UiO : Department of Technology Systems
University of Oslo

TEK5530 - Measurable Security for the Internet of Things

L2 - Internet of Things

György Kálmán,
UiO
gyorgy.kalman@its.uio.no

Josef Noll
UiO
josef.noll@its.uio.no

https://its-wiki.no/wiki/TEK5530, #IoTSec, #IoTSecNO

L2- Overview

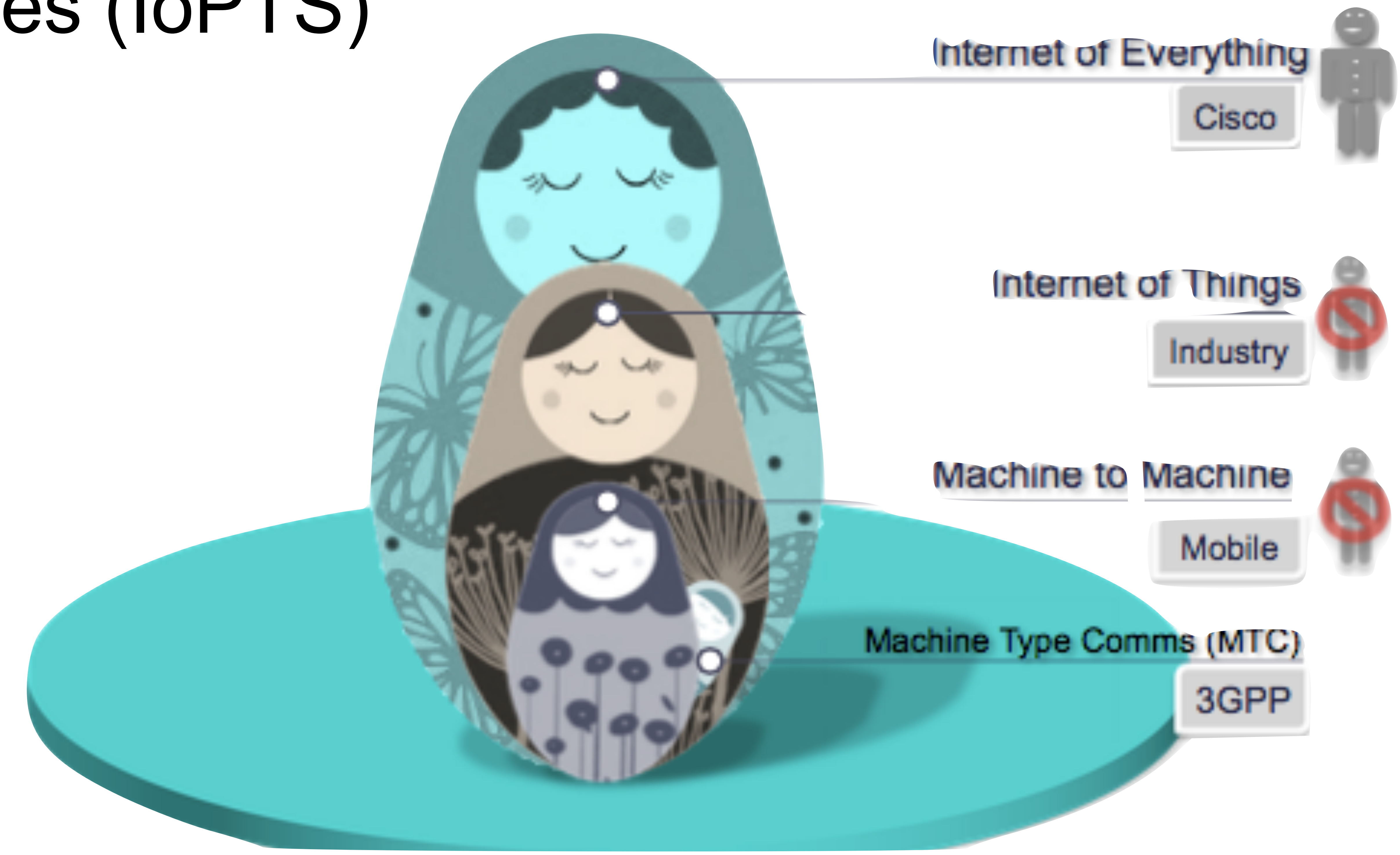
- History of Internet of things (IoT)
- Merging several domains
  - ➡ Things
  - ➡ Semantics
  - ➡ Internet
- What about?
  - ➡ Security
  - ➡ Privacy
  - ➡ Multi-owner requirements

Expected outcome:

- Describe the domains being merged in IoT
- Provide examples of challenges in each of the domains
- Establish requirements for multi-owner service requests of “a thing”
- Analyse security and privacy requirements in an envisaged scenario

Internet of Things aspects

- The Internet of People Things and Services (IoPTS)
  - The Internet of Things (IoT)
  - The Internet of Everything (IoE)
- Identity in the IoT
  - Identity and trust between people
  - Identity in IoT
- Privacy and Security
  - Privacy, Context-awareness
  - Measurable Security
  - Innovation through Measurable Security



[Source: Monique Morrow, Cisco]

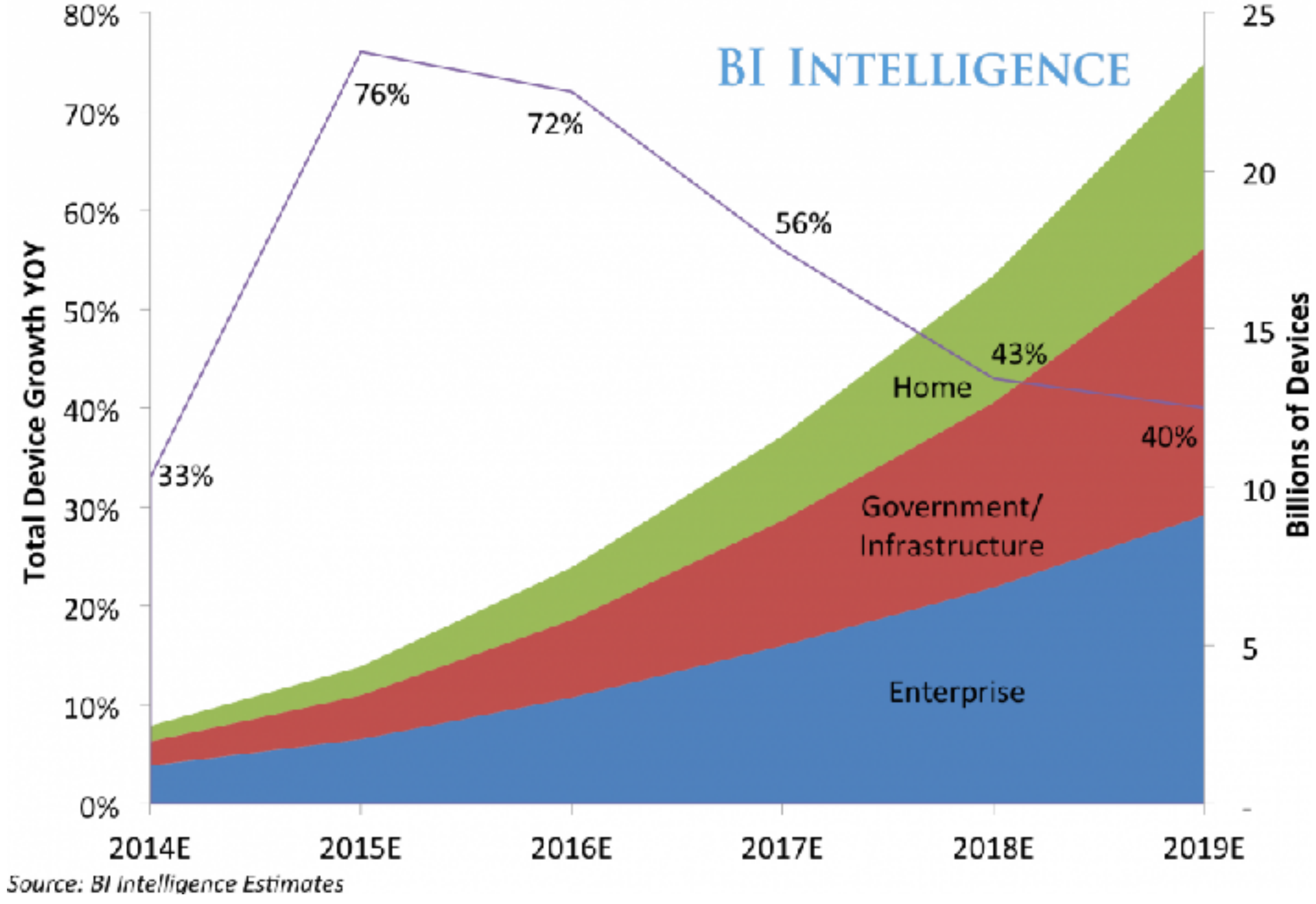
DNV report 2013, DNV GL report 2014

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

Estimated Number of Installed IoT Devices by Sector

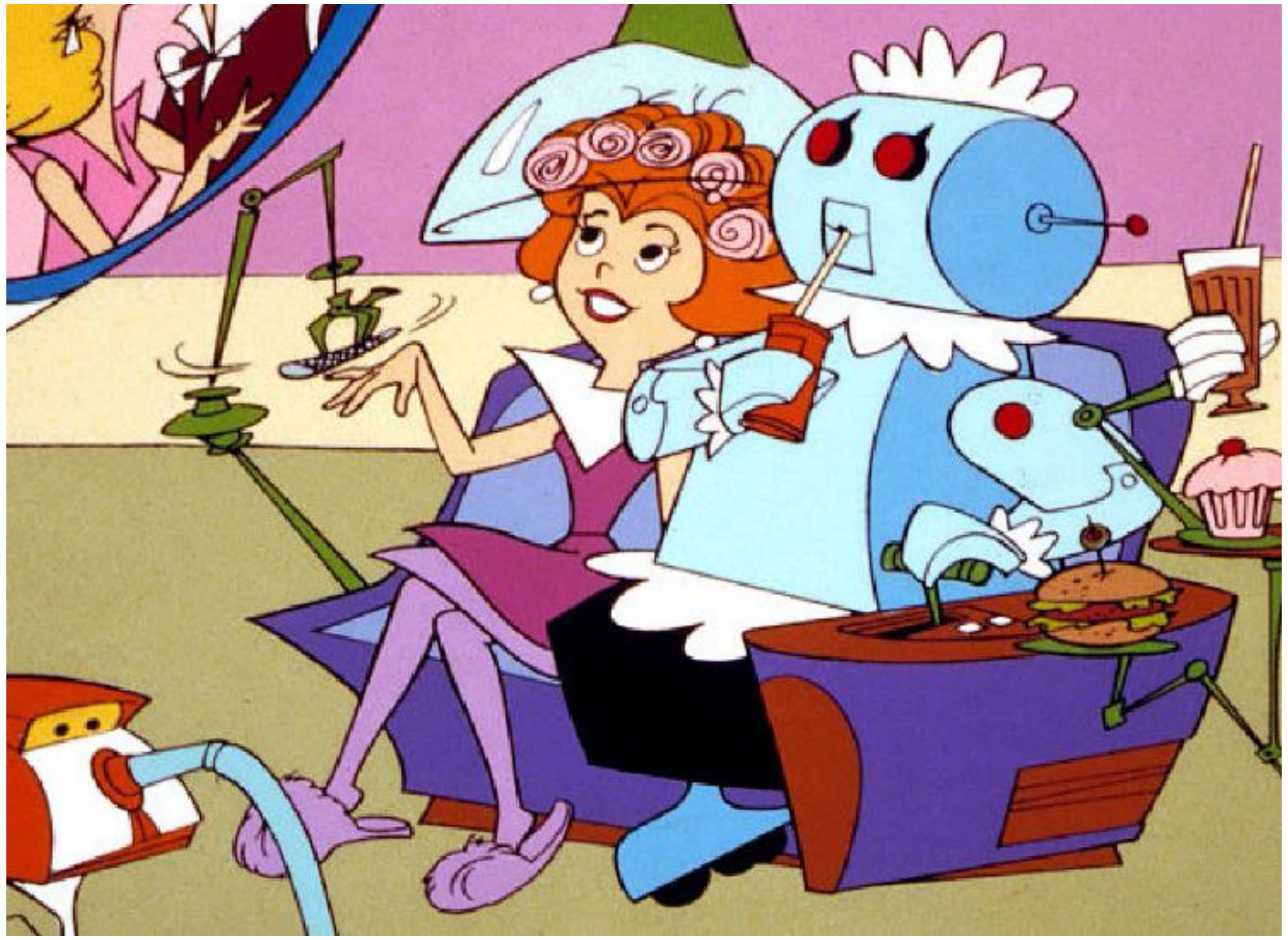


Source: BI Intelligence Estimates

Internet of Things – Life, Jetsons style

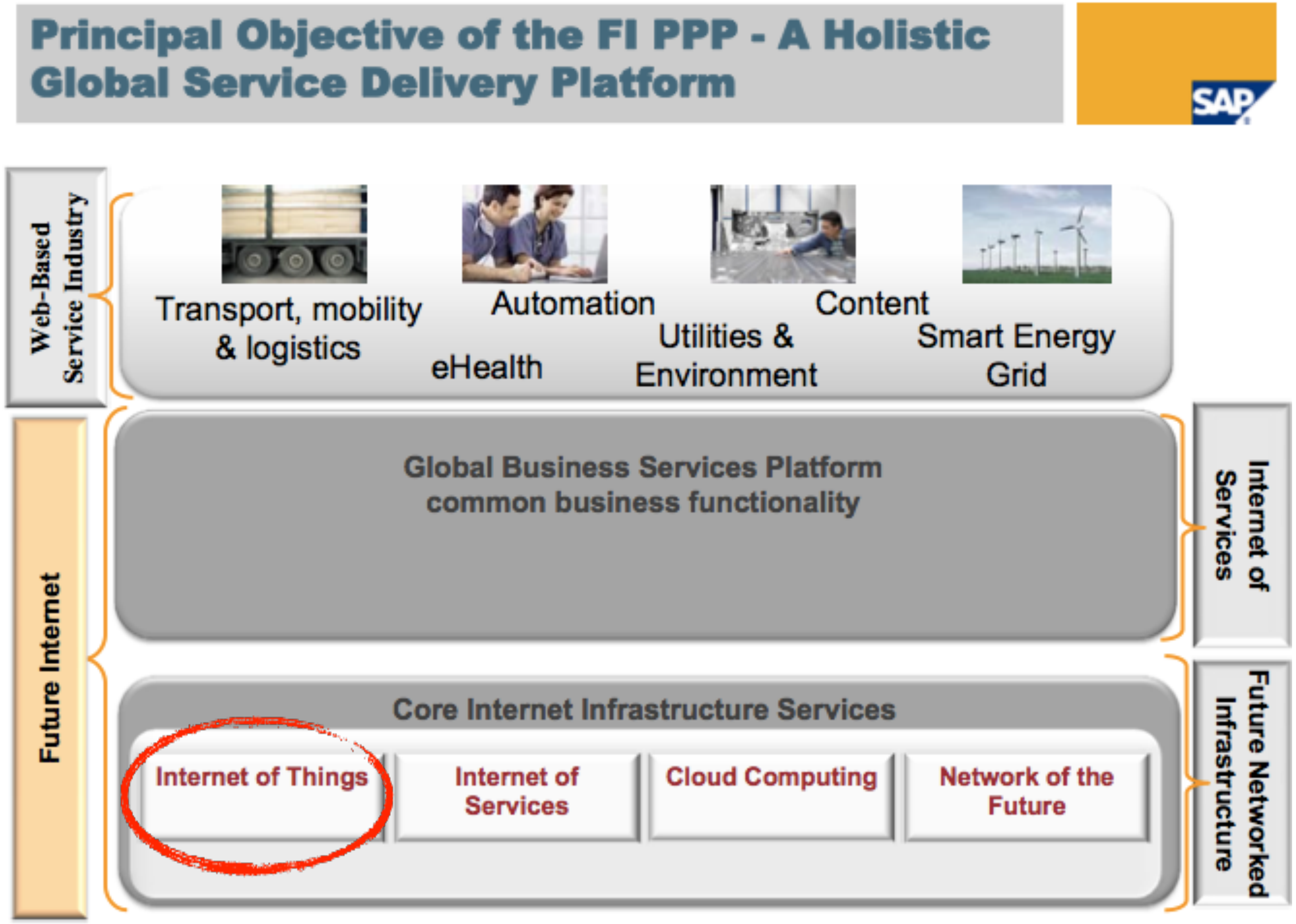
- From "Internet of PCs" towards the "Internet of Things" with 20-30 billion devices connected to the Internet by 2020
- Intelligence hidden from the user
- «Seamless» operation
- Adaptive and personal

- Inability to manage full depth
- Multi-owner situations
- Depth and breadth of services are in direct tradeoff with privacy and security



Internet of Things – Components

- Future internet components as seen by SAP
- Internet of Things being the link to the physical world
- Internet of Services enables automatic service composition and deployment
- Cloud is offering elastic, cheap and readily available infrastructure
- Network of the future offers the mesh connecting all


Principal Objective of the FI PPP - A Holistic Global Service Delivery Platform
SAP
Web-Based Service Industry
Transport, mobility & logistics
Automation
eHealth
Utilities & Environment
Content
Smart Energy Grid
Future Internet
Global Business Services Platform common business functionality
Internet of Services
Core Internet Infrastructure Services
Internet of Things
Internet of Services
Cloud Computing
Network of the Future
Future Networked Infrastructure

[Source: J. Schaper, FI PPP Constituency Event Nice, March 2010]

Paper analysis:
The Internet of Things

- Paper: L. Atzori et al., The Internet of Things: A survey, Comput. Netw. (2010),
  - link on the http://its-wiki.no/wiki/TEK5330 page

- Internet
- Things
- Semantics

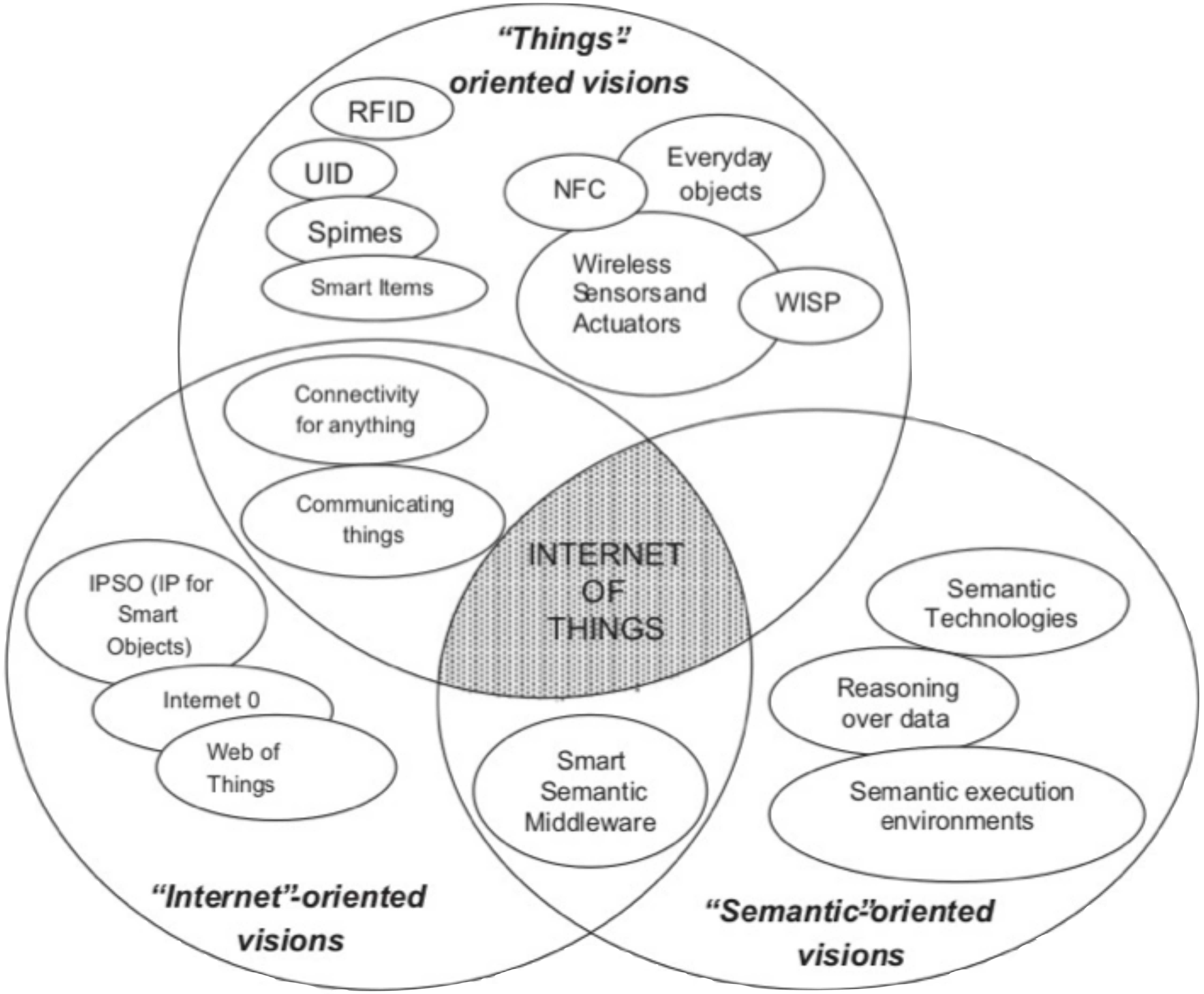

"Things" oriented visions
RFID
UID
Spimes
Smart Items
NFC
Everyday objects
Wireless Sensors and Actuators
WISP
Connectivity for anything
Communicating things
INTERNET OF THINGS
IPSO (IP for Smart Objects)
Internet 0
Web of Things
Smart Semantic Middleware
Semantic Technologies
Reasoning over data
Semantic execution environments
"Internet"-oriented visions
"Semantic"-oriented visions

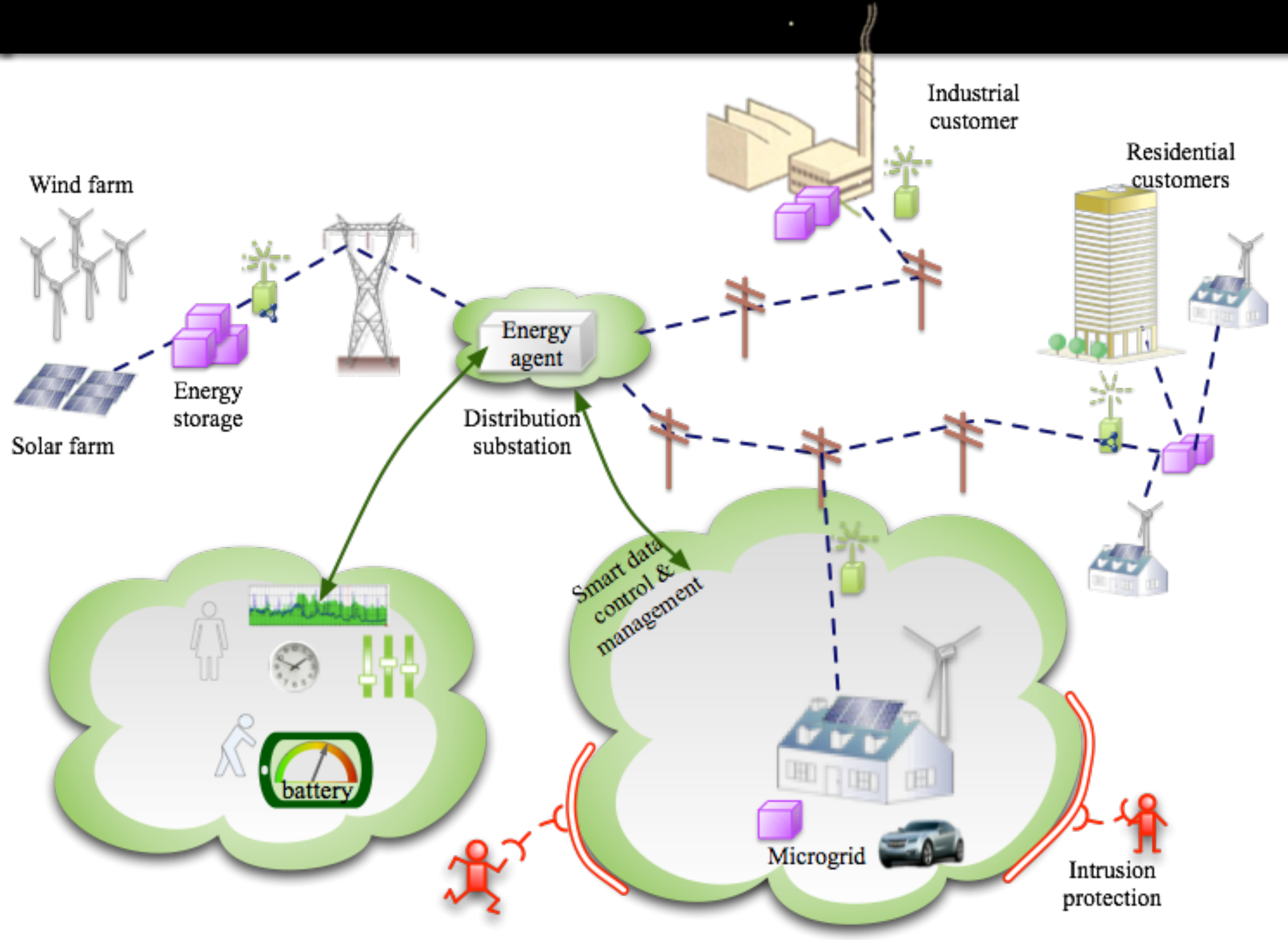
Fig. 1. "Internet of Things" paradigm as a result of the convergence of different visions.

Main drivers for IoT

- Cheap sensors
- Wireless connectivity
- Apps
- on-time monitoring

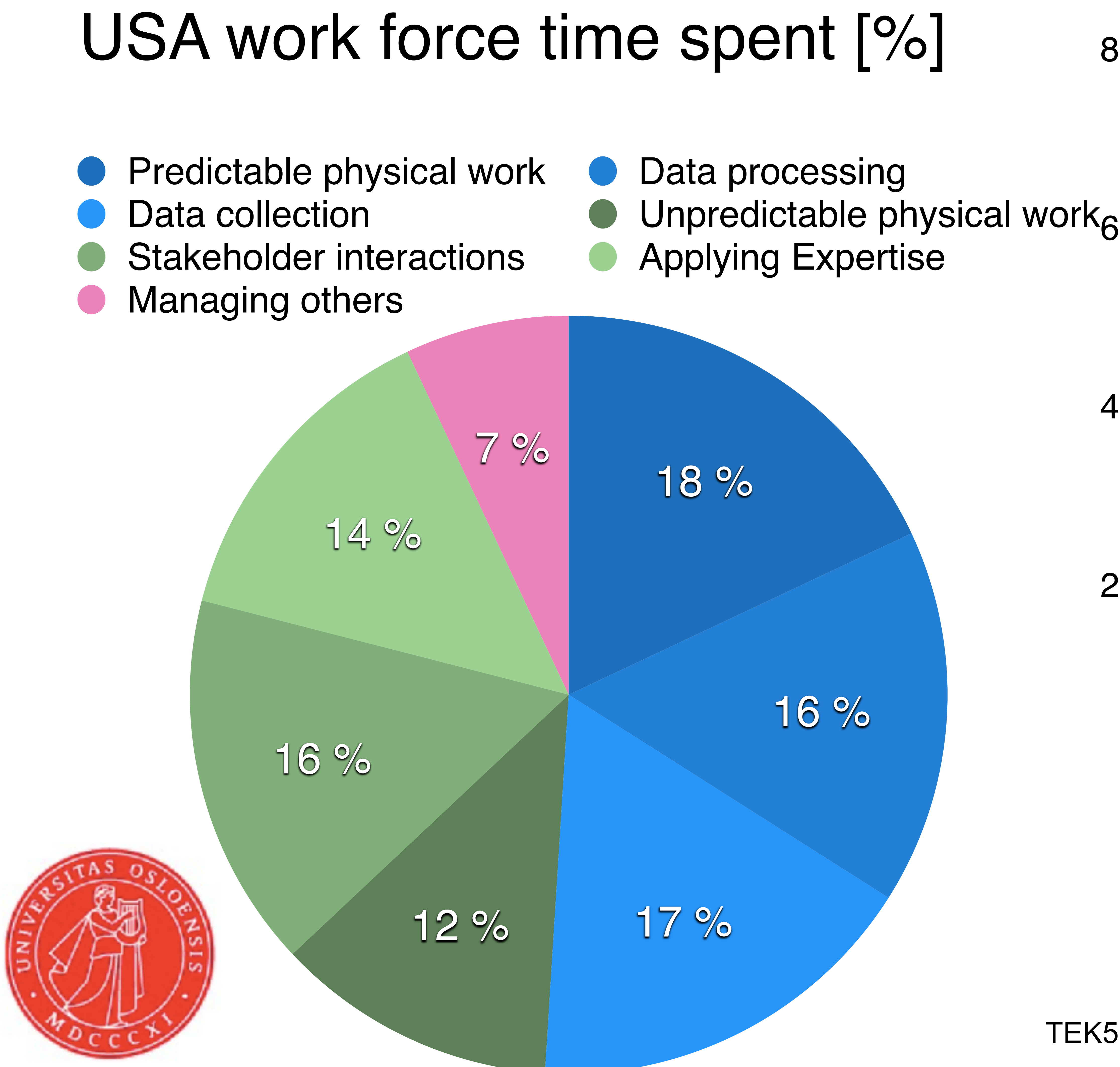
Business drivers

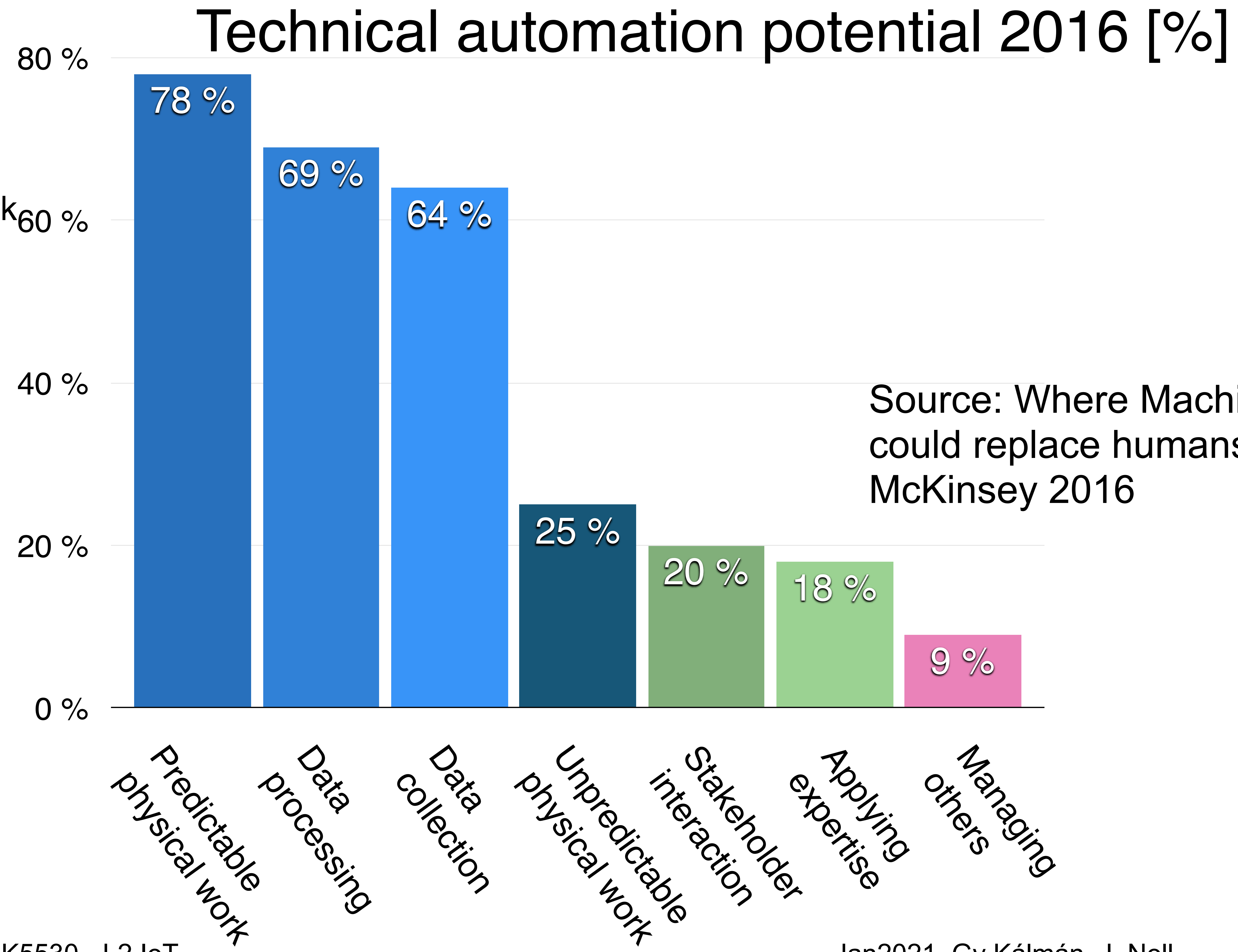
- costs
- efficiency
- novel services



- smart grid
- various control mechanisms
- attack scenarios
- critical infrastructure

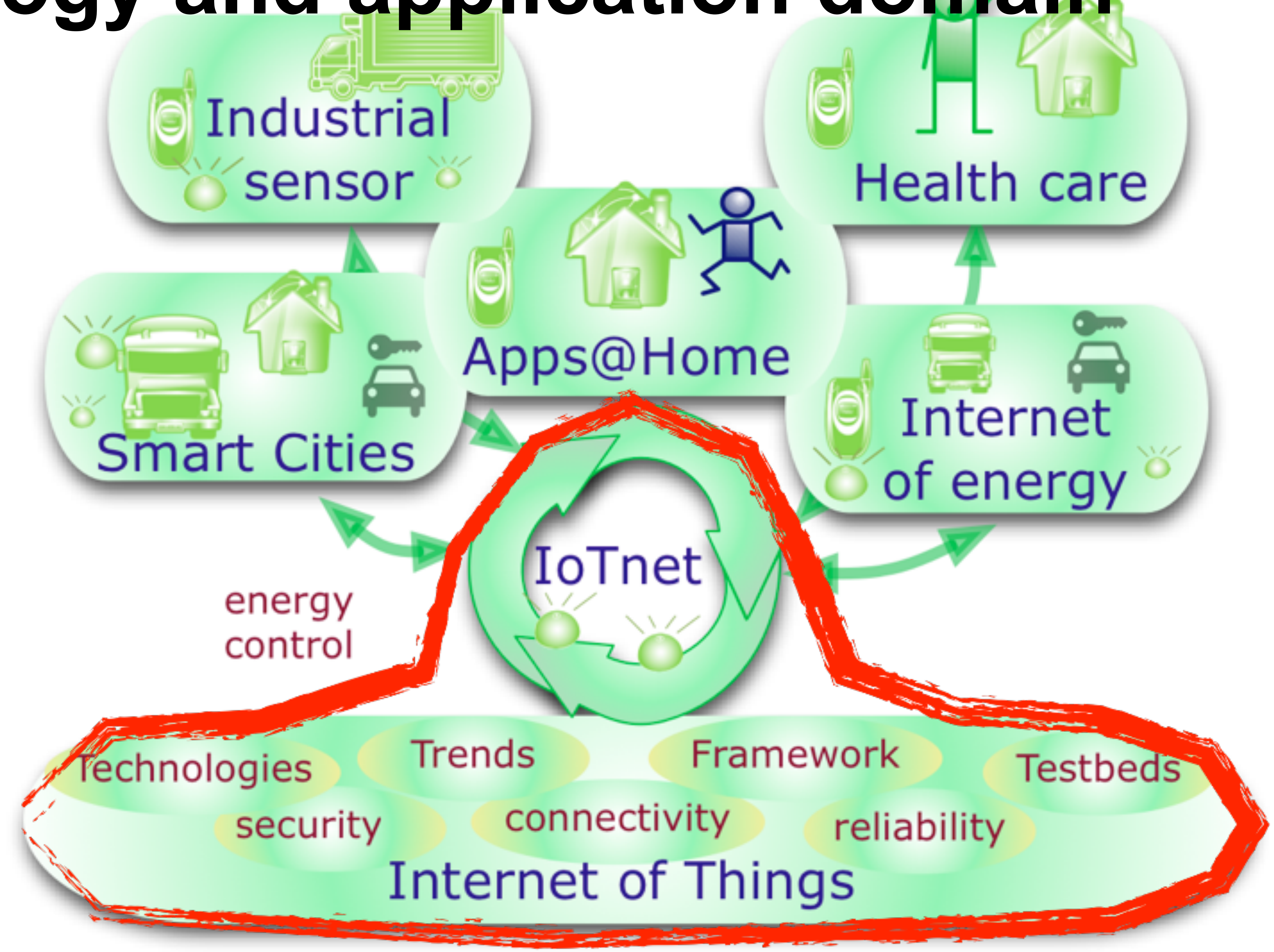
Automation will come



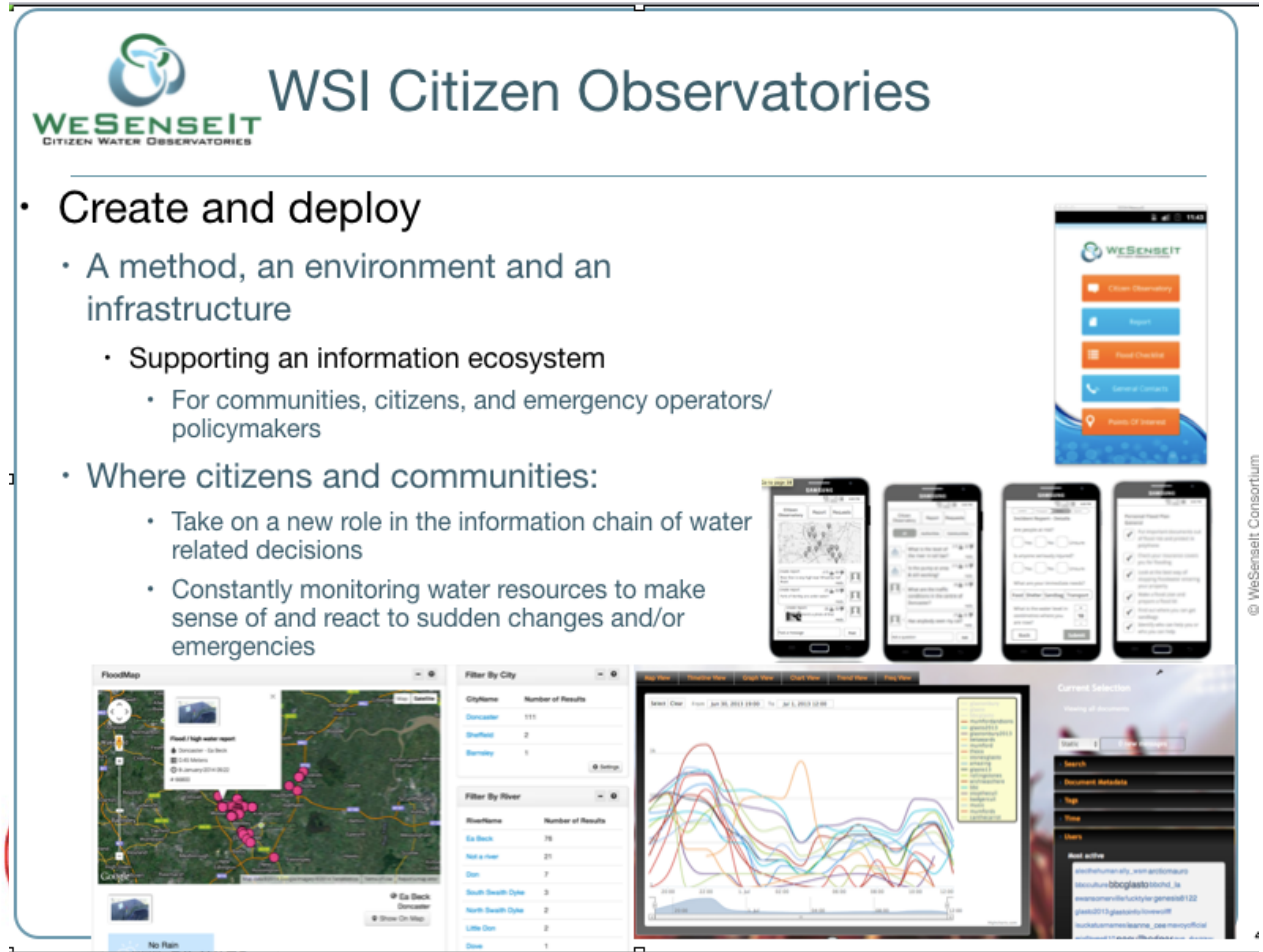


Source: Where Machines could replace humans, McKinsey 2016

IoT technology and application domain



Examples of future IoT applications

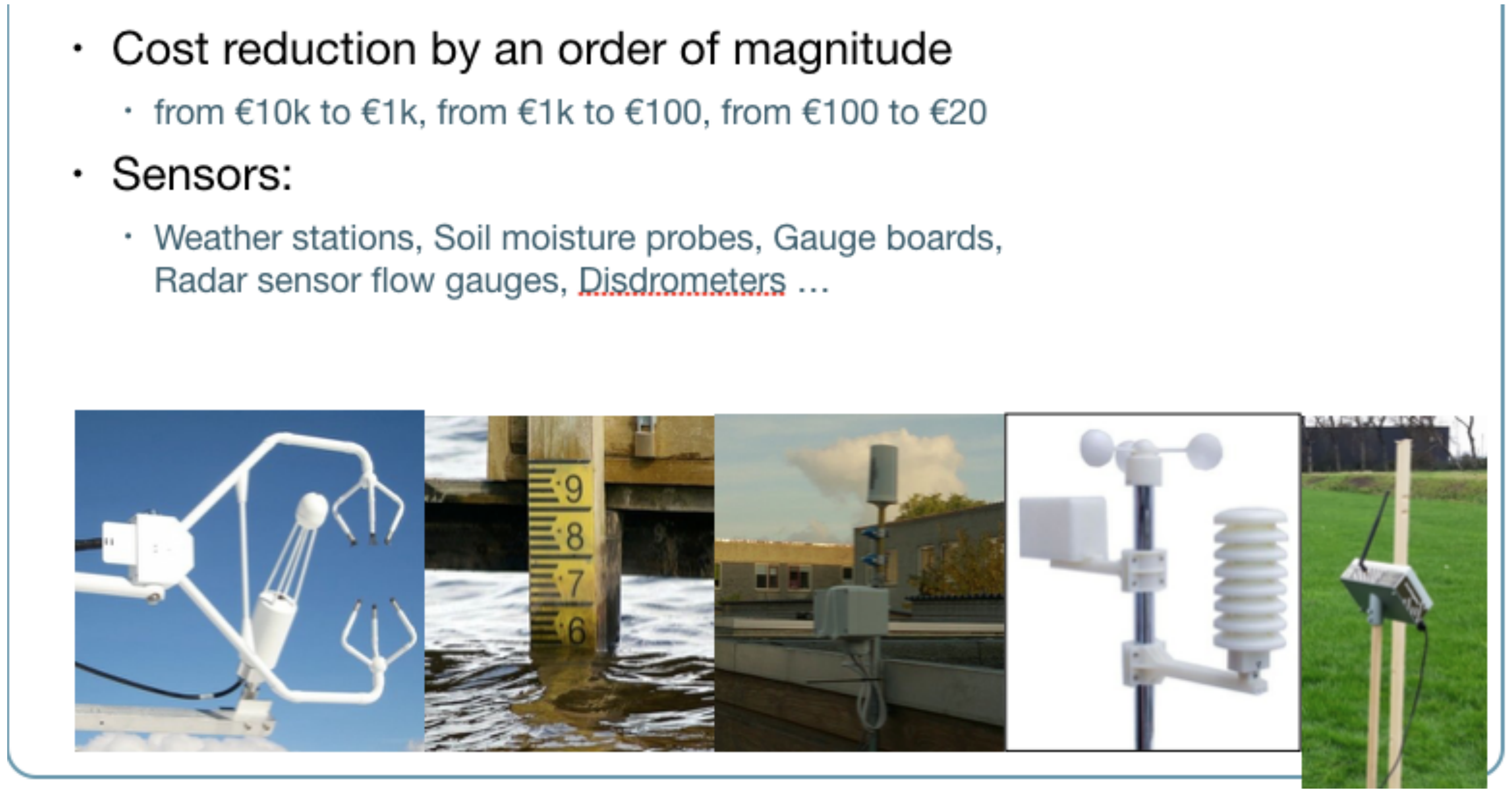


WESENSEIT CITIZEN WATER OBSERVATORIES

WSI Citizen Observatories

- Create and deploy
  - A method, an environment and an infrastructure
    - Supporting an information ecosystem
      - For communities, citizens, and emergency operators/ policymakers
  - Where citizens and communities:
    - Take on a new role in the information chain of water related decisions
    - Constantly monitoring water resources to make sense of and react to sudden changes and/or emergencies

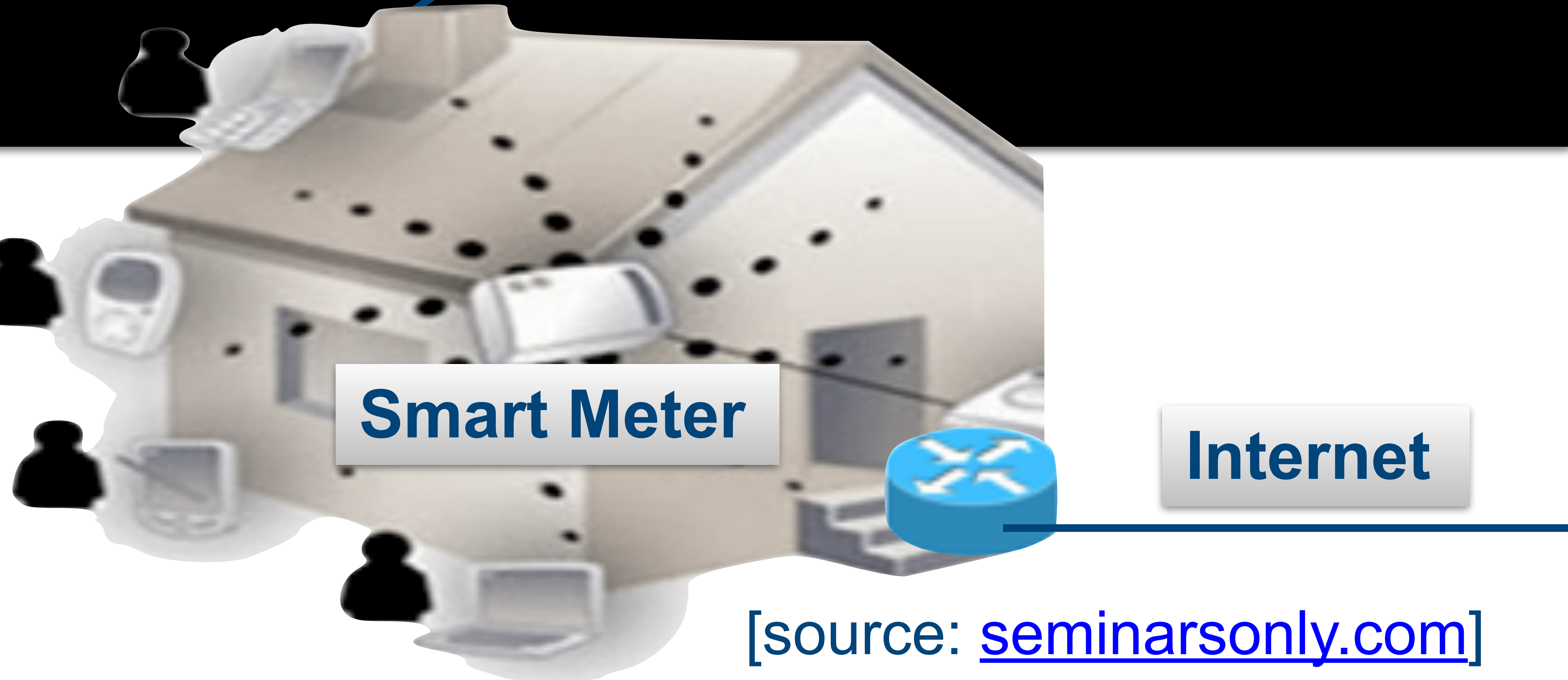
© WeSenseIt Consortium



- Cost reduction by an order of magnitude
  - from €10k to €1k, from €1k to €100, from €100 to €20
- Sensors:
  - Weather stations, Soil moisture probes, Gauge boards, Radar sensor flow gauges, Disdrometers …

© WeSenseIt Consortium

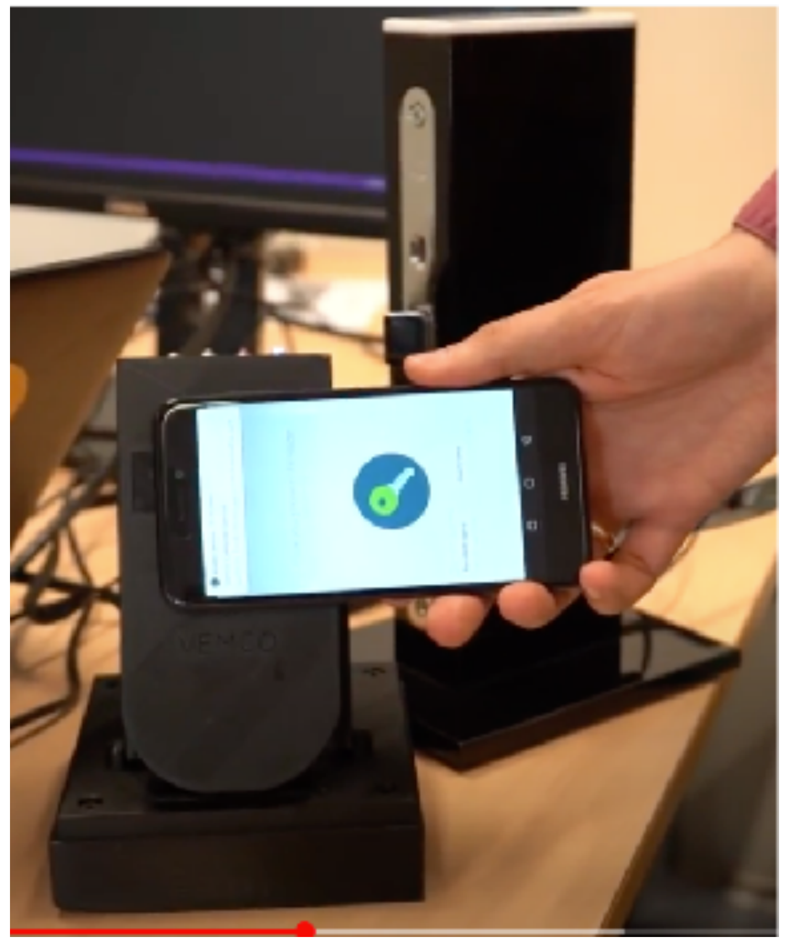
Smart Grid Services in the home



[source: seminarsonly.com]

- Example: automatic meter reading (AMR) and -system (AMS)
- Billing
- Alarm (temperature, security, fire, water)
- Health (surveillance of people and infrastructure)
  - Fridge with open door
  - Person who has fallen

    https://www.youtube.com/watch?v=r9VnE2F3Kn0
- Electricity (monitoring, securing supply)



“Virtual fall sensor”
- measure water & electricity
- profile the user
- estimate: probability of an accident

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

[Source: Cisco, Mikhail Kader, DSE, Cisco, ITU Workshop on "ICT Security Standardization for Developing Countries"]

Smart City

CONNECTED TRAFFIC SIGNALS

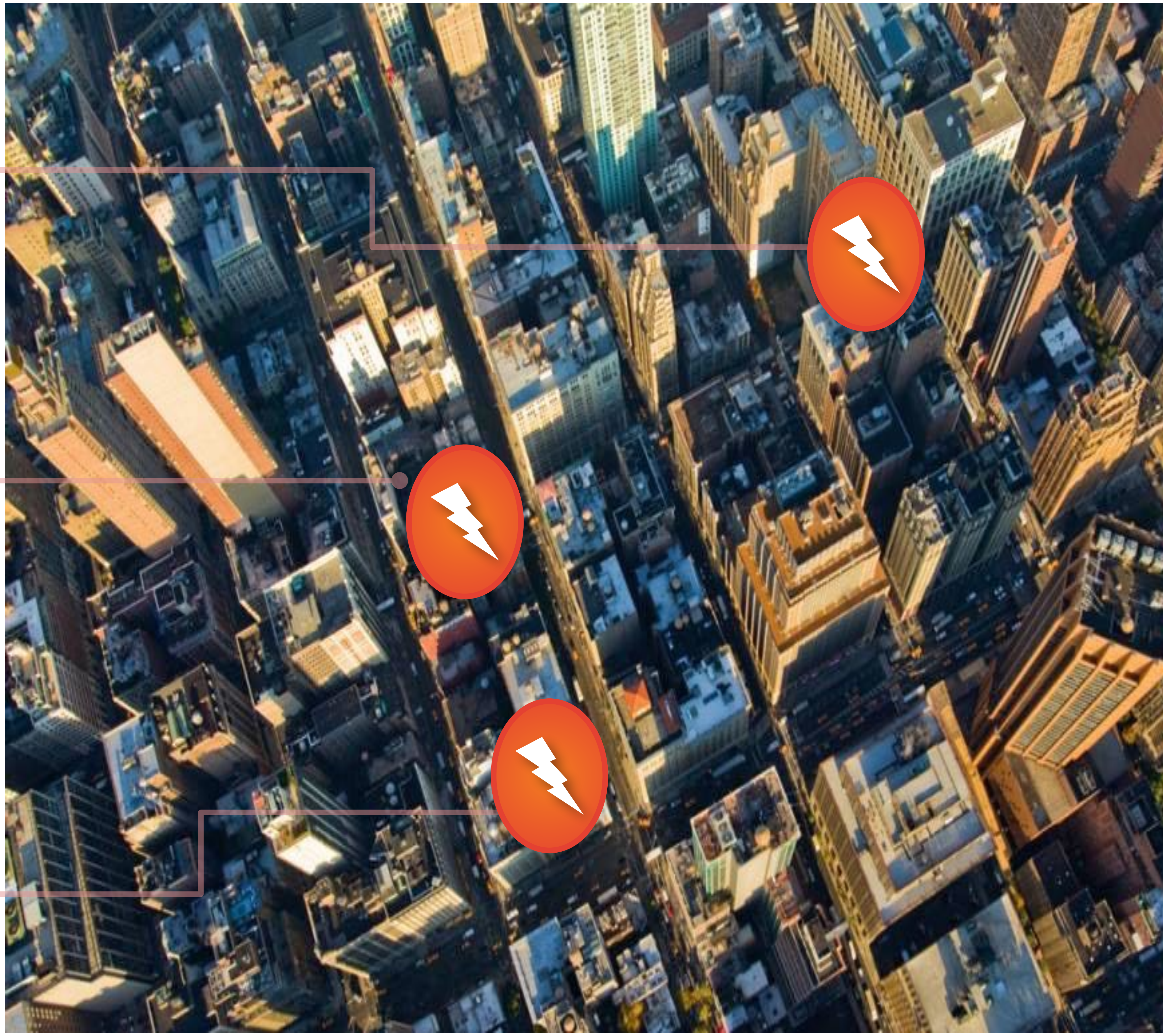
- Reduced congestion
- Improved emergency services response times
- Lower fuel usage

PARKING AND LIGHTING

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

CITY SERVICES

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



[Source: Cisco, Mikhail Kader, DSE, Cisco, ITU Workshop on “ICT Security Standardization for Developing Countries”]

The Connected Car

WIRELESS ROUTER

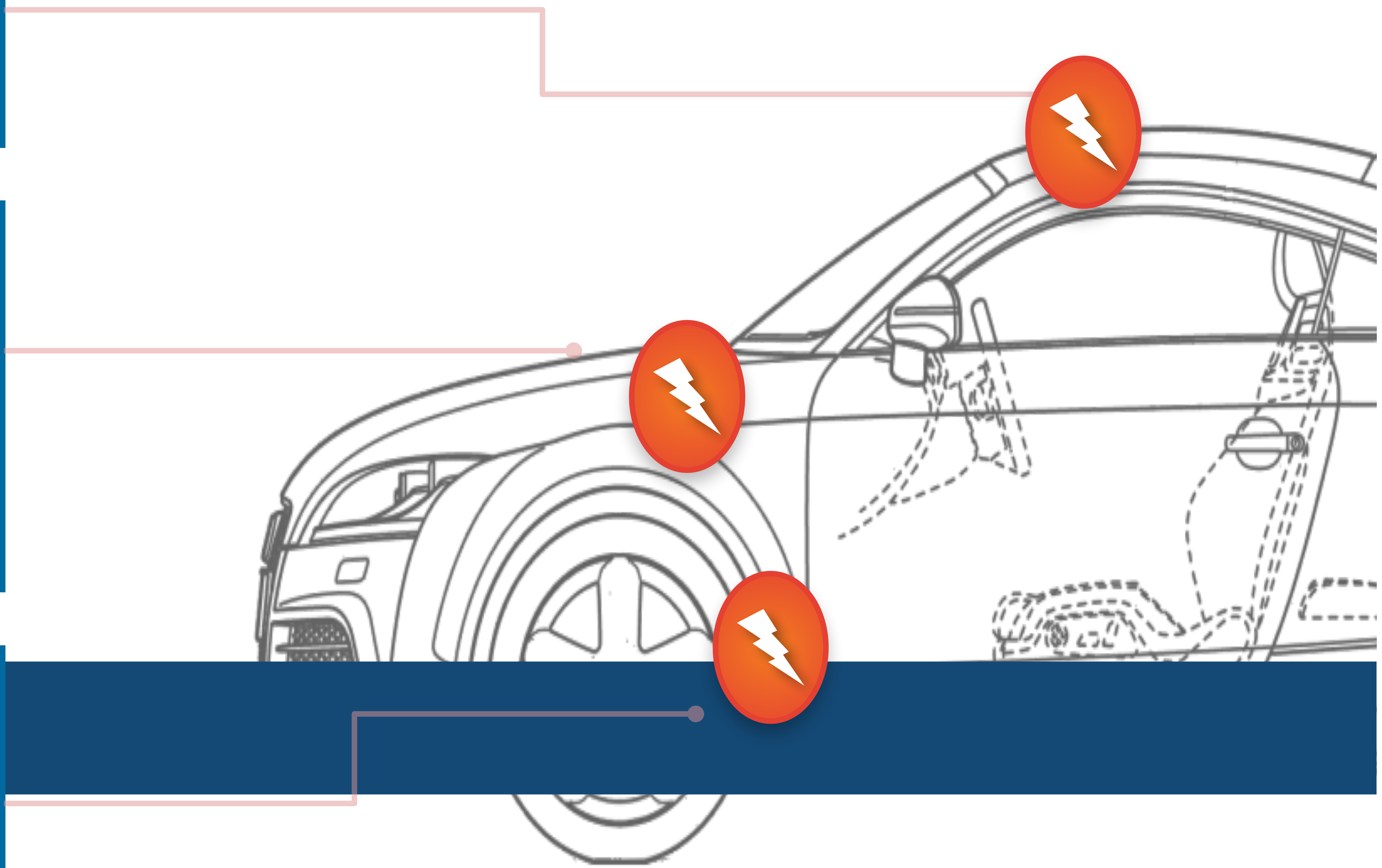
- Online entertainment
- Mapping, dynamic re-routing, safety and security

CONNECTED SENSORS

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

URBAN CONNECTIVITY

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



[Source: Cisco, Mikhail Kader, DSE, Cisco, ITU Workshop on “ICT Security Standardization for Developing Countries”]

IoT services

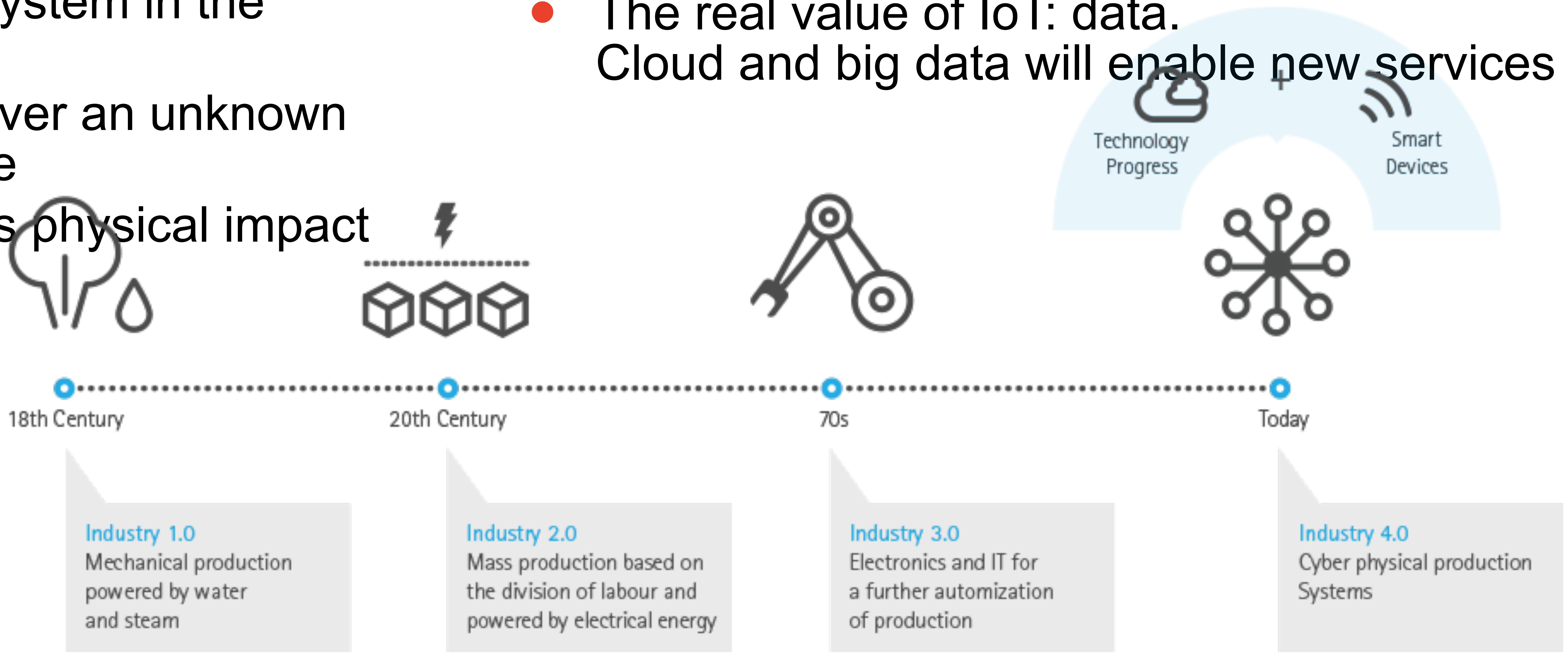
- Enabled by wide scale data gathering
- Monitoring of massive systems
- Real-time insight to processes
- Observation of systems
- Performance measurement and optimisation

- Proactive and predictive methods
- To serve the automation goals, the services provided must be:
  - scalable,
  - distributed,
  - have a real reference to the physical 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

Merging sensors with industrial production
Generating Data and Services

- 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



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

The Security and Trust Dimension

Source: L. Atzori et al., The Internet of Things: A survey, Comput. Netw. (2010), doi:10.1016/ j.comnet.2010.05.010

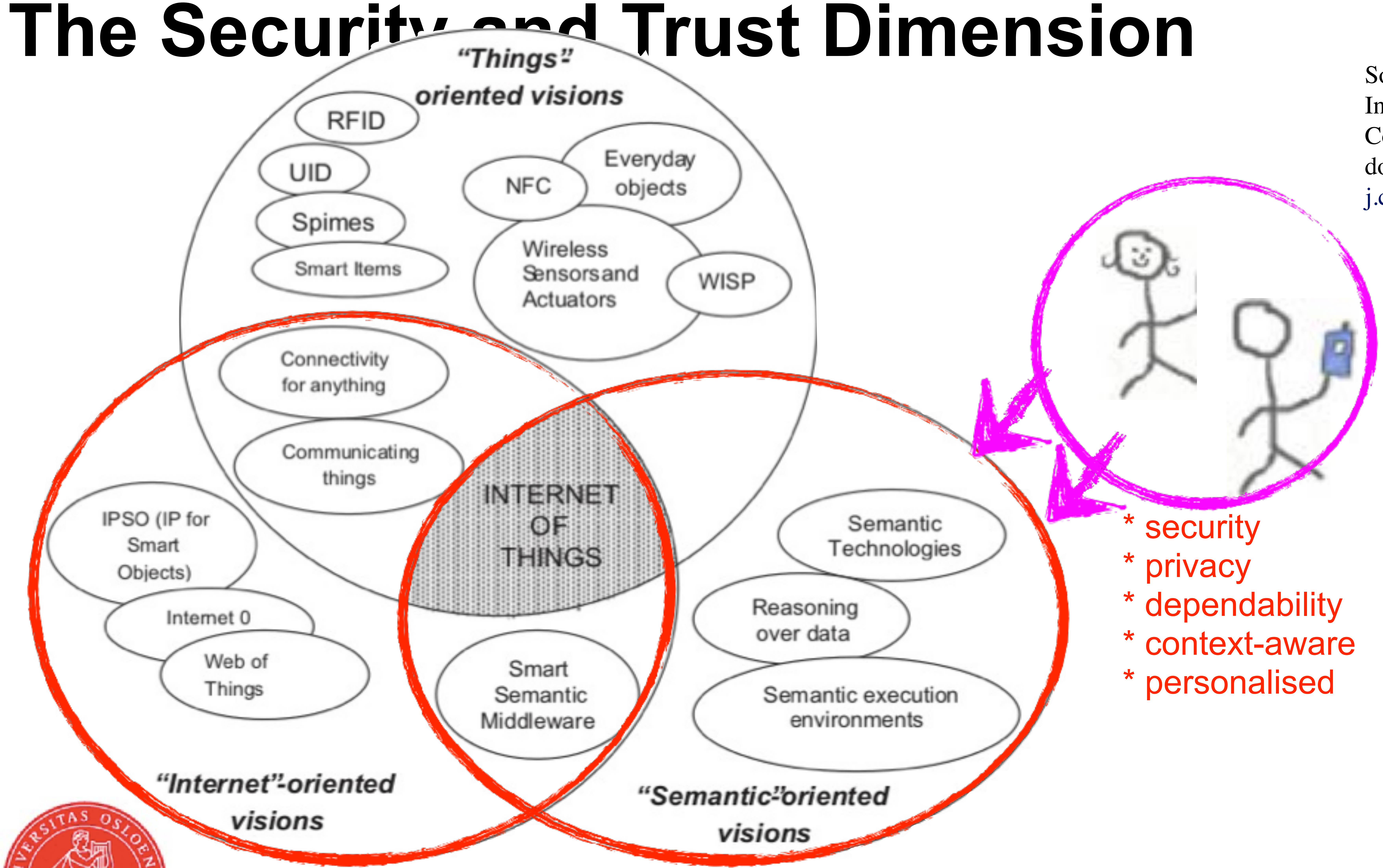

“Things”-oriented visions
RFID
UID
Spimes
Smart Items
NFC
Everyday objects
Wireless Sensors and Actuators
WISP
Connectivity for anything
Communicating things
IPSO (IP for Smart Objects)
Internet 0
Web of Things
INTERNET OF THINGS
Smart Semantic Middleware
Semantic Technologies
Reasoning over data
Semantic execution environments
“Internet”-oriented visions
“Semantic”-oriented visions

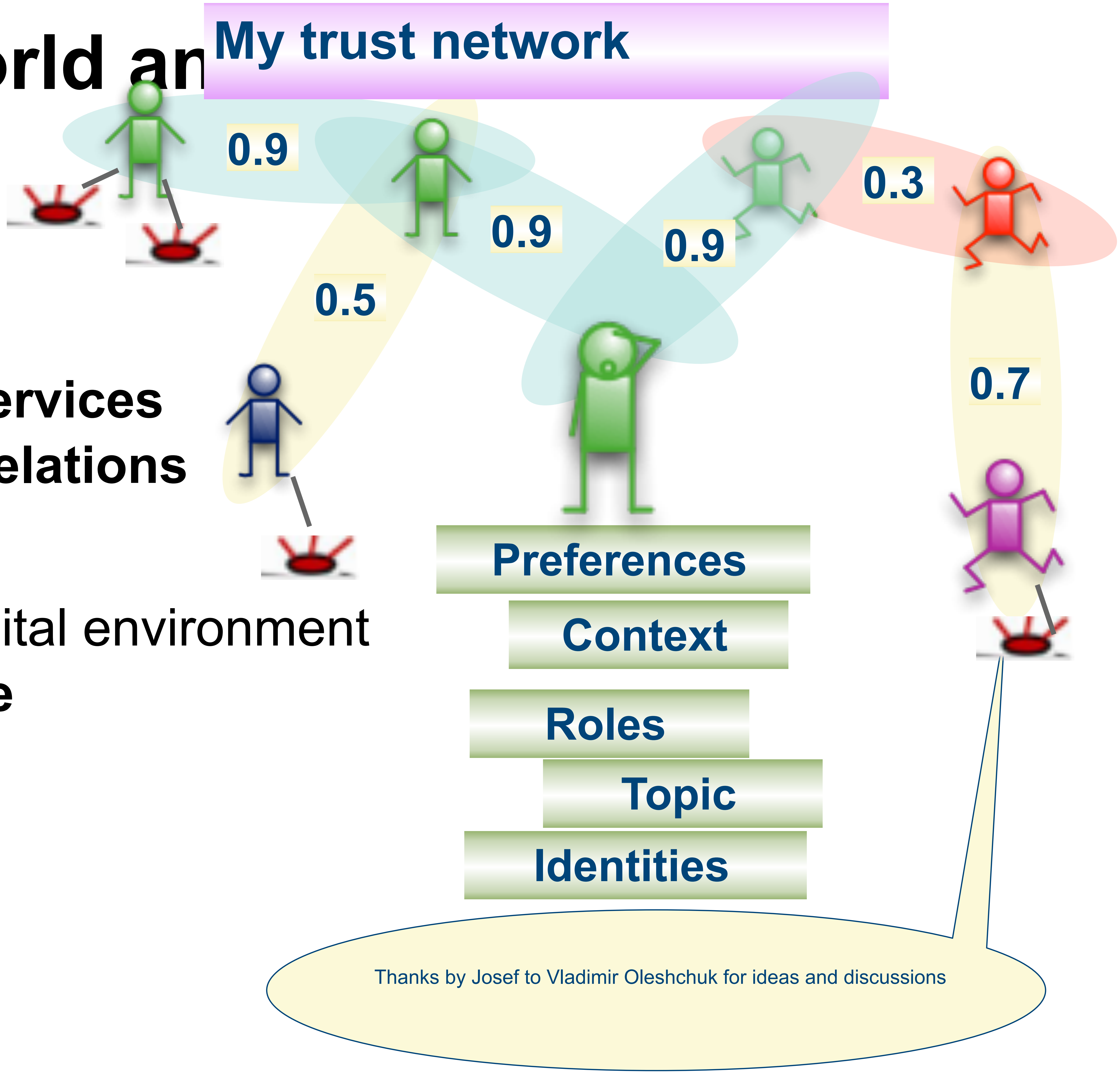
Fig. 1. “Internet of Things” paradigm as a result of the convergence of different visions.

- * security
- * privacy
- * dependability
- * context-aware
- * personalised

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

Paradigm change for
The Internet of the Real World an

- Trust related privacy
  -> **Representing the user adequately**
- Connecting to **sensors**, **devices** and **services**
  -> **Provide privacy and ensure trust relations**
- An ever increasing complexity in the digital environment
  -> **Hiding the complexity from the use**



Preferences

Context

Roles

Topic

Identities

Thanks by Josef to Vladimir Oleshchuk for ideas and discussions

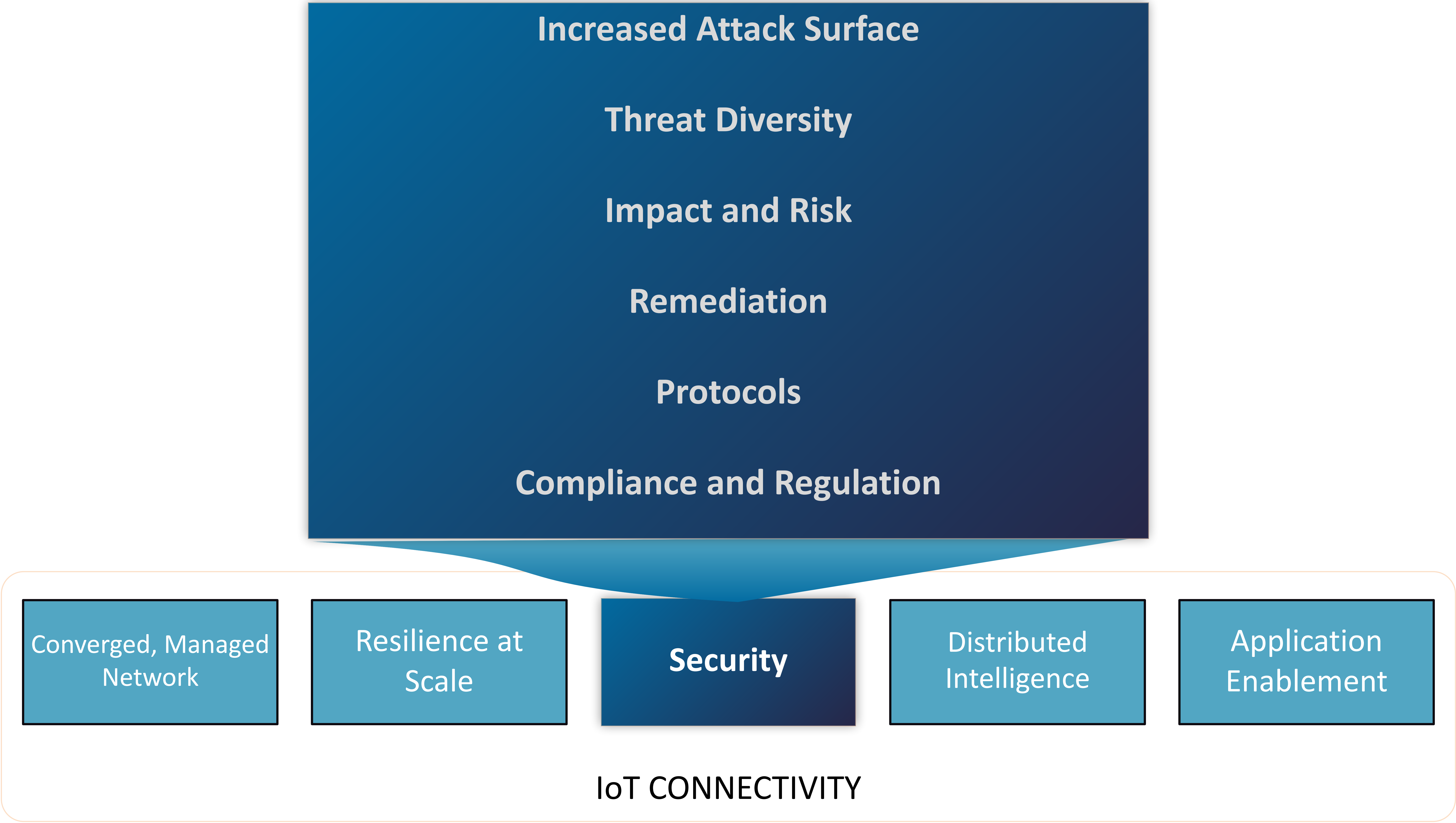
Sociable Internet of Things

- Things become socially intelligent
  - yes, without doubts
  - requires new trust model
  - measurable security
- Growing Internet of Things (IoT) market
  - broad connectivity
  - essential openness of smart "*everything*"
  - security, privacy, dependability

- «

> Imagine a world where things are connected, but unsociable. Every interaction would have to be explicitly scripted or it wouldn't happen. Oh wait, you don't have to imagine it. That's the current model for the IoT, and it won't scale.
>
> http://www.linuxjournal.com/content/true-internet-things

IoT Expands Security Needs



Increased Attack Surface

Threat Diversity

Impact and Risk

Remediation

Protocols

Compliance and Regulation

Converged, Managed Network

Resilience at Scale

Security

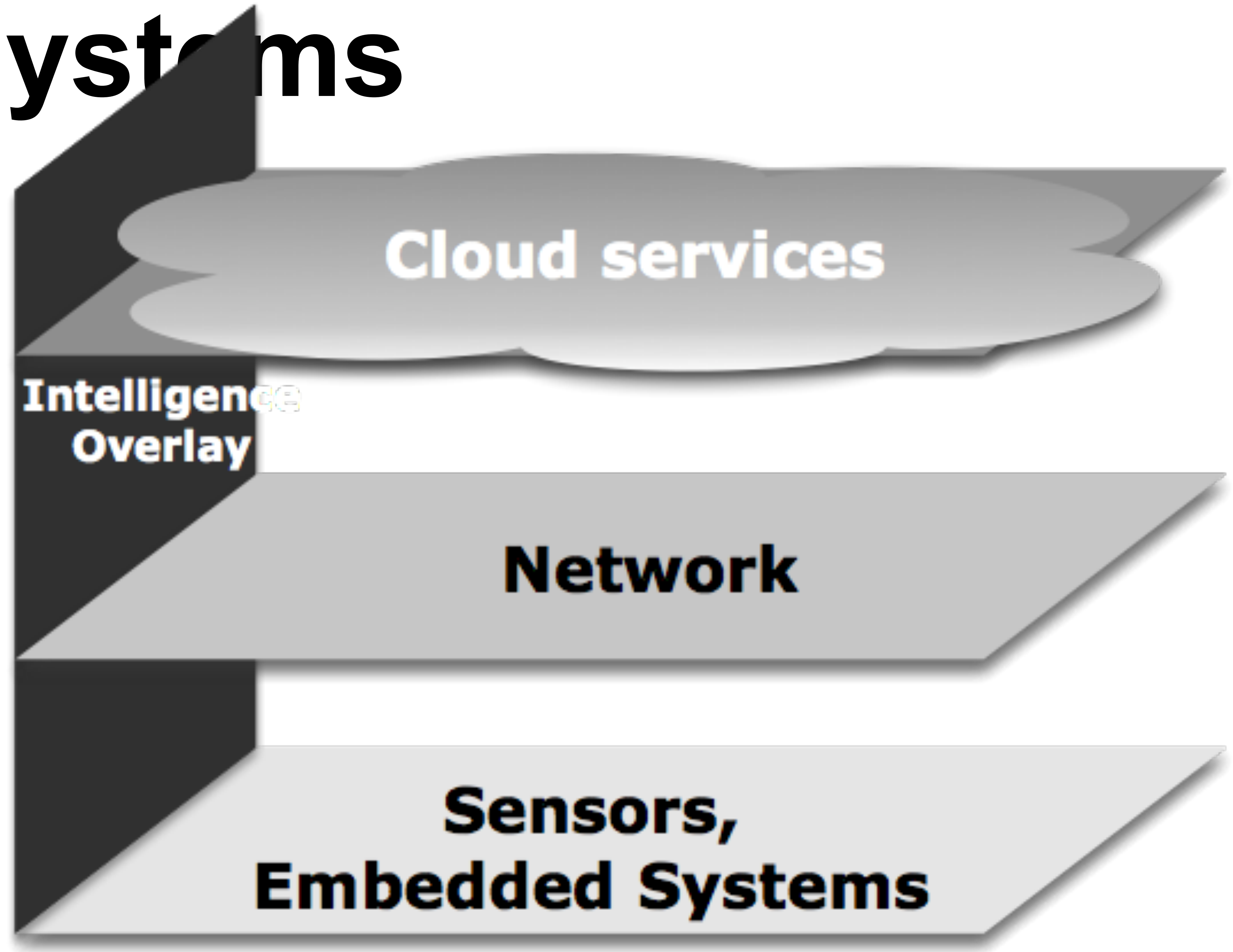
Distributed Intelligence

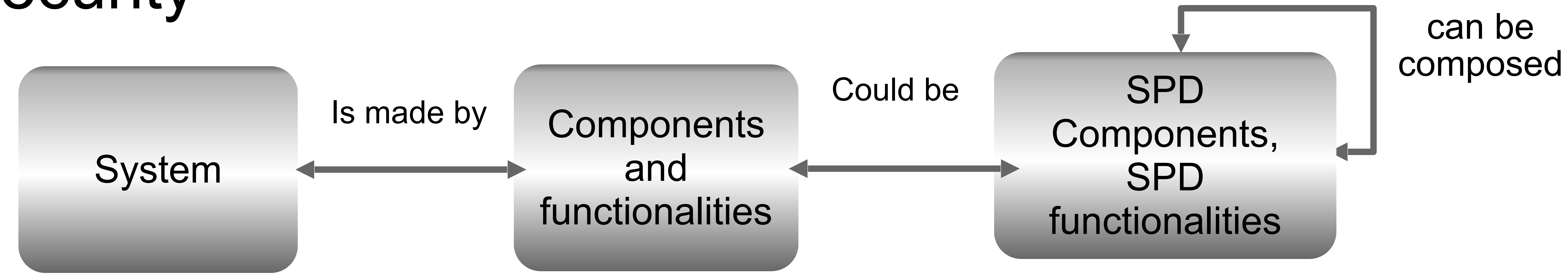
Application Enablement

IoT CONNECTIVITY

Common architecture of IoT systems

- Core system consists of
  - sensors and devices
  - network and communications
  - services
  - intelligent overlay
- Ability to adjust
  - from sensors to services
- Composing security




System
Is made by
Components and functionalities
Could be
SPD Components, SPD functionalities
can be composed

L2- Conclusion

- What we mean with IoT
- Domains being addressed
  - ➡ Things
  - ➡ Semantics
  - ➡ Internet
- Security and privacy challenges
  - ➡ Security
  - ➡ Privacy
  - ➡ Multi-owner requirements
- Architecture components

- Services and Ecosystem

- Describe the domains being merged in IoT
- Provide examples of challenges in IoT with focus on services, security and privacy
- Multi-owner service requests
- Analyse security and privacy requirements in an example scenario