Ecosystems for Future Services



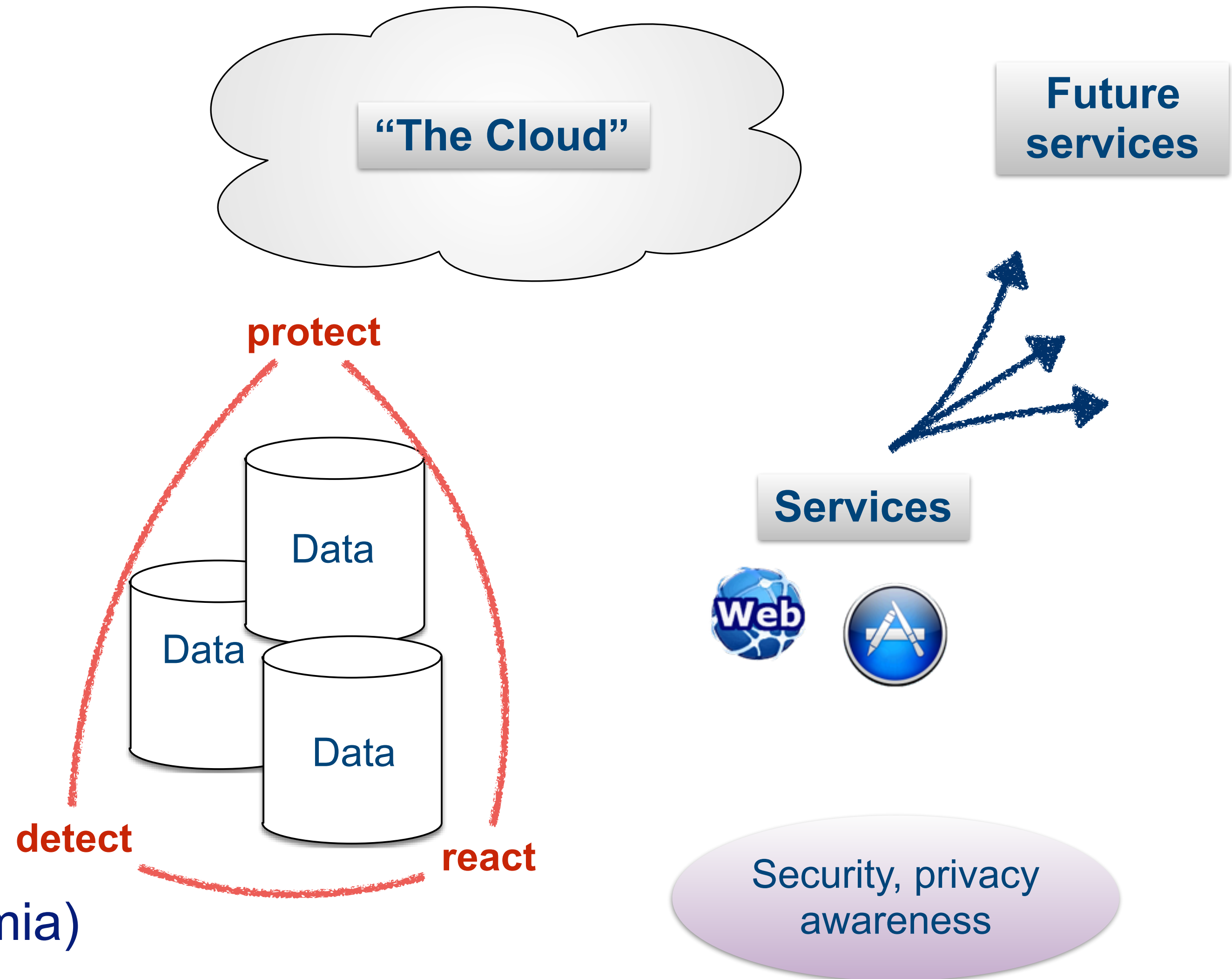
- Ongoing collaborations
- KraftCert & mnemonic
 - ➔ operational surveillance of the transport network
 - ➔ attack on the power infrastructure
- Smartgridsenteret
 - ➔ Conversion from power lines to smart grids
 - ➔ Conversion of industry
- A lot more to do ...



Smart Grid Security Centre (SGSC) Challenges from Public Partners



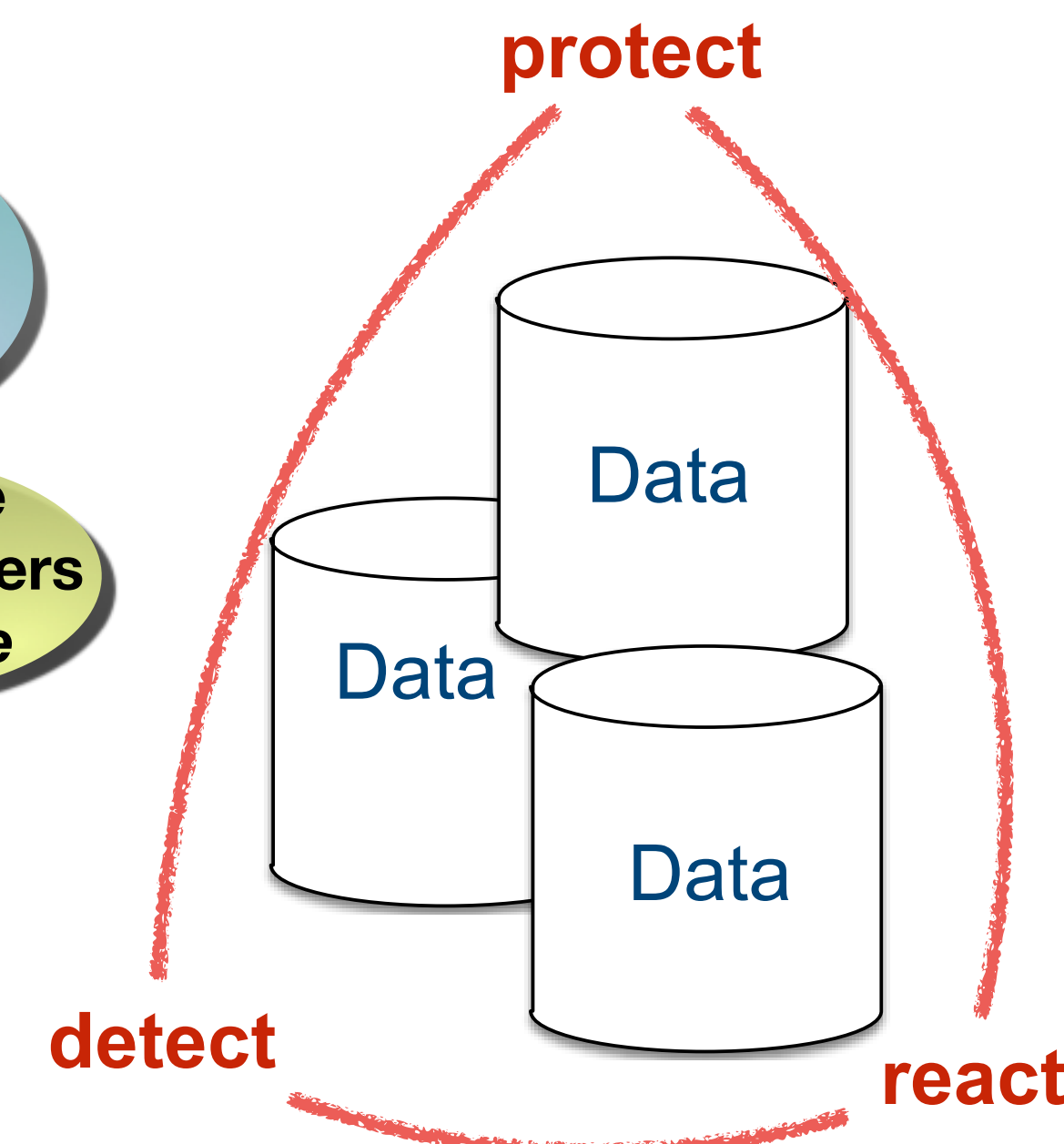
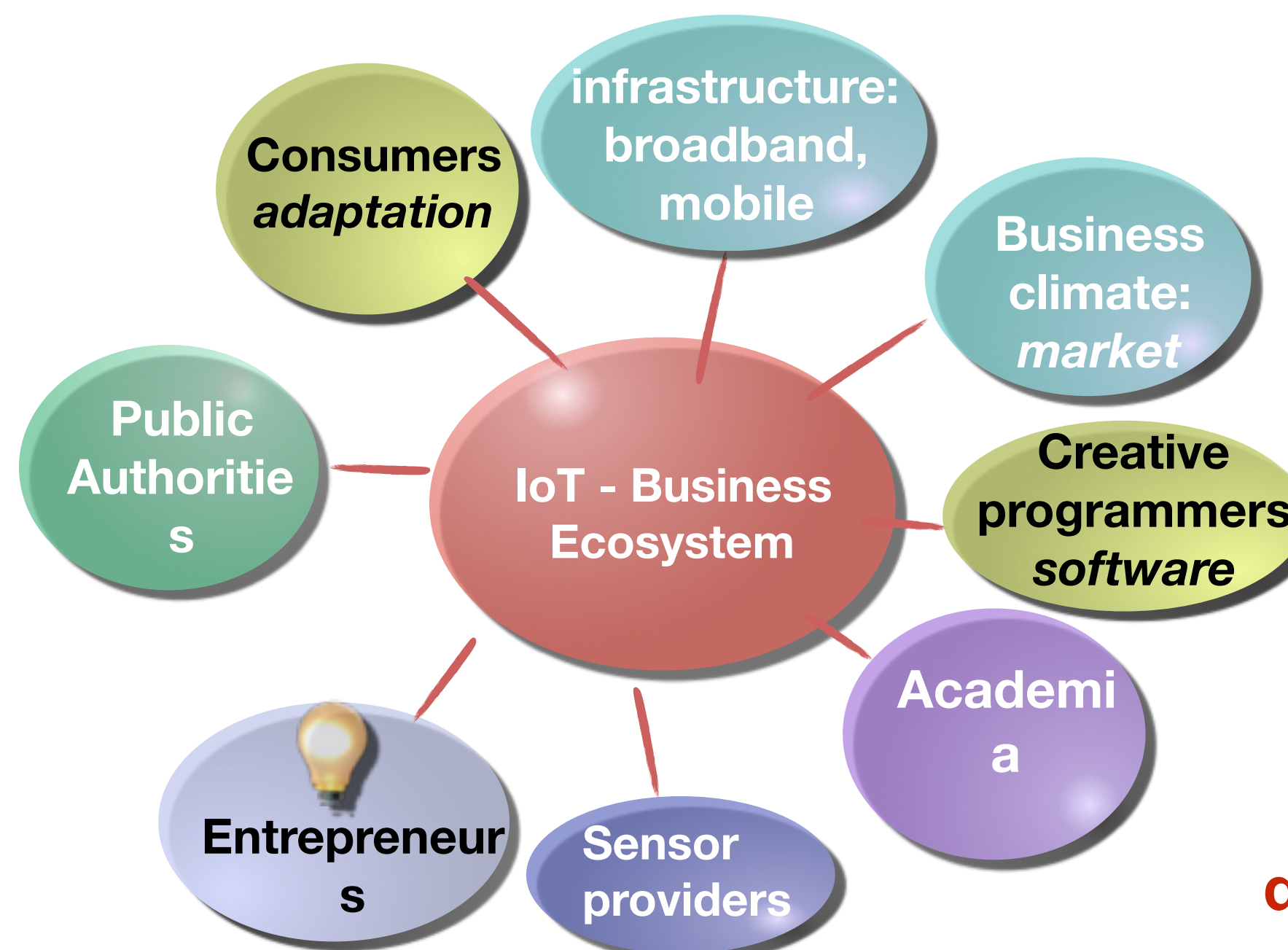
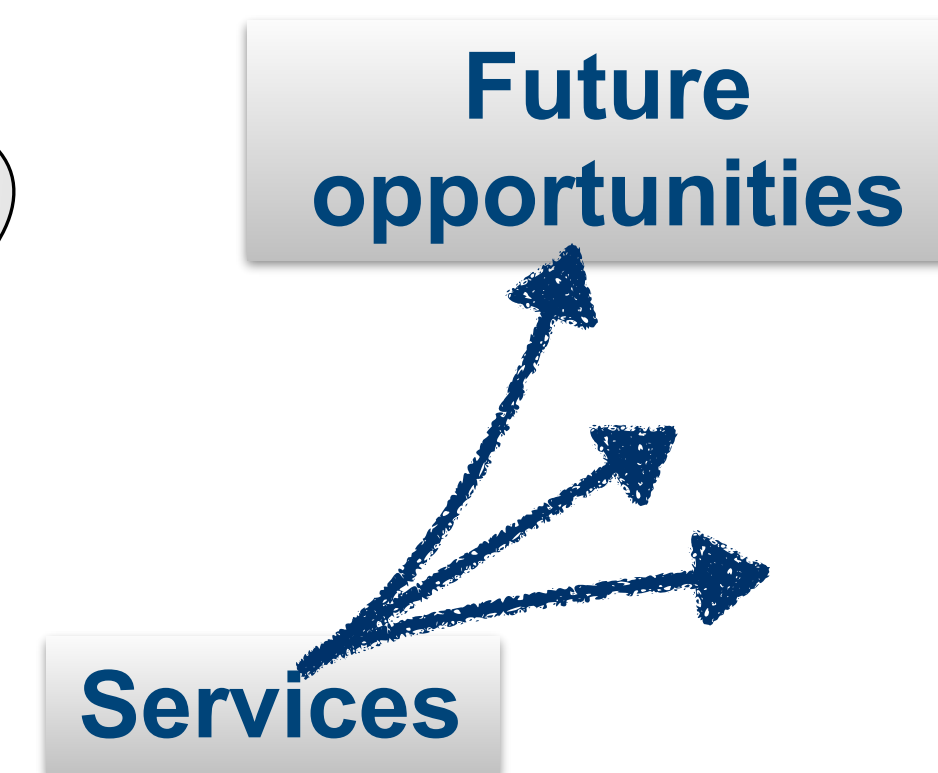
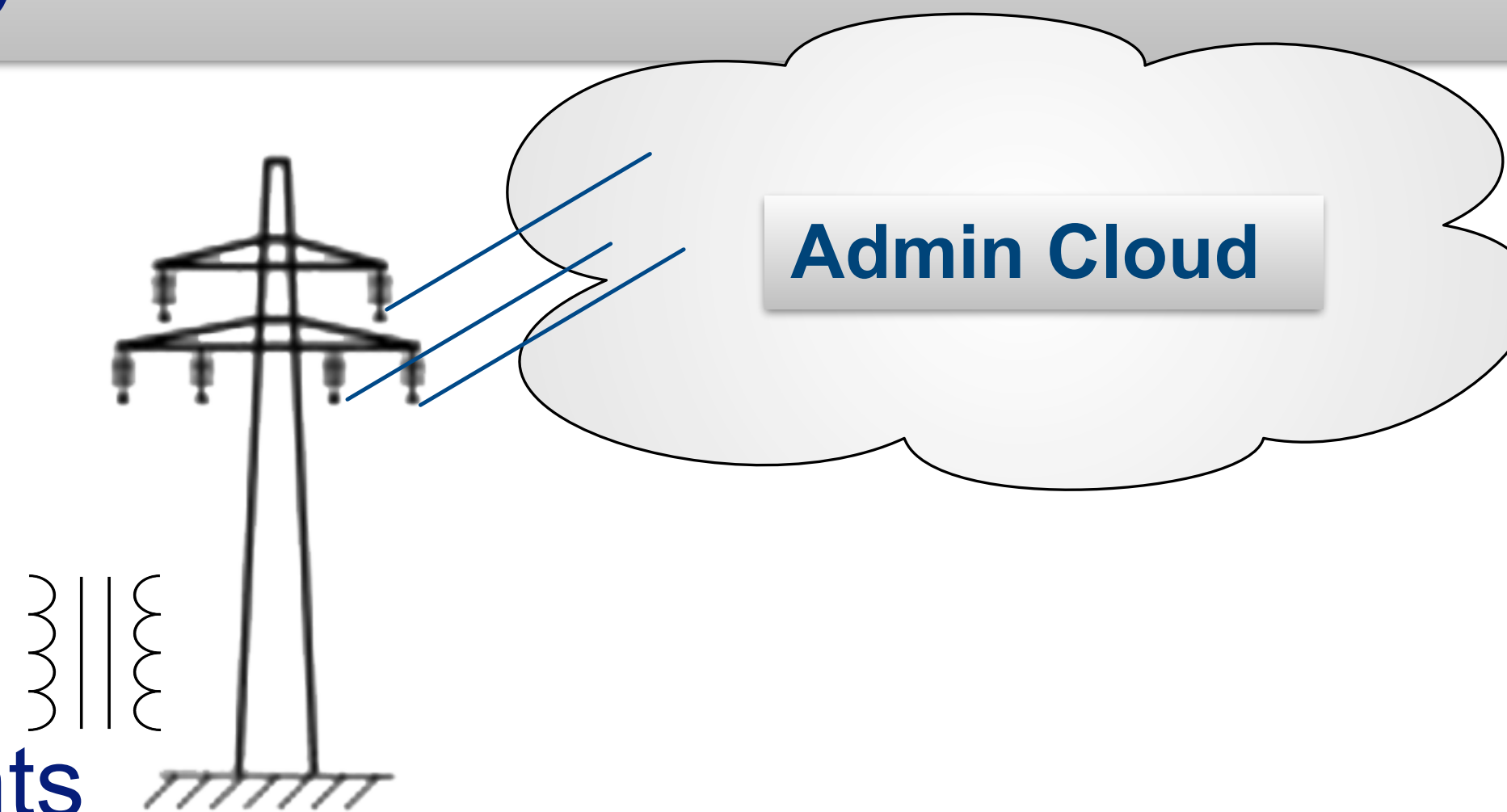
- The Cloud
 - ➔ Information handling
 - ➔ Information flow
- Security of infrastructures
 - ➔ Data handling
 - ➔ Data protection
- Demand of inhabitants
 - ➔ new services
 - ➔ technology inclusion
- Future services
 - ➔ Upcoming challenges (SGSC)
 - ➔ Analysis of information flow (Academia)
 - ➔ In-depth analysis (Institutes)



Smart Grid Security Centre (SGSC) Offerings to Electricity distributors



- Proactive maintenance
 - ➔ cost saving, reliability
 - ➔ security
- Novel services
 - ➔ Security and Privacy requirements
 - ➔ Opportunities
- Changing Business Ecosystem
 - ➔ Innovation
 - ➔ digital industries



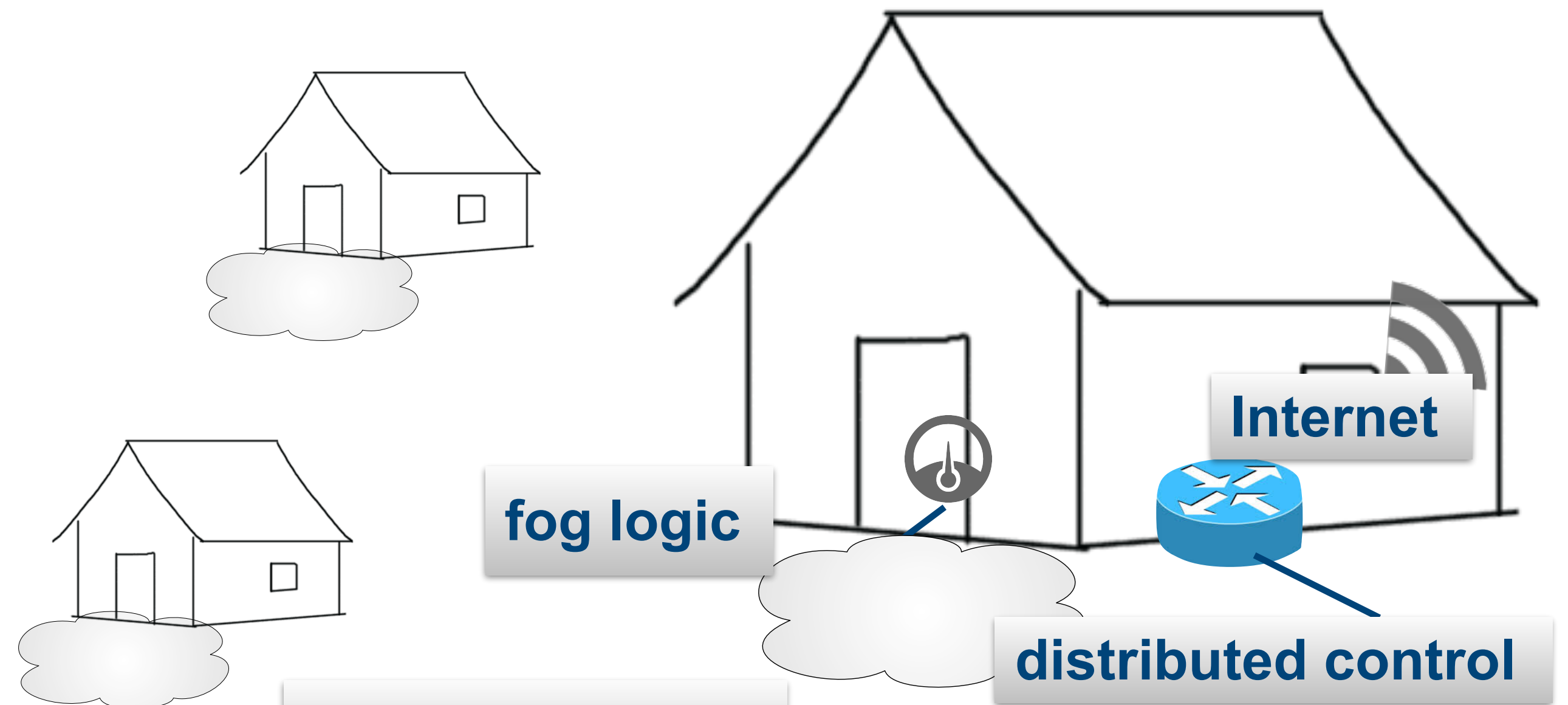
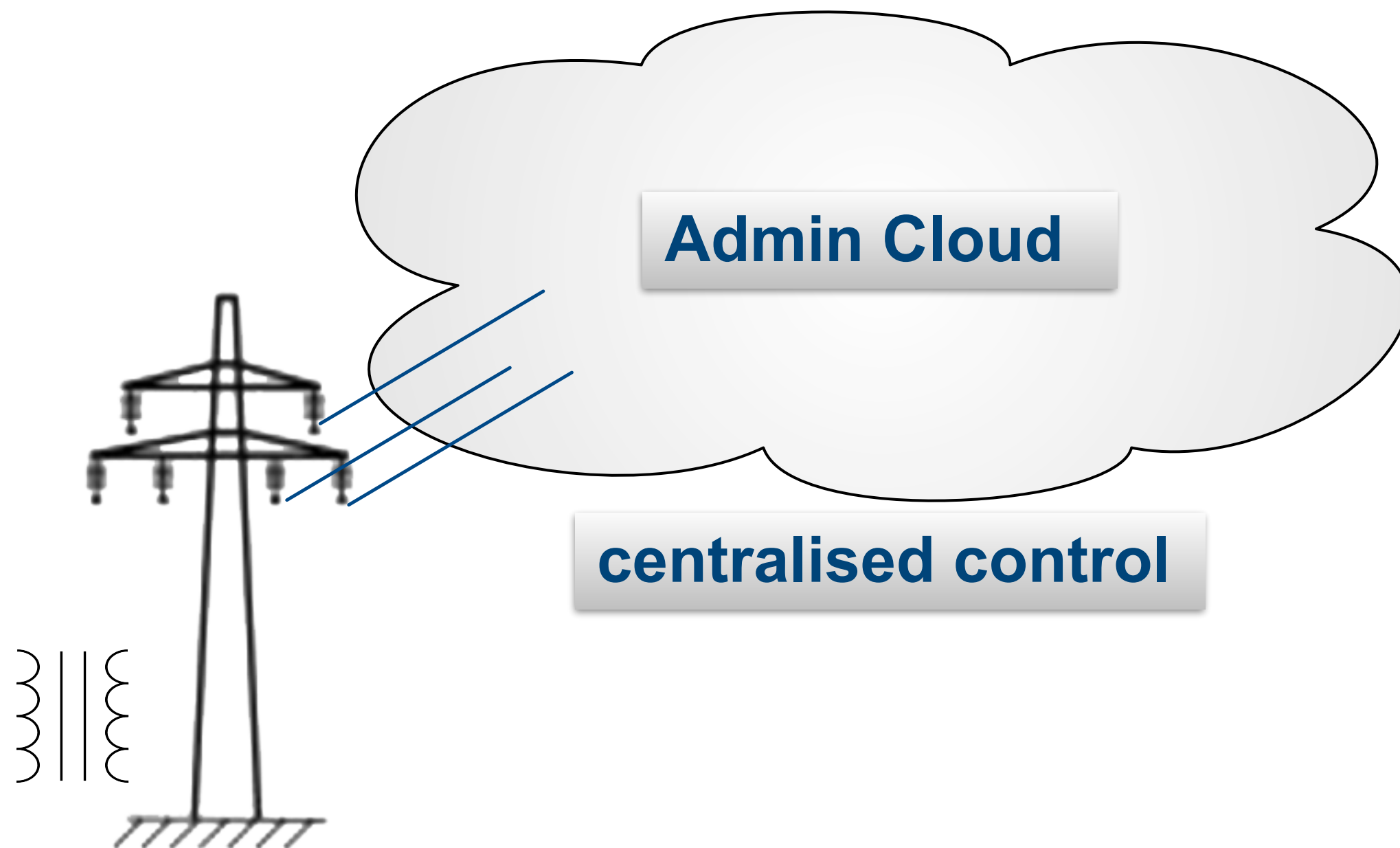
Smart Grid Security Centre (SGSC)

The main game changers



- Centralised Architectures
 - ➔ cloud administration
 - ➔ concentrated logic
- EU directive
 - ➔ Privacy, Health data, ...

- De-centralised architectures
 - ➔ smart grid & Internet
 - ➔ distributed logic & control
 - ➔ Internet & Smart Grid Infrastructure
 - ➔ trust & privacy handling
 - ➔ novel services in the home



Opportunities for Smart Grids



- Smart House/Building

- ➔ Power distribution

- proactive maintenance
- reliability

- ➔ Meter infrastructure

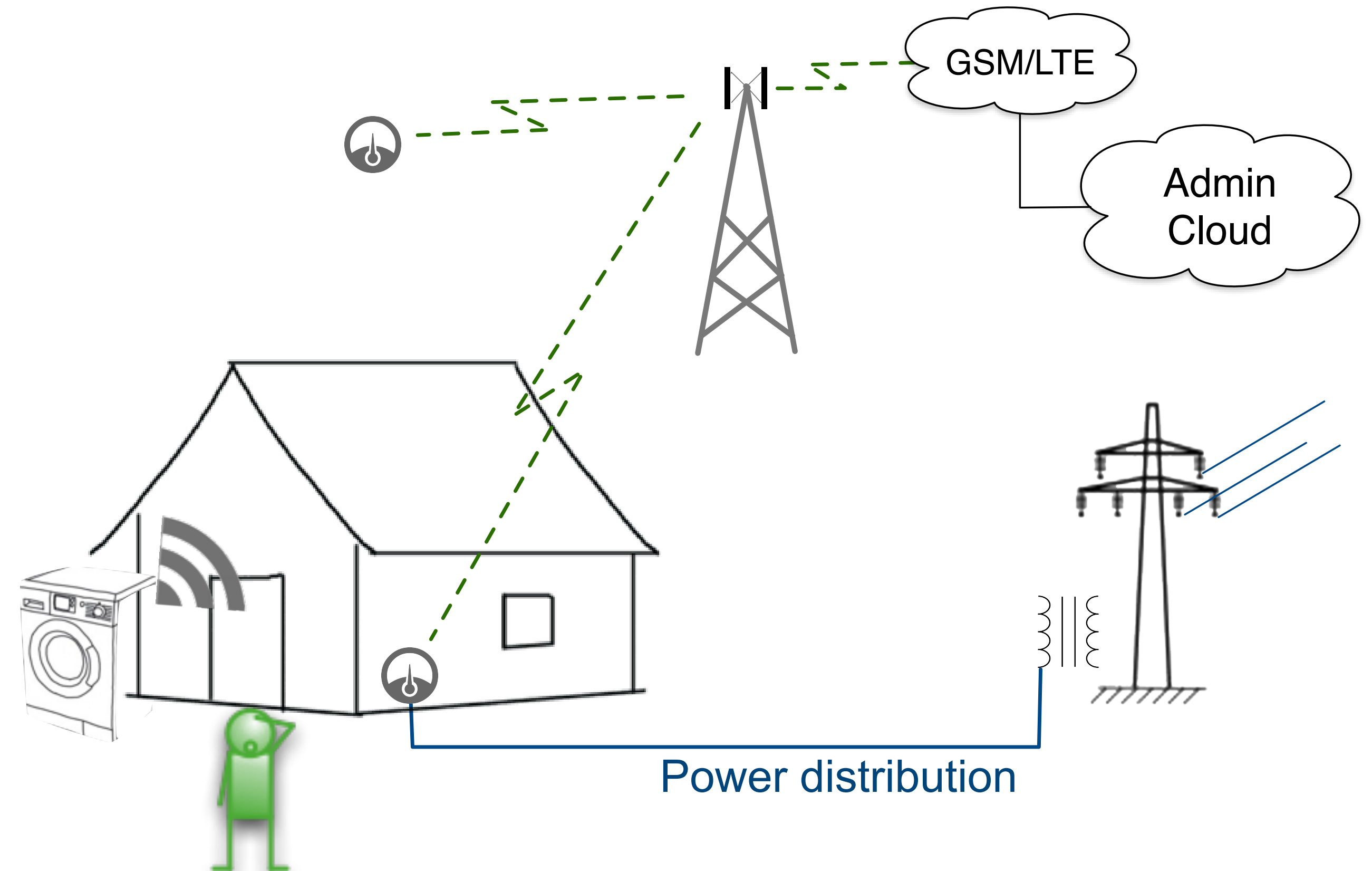
- Automatic Meter
- Collector
- Admin Cloud

- ➔ House infrastructure

- Hot-water, Heating
- White goods

- Novel services

- ➔ energy saving
- ➔ alarm
- ➔ virtual fall sensor



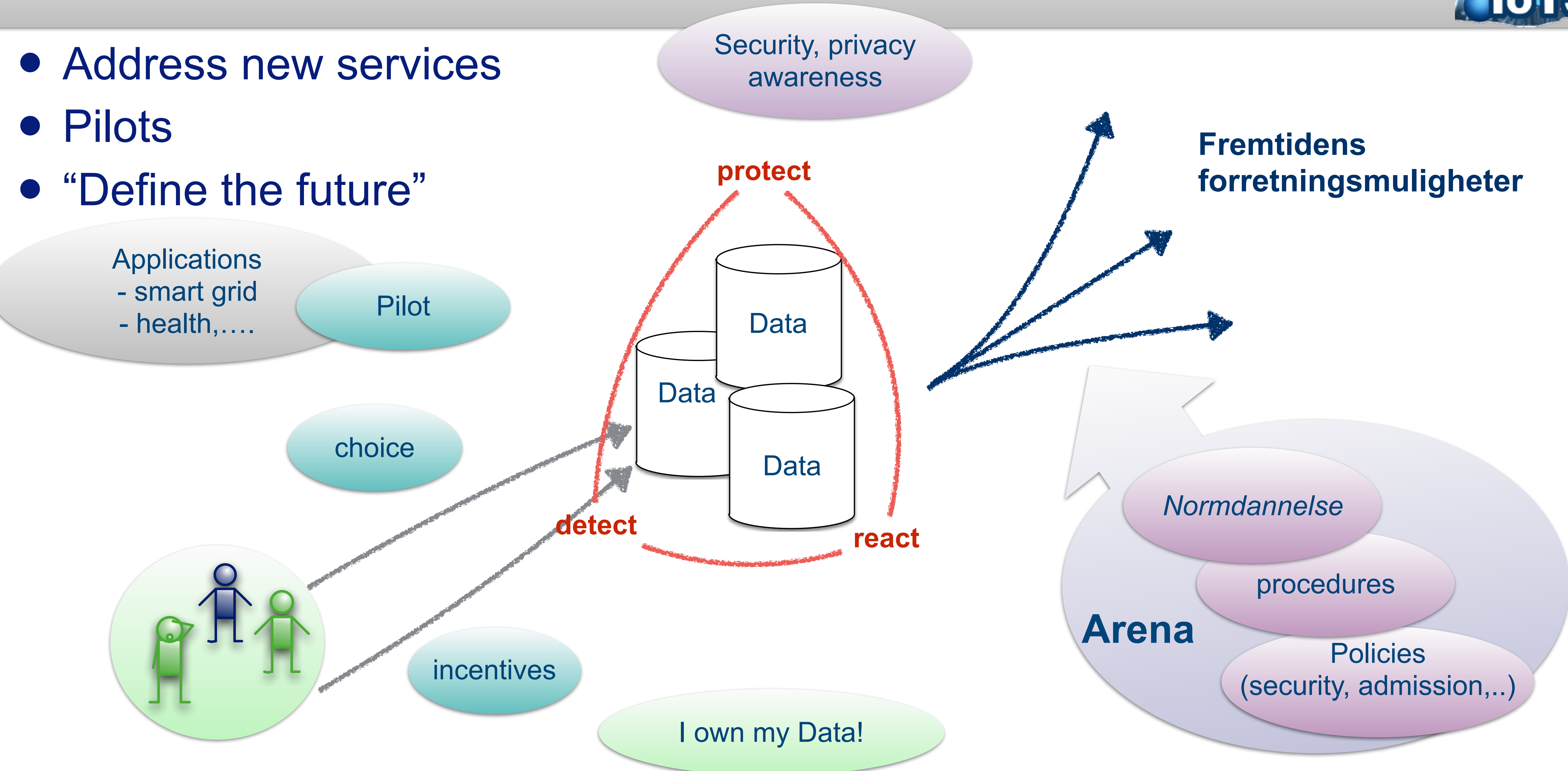
Future infrastructure/services

- digitisation/Home4.0
- Digital Society
- alarm, “green”

Opportunities for End-Customers

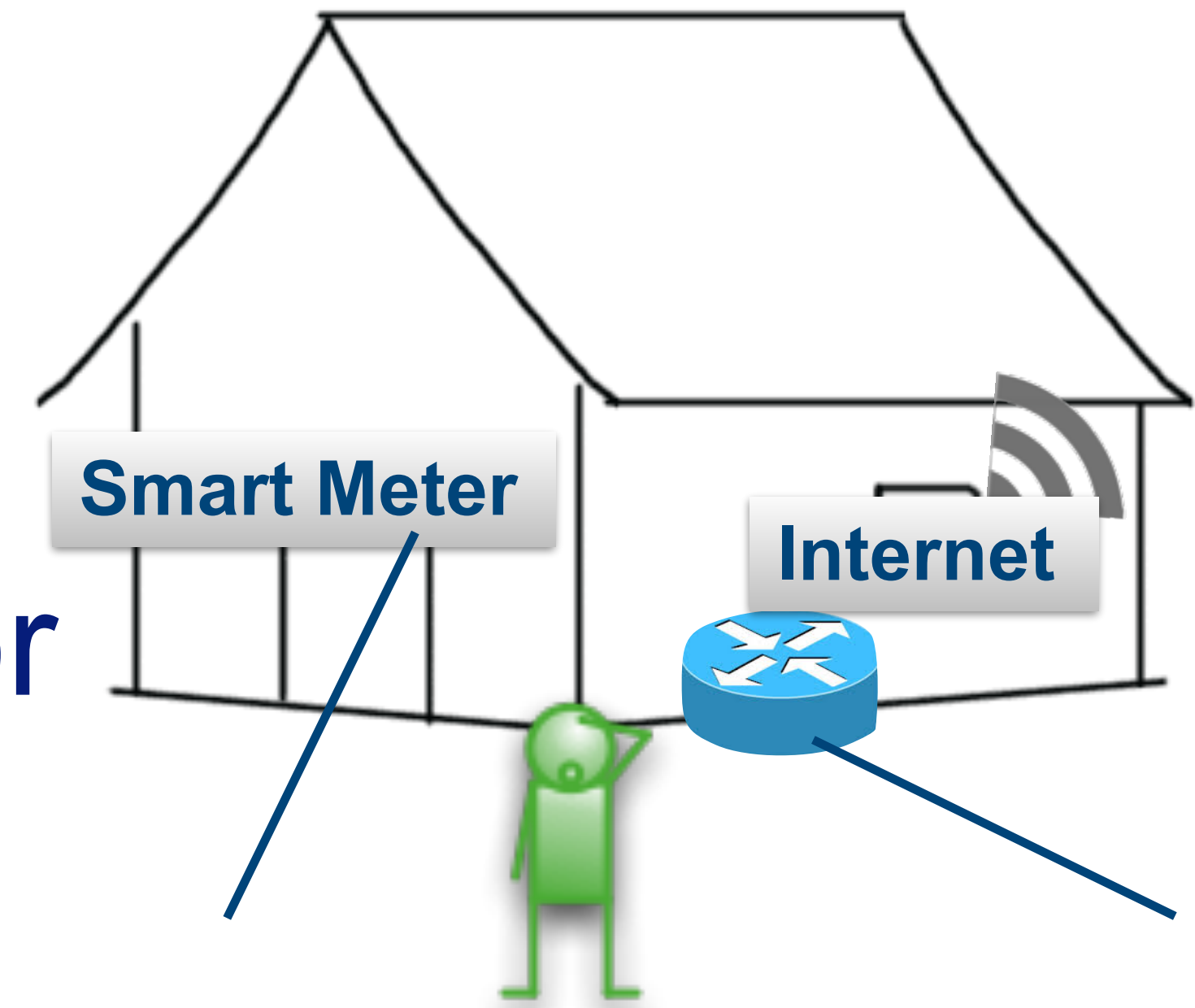


- Address new services
- Pilots
- “Define the future”



IoTSec.no

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



<http://IoTSec.no>



Knowledge and collaboration space

<http://IoTSec.no> - #IoTSec, #IoTSecNO



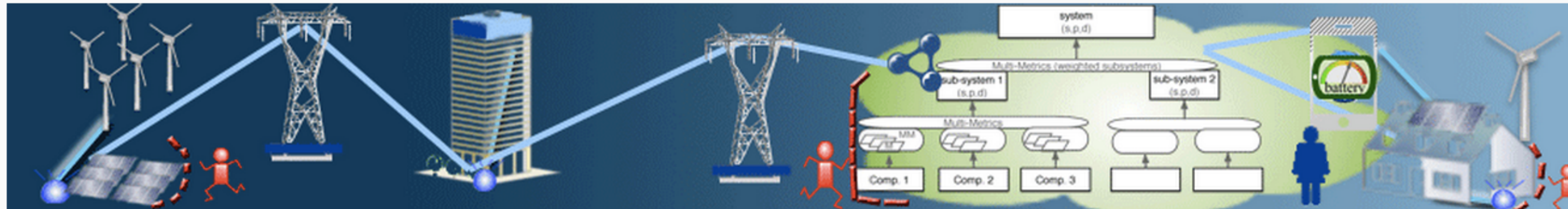
Home

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 Excellence (NCE Smart).

About

The IoTSec initiatives drives Research for secure IoT and Smart Grids

#iotsecno



Josef Noll
@josefnoll

11 Nov

NCE Smart Partnerkonferansen med @KristinHalvorsen og Nasjonalt senter for Sikkerhet



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

The threat dimension

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

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

So lässt sich das UMTS-Netz knacken



[source: www.rediff.com]

[source: Süddeutsche Zeitung, 18Dec2014]

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