



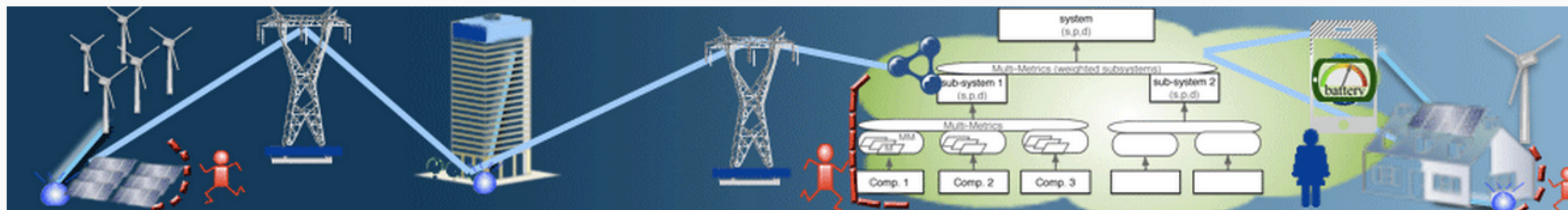
IoTSec Project Meeting 2Dec2015

Security in IoT for Smart Grid - IoTSec.no

Bernt A. Bremdal, Bjarne Tarjei Haugen, Christian Johansen, Dang Ha The Hien, Davide Roverso, Dieter Hirdes, Einar Snekkenes, Erik Åsberg, Habtamu Abie, Heidi Tuiskula, Iñaki Garitano, Jan Pedro Tumusok, Jayaprakash Rajasekharan, Josef Noll, Ketil Johansen, Knut Johansen, Leif Nilsen, Linda Firveld, Olaf Owe, Ole Gabrielsen, Otto Andreas Rustand, Paal Engelstad, Seraj Fayyad, Stein Gjessing, Stian Løvold, Vidar Kristoffersen, Yan Zhang, Åsmund Skomedal

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*

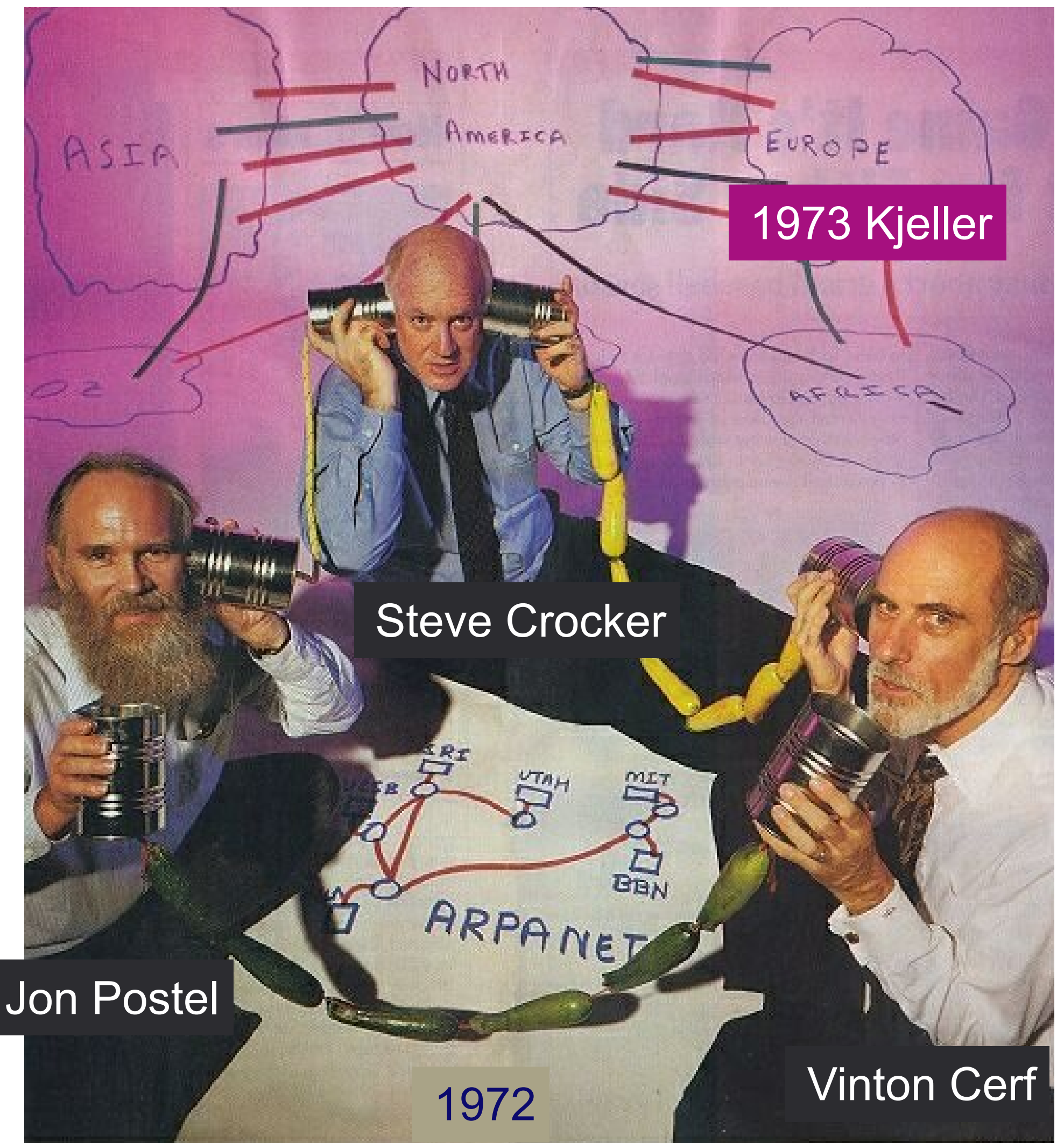
How come these guys didn't think of security?



UNIK and the Internet



- The building where the Internet (Arpanet) came to Europe in June 1973



: <http://www.michaelkaul.de/History/history.html>

The threat dimension

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

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

So lässt sich das UMTS-Netz knacken



[source: www.rediff.com]

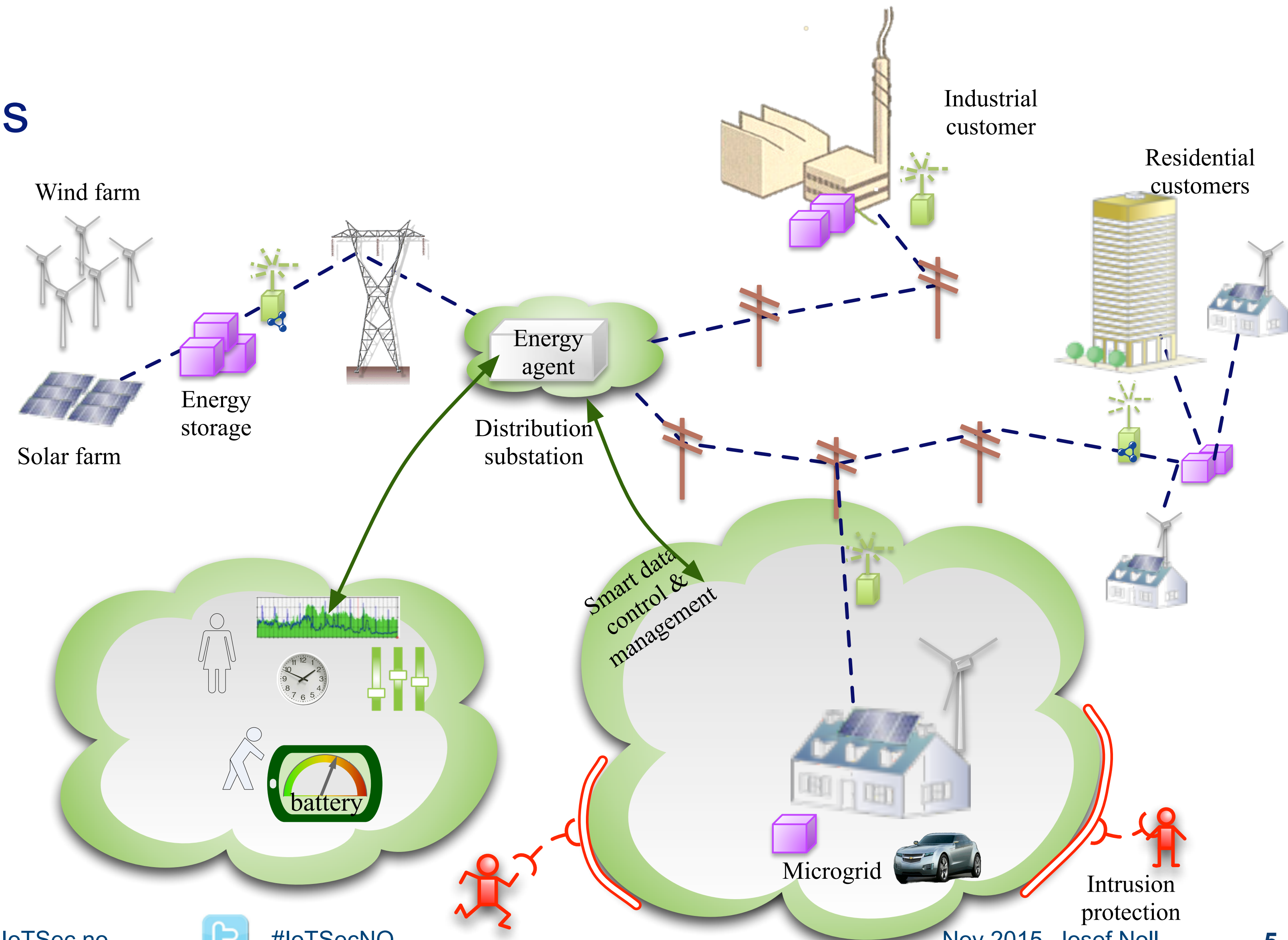
[source: Süddeutsche Zeitung,
18Dec2014]

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

The Smart Grid in the close future



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



Energy sector tops list of US industries under cyber attack, says Homeland Security report

12 March, 2015 at 6:38 PM Posted by: Jeremy Cowan

Washington, DC. March 12, 2015 — A report issued today by the US Department for Homeland Security says that in 2014 the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to 245 incidents reported by asset owners and industry partners.

The energy sector, says *Jeremy Cowan*, led all others again in 2014 with 79 reported incidents, followed by manufacturing at 65 and worryingly healthcare at 15 reported incidents. ICS-CERT's continuing partnership with the Energy sector reportedly provides many opportunities to share collaborate on incident response efforts.



Power Grid Cyber Attacks Keep the Pentagon Up at Night

A detailed look at why computers running the U.S. electrical infrastructure are so vulnerable to digital threats

By Michael McElfresh and The Conversation | June 8, 2015

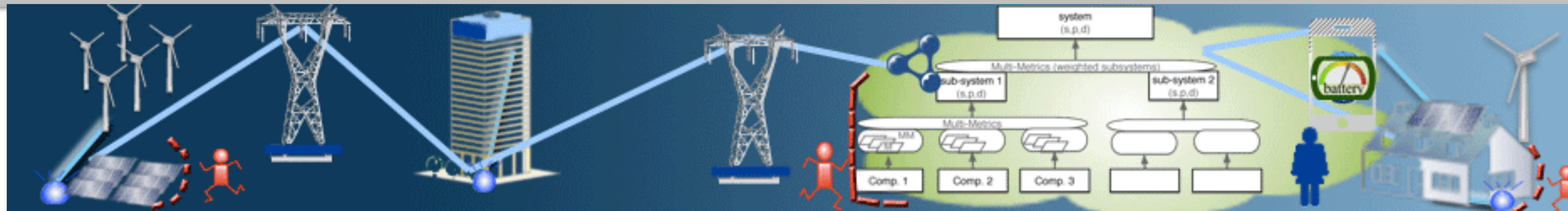
The following essay is reprinted with permission from [The Conversation](#), an online publication covering the latest research.

It's very hard to overstate how important the US power grid is to American society and its economy. Every critical infrastructure, from communications to water, is built on it and every important business function from banking to milking cows is completely dependent on it.



Scott Wylie/Flickr

#IoTSecNO, #IoTSec IoTSec.no facts



- Research Initiative: Security in IoT for Smart Grids
 - applicable for Internet of Things (IoT)
 - focussed on Smart Grid security
- Facts
 - 1Oct2015 - 30Sep2020, 32 MNOK budget (25 MNOK NFR)
 - 10 founding partners,
 - 18 partners (Nov2015)
- Main outcome
 - Research in Security for Smart Grid
 - Industrial Smart Grid Security Centre



Partners



- Founding partners

- University of Oslo (UiO) through the Institute for Informatics (Ifi) and the University Graduate Centre (UNIK),
- Norwegian Computing Centre (NR)
- Simula Research Laboratory (SRL)
- Gjøvik University College
- NCE Smart Energy Markets (NCE Smart)
- eSmart Systems (eSmart)
- Frederikstad Energi (FEN)
- EB Nett (EB)
- Movation (MOV)

- Associated Academic Members

- Mondragon Unibersitatea, Spain
- University of Victoria, Canada
- Universidad Carlos III de Madrid, Spain
- University of Roma La Sapienza, Italy

- Associated Industrial Members

- Mondragon Unibersitatea, Spain
- Fredrikstad kommune
- EyeSaaS
- Nimbeo
- H2020 and ECSEL projects

- COINS Academic Research School

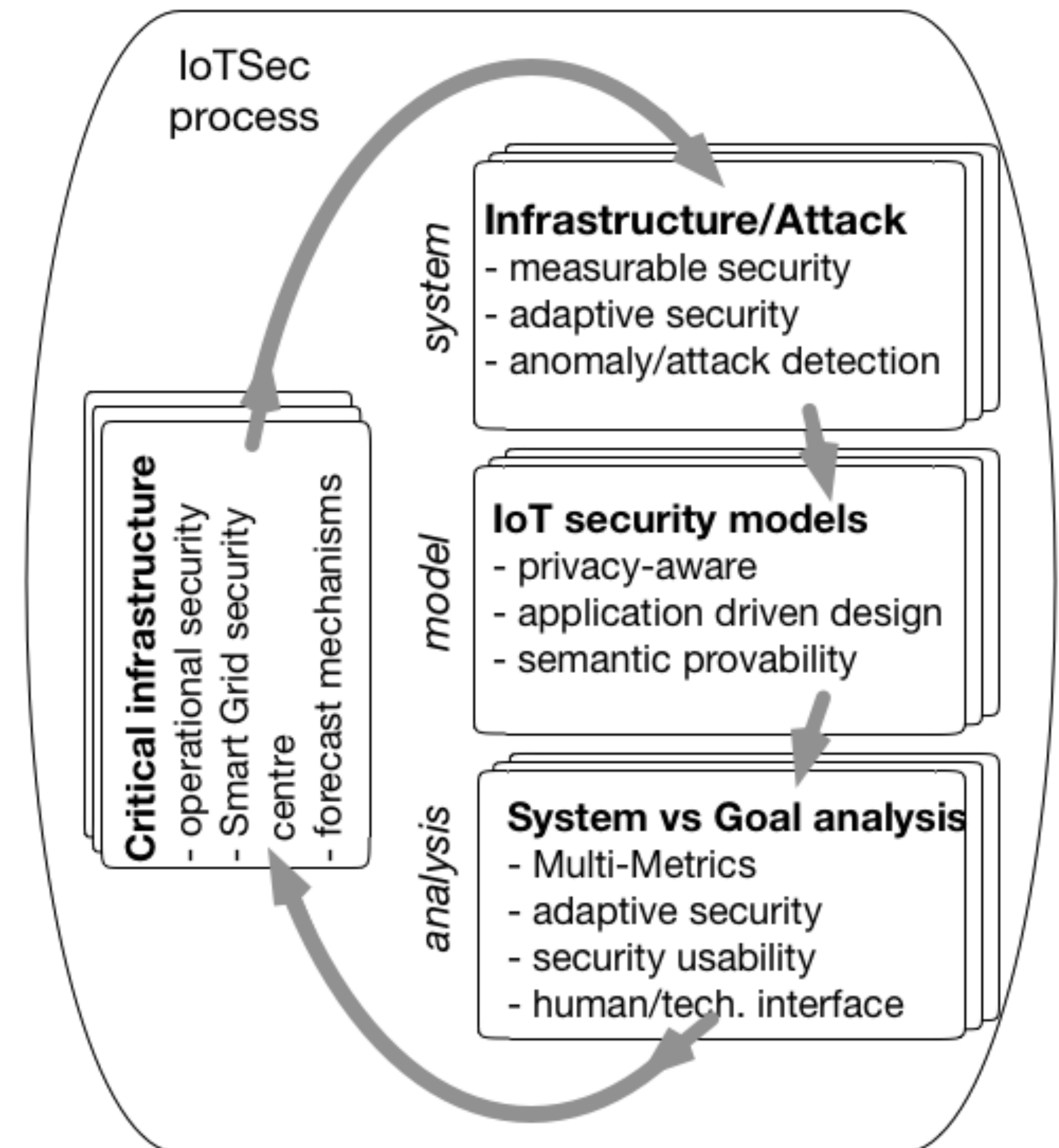
Research Topics



- Tailoring «security challenges» to targeted research
- Security in IoT Ecosystem
- Semantic modelling and provability
- Measurable Security, Privacy and Dependability
- Adaptive security

Operational requirements

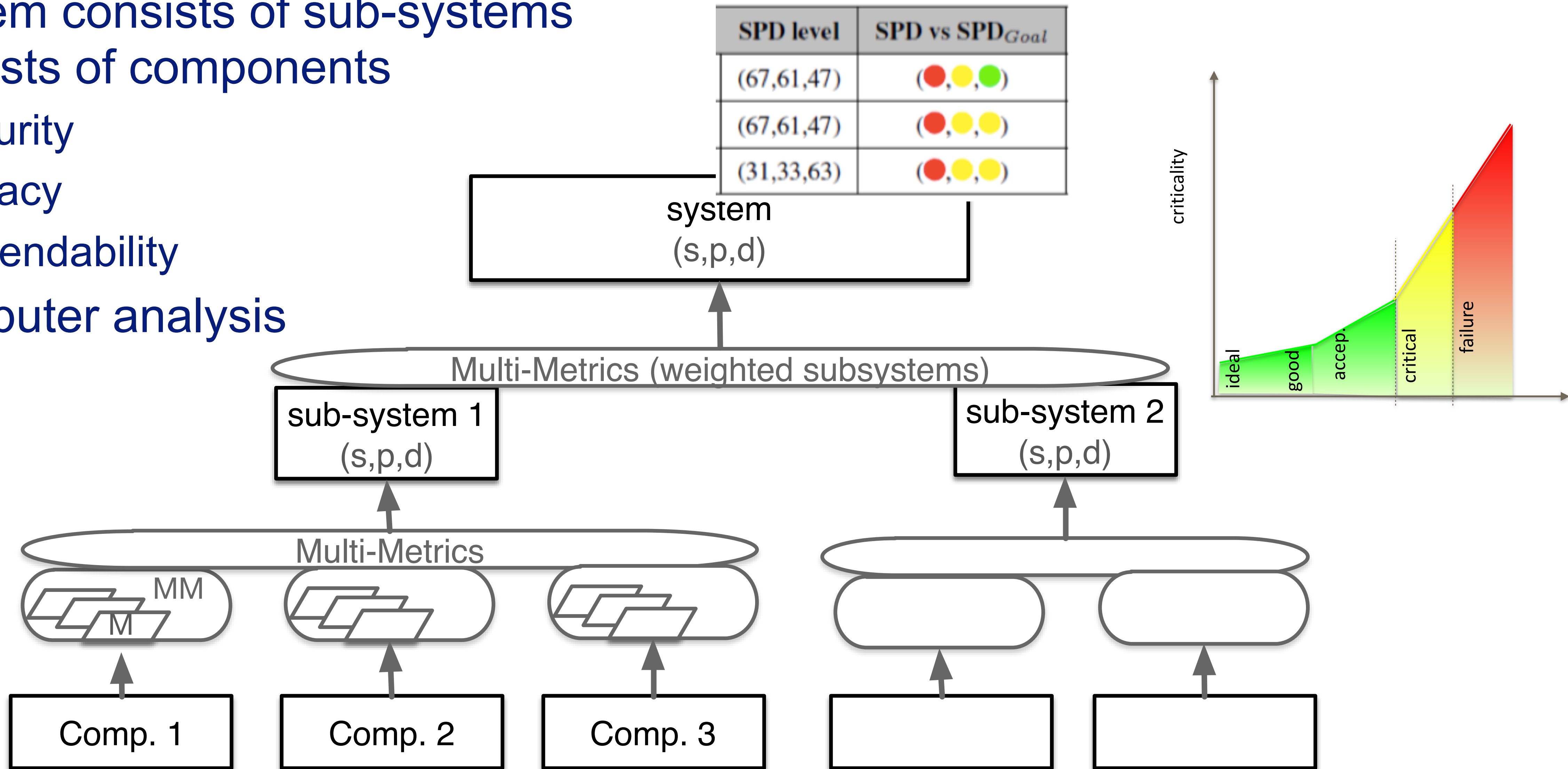
- Operational security
- Forecast mechanisms
- Operation Centre (from Smart Grid to Smart City)



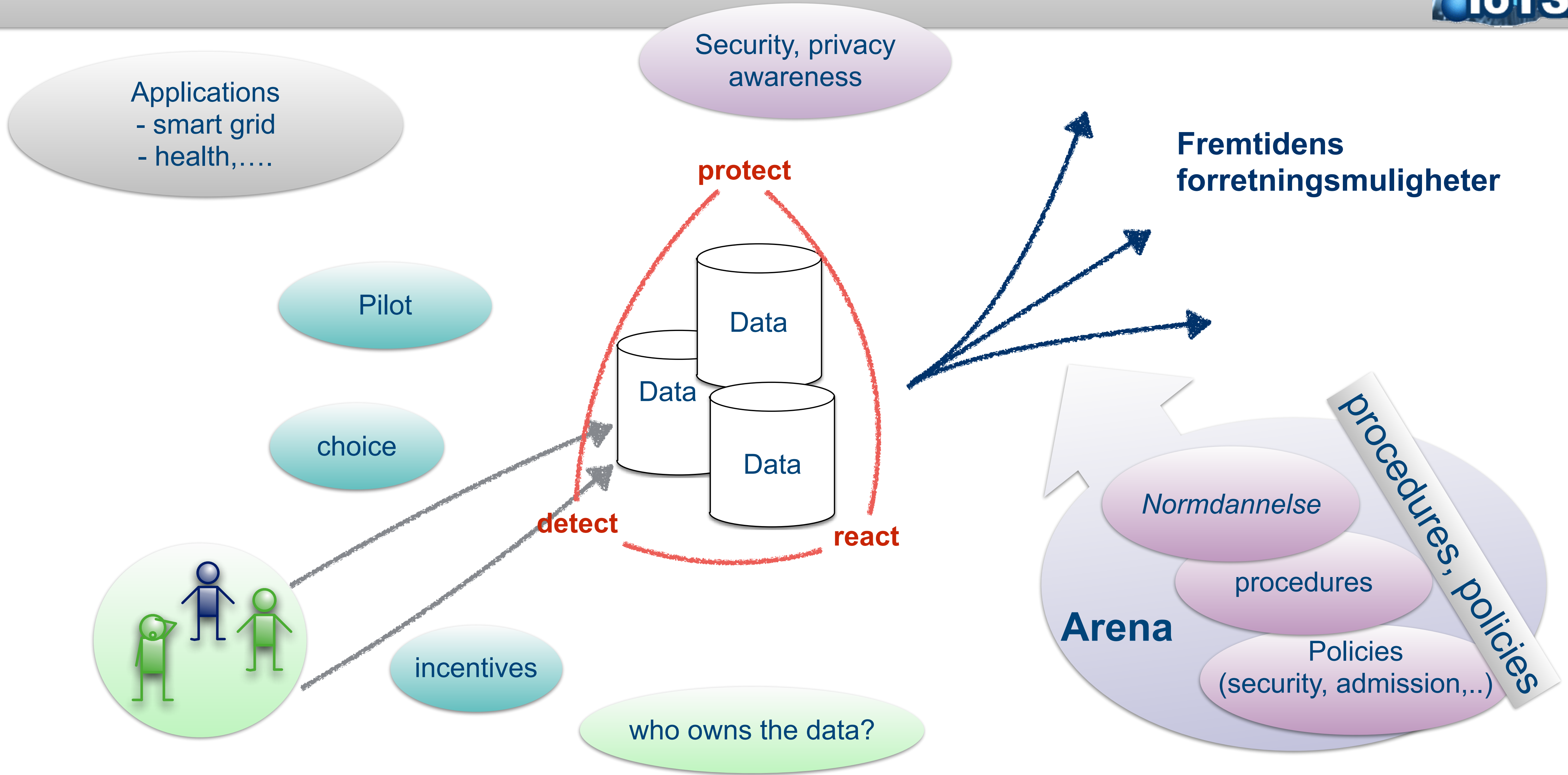
Example of Research: Multi-Metrics - system composition



- System consists of sub-systems
consists of components
 - security
 - privacy
 - dependability
- Computer analysis



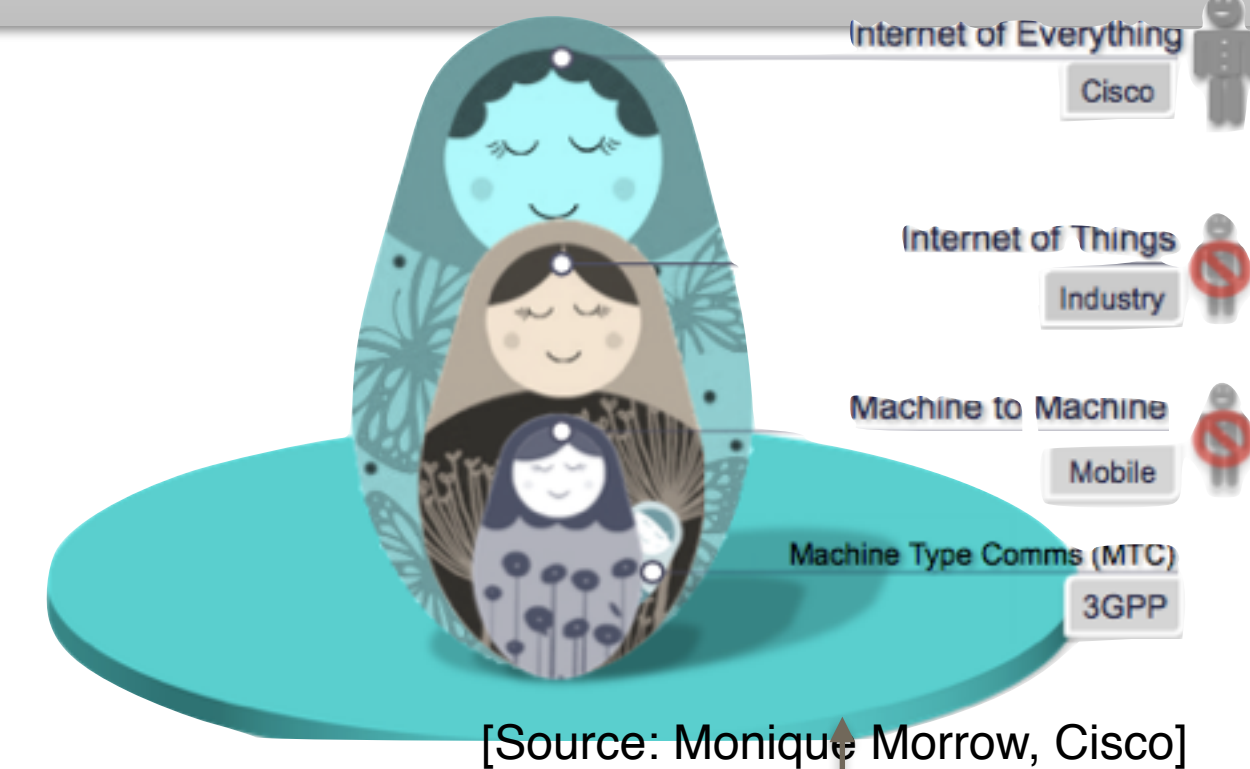
Ecosystem for Innovasjon



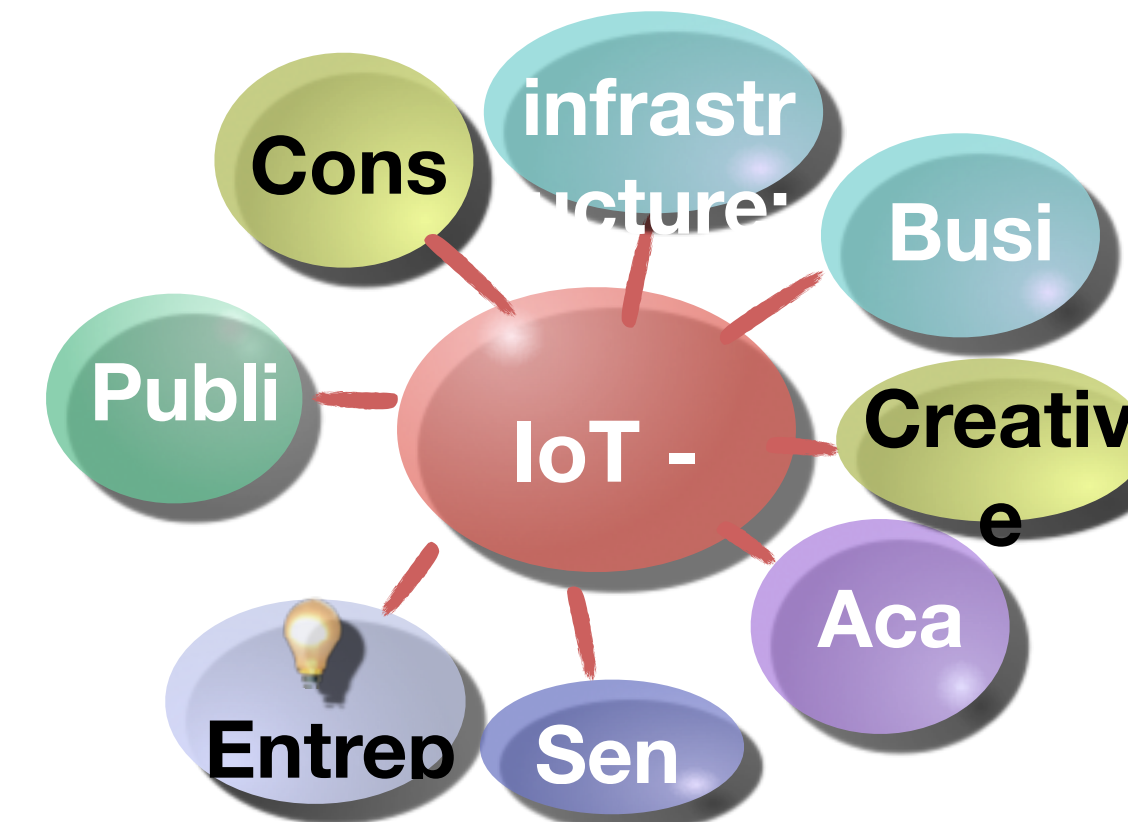
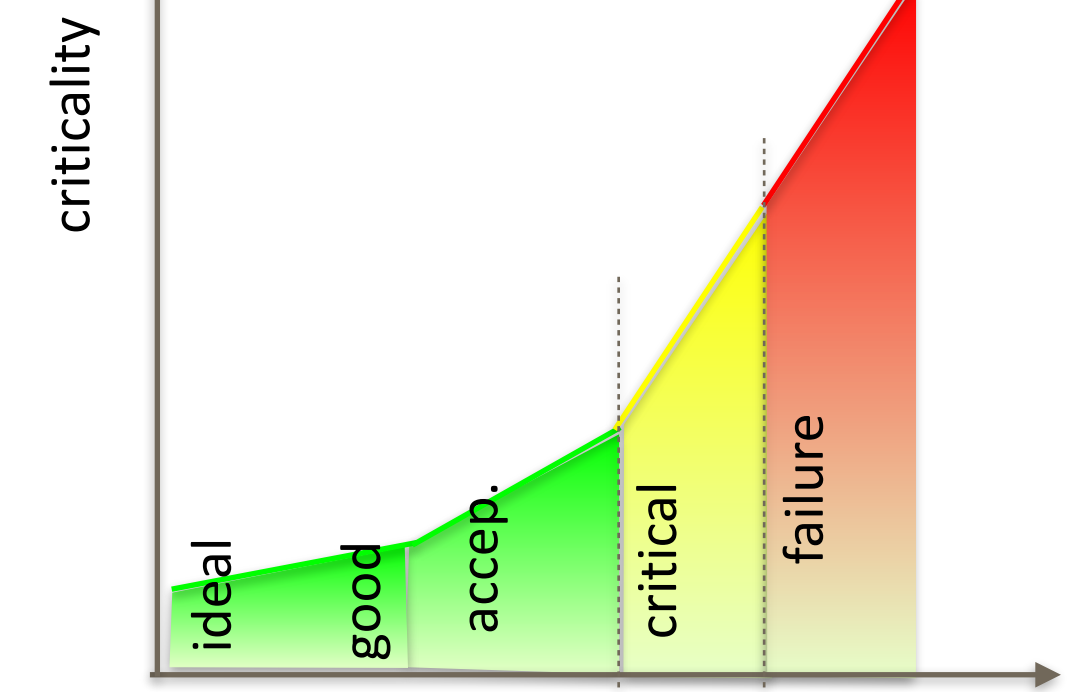
Conclusions



- Internet of Things (IoT) is a game changer
 - Unfair advantage in the Nordics
 - Autonomous systems, Critical Infrastructure
- Collaborative approach for a (more) secure society
 - trust is not enough, need for measurable
 - partnership for security: threats, measures, counter activities
- Measurable Security and Privacy for IoT
 - IoTSec.no - Security for Smart Grid
 - Dependable access
 - Industrial impact: Security Centre for Smart Grid
- Innovation ecosystem with security and privacy
 - Pilots for Procedures, Norms & Policies
- *Join us for a more secure Innovation Ecosystem*



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





Interested to join our Initiative?
- contact one of the partners
- call, SMS 9083 8066, @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 end users of additional IoT services by exploring use cases and the intent to design the building blocks for a secure and privacy-aware ecosystem for the Internet of Things. If you want to contribute with your industrial requirements, your knowledge or your infrastructure, please contact us for collaboration.

Benefits of partnership [\[edit\]](#)

Our aim is to contribute to a secure and privacy-aware ecosystem for the Internet of Things. If you want to contribute with your industrial requirements, your knowledge or your infrastructure, please contact us for collaboration.

About

The IoTSec initiatives drives Research for secure IoT and Smart Grids.

[IoTSec](#) [\[edit\]](#)

The vision of **IoTSec - Security in IoT for Smart Grids** is to promote the development of a safe and secure Internet-of-Things (IoT)-enabled smart power grid infrastructure. IoTSec will apply the research in the envisaged Security Centre for Smart Grids, co-located with the Norwegian Centre of Excellence (NCE Smart). [Read more ...](#)

Consortium [\[edit\]](#)

The founding partners of the initiative were:

- University of Oslo (UiO) through the Institute for Informatics (Ifi) and the University Graduate Centre (UNIK),
- Norwegian Computing Centre (NR)
- Simula Research Laboratory (SRL)
- Gjøvik University College
- NCE Smart Energy Markets (NCE Smart)
- eSmart Systems (eSmart)
- Frederikstad Energi (FEN)
- EB Nett (EB)
- Movation (MOV)

As of 2015, the consortium includes the following partners:

- Spain
- Madrid, Spain
- Italy
- include