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

TEK5530: Lecture plan

- **16.01**
  - **L1: Introduction (Josef Noll)**
  - **L2: Internet of Things (Gyorgy Kalman)**
- 23.01 (Gyorgy Kalman)
  - L3: Security of IoT + Paper list
  - L4: Smart Grid, Automatic Meter Readings
- 06.02 (Josef Noll)
  - L5: Practical implementation of ontologies
  - L6: Multi-Metrics Method for measurable Security
- 13.02 (Josef Noll)
  - L7: Multi-Metrics Weighting of an AMR sub-system
  - L8: System Security and Privacy analysis
- 20.02 --- Winter holiday
- 27.02 (Josef Noll)
  - L9-10: Paper analysis with 25 min presentation
- 05.03 (Gyorgy Kalman)
  - L11: Service implications on functional requirements
  - L12: Intrusion Detection
- 12.03 (Gyorgy Kalman)
  - L13: Technology mapping
  - L14: Communication and security in current industrial automation
- 19.03 (Gyorgy Kalman)
  - L15: Cloud basics and cloud architecture
  - L16: Cloud security, IoT and service examples from AWS
- 26.03 (Gyorgy Kalman)
  - L17: Selected recent topics from IoT security
  - L18: Wrap-up of the course
- 02.04 ---- No lecture, prepare for exam, consultation possibility
- 09.04 ---- Easter holiday, no lecture
- 16.04 ---- Exam

L2- Overview

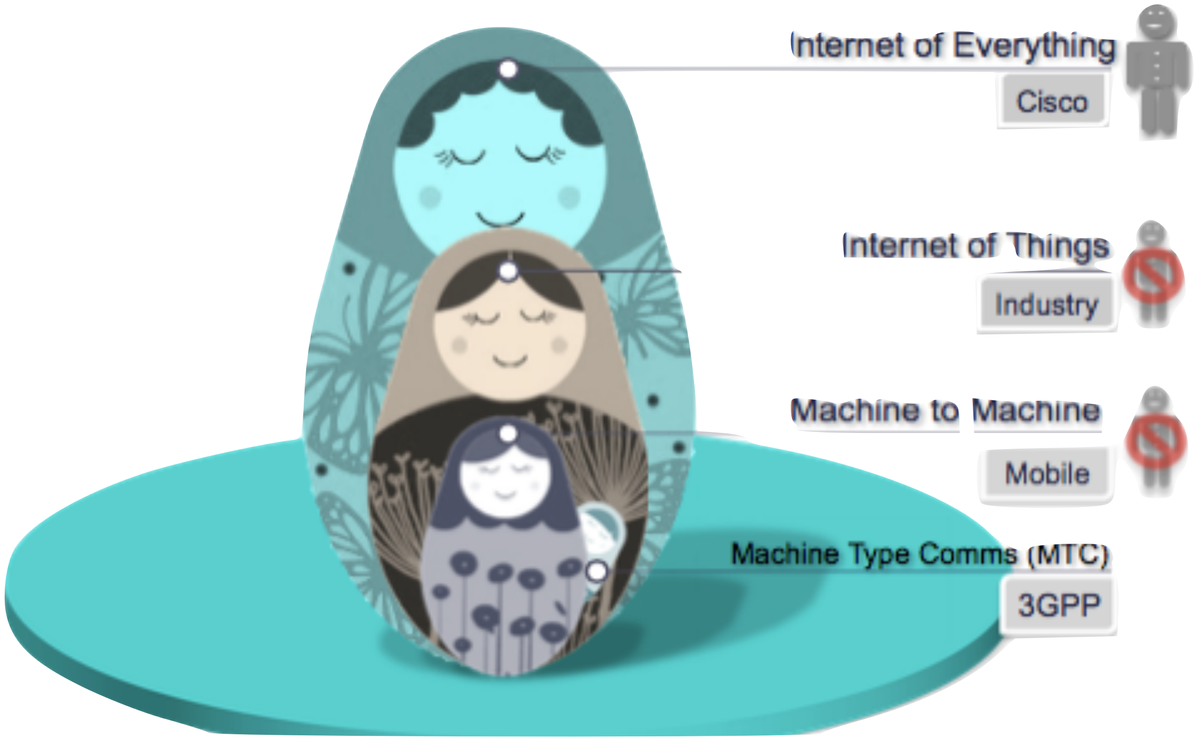
- History of Internet of things (IoT)
- Merging several domains
  - Things
  - Semantics
  - Internet
- What about?
  - Security
  - Privacy
  - Multi-owner requirements

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

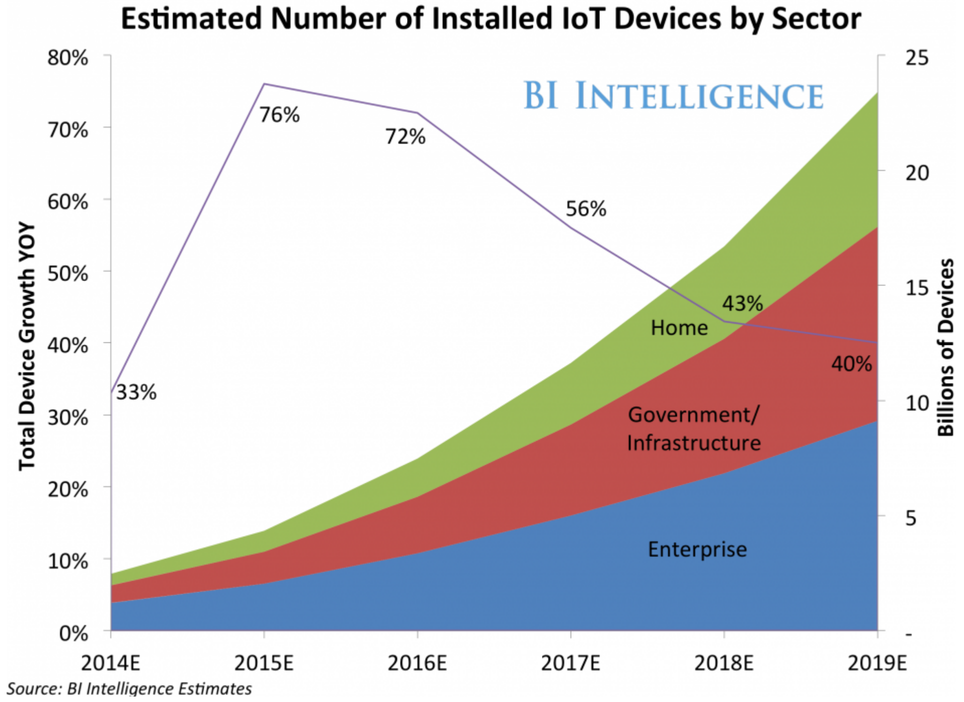
- Technology applications in Maritime, Renewables & Electricity, Health Care, Oil & Gas and Food & Water industries

  sensors will drive automated data management

  from passive data to automated decisions

  automated decision tools by 2020

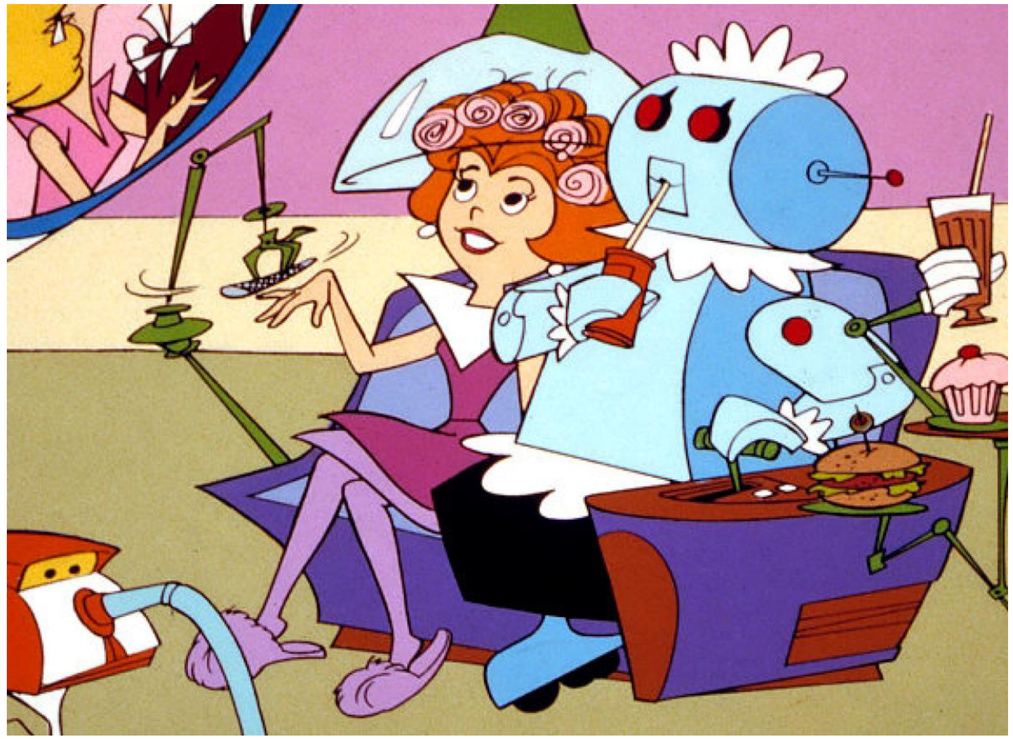
- Maritime: «policy driven»
- Health care: «trust» on sensor and mobile apps



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

[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), doi:10.1016/j.comnet.2010.05.010 (link on the wiki page)
- Create groups of 2-3 people
- Analyse the paper
  - Read 20 min
  - Discuss 15 min
- Establish aspects of IoT, e.g.
  - technologies
  - interfaces
  - standards
- Present your “top 5”

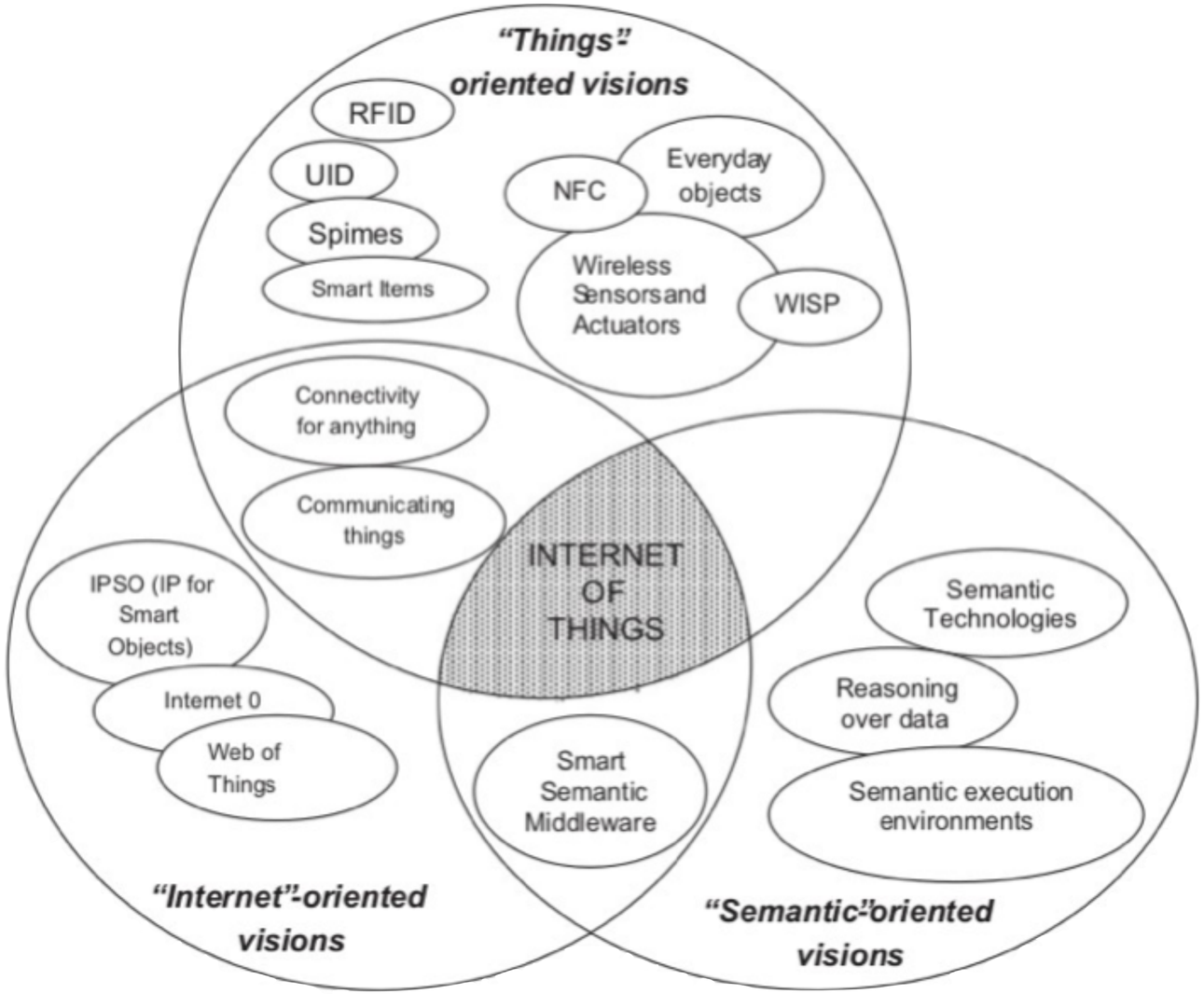


Fig. 1. "Internet of Things" paradigm as a result of the convergence of different visions.

“Your take on IoT”

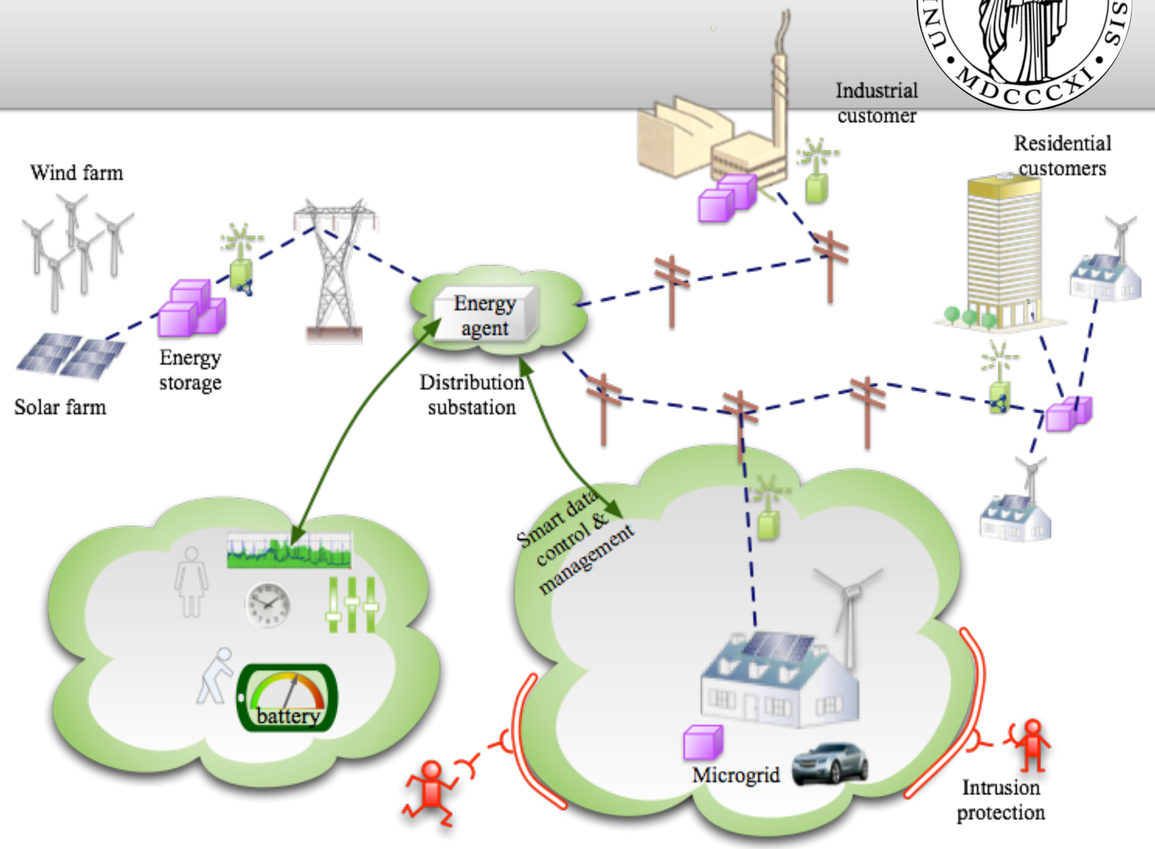
- ….

Main drivers for IoT

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

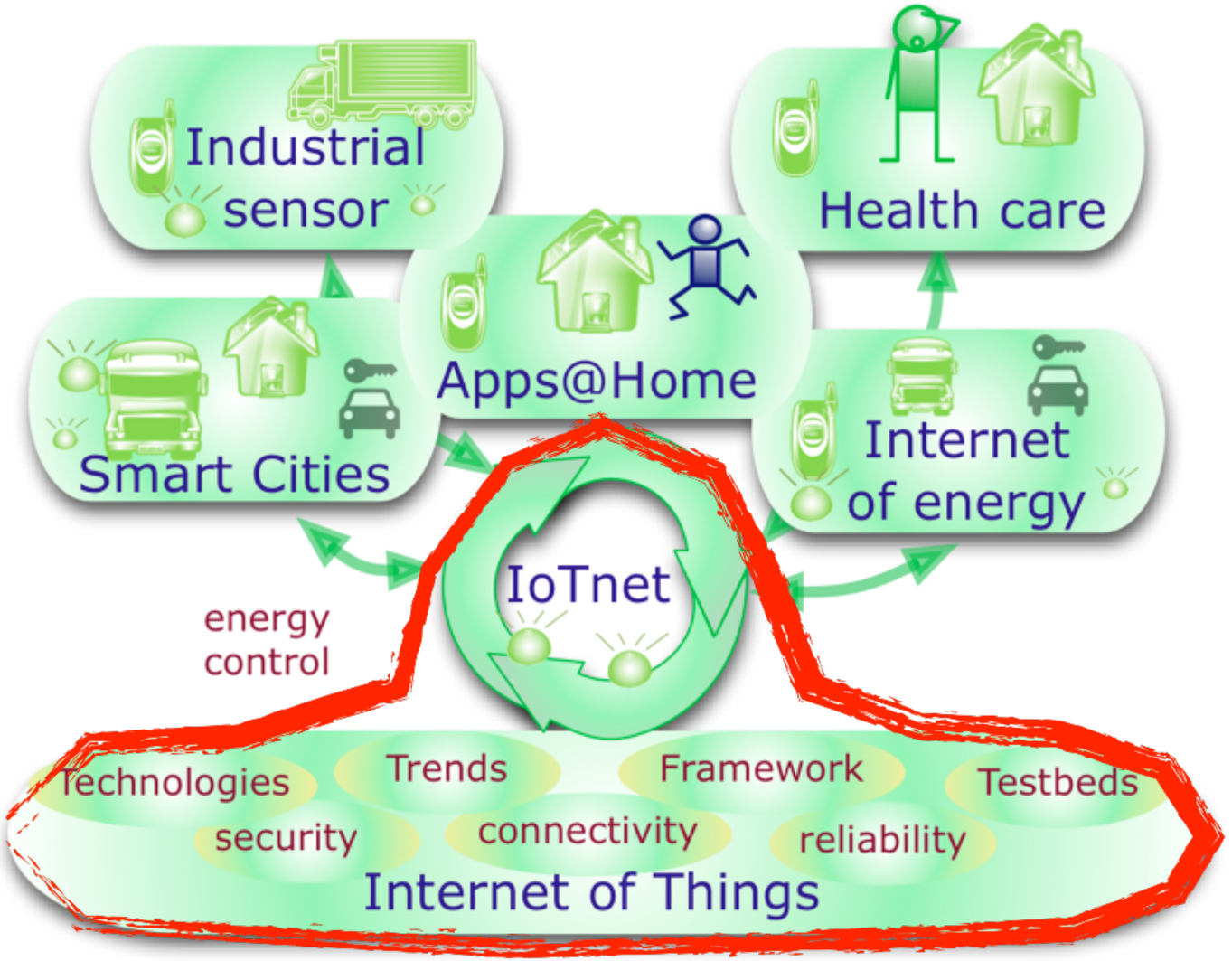
Business drivers

- costs
- efficiency
- novel services



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

IoT technology and application domain



Examples of future IoT applications

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

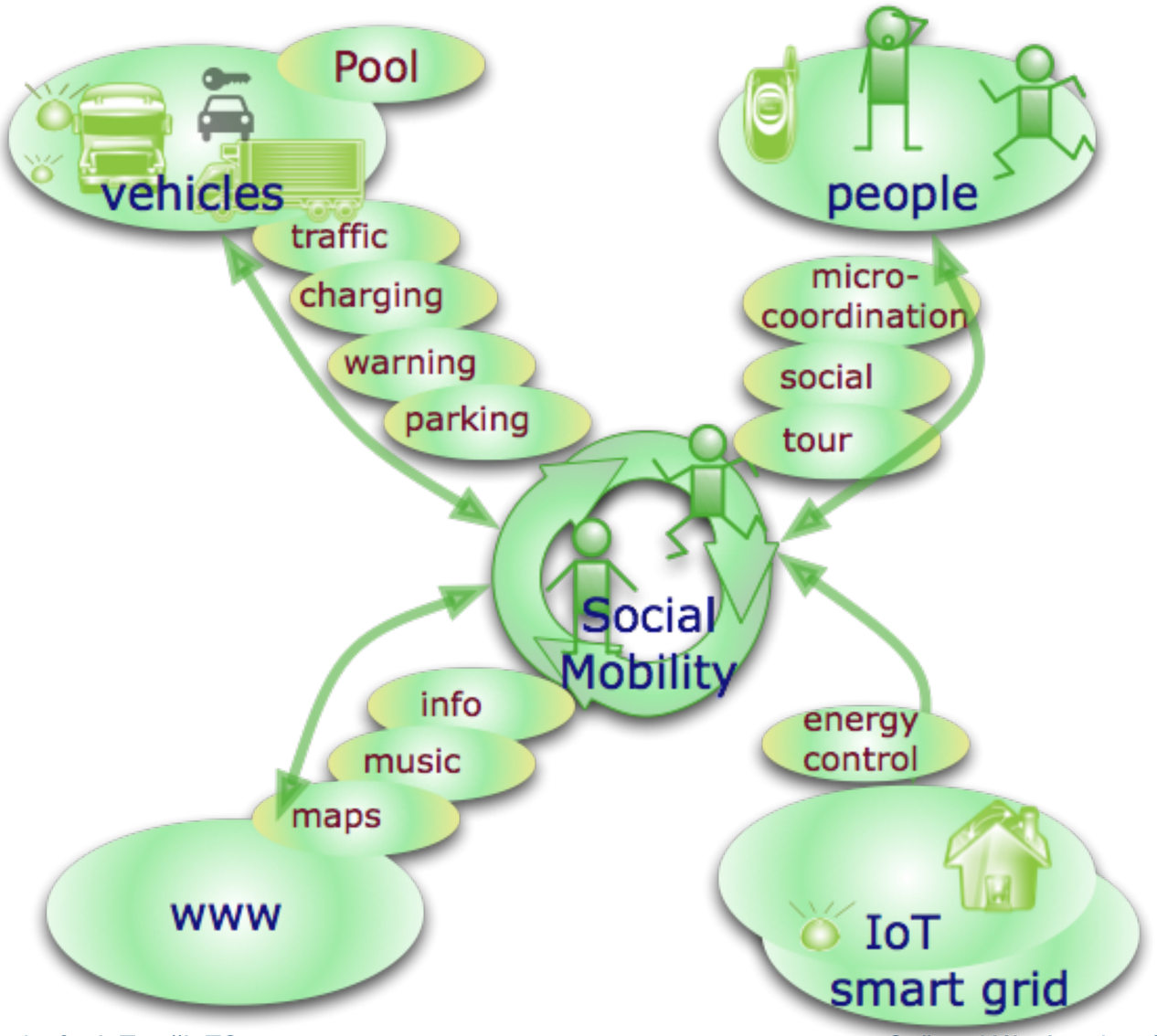
Smart Grid Services in the home

- 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
- Electricity (monitoring, securing supply)

[source: seminarsonly.com]

Application Example: Socialtainment (eMobility)

- From Entertainment to Socialtainment
- Social mobility through inclusion of social networks
- Potentially improved efficiency



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

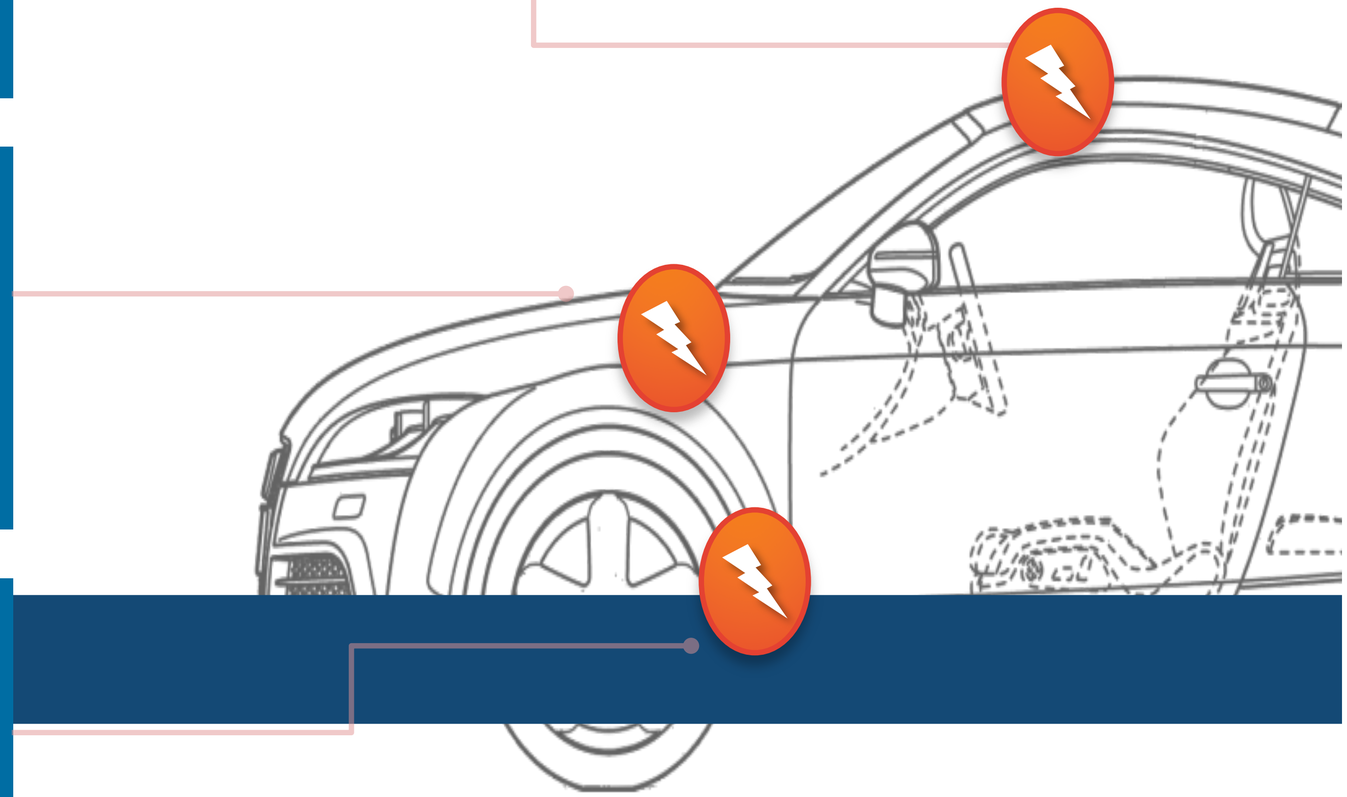
[Source: Cisco, Mikhail Kader, DSE, Cisco, ITU Workshop on “ICT Security Standardization for Developing Countries”]

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”]

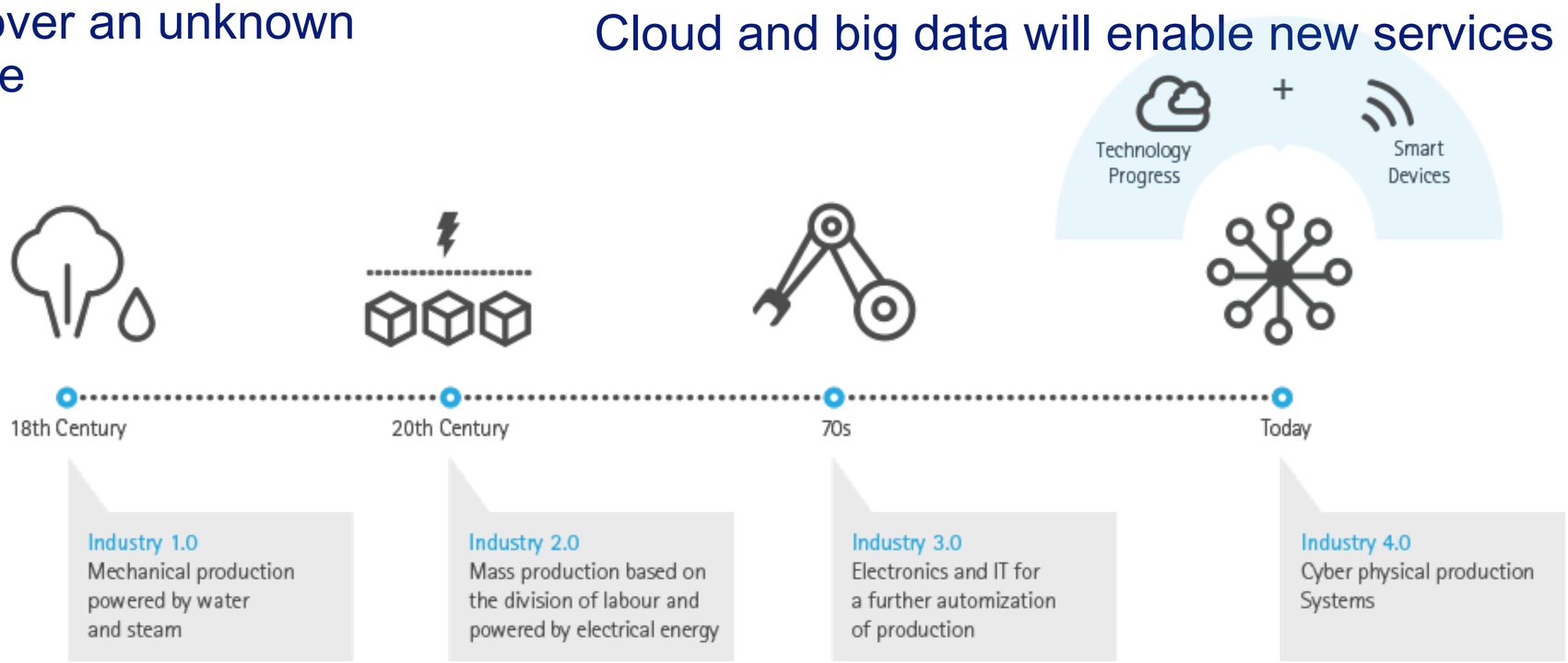
IoT services

- 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



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

The Security and Trust Dimension

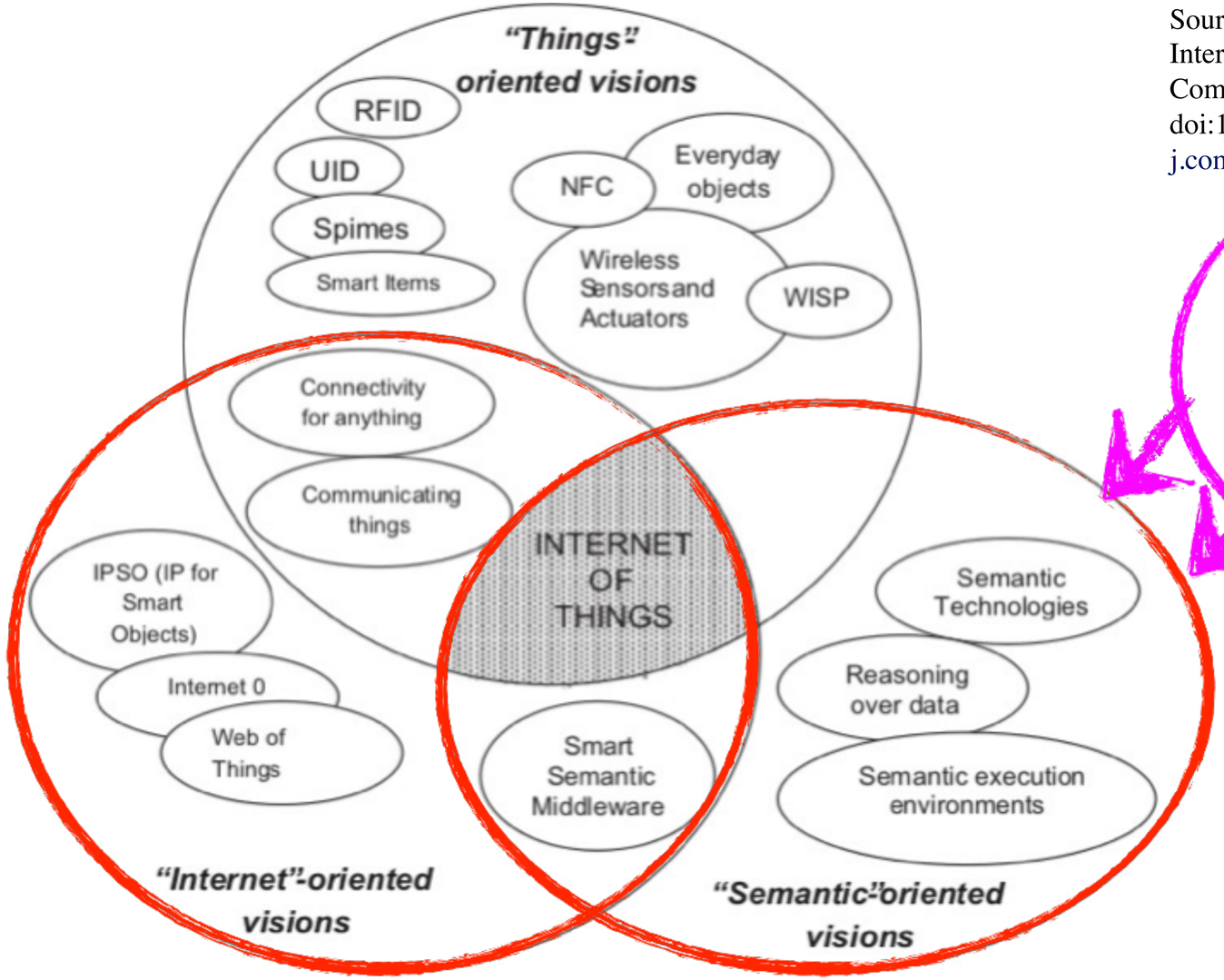


Fig. 1. "Internet of Things" paradigm as a result of the convergence of different visions.

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

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

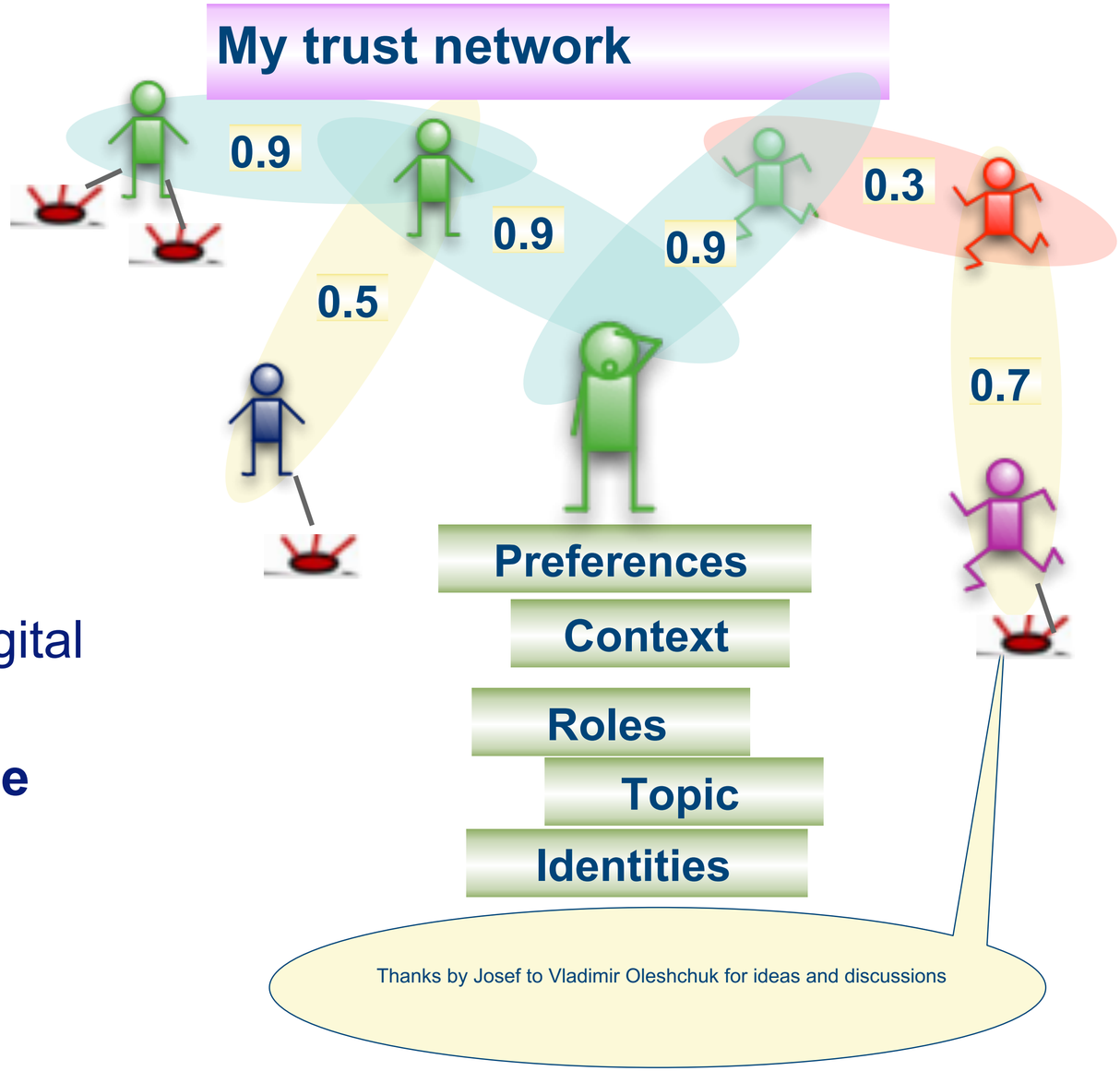
"Only 59% of the public trust the energy industry," (Edelman Trust Barometer 2013)

Paradigm change for
The Internet of the Real World and IoT

- 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**



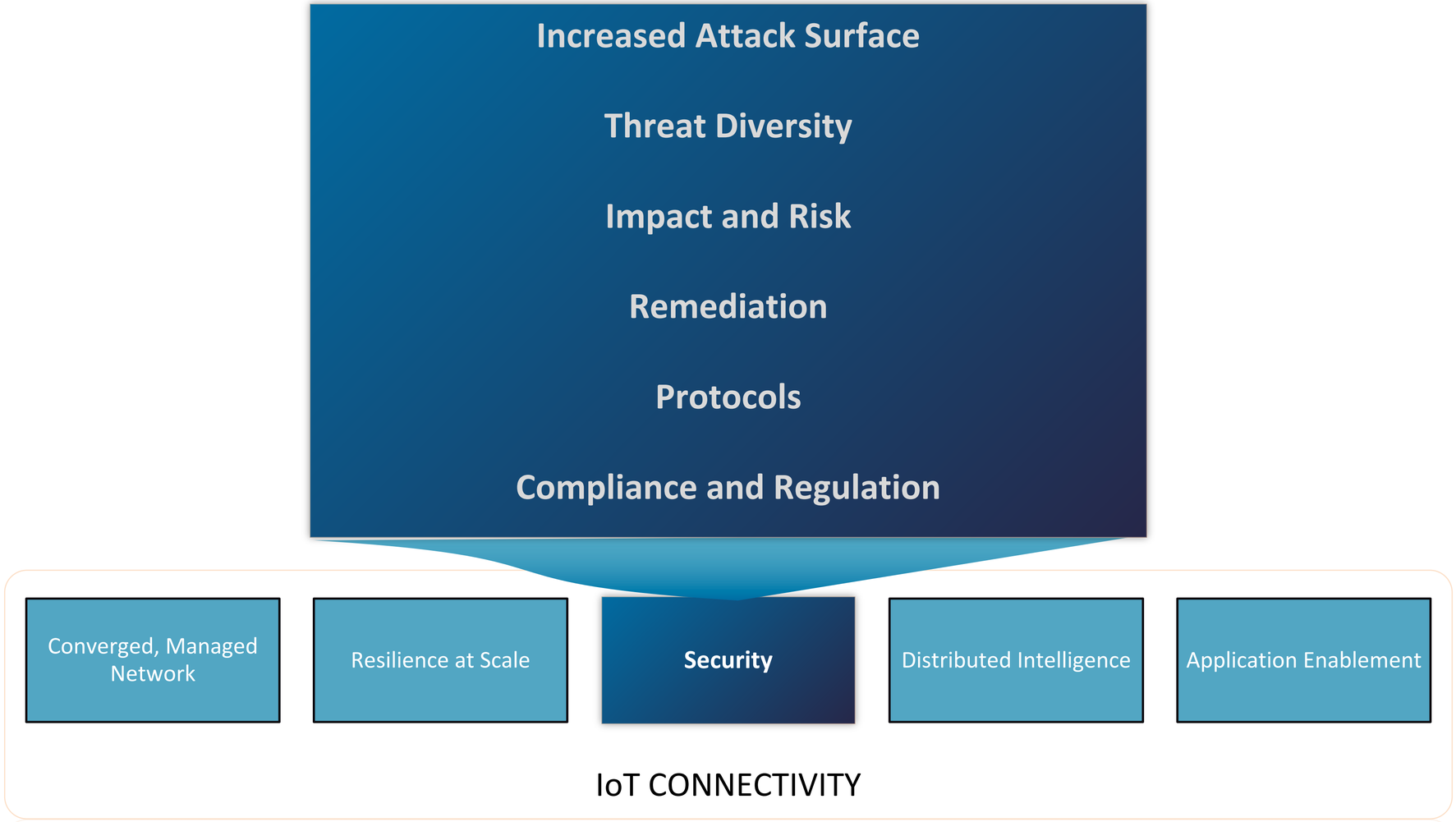
Sociable Internet of Things

- 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

- «What about me?»
  - The Internet of People, Things and Services (IoPTS)

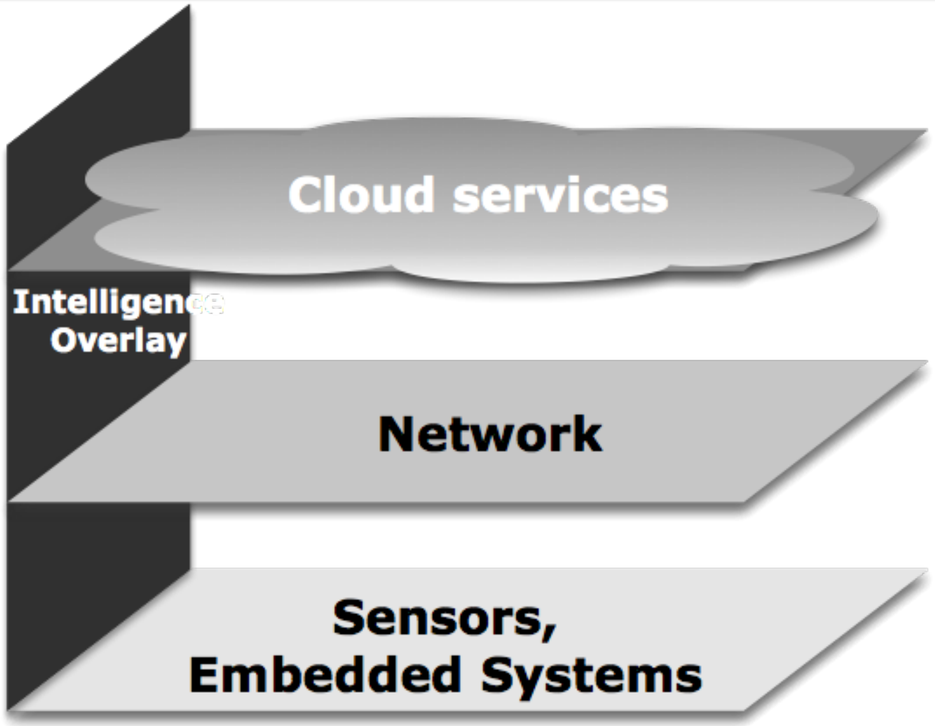
> Imagine a world where things are connected, but unsociable. Every interaction would have to be explicitly scripted or it wouldn't happen. Oh wait, you don't have to imagine it. That's the current model for the IoT, and it won't scale.
>
> http://www.linuxjournal.com/content/true-internet-things

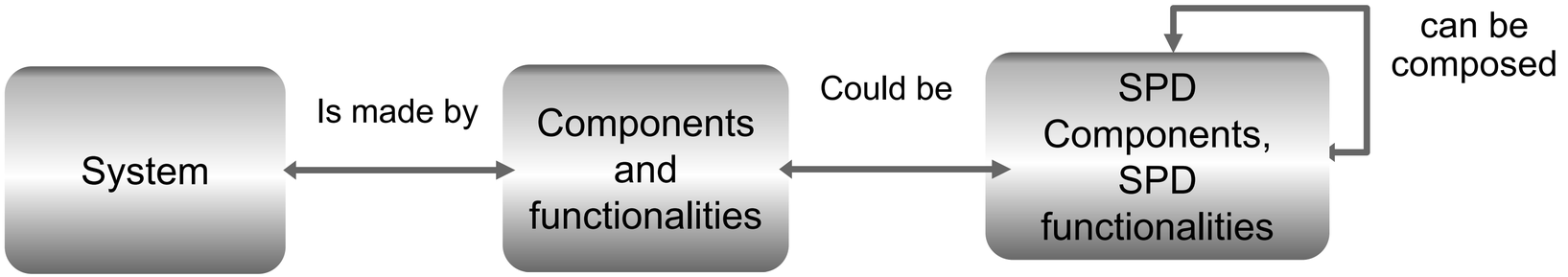
IoT Expands Security Needs



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





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