Center for Wireless Innovation Norway
cwin.no

CWI
Norway

UNIK
UNIVERSITY GRADUATE CENTER

Strategic Workshop - Malaga - May 2013

Measurable Security for the Internet of Things

Josef Noll

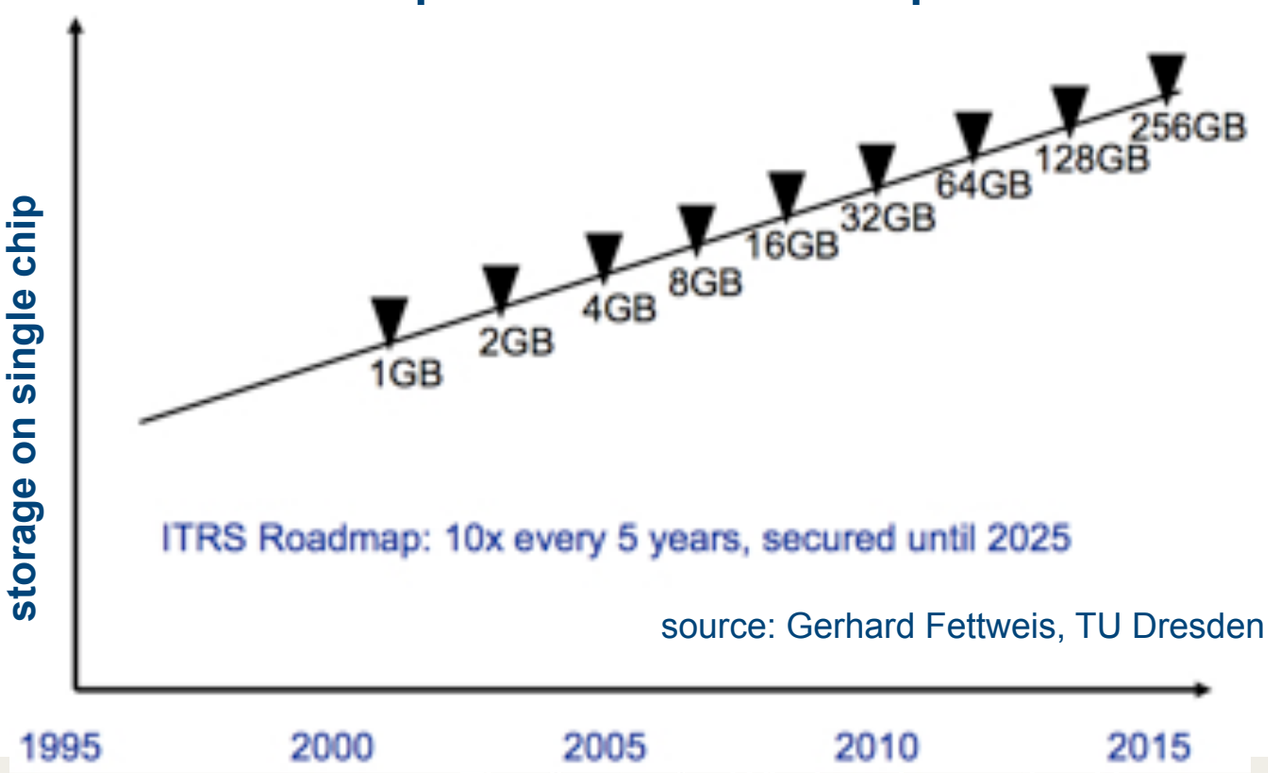
Prof. at **University Graduate Studies (UNIK), University of Oslo (UiO)**
Chief technologist at **Movation AS**
Steering board member, Norway section at **MobileMonday**
Oslo Area, Norway

Outline

- Measurable Security
  - Application in the IoT
  - threat, goal, architecture
- Approach
  - Ontologies for security, system, component functionality
  - Metrics based assessment
  - context-aware security
- Discussion
  - Specific ontologies for each threat
  - Sensor/device standardisation
  - distributed or universal metrics
- ~~Conclusions~~

IoT paradigm

- From "Internet of PCs" towards the "Internet of Things" with 50 to 100 billion devices connected to the Internet by 2020. [CERP-IoT, 03.2010]
- Things have their own identity, communicate with other things and humans (IoPTS)
- The speed of development



source: Gerhard Fettweis, TU Dresden

"Now (2010) we have roughly 5.2 Mio mobile subscribers. In some year we will have 30...50 Mio devices on the mobile network"
– Hans Christian Haugli, CEO, Telenor Objects

The Semantic Dimension

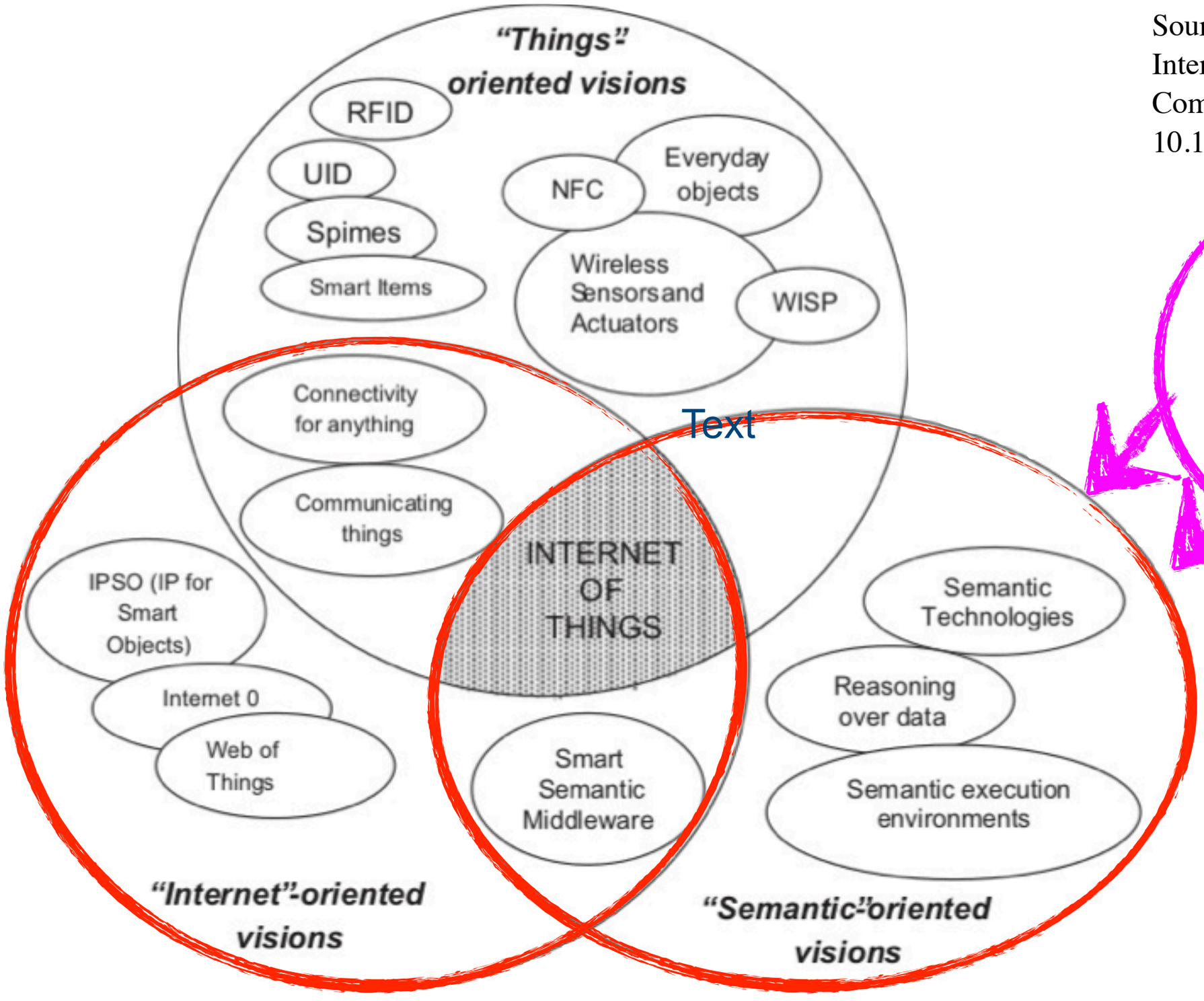
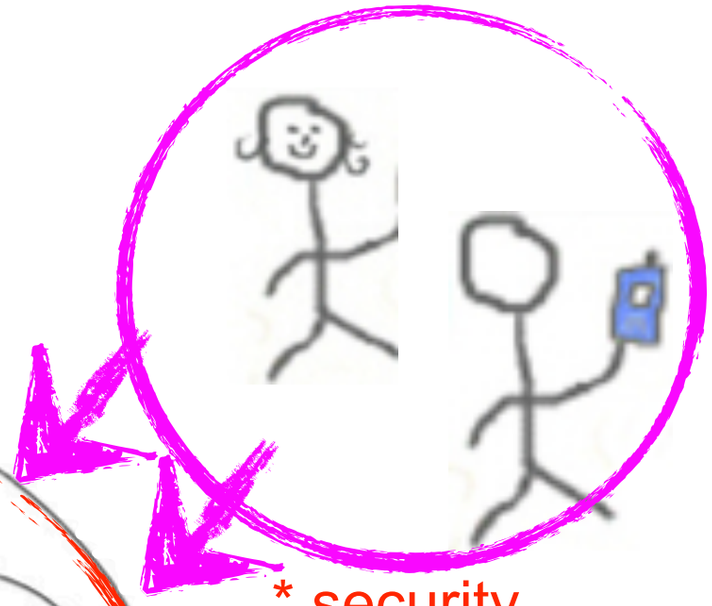


Fig. 1. "Internet of Things" paradigm as a result of the convergence of different visions.

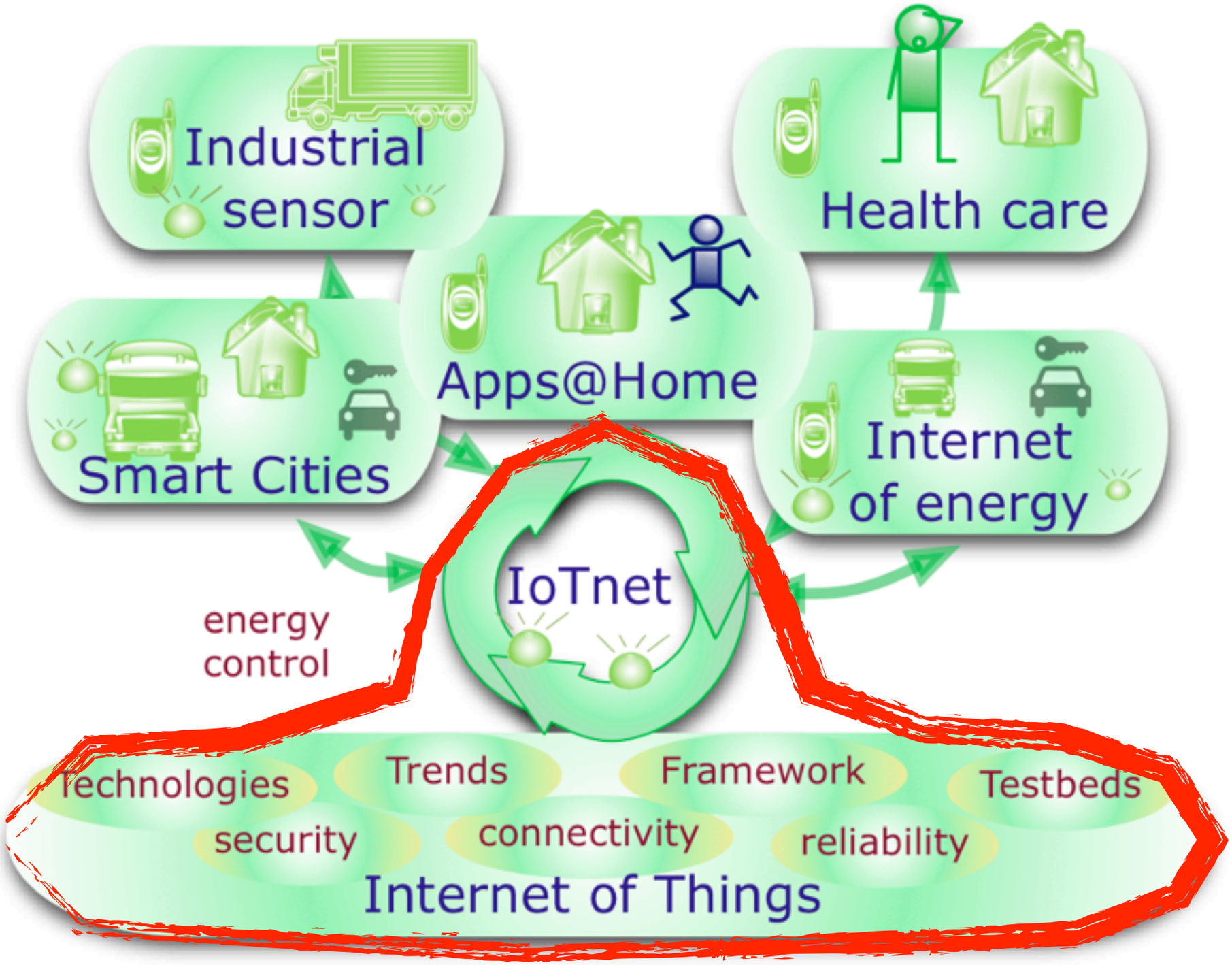
Source: L. Atzori et al., The Internet of Things: A survey, Comput. Netw. (2010), doi: 10.1016/ j.comnet.2010.05.010

Text



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

The IoT technology and application domain



Security challenges

- heterogeneous infrastructures
  - sensors, devices
  - networks, cloud
  - services, app stores
- BYOD - bring your own device

➡ you can't control

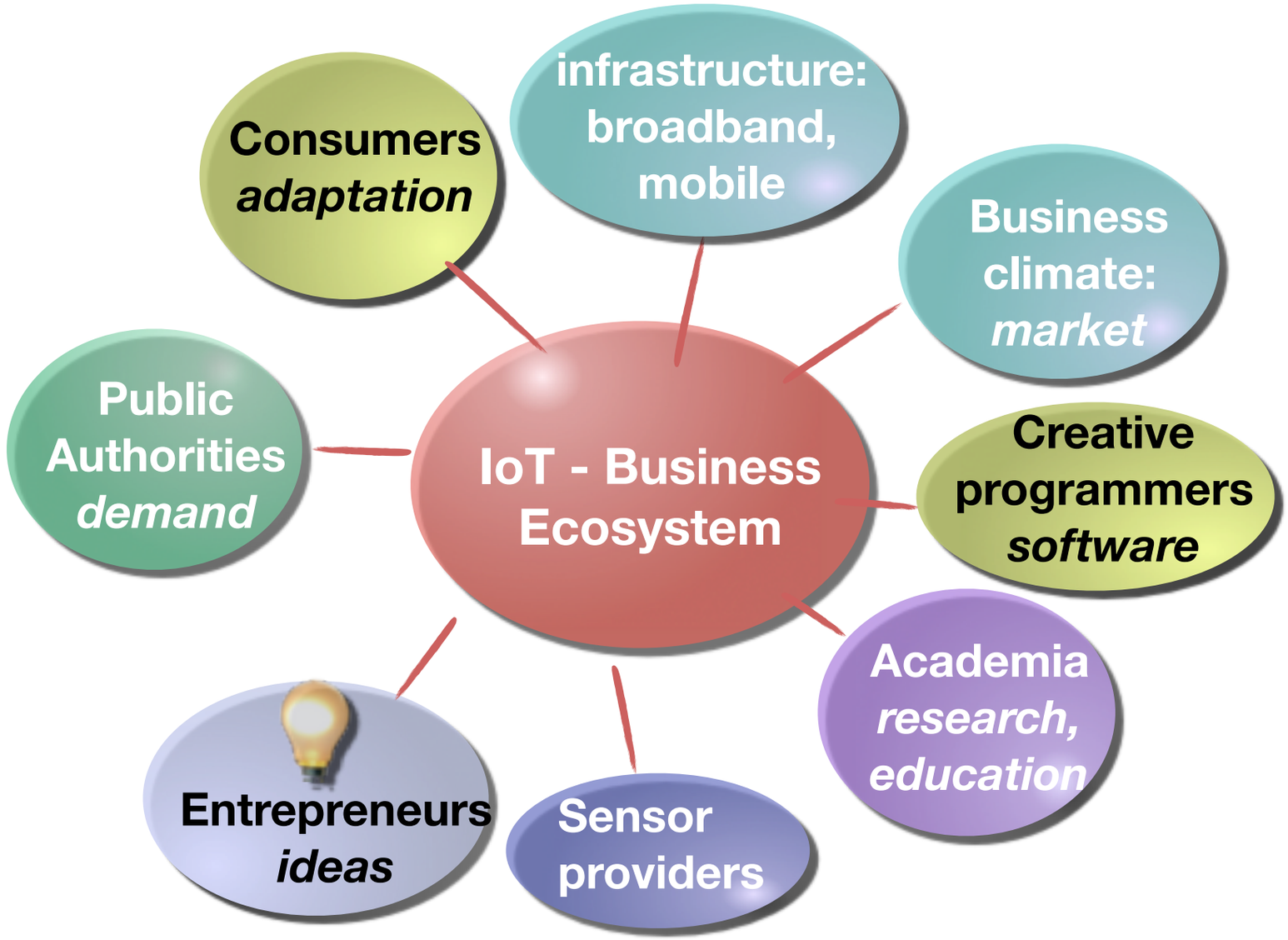
➡ concentrate on the core values

- Internet of People, Things and Service (IoPTS)
  - content aware
  - context aware
  - user centric: "Life Management Platform"

➡ Measure your values

IoT success, more than technology

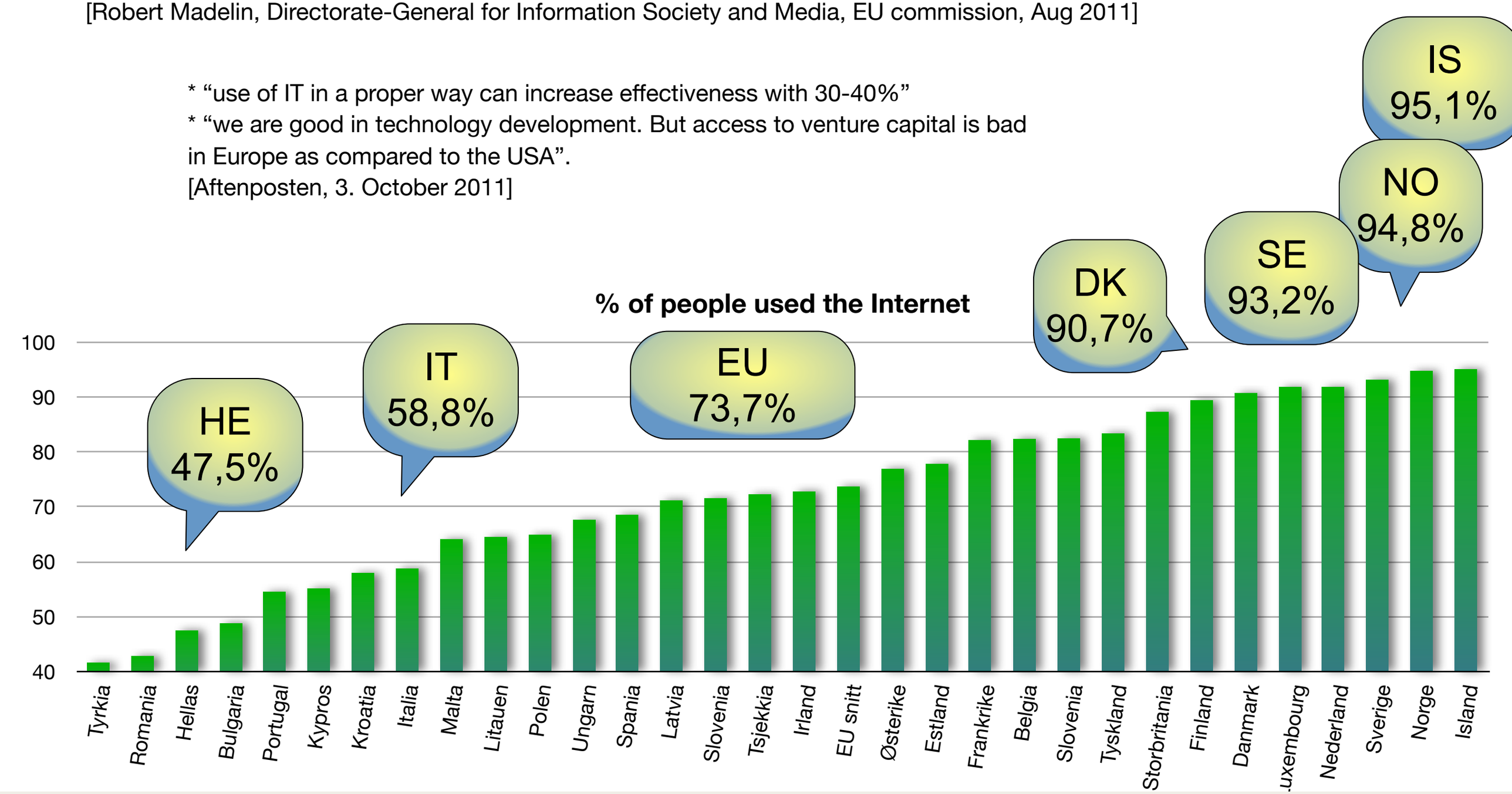
- Creating business
  - openness, competitive
  - climate for innovation
- Public authorities
  - trust, confidence
  - demand
- Consumers
  - (early) adapters
  - education
- Infrastructure
  - broadband, mobile
  - competition



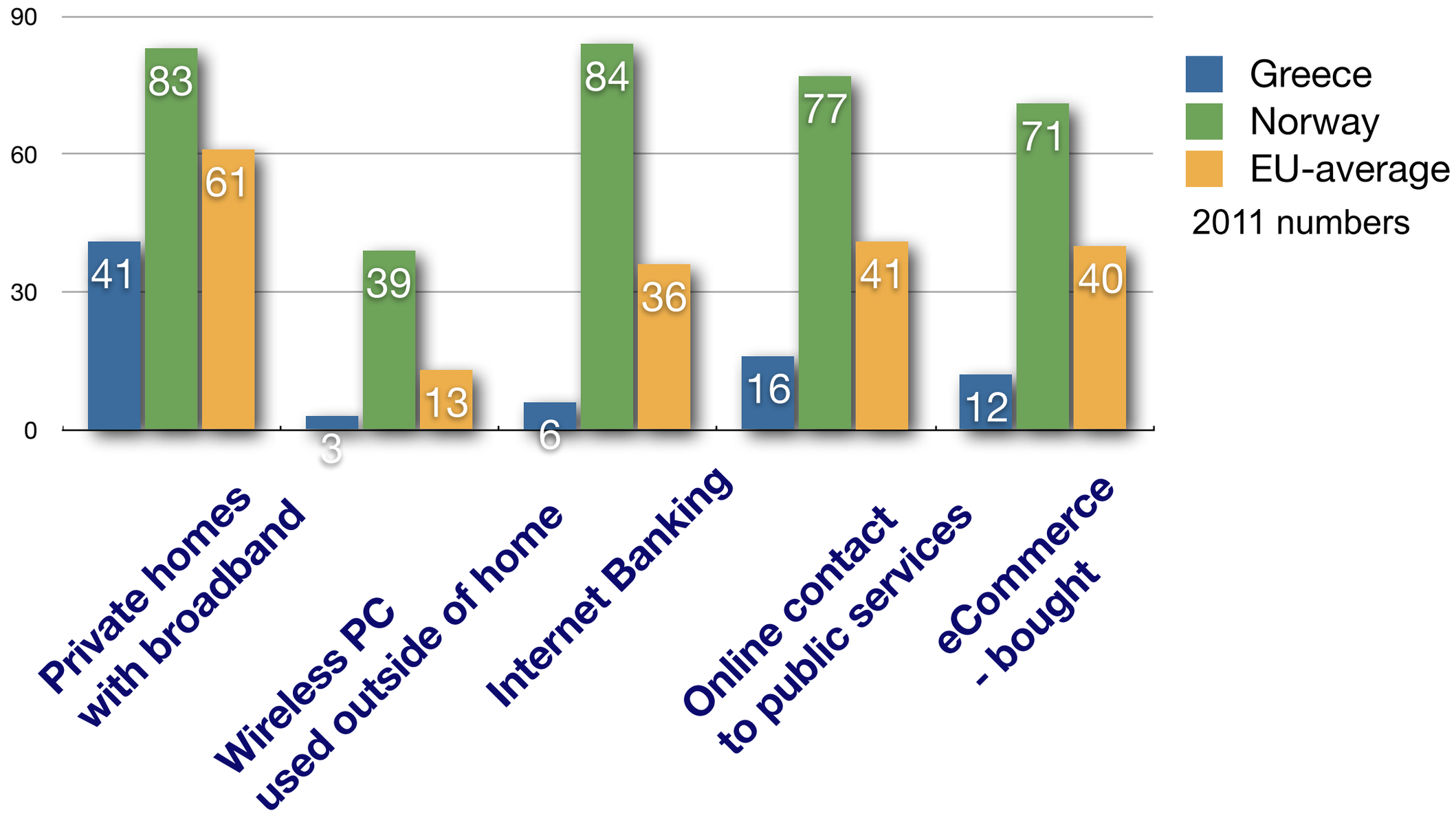
Internet usage in Scandinavia

[Robert Madelin, Directorate-General for Information Society and Media, EU commission, Aug 2011]

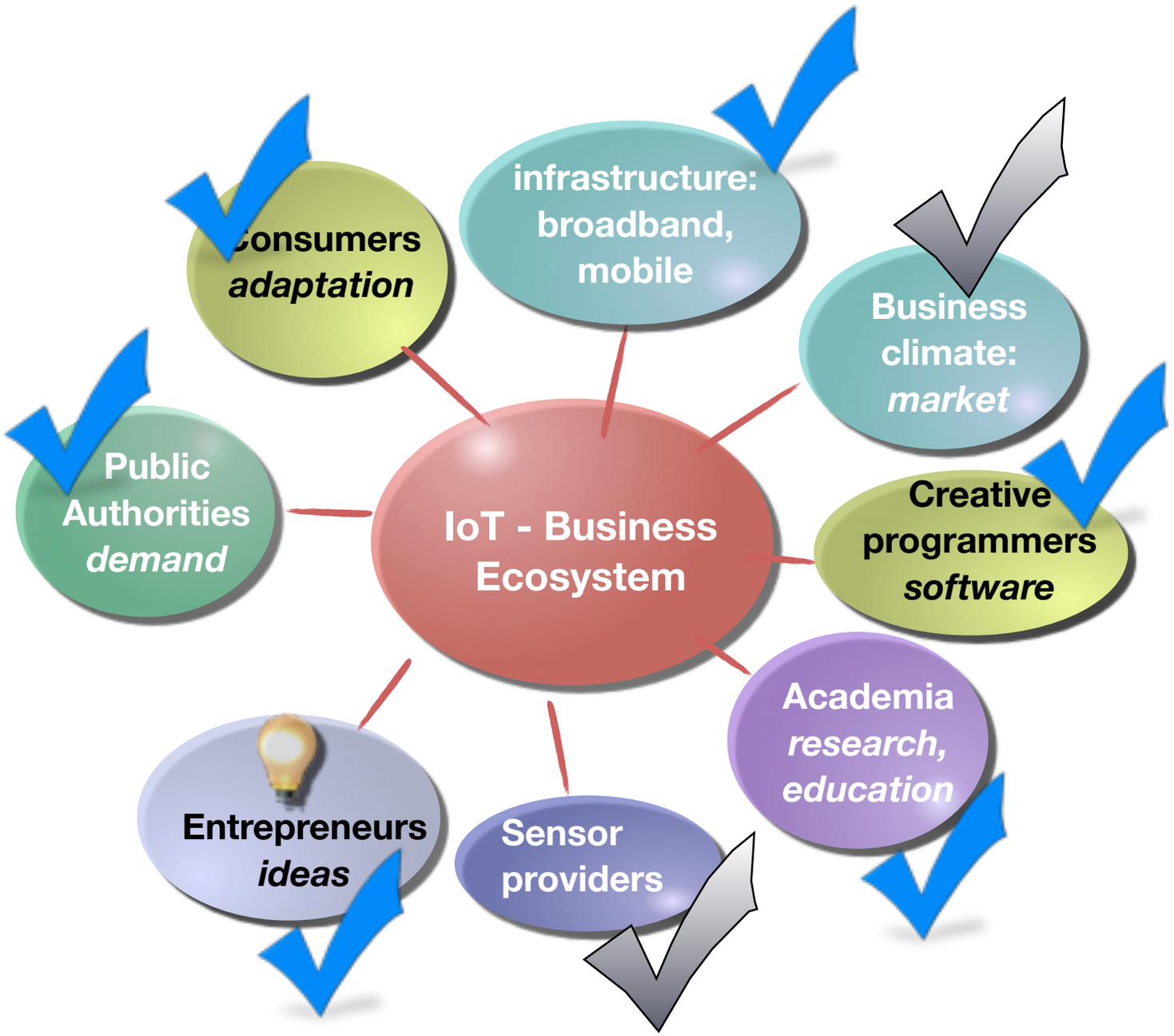
* “use of IT in a proper way can increase effectiveness with 30-40%”
* “we are good in technology development. But access to venture capital is bad in Europe as compared to the USA”.
[Aftenposten, 3. October 2011]



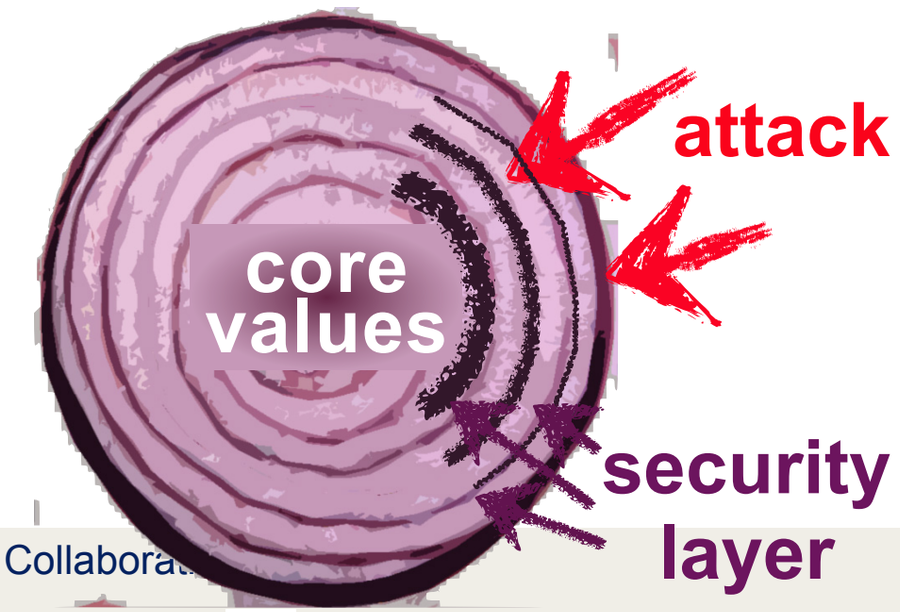
Internet service usage



Create a successful ecosystem

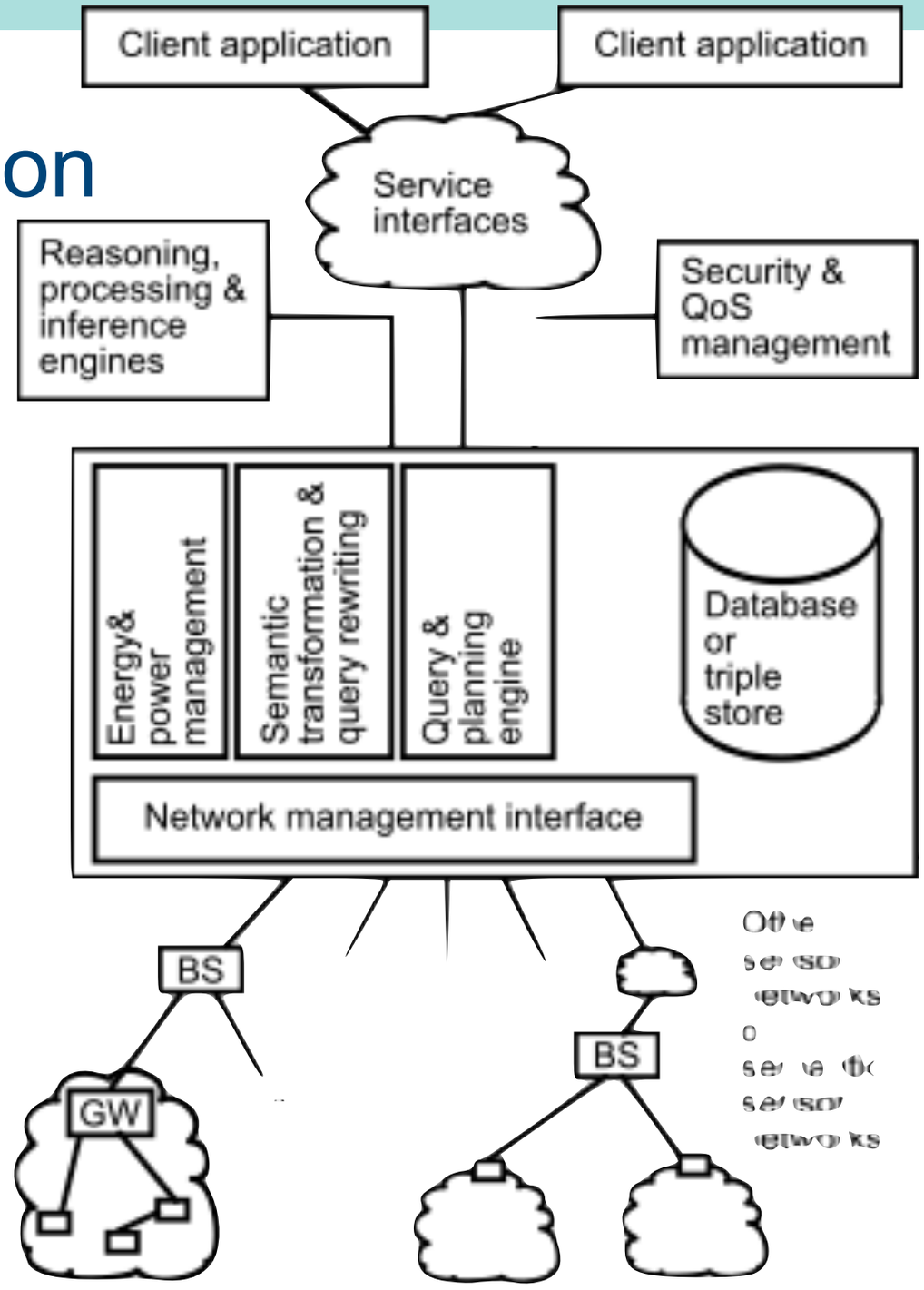


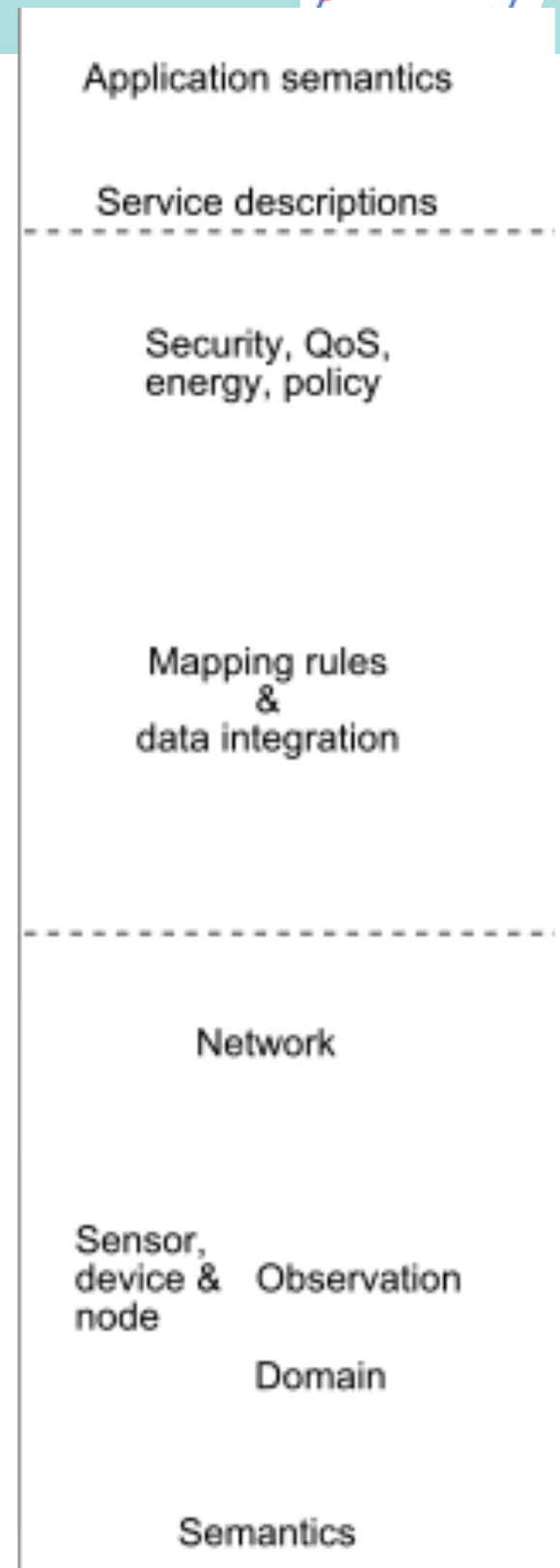
- Demand
  - mobile/wireless
  - autonomy
  - "me", context-/content-aware
- Adaptation
  - infrastructure
  - business environment
  - trust
- Security, privacy



Sensor Network Architecture

- Semantic dimension
  - Application
  - Services
  - Security, QoS,
  - Policies
  - mapping
- System
  - sensor networks
  - gateway
  - base station

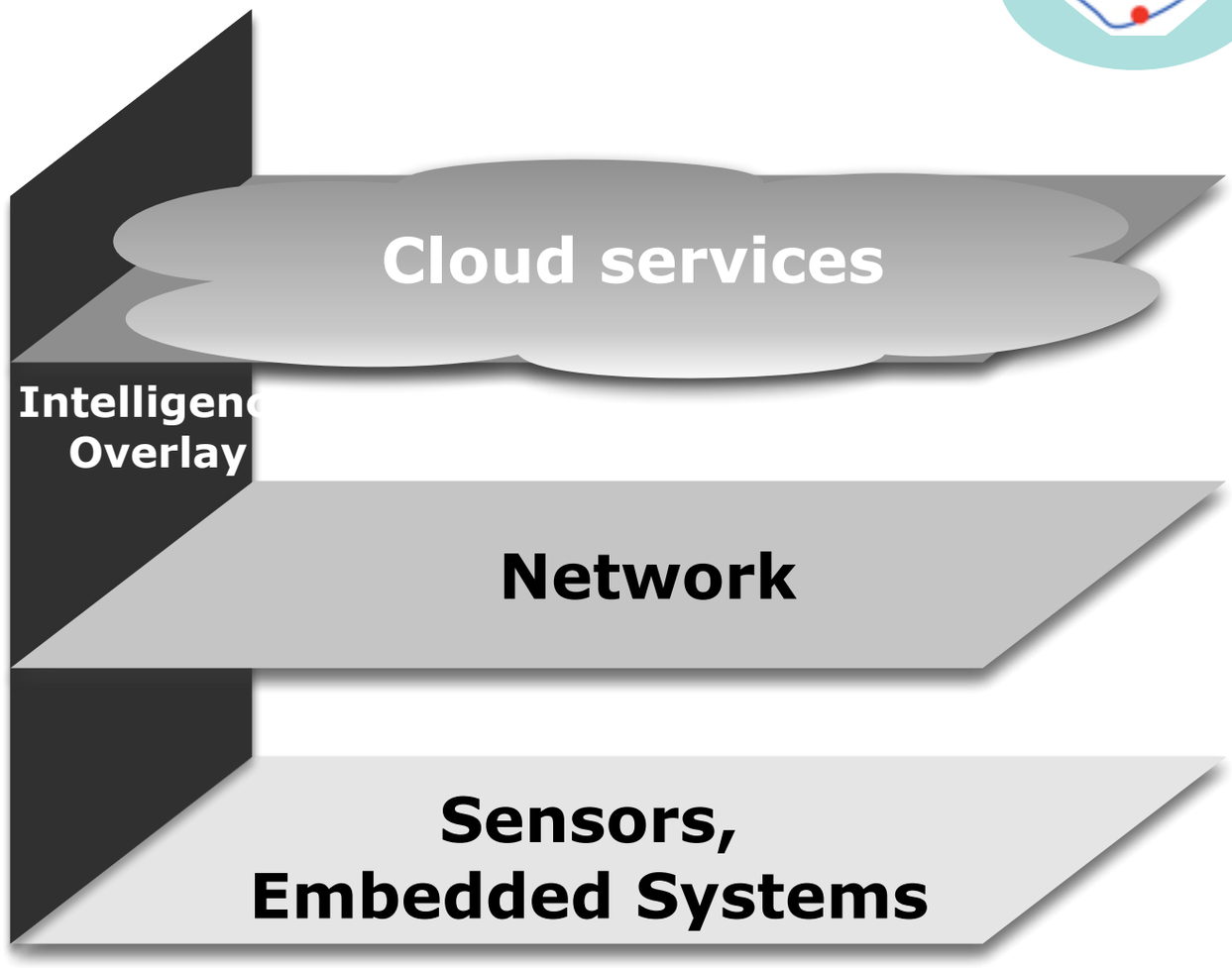


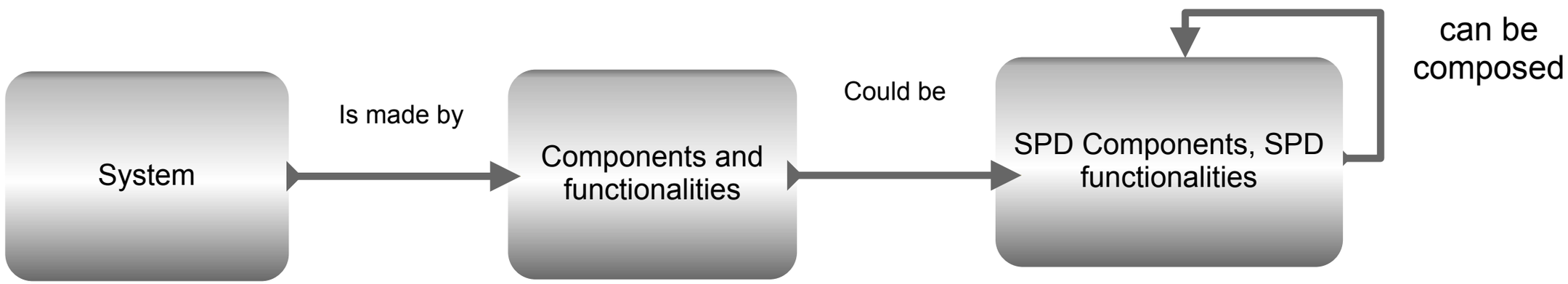


Source: Compton et al., A survey of semantic specification of sensors, 2009

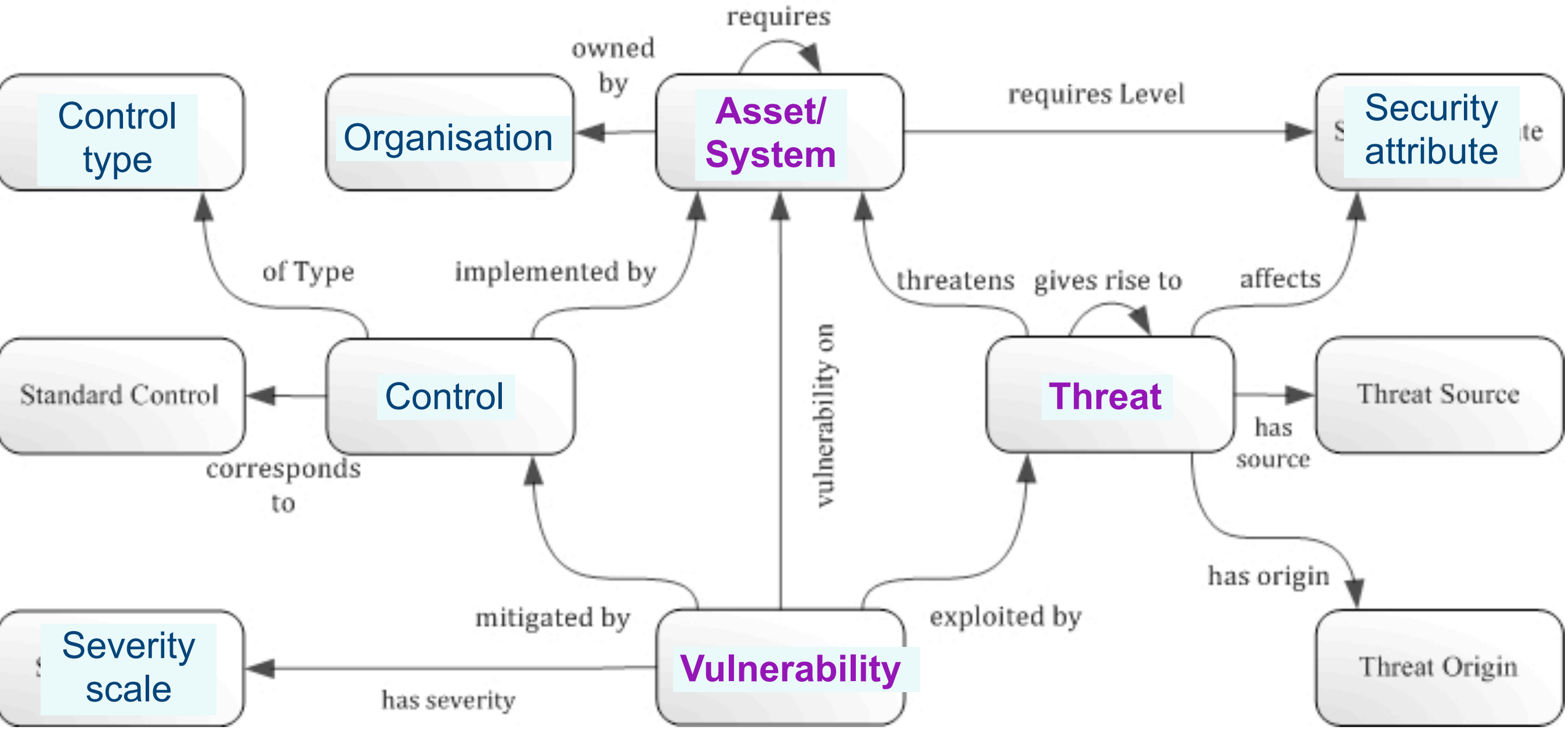
newSHIELD.eu approach

- Security, here
  - security (S)
  - privacy (P)
  - dependability (D)
- across the value chain
  - from sensors to services
- measurable security





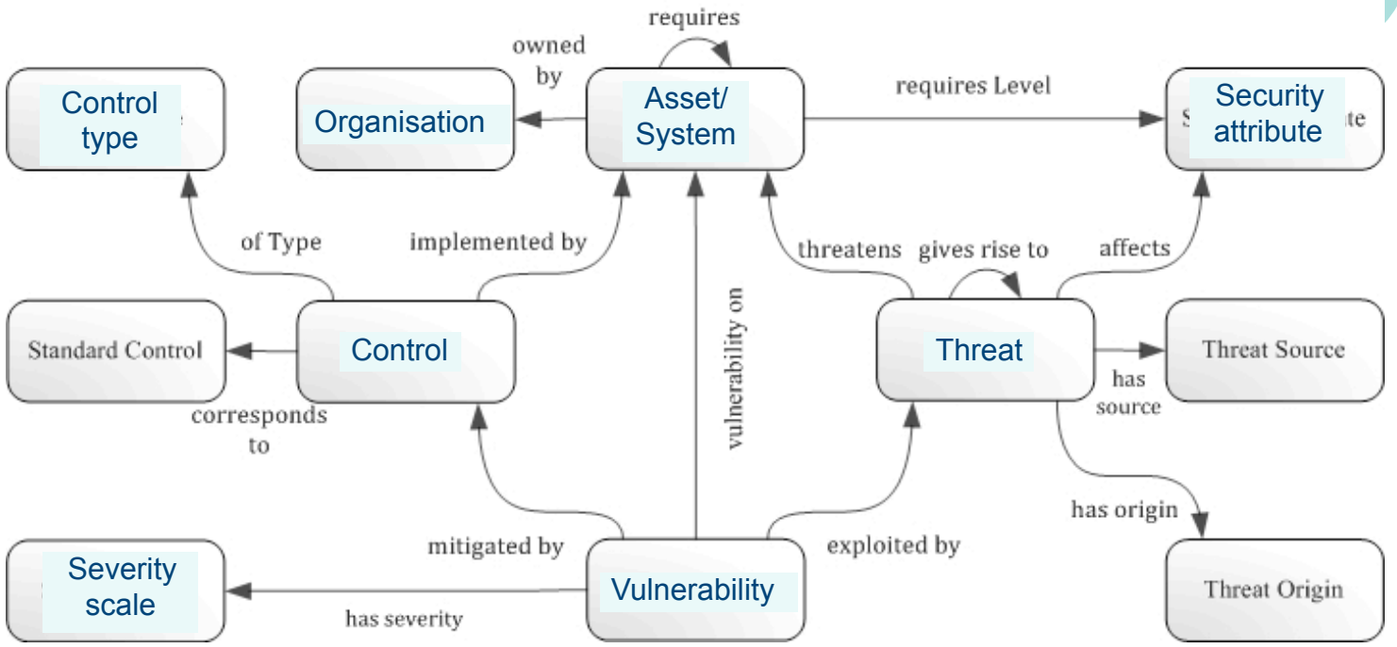
Traditional approach



[source: http://securityontology.sba-research.org/]

Limitations of the traditional approach

- Scalability
  - Threats
  - System
  - Vulnerability
- System of Systems
  - sensors
  - gateway
  - middleware
  - business processes



1 diagram per threat ⟷ *1 diagram per topic:*
-security
- system
- threats
...

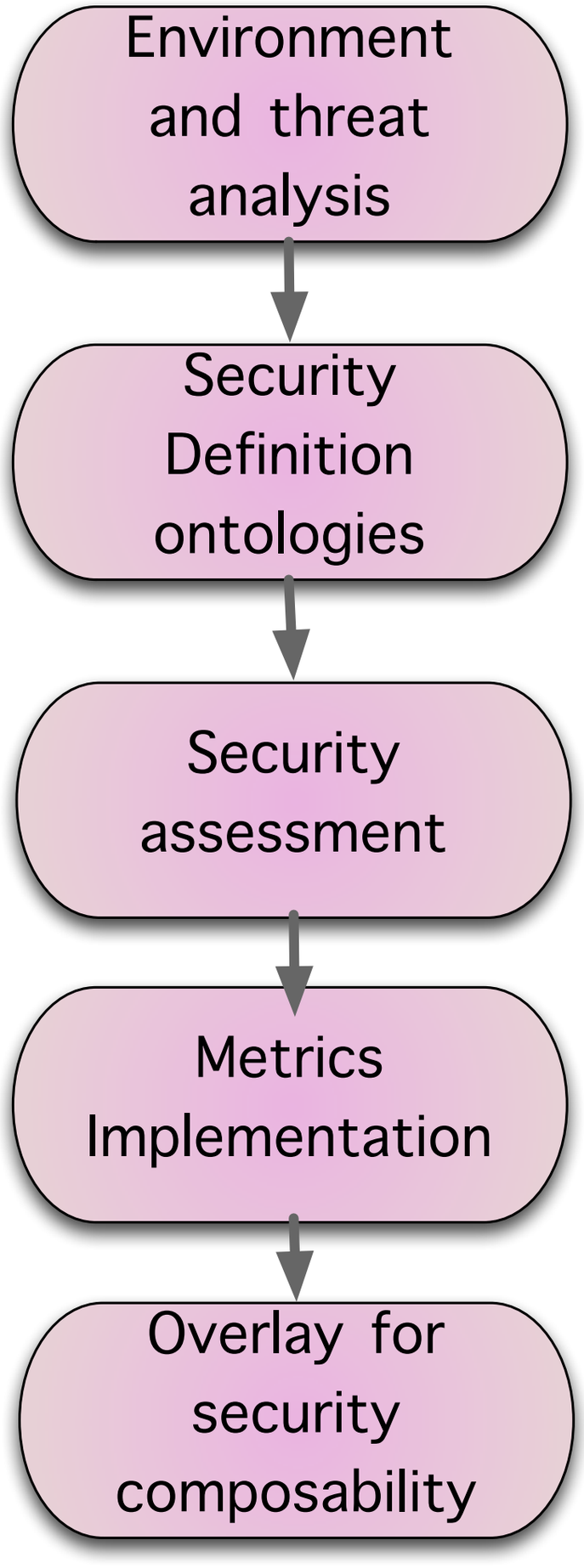
[source: http://securityontology.sba-research.org/]

The nSHIELD approach

- nSHIELD is an JU Artemis project
- focus on “measurable security” for embedded systems

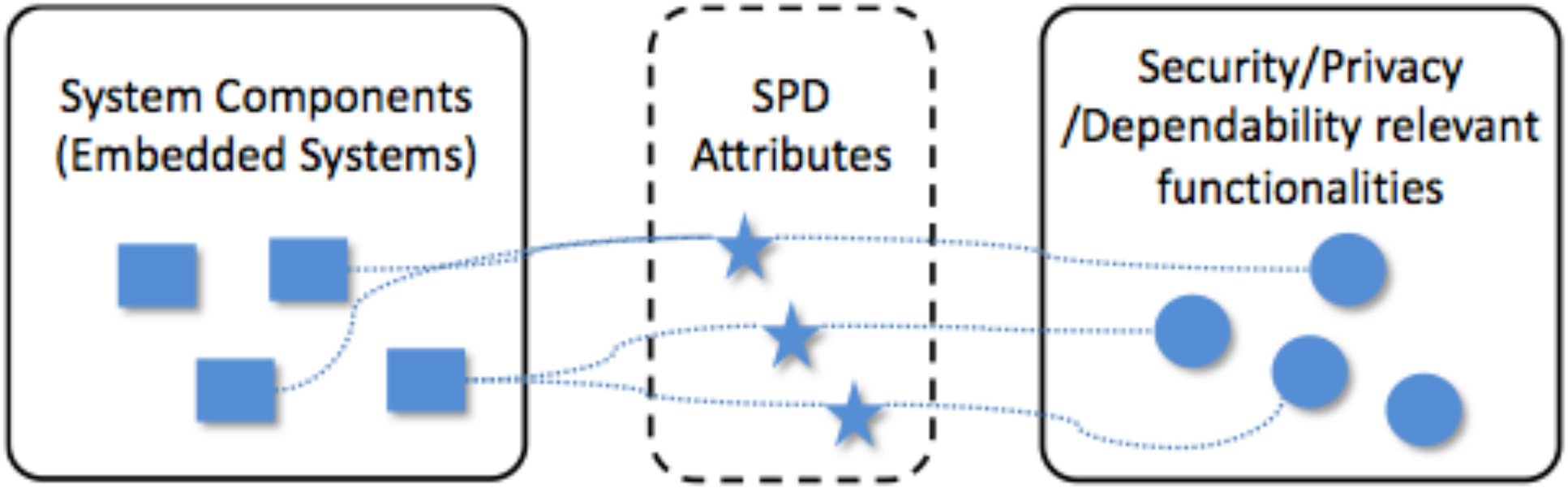
Core concept

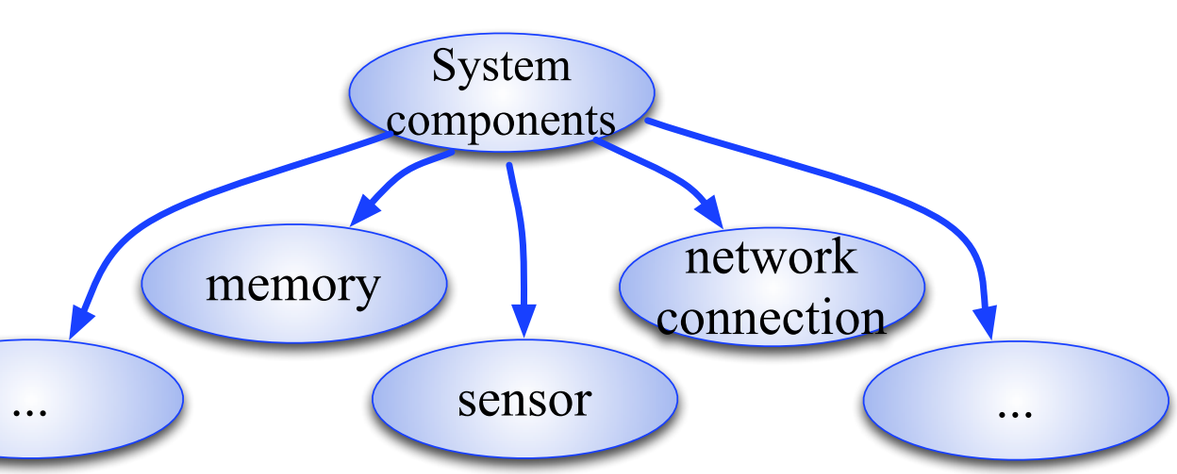
- Threat analysis
- Goal definition
- Semantic security description
- Semantic system description
- Security composability

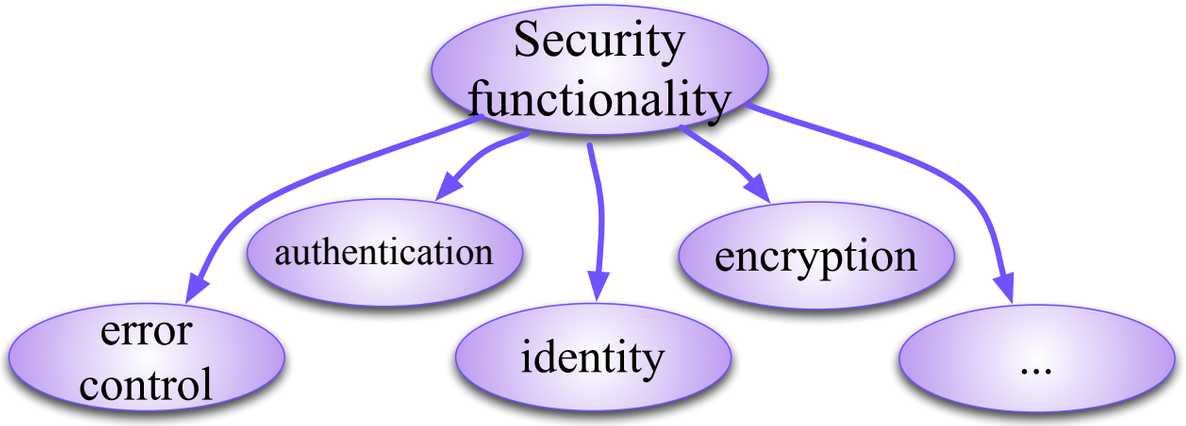


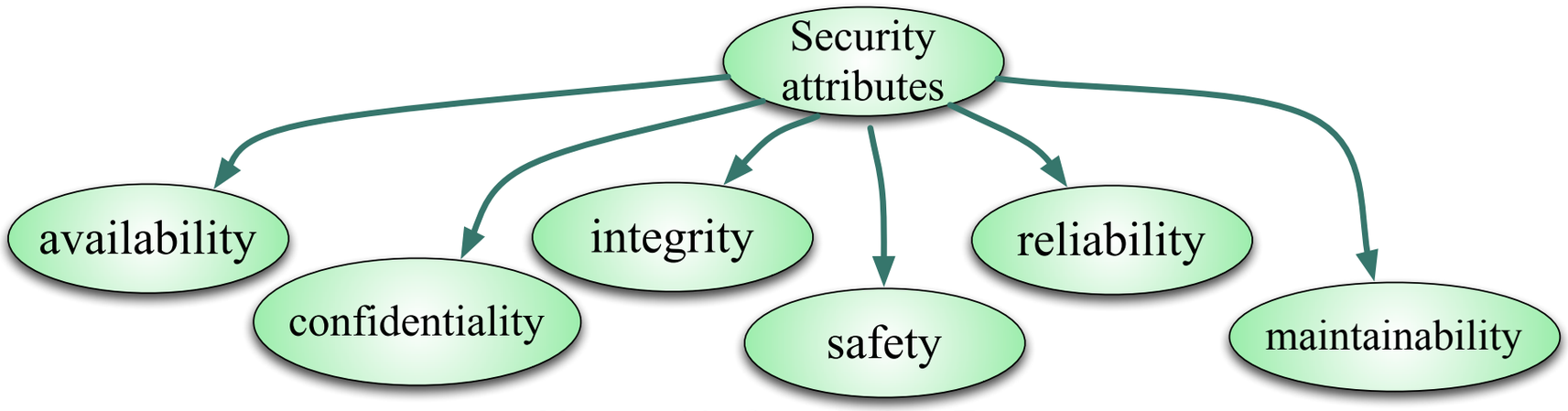
http://newSHIELD.eu

Security description









Goal description

- based on application specific goal, e.g. *high reliability*

- Specific parameters for each application?
  - availability = 0.8
  - confidentiality = 0.7
  - reliability = 0.5
  - ...

this way?

- more specific
- easier to understand(?)

- Common approach?
  - SPD = level 4

that way?

- universal approach
  - code “red”

Threat description through Metrics

Minimum attack potential value to exploit a vulnerability
= **SPD value**

where

Calculated attack potential

Factors to be considered

- Elapsed Time
- Expertise
- Knowledge of functionality
- Window of opportunity
- Equipment

with

Attack scenarios

SPD level → SPD attributes → SPD threats

Essential to build

Base of knowledge

System → Functionality → SPD system

SPD = security, privacy, dependability

Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3*(1)
Expert	6
Multiple experts	8
Knowledge of functionality	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
Unfeasible	25**(2)
Equipment	
Standard	0
Specialised	4(3)
Bespoke	7
Multiple bespoke	9

Discus…major topics

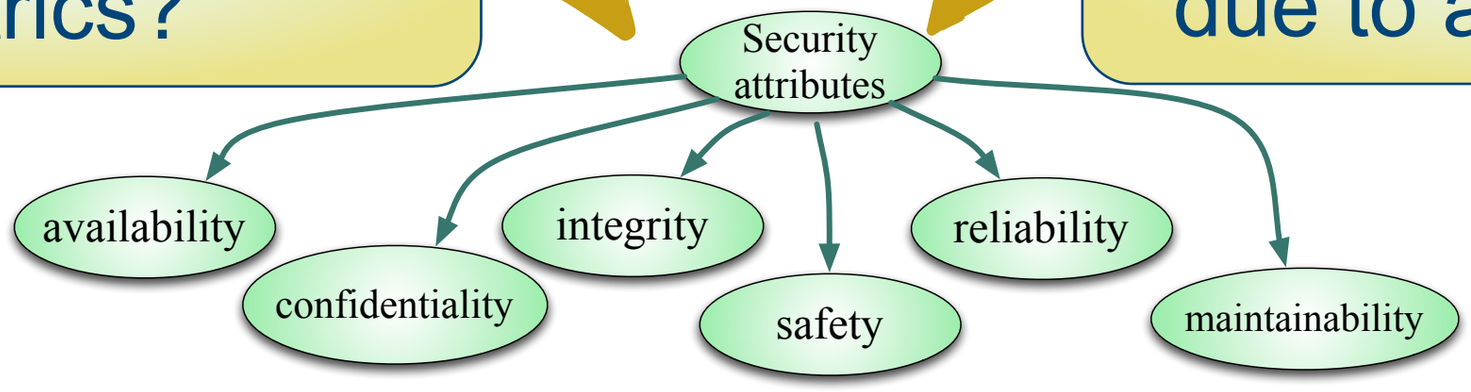
I need your help

specific application ontologies?

ontologies for security, systems, functionality

universal threat metrics?

selection of metrics due to application?



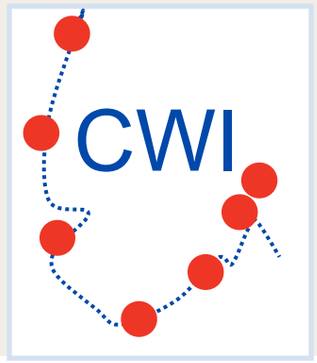
Sensor/Device System description?

Semantic Sensor Network (SSN) ontology

SensorML

SenML

My special thanks to



- JU Artemis and the Research Councils of the participating countries (IT, HE, PT, SL, **NO**, ES)
- Andrea Fiaschetti for the semantic middleware and ideas
- Inaki Eguia Elejabarrieta,Andrea Morgagni, Francesco Flammini, Renato Baldelli, Vincenzo Suraci for the Metrices
- Przemyslaw Osocha for running the pSHIELD project
- Cecilia Coveri (SelexElsag) for running the nSHIELD project
- Sarfraz Alam (UNIK) and Geir Harald Ingvaldsen (JBV) for the train demo
- Zahid Iqbal and Mushfiq Chowdhury for the semantics
- Hans Christian Haugli and Juan Carlos Lopez Calvet for the Shepherd ® interfaces
- and all those I have forgotten to mention

Høgskolen i Telemark NTNU UNIVERSITETET I AGDER UNIVERSITETET I OSLO HØGSKOLEN I BERGEN UNIK UNIVERSITETSSTUDIENE PÅ KJELLER Universitetet i Stavanger