UNIK4750 - Measurable Security for the Internet of Things

L1 – Introduction

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

Josef Noll
UiO/UNIK
josef@unik.no

http://cwi.unik.no/wiki/UNIK4750, #IoTSec, #IoTSecNO

Overview

- Expectations
- Lecture overview
- Exam
- Topic introduction

Expected outcome:

- Describe application-driven security and establish challenges of sensor-driven systems
- Provide industrial examples, e.g. Smart Grid and automatic meter readings
- Establish application-driven security goals as well as the semantics of your system
- Generate matrices to describe the security impact of components and sub-systems, and perform a multi-metrics analysis to establish the system security
- Analyse application goal versus system security and suggest improvements

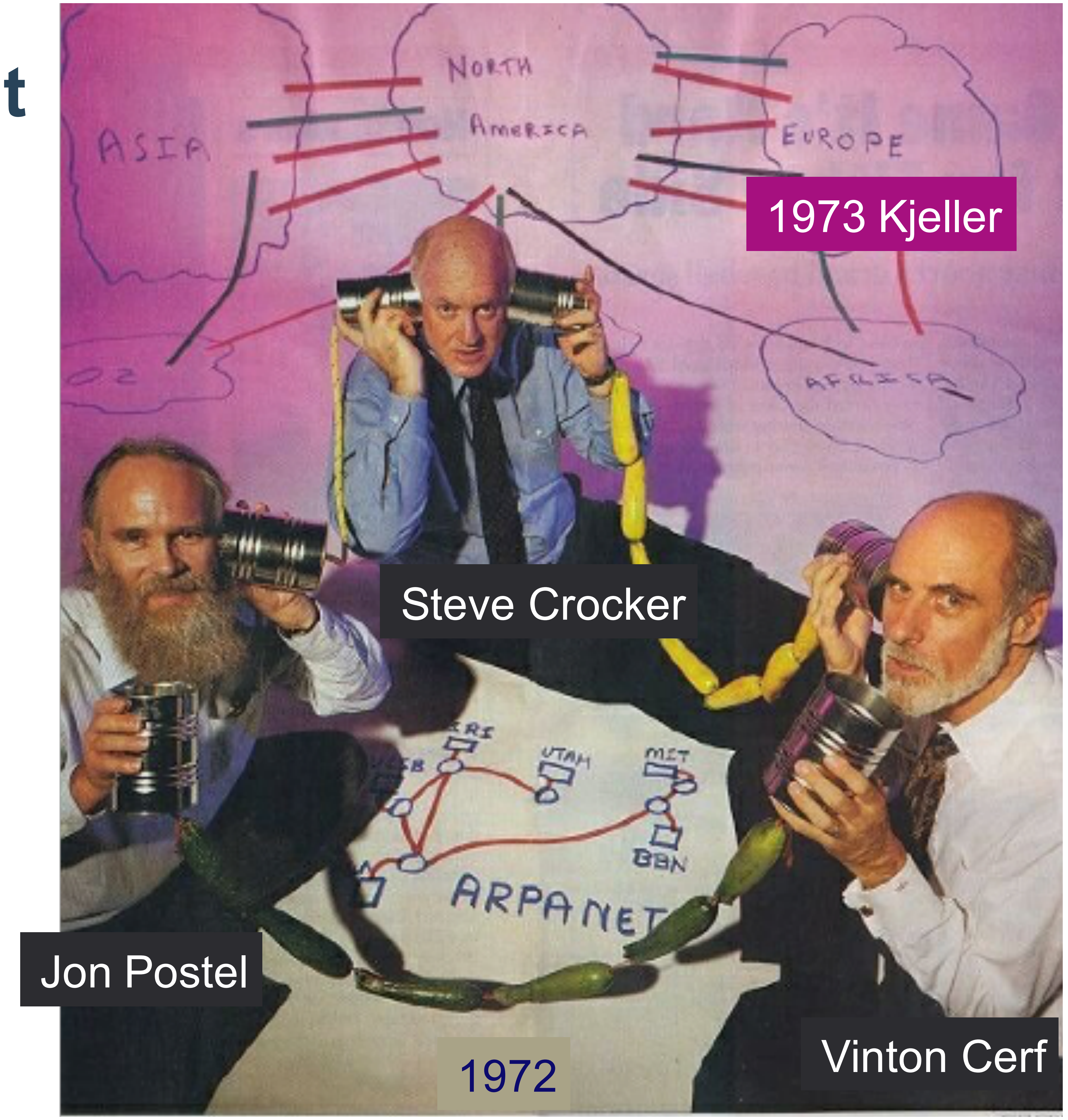
UNIK4750: Lecture plan

- 21Jan - L1: Introduction
- 28Jan - L2: Internet of Things
- 4Feb - L3: Security of IoT- Paper selection
- 11Feb - L4: Smart Grid, Automatic Meter Readings (AMR)
- 18Feb - L5: Service implications on functional requirements
- *25Feb - vinterferie*
- 3Mar - L6: Technology mapping
- 10Mar - L7: Paper analysis with 15-20 min presentation
- 17Mar - L8: Practical implementation of ontologies
- *24Mar - Easter Holidays*
- 31Mar - L9: Logical binding - industrial example - possible guest lecture
- 7Apr - L10: Multi-Metrics Method for measurable Security
- 14Apr - L11: Multi-Metrics Weighting of an AMR sub-system
- 21Apr - L12: System Security and Privacy analysis
- 28Apr - L13: Phenomena "intrusion-detection", possible guest lecture
- *5May - Kristi Himmelfart - fridag*
- 12May - L14: Real world examples - IoTSec infrastructure
- 19May - L15: Real world IoT service evaluation group work
- 26May - Exam

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



1973 Kjeller

Steve Crocker

Jon Postel

1972

Vinton Cerf

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 Abhören von Handys

So lässt sich das UMTS-Netz knacken

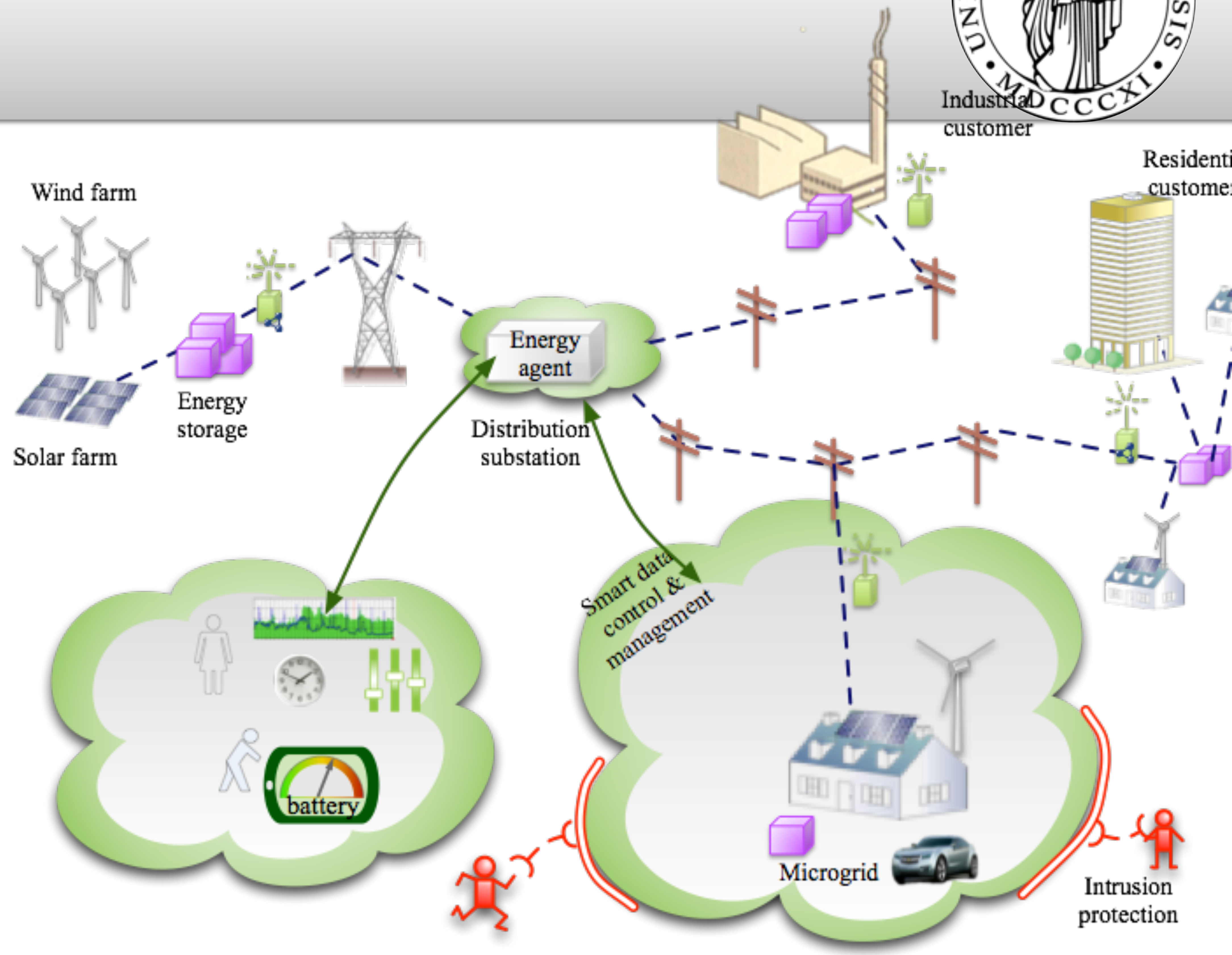
[source: Süddeutsche Zeitung, 18Dec2014]

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

[source: www.rediff.com]

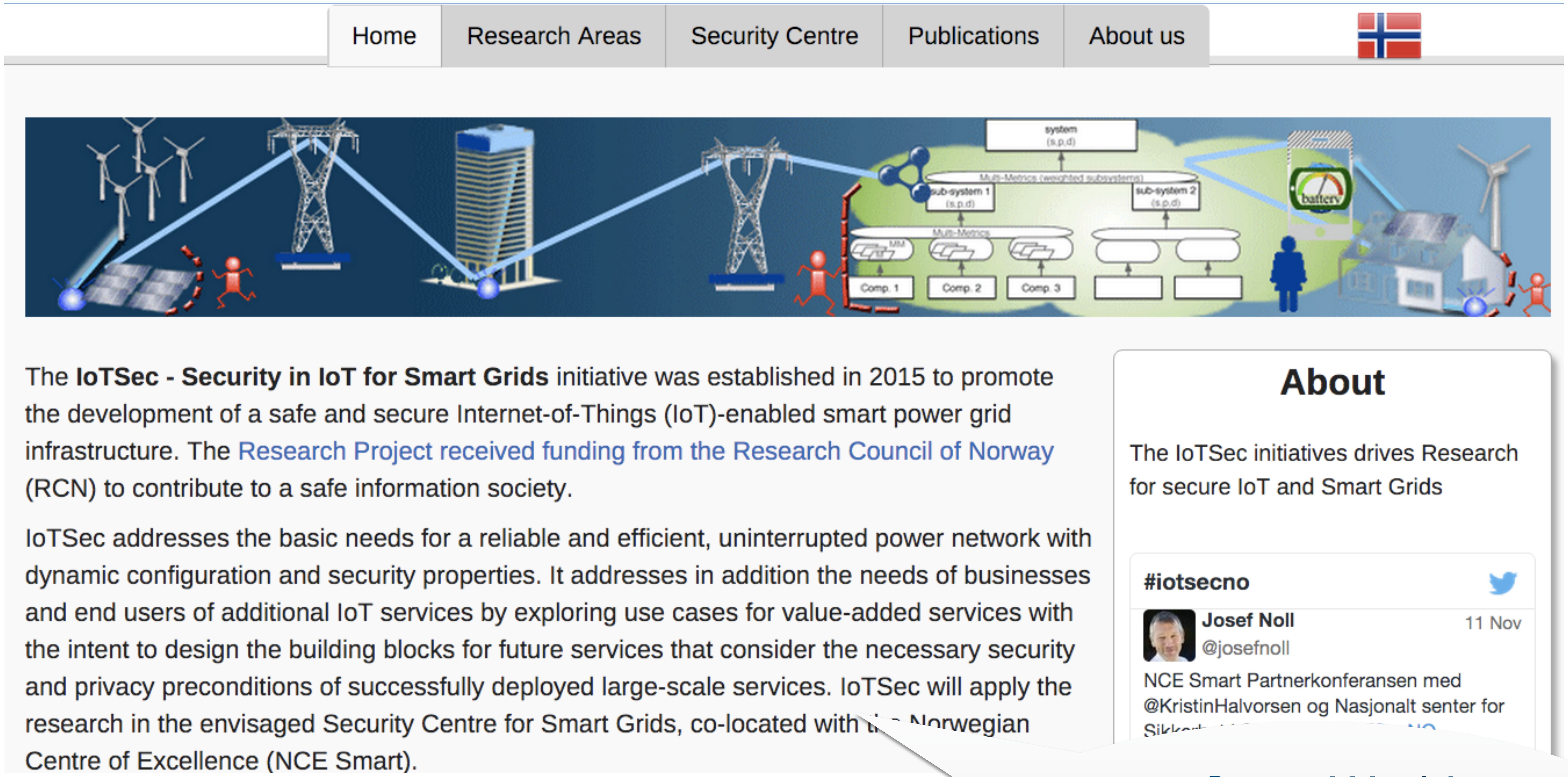
L1 - L3: Introduction to se

- This first part will provide the introduction into the Internet of Things (Lecture 1 - L2), with industrial examples
  - ➡ Smart Grid and automatic meter system (AMS)
  - ➡ Smart Homes with sensors
  - ➡ Wireless System upgrade of cars
- The part will further address potential security threats (L3), as example for the future smart grid.



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

Knowledge and collaboration space
http://IoTSec.no - #IoTSec, #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 Excellence (NCE Smart).

About

The IoTSec initiatives drives Research for secure IoT and Smart Grids

#iotsecno

Josef Noll @josefnoll 11 Nov

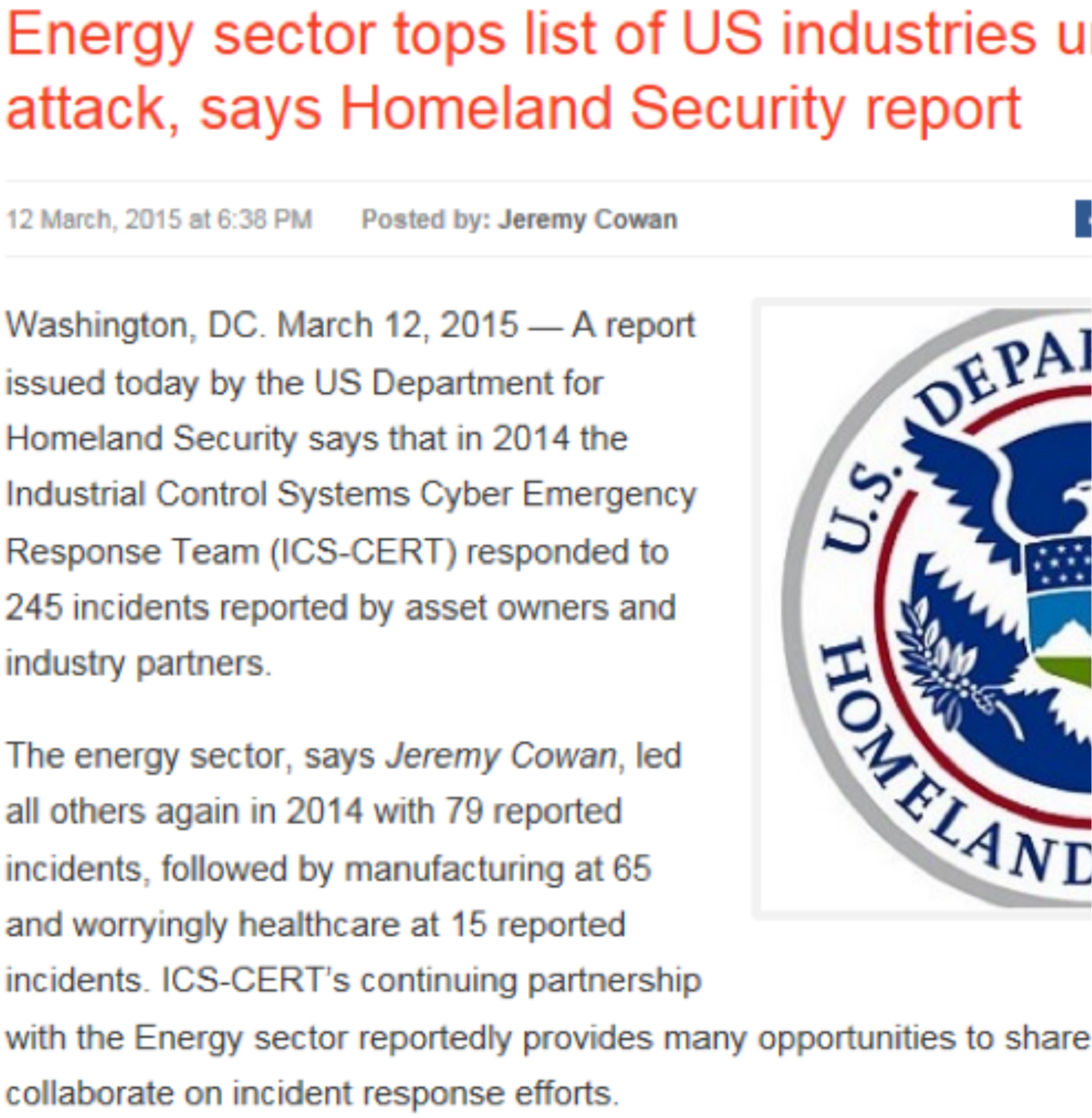
NCE Smart Partnerkonferansen med @KristinHalvorsen og Nasjonalt senter for Sikk

Norge
Norway
Gjøvik
Kjeller
Oslo
Halden

«Open World Approach»

everything that is not declared closed is open

Internet of Things Security

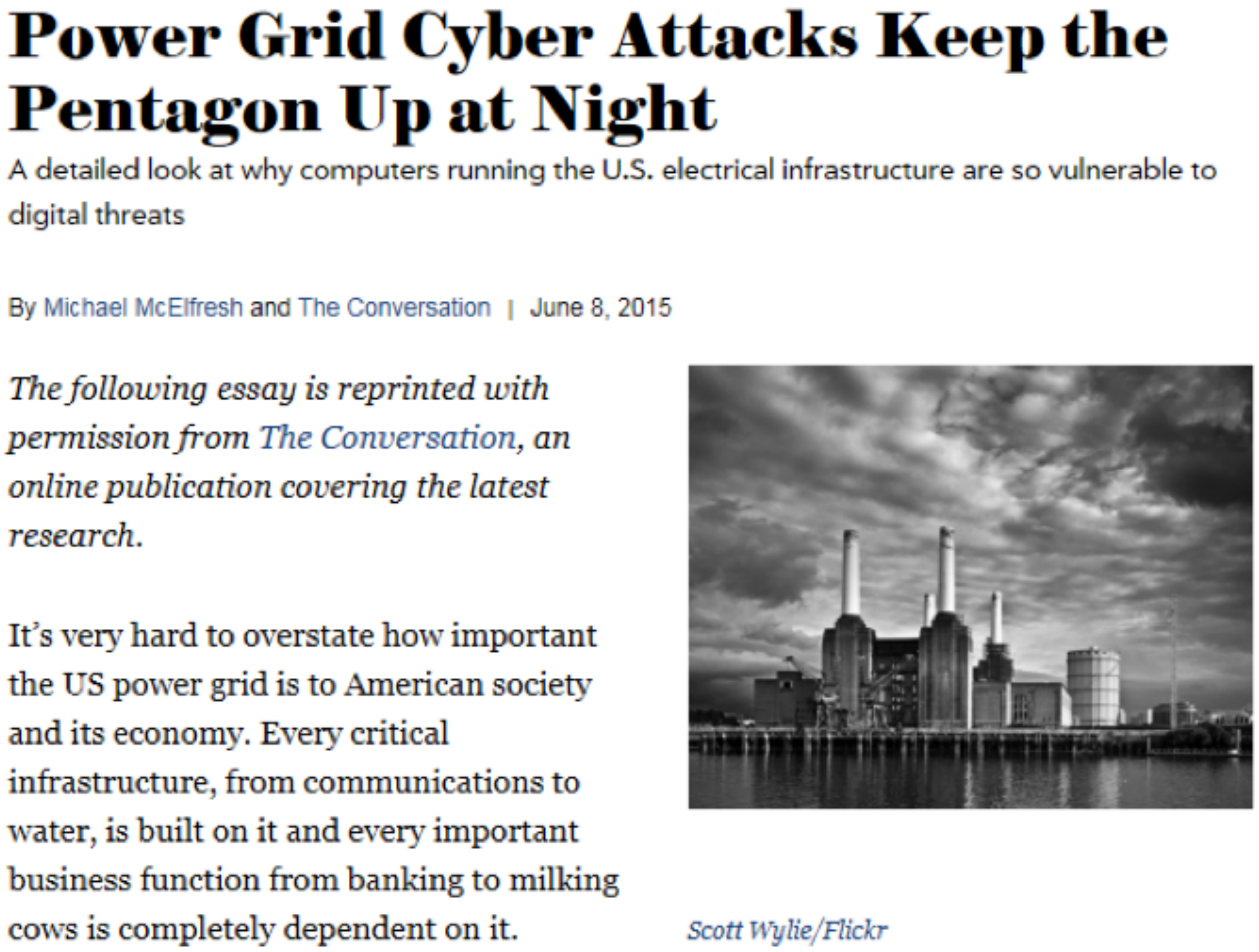


Energy sector tops list of US industries under cyber attack, says Homeland Security report

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

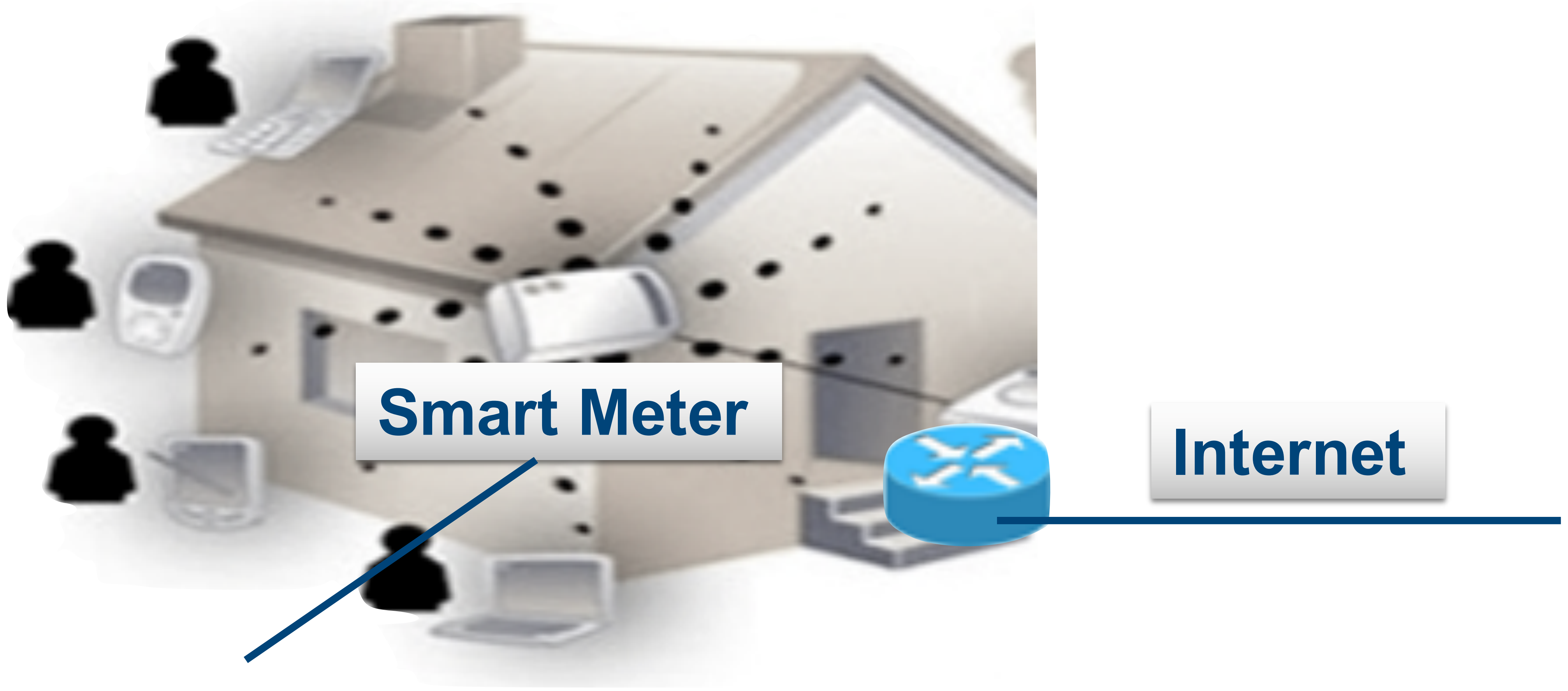
The following essay is reprinted with permission from The Conversation, an online publication covering the latest research.

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

L4-L6 Security and Privacy challenges

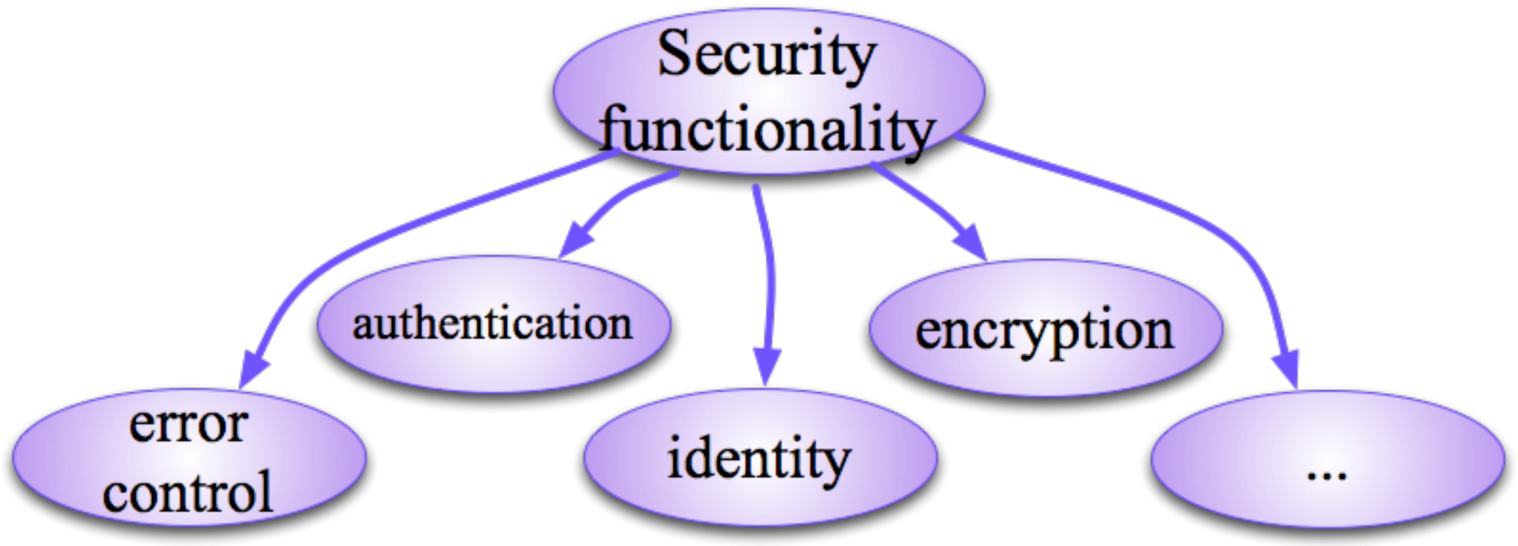
- Example: automatic meter reading (AMR) and -system (AMS)
- Mapping from functional requirements towards mapping into technology.
- Example: translation of privacy requirements - can somebody see from my meter reading if I'm at home - towards technology parameters like how often are values read and published.

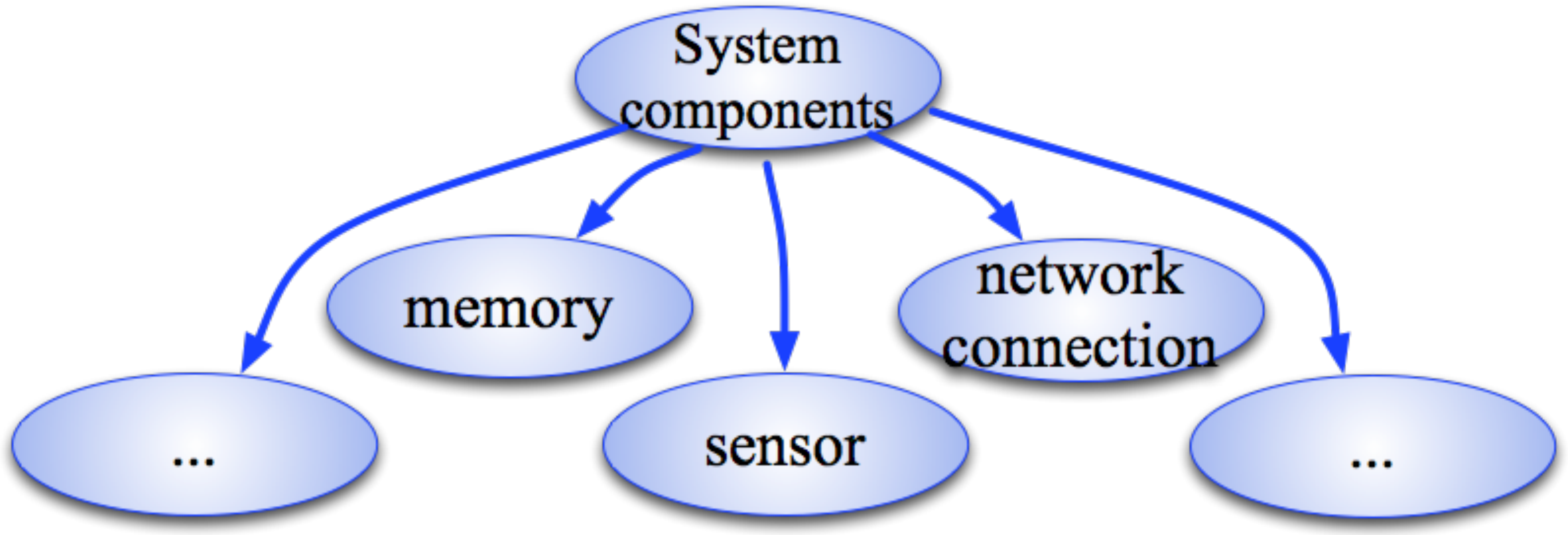


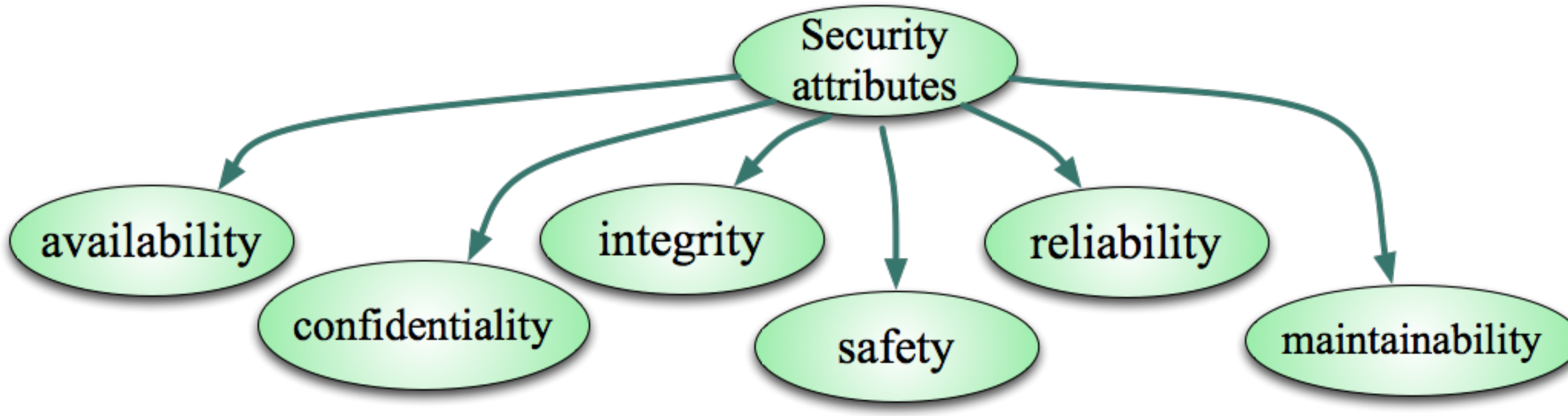
[source: seminarsonly.com]

L6-L8 Machine-readable descriptions

- Describe a system based on security attributes
- Introduction to the Semantic Web
  - ➡ Ontologies
  - ➡ Web-Protégé
- Rules & Reasoning
  - ➡ make decisions





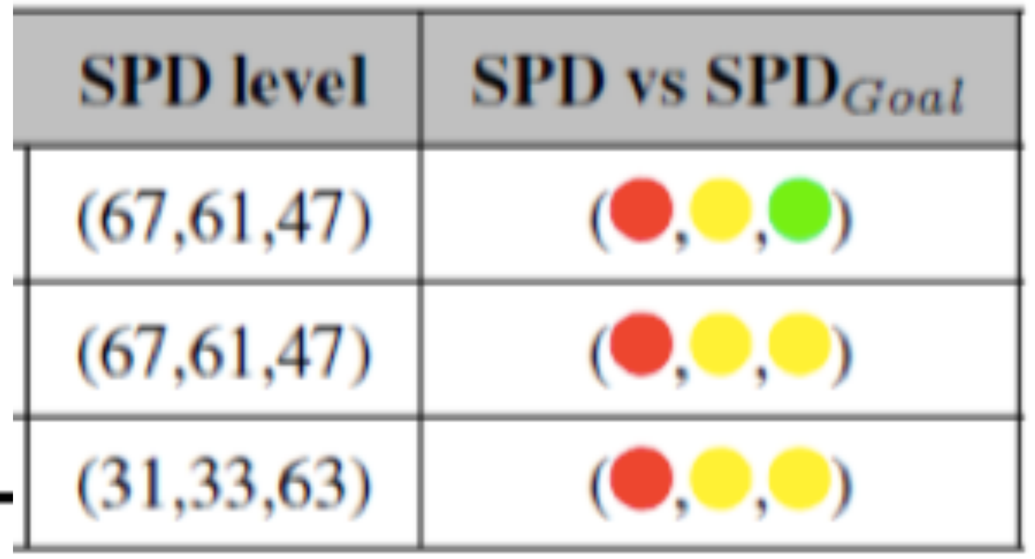


L7 - Paper presentation

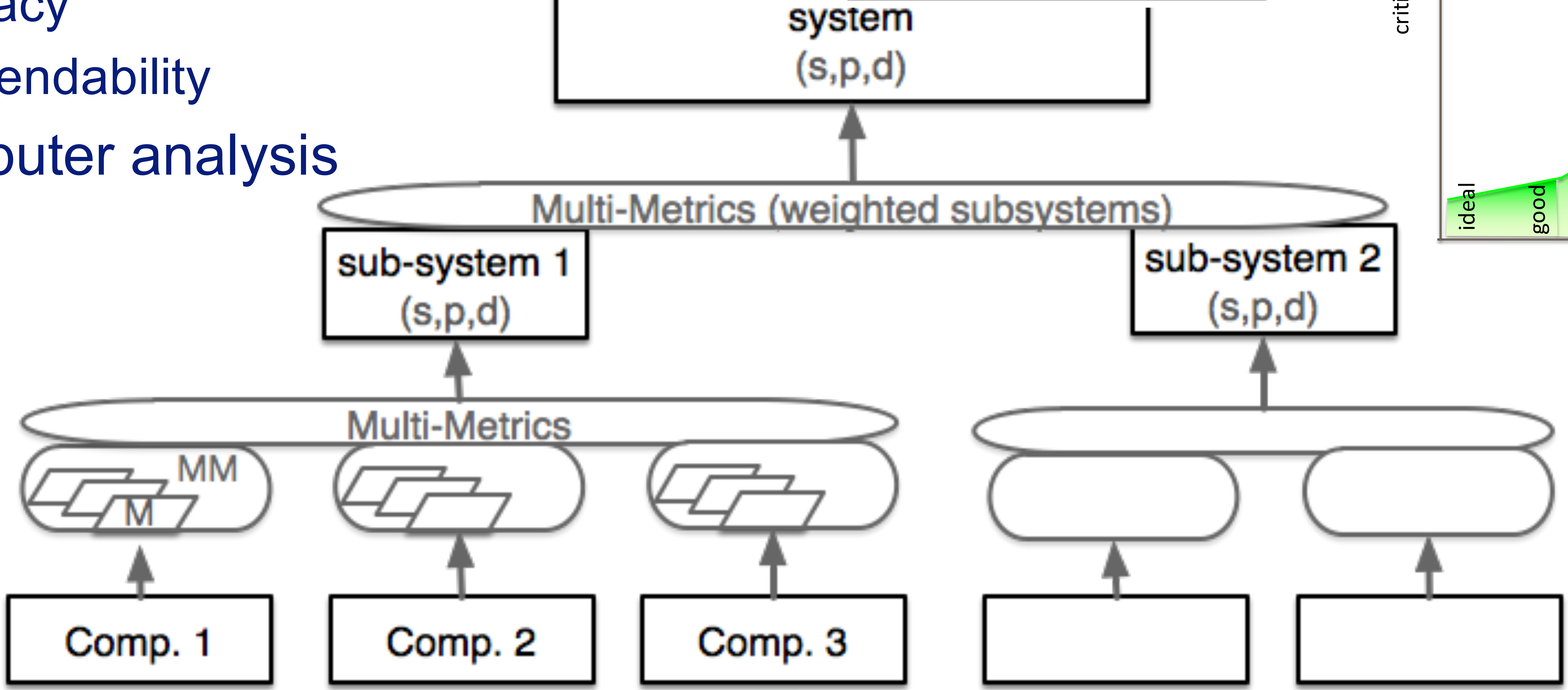
- Methodology:
  - ➡ Select (or search) for scientific papers
  - ➡ Present the paper
  - ➡ Discuss issues which you find interesting
- Outcome
  - ➡ Learn to read (and criticise) scientific literature

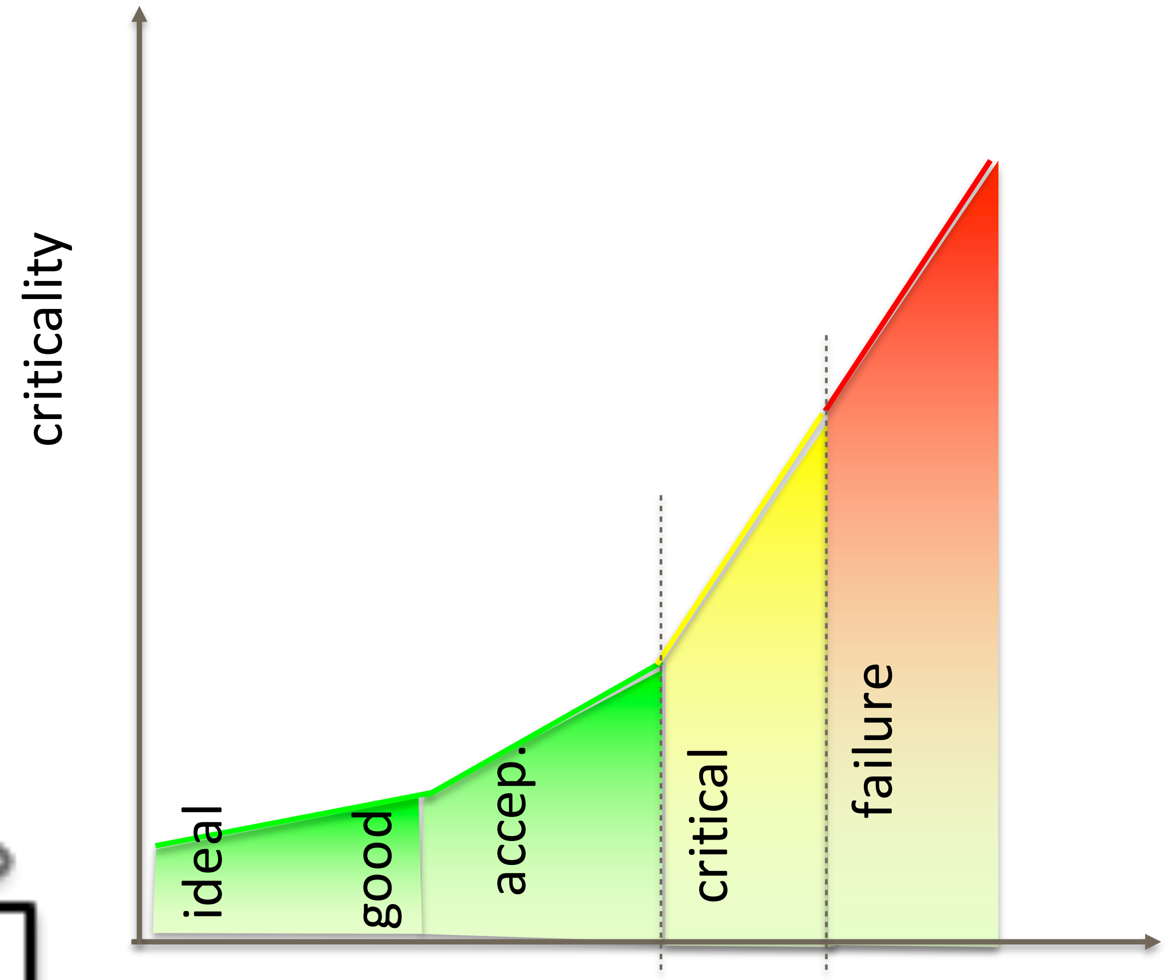
L9-L12: Multi-Metrics method

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



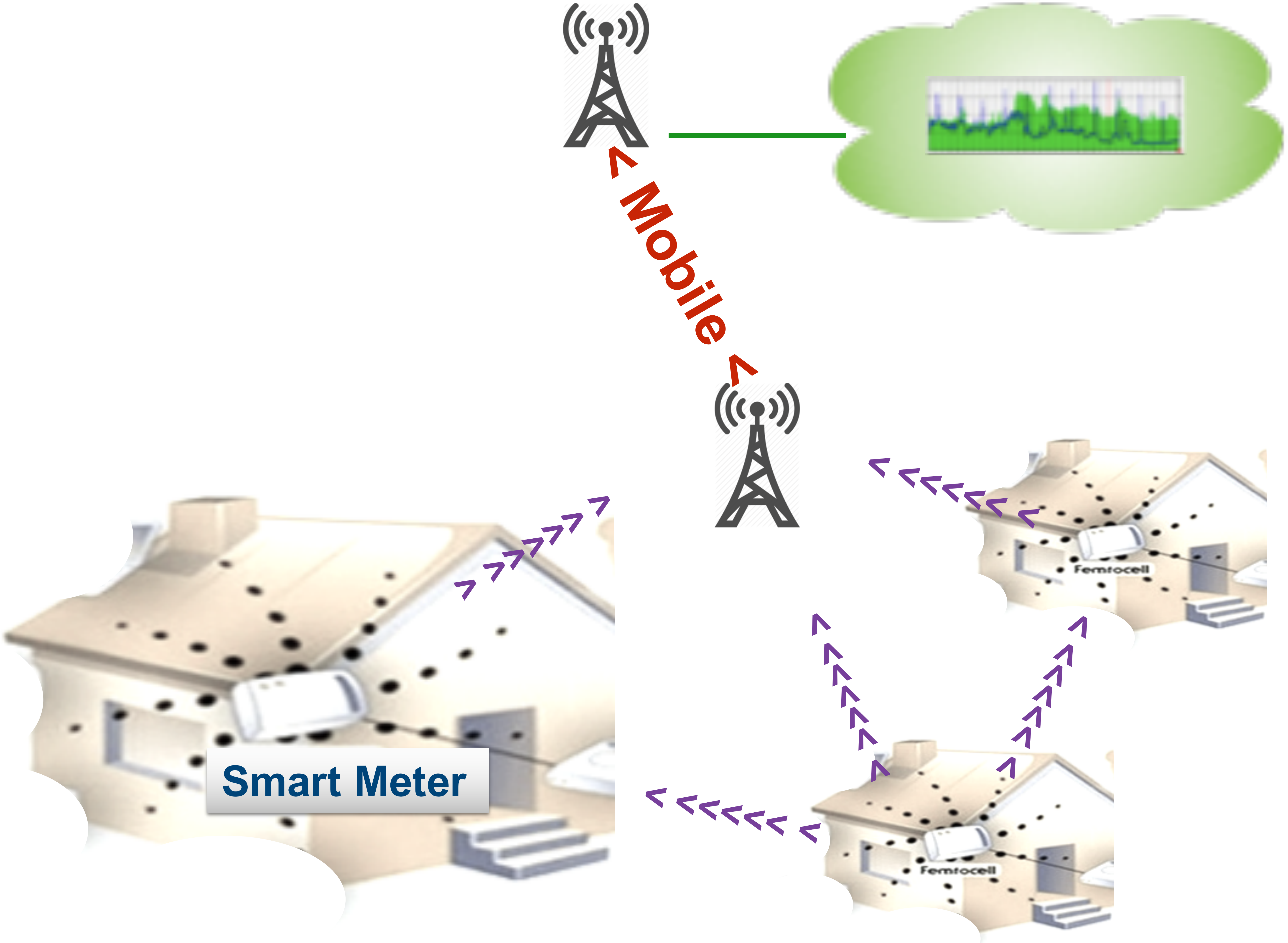
SPD level	SPD vs SPD$_{Goal}$
(67,61,47)	(🔴,🟡,🟢)
(67,61,47)	(🔴,🟡,🟡)
(31,33,63)	(🔴,🟡,🟡)





L13 - L15 Real World Examples

- Real world examples
  - ➡ taken from industry, e.g. Smart Meter
  - ➡ billing,
  - ➡ controlling
- Your own analysis
  - ➡ select system of choice
  - ➡ perform an analysis
  - ➡ suggest: group work



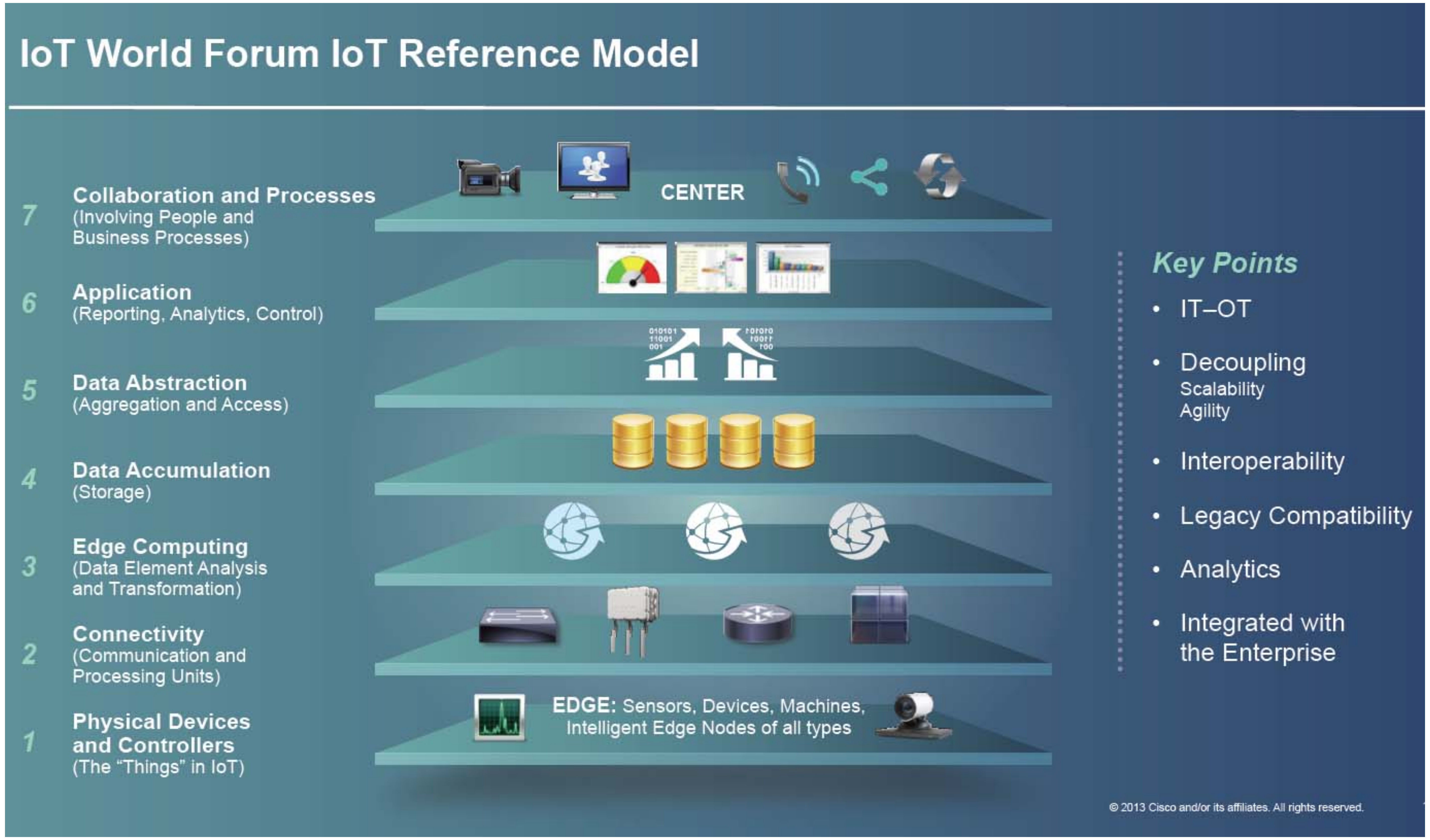
[source: seminarsonly.com]

UNIK4750 exam

- The final grade is based on
  - ➡ a portfolio assessment (40%)
  - ➡ an oral exam (60%). In the case of many students, the final exam may be held as a written exam; this will be decided early in the semester.
- Portfolio
  - ➡ your paper presentation
  - ➡ group work
- Oral exam
  - ➡ explain your group work
  - ➡ questions to the group work
  - ➡ topics of the course

Internet of Things

- Heading toward a fully connected world
- In a more focused way, in this course we speak about industrial internet of things
- The substantial difference is, that these systems have a physical dimension
- Considered as the next industrial revolution
- Automation to a new connectivity level – the internet is coming to automation
- Main challenges: how to join the physical and the logical world, how to achieve interoperability in a heterogeneous and conservative industry?



IoT World Forum IoT Reference Model

7 Collaboration and Processes (Involving People and Business Processes)

6 Application (Reporting, Analytics, Control)

5 Data Abstraction (Aggregation and Access)

4 Data Accumulation (Storage)

3 Edge Computing (Data Element Analysis and Transformation)

2 Connectivity (Communication and Processing Units)

1 Physical Devices and Controllers (The "Things" in IoT)

CENTER

EDGE: Sensors, Devices, Machines, Intelligent Edge Nodes of all types

Key Points

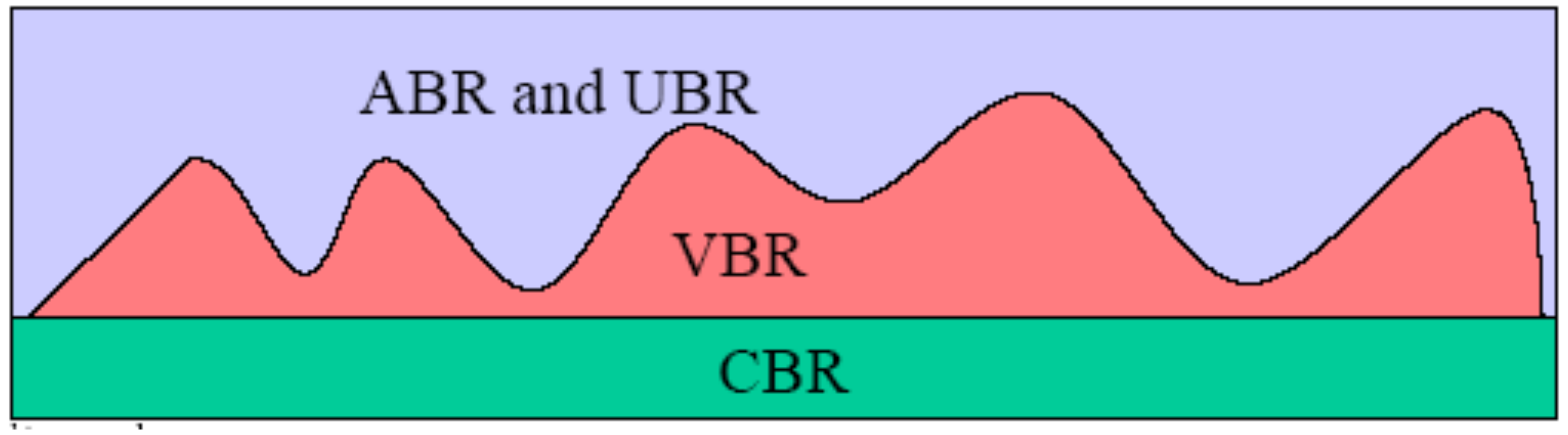
- IT–OT
- Decoupling
  Scalability
  Agility
- Interoperability
- Legacy Compatibility
- Analytics
- Integrated with the Enterprise

© 2013 Cisco and/or its affiliates. All rights reserved.

Internet as we know it

- Intelligence in the end nodes
- Best effort traffic
- Infrastructure = network equipment
- Operated by IT or telecom
- No direct physical dimension
- Mostly built to serve human-generated traffic

- QoS: best effort, adopted to the human consumer: 10s of ms of drop is not a problem, stable delay is accepted, majority of applications are bursty
- Reaction time in 0.5-1s range
- Stochastic → services do exploit this (like Erlang-B formula for capacity estimation or lossy compression in nearly everything)



Automation as we know it

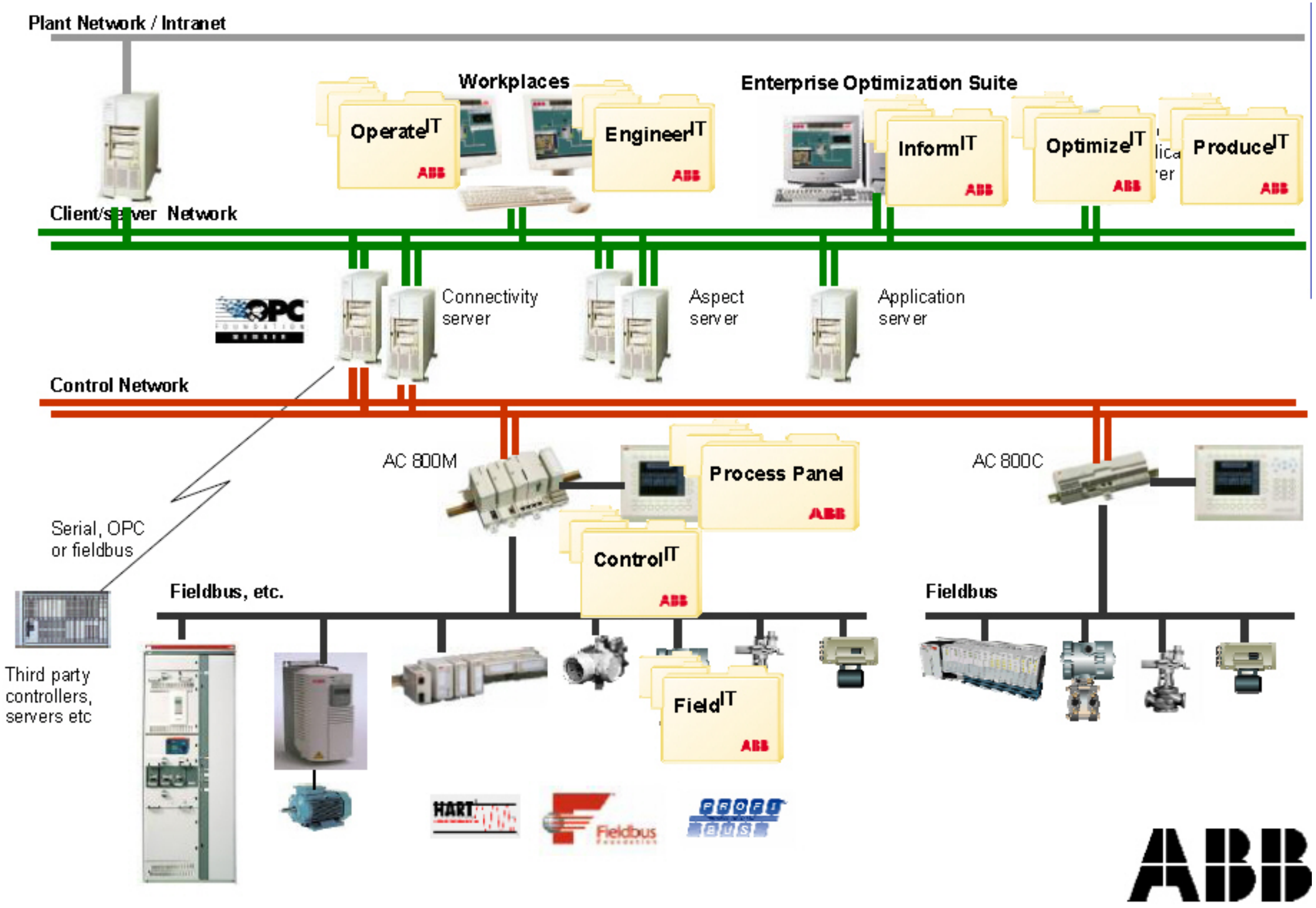
- Centralized intelligence
- Traditionally operated as islands by operations
- Direct connection with the physical world
- Is made for information gathering and processing by machines
- Has a lag of approx. 15-20 years (one generation of devices)
- Still a current question: collisions on Ethernet, what happens if one has to share infrastructure with others, how to operate a link with long step-out distance
- Economic press leads to adoption of internet-based services which *require* a paradigm change

Mine (Boliden)

ABB robots

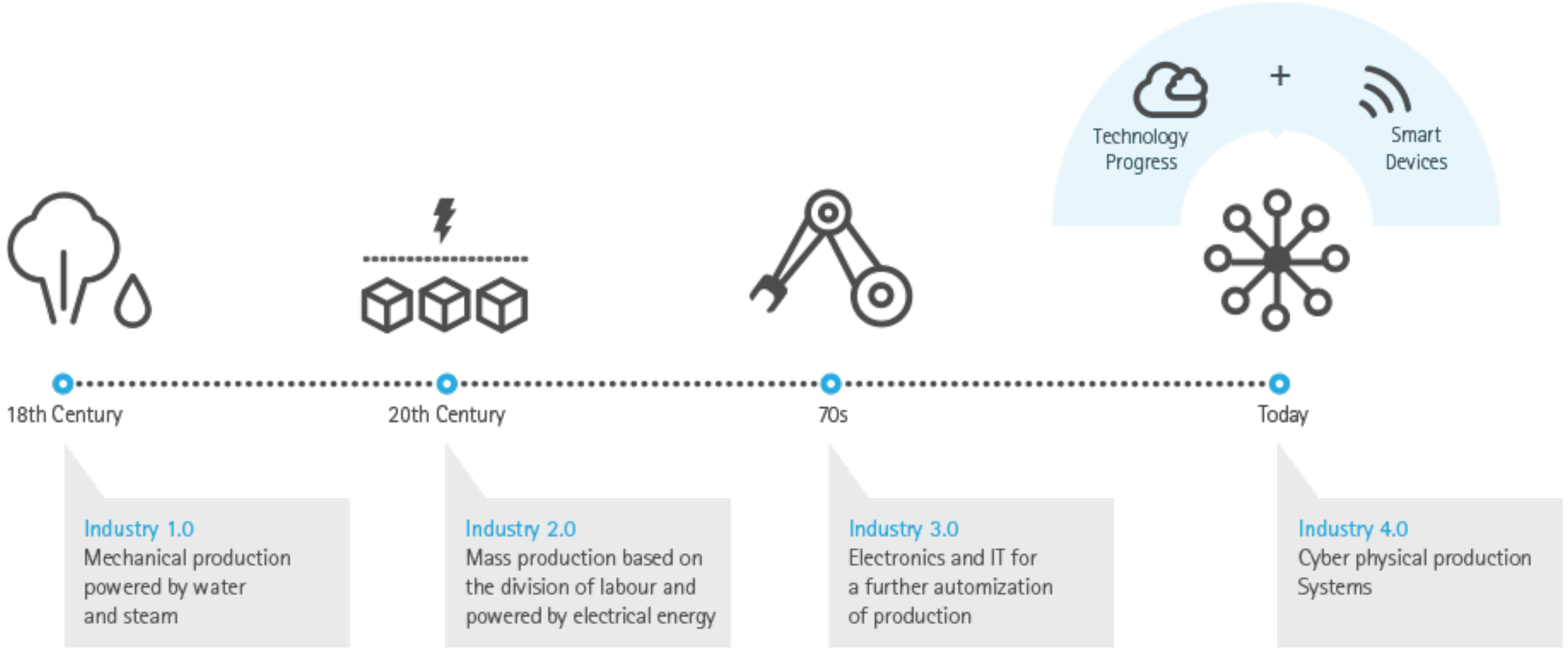
http://www07.abb.com/images/librariesprovider104/Extended-Automation/control-room-consolidation-by-abb.png?sfvrsn=1

Typical traditional industrial network



Merging these two

- Internet is the infrastructure – sensor, actuator, controller not on the same physical network any more
- ”dissolves” the automation system in the internet
- Automation processes run over an unknown communication infrastructure
- Network communication gets physical impact
- Automation meets real internet-type deployment
- Already happening
- The real value of IoT: data.
  Cloud and big data will enable new services


Technology Progress
+
Smart Devices
18th Century
20th Century
70s
Today
Industry 1.0
Mechanical production powered by water and steam
Industry 2.0
Mass production based on the division of labour and powered by electrical energy
Industry 3.0
Electronics and IT for a further automization of production
Industry 4.0
Cyber physical production Systems

http://prd.accenture.com/microsites/digital-industry/images/digital/industrial-infographic-large.png

Interesting challenges

- Architecture: physical impact, end-to-end resource reservation, discovery, safety, security and privacy
- Governance, interoperability, standardization
- Managing risk in a system with impact on both logical and physical level
- Provide QoS over a best effort infrastructure – with a price pressure

- Aggregation of data: here lies the added value, enables novel services and higher efficiency
- Distribution of intelligence: make the automation system more internet-like: intelligence in the end-nodes. Support it with the recent it trends of cloud and big data. Challenge for traditional automation mindset.
- Open architectural model
- Security concerns are a critical barrier for wide scale adoption of IoT

- See when IT has arrived to the phone industry. Or when IT has arrived into telco backhaul. IT is arriving to automation.

IoT services

- Enabled by wide scale data gathering
- Monitoring of massive systems
- Real-time insight to processes
- Observation of systems
- Performance measurement and optimization
- Proactive and predictive methods
- To serve the automation goals, the services provided must be: scalable, distributed, have a real reference to the phyisical world (e.g. time), must ensure security and privacy of the users
- Just using existing security solutions is not leading to secure IoT deployments
- Composed by IT, operations and the IoT enabled objects

- * Following slides are from the presentation of Mikhail Kader, DSE, Cisco, presented on the ITU Workshop on “ICT Security Standardization for Developing Countries”

Connected Rail Operations *

PASSENGER SECURITY

- In-station and onboard safety
- Visibility into key events

ROUTE OPTIMIZATION

- Enhanced Customer Service
- Increased efficiency
- Collision avoidance
- Fuel savings

CRITICAL SENSING

- Transform “data” to “actionable intelligence”
- Proactive maintenance
- Accident avoidance

Cost savings, improved safety, superior service

Smart City *

CONNECTED TRAFFIC SIGNALS

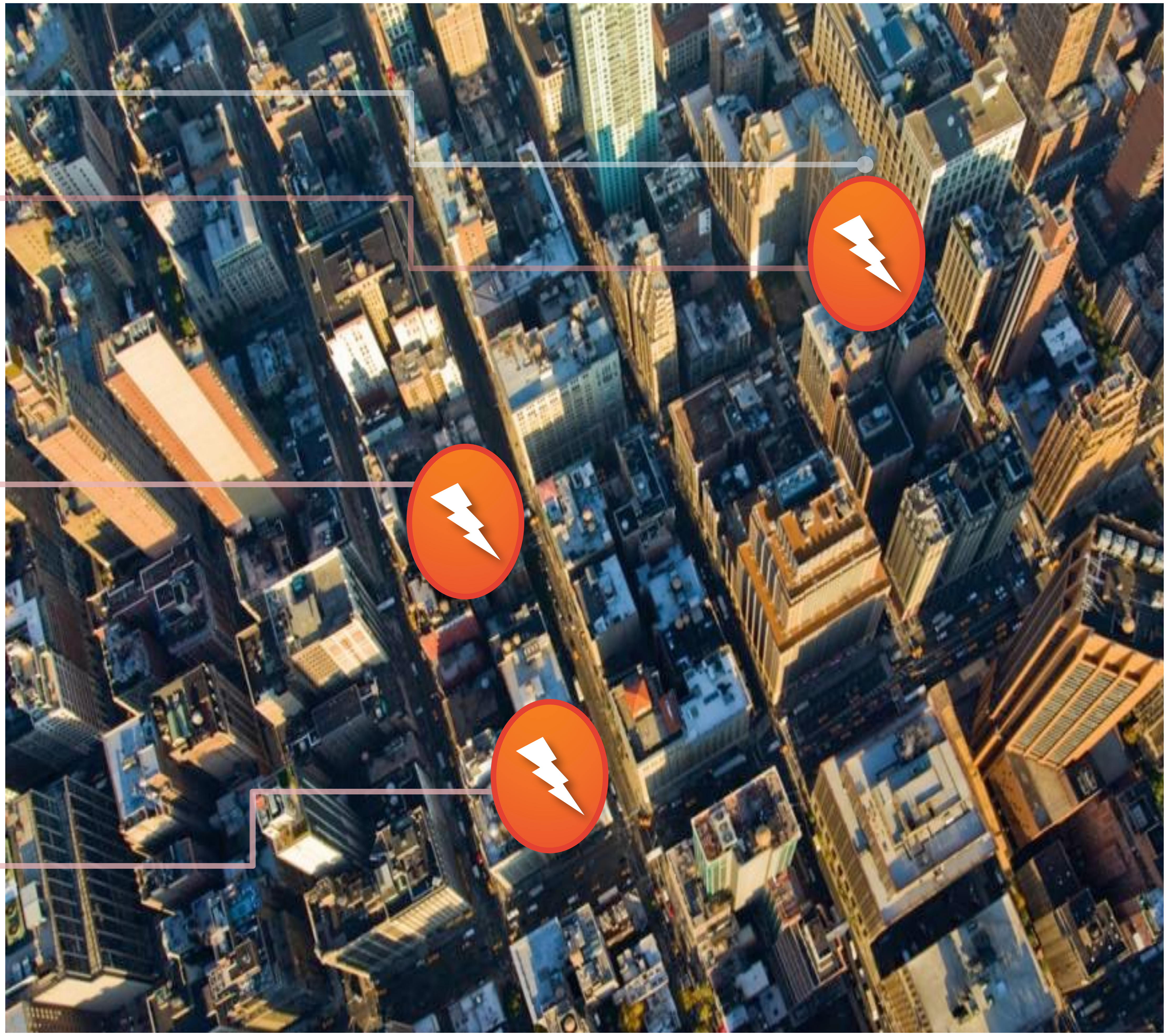
- Reduced congestion
- Improved emergency services response times
- Lower fuel usage

PARKING AND LIGHTING

- Increased efficiency
- Power and cost savings
- New revenue opportunities

CITY SERVICES

- Efficient service delivery
- Increased revenues
- Enhanced environmental monitoring capabilities



The Connected Car *

WIRELESS ROUTER

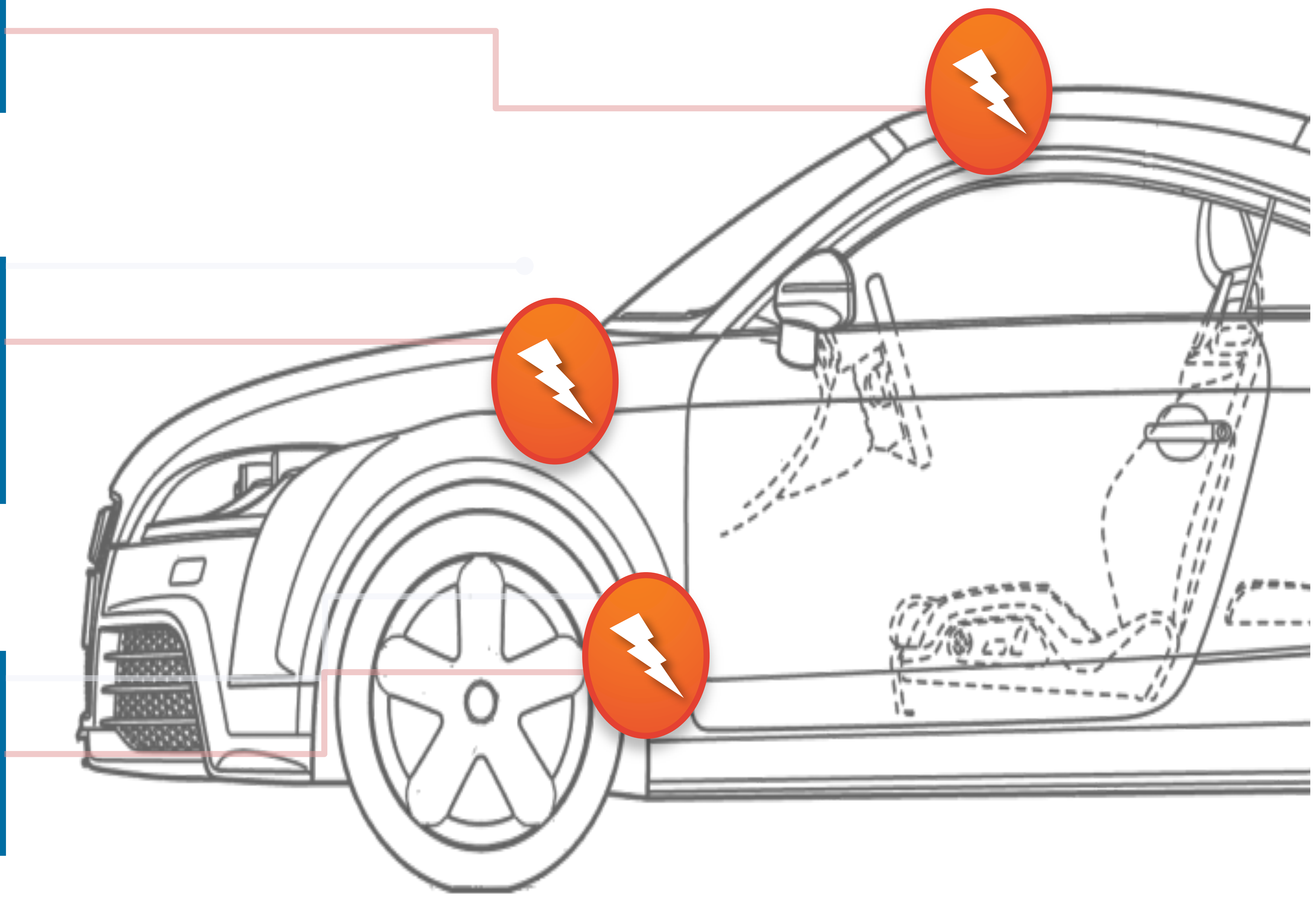
- Online entertainment
- Mapping, dynamic re-routing, safety and security

CONNECTED SENSORS

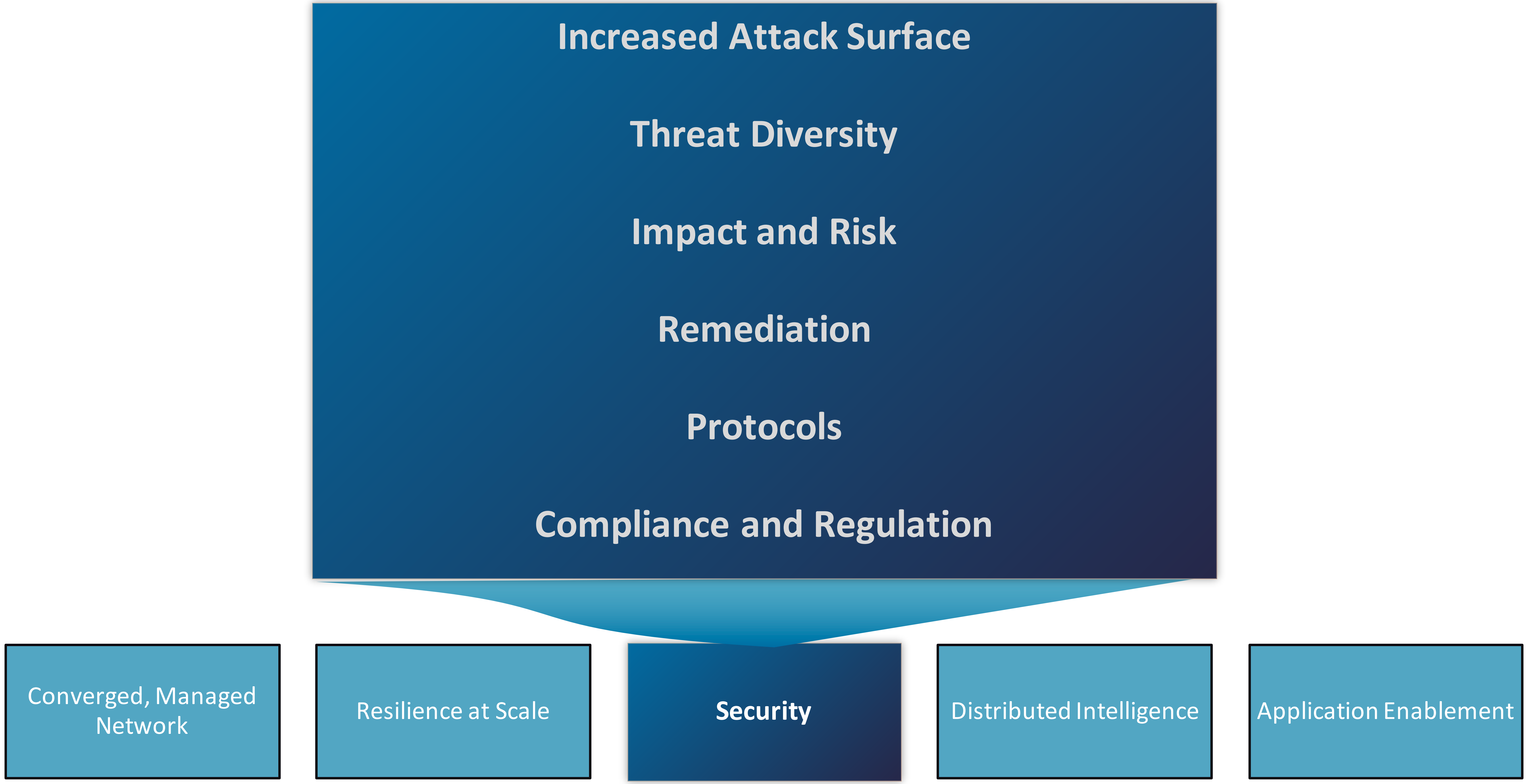
- Transform “data” to “actionable intelligence”
- Enable proactive maintenance
- Collision avoidance
- Fuel efficiency

URBAN CONNECTIVITY

- Reduced congestion
- Increased efficiency
- Safety (hazard avoidance)



IoT Expands Security Needs *



Increased Attack Surface

Threat Diversity

Impact and Risk

Remediation

Protocols

Compliance and Regulation

Converged, Managed Network

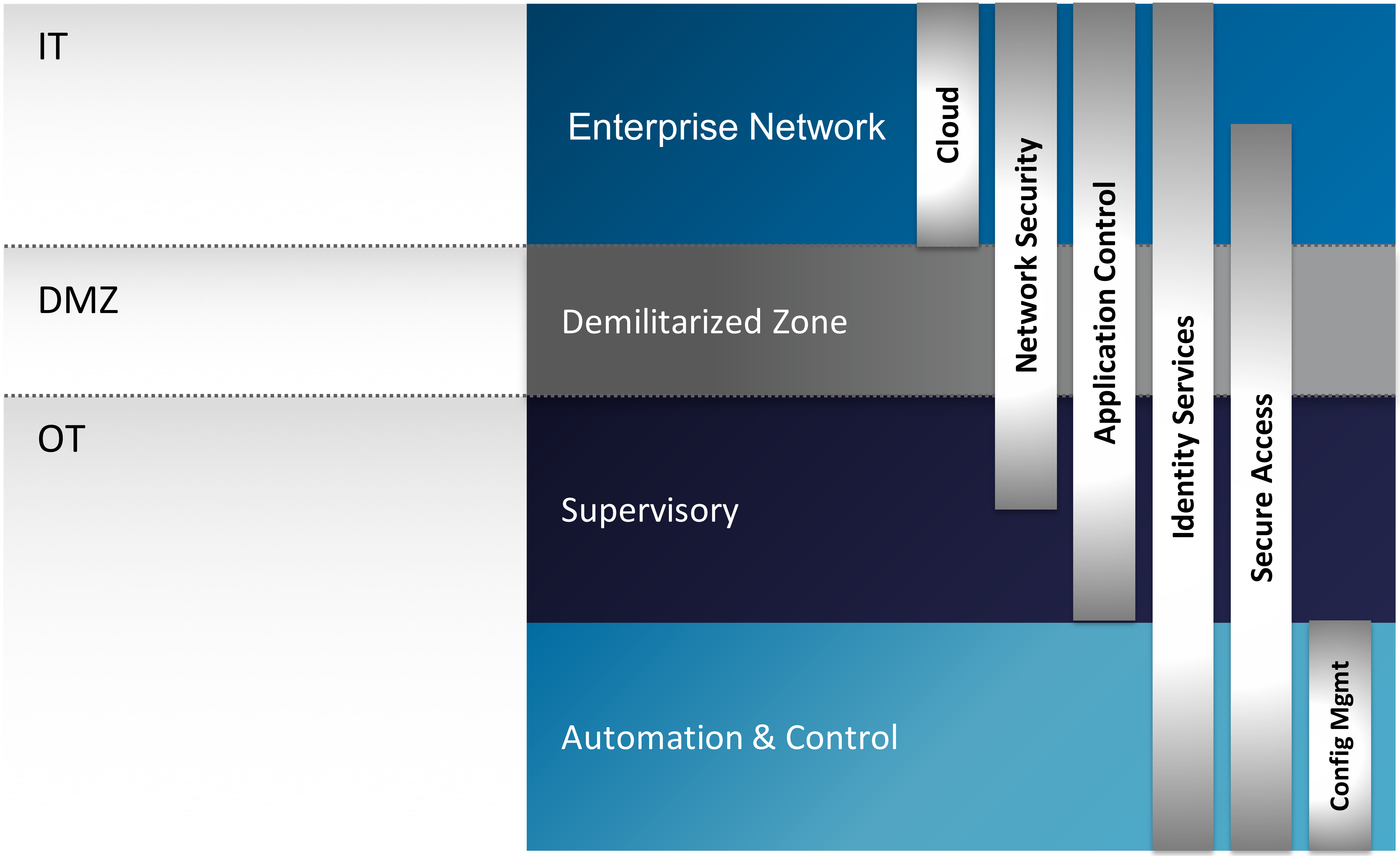
Resilience at Scale

Security

Distributed Intelligence

Application Enablement

IT/OT Converged Security Model *



IT and OT are Inherently Different *

- IT
  - Connectivity: “Any-to-Any”
  - Network Posture: Confidentiality, Integrity, Availability (CIA)
  - Security Solutions: Cybersecurity; Data Protection
  - Response to Attacks: Quarantine/Shutdown to Mitigate

- OT
  - Connectivity: Hierarchical
  - Network Posture: Availability, Integrity, Confidentiality (AIC)
  - Security Solutions: Physical Access Control; Safety
  - Response to Attacks: Non-stop Operations/Mission Critical – Never Stop, Even if Breached

What Can Breach IoT Networks?

- What can’t?
  - ➡ Billions of connected devices
  - ➡ Secure and insecure locations
  - ➡ Security may or may not be built in
  - ➡ Life cycle mismatch between IT and automation devices
  - ➡ Installed base
  - ➡ Clash between IT and OT, IT has to accept the traffic

- Any node on your network can potentially provide access to the core

L1 Conclusions

- Overview over lectures
- Explanation of portfolio and exam
- Introduction to topic blocks
- Discussion

[Source: Monique Morrow, Cisco]