Center for Wireless Innovation Norway
cwin.no

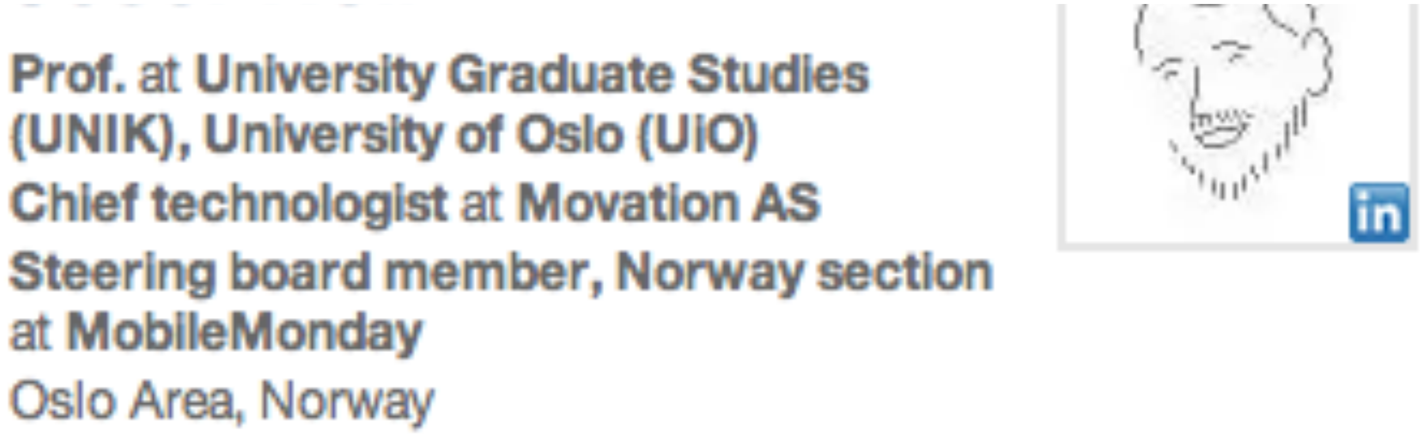
CWI
Norway

UNIK
UNIVERSITY GRADUATE CENTER

ISO 15926 and Semantic Technologies
Sogndal, 5.-6.Sep2013

Attribute based access to industrial life-cycle data, the semantic dimension

Josef Noll, Martin Follestad, Zahid Iqbal



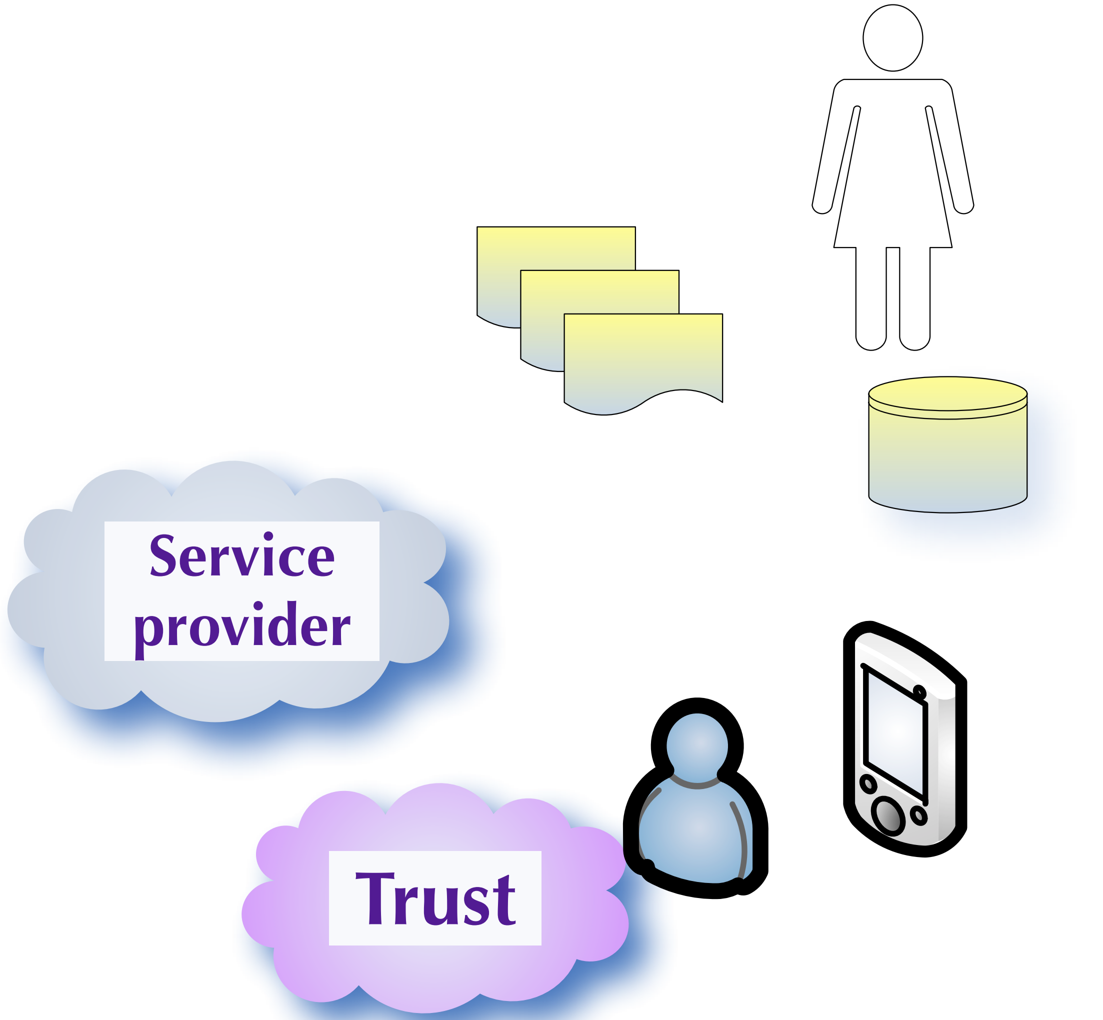
Prof. at University Graduate Studies (UNIK), University of Oslo (UiO)
Chief technologist at Movation AS
Steering board member, Norway section at MobileMonday
Oslo Area, Norway

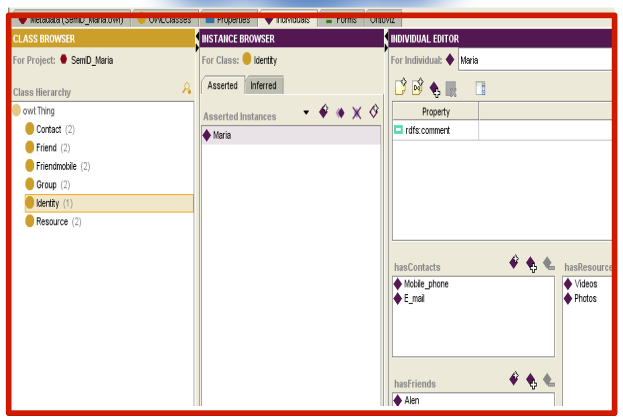
Outline

- Industrial Lifecycle
  - Planning, Execution, Extension
  - Information analysis & information flow control
- Security for industrial products
- Measurable security
  - Application in the IoT
  - Access, Authentication,... for People, Things And Services (IoPTS)
- Semantic Approach
  - Ontologies for security, system, component functionality
  - Metrics based assessment
  - Semantic attribute based access
- Attribute-based access
  - context-aware security - for people, things and services
- Experiences and Conclusions

Industrial Lifecycle

- Planning
  - based on “hidden knowledge”
- Execution
  - ongoing control of inventory
- Extension
  - Information analysis
  - Information flow control
- Semantic Approach
  - who has access?
  - Identity/Roles





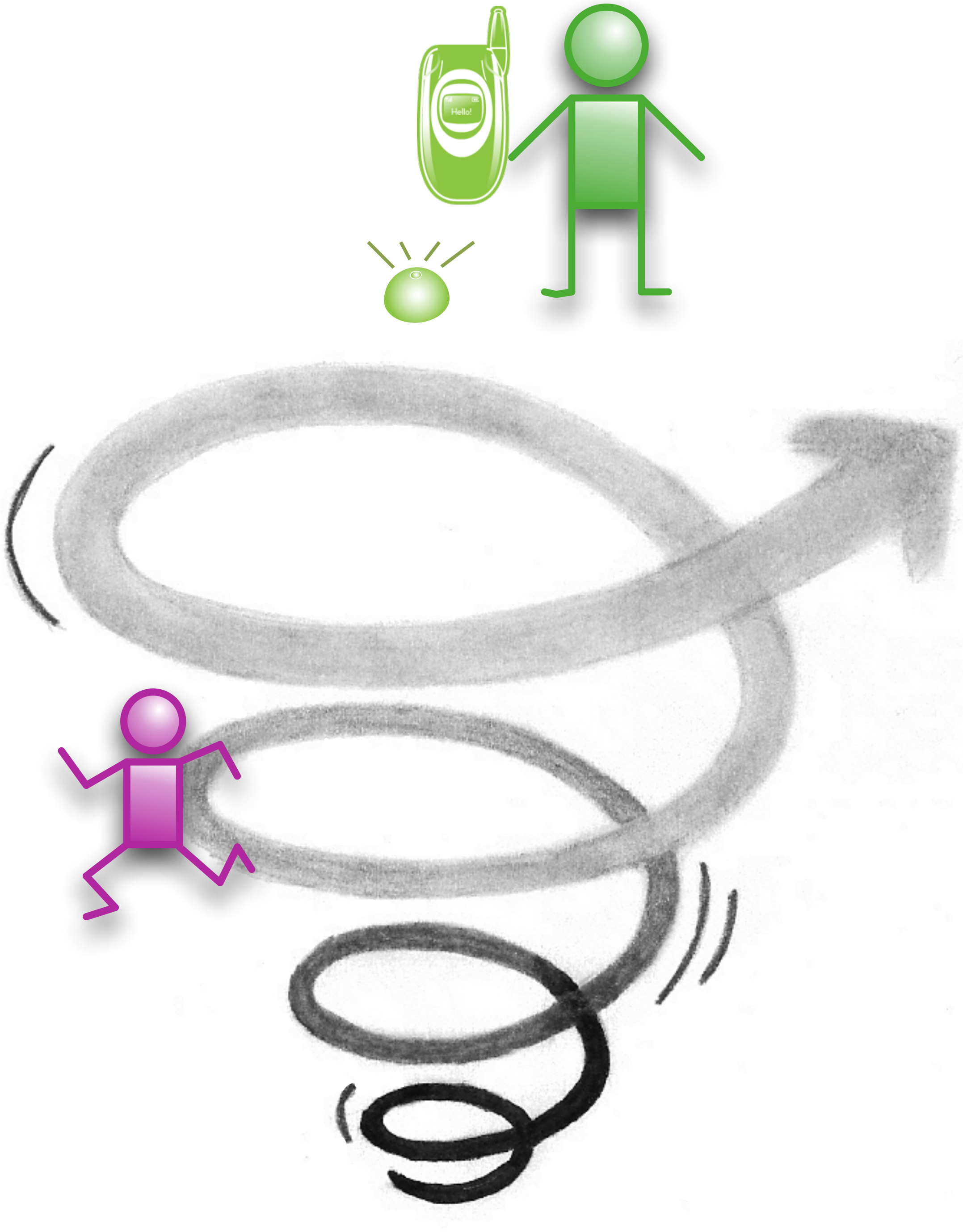
For Project: SemID_Maria

For Class: Identity

For Individual: Maria

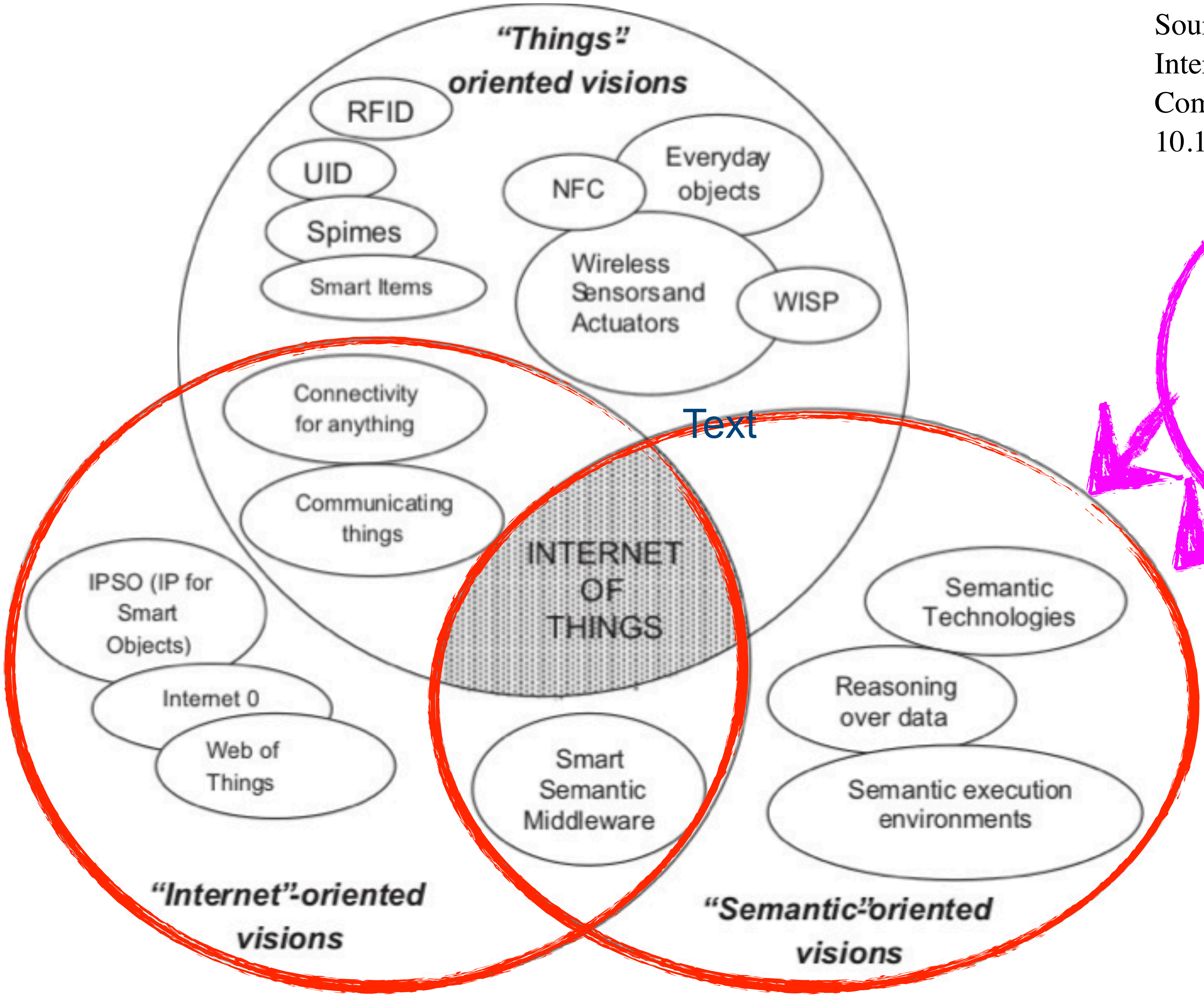
Security for industrial products

- Designed for an application in mind
  - security considerations?
- Novel application area
  - Used “somewhere else”
- New attack scenario
  - Increased customer demands
  - New regulations
- Retro-fit versus New Sensors
  - existing infrastructure
  - “remote operation”



[source: Living on purpose, telus.net]

The Semantic Dimension of
the Internet of Things (IoT)



"Things"-oriented visions
RFID
UID
Spimes
Smart Items
NFC
Everyday objects
Wireless Sensors and Actuators
WISP
Connectivity for anything
Communicating things
INTERNET OF THINGS
Text
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

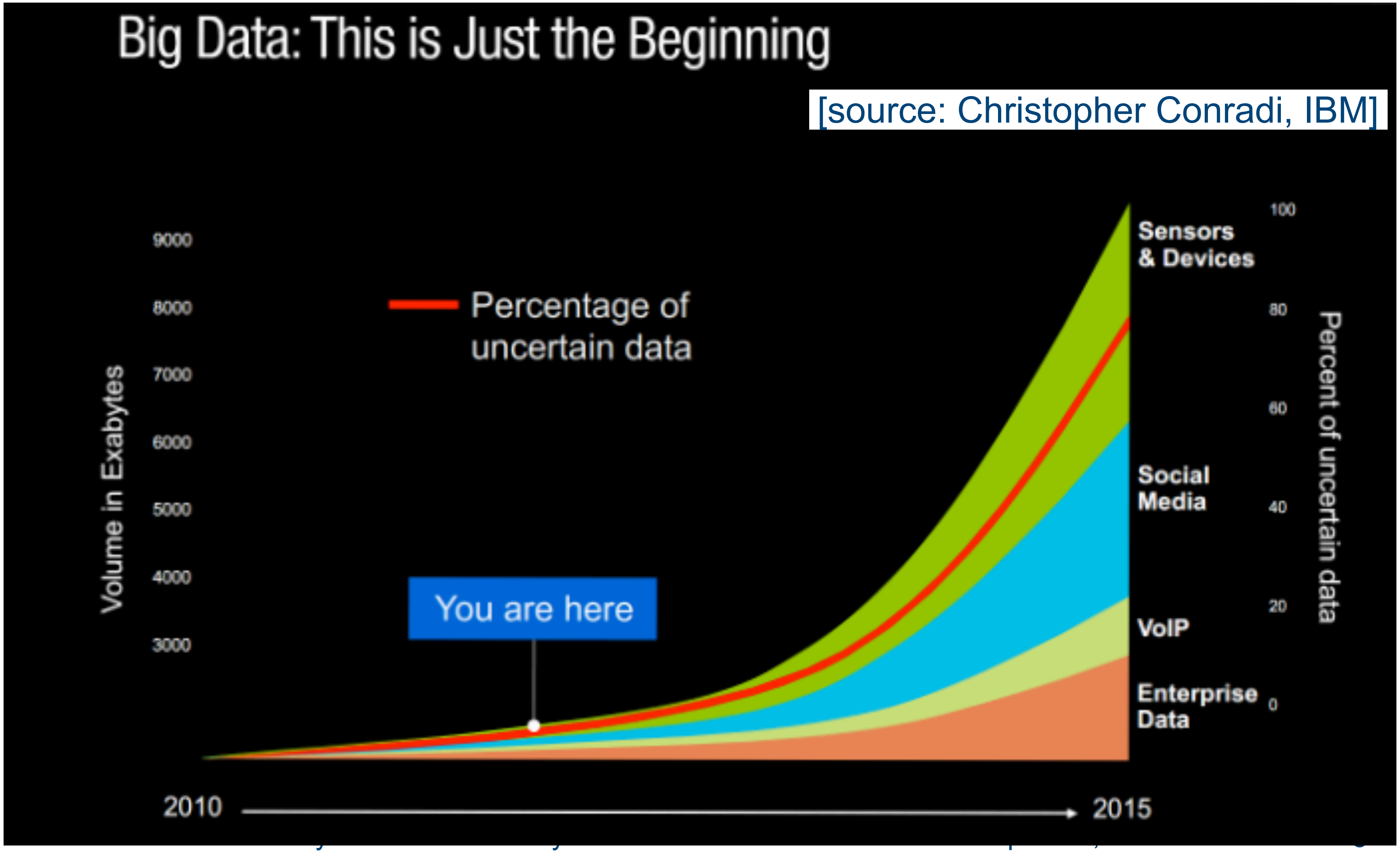
Fig. 1. "Internet of Things" paradigm as a result of the convergence of different visions.

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
  - content
* personalised

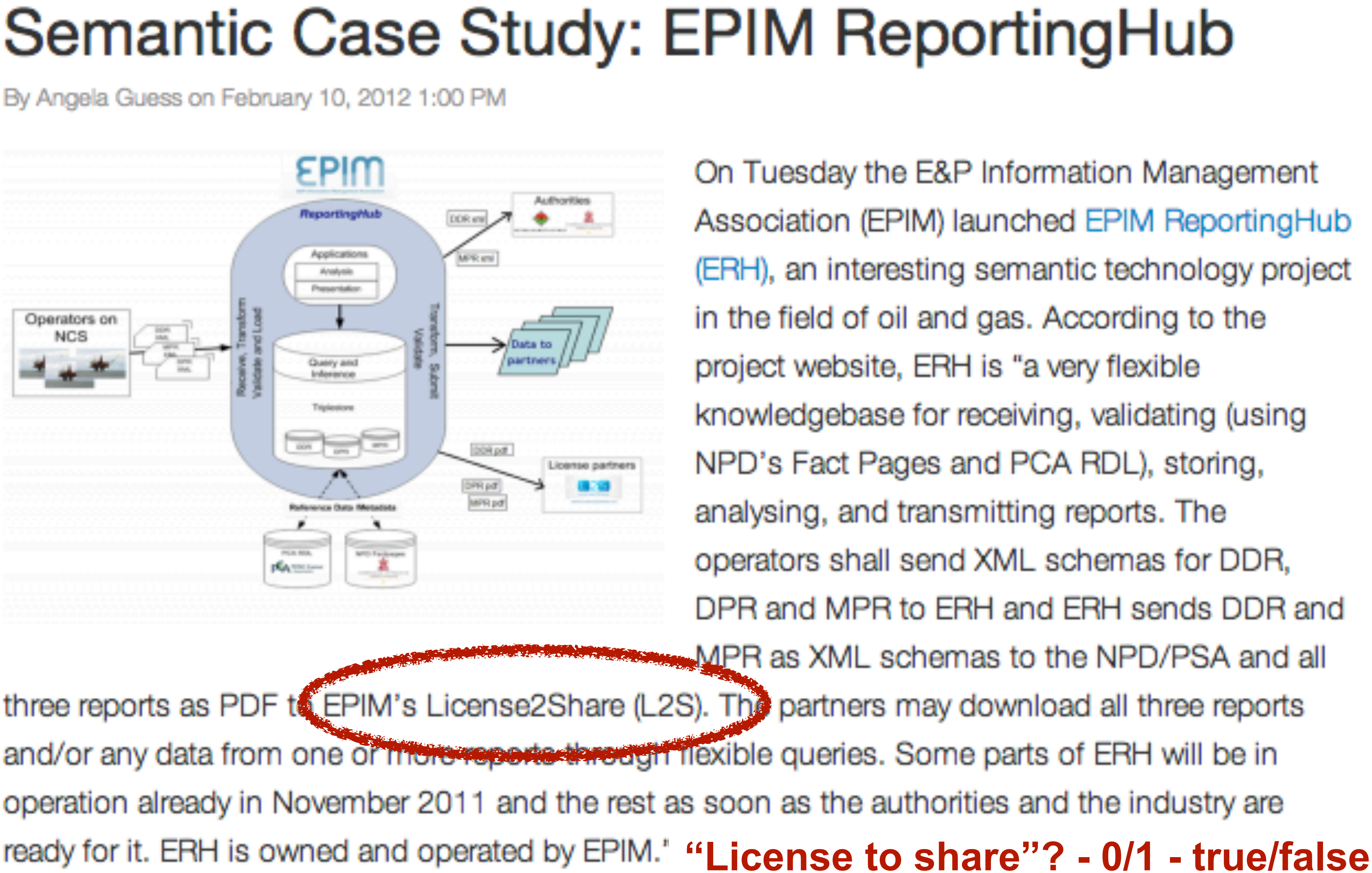
Information “truth”

- Measurable Security
- Retro-fit versus Cognitive Computing
- Information handling



[source: Christopher Conradi, IBM]

IoT application in Oil and Gas



Semantic Case Study: EPIM ReportingHub

By Angela Guess on February 10, 2012 1:00 PM

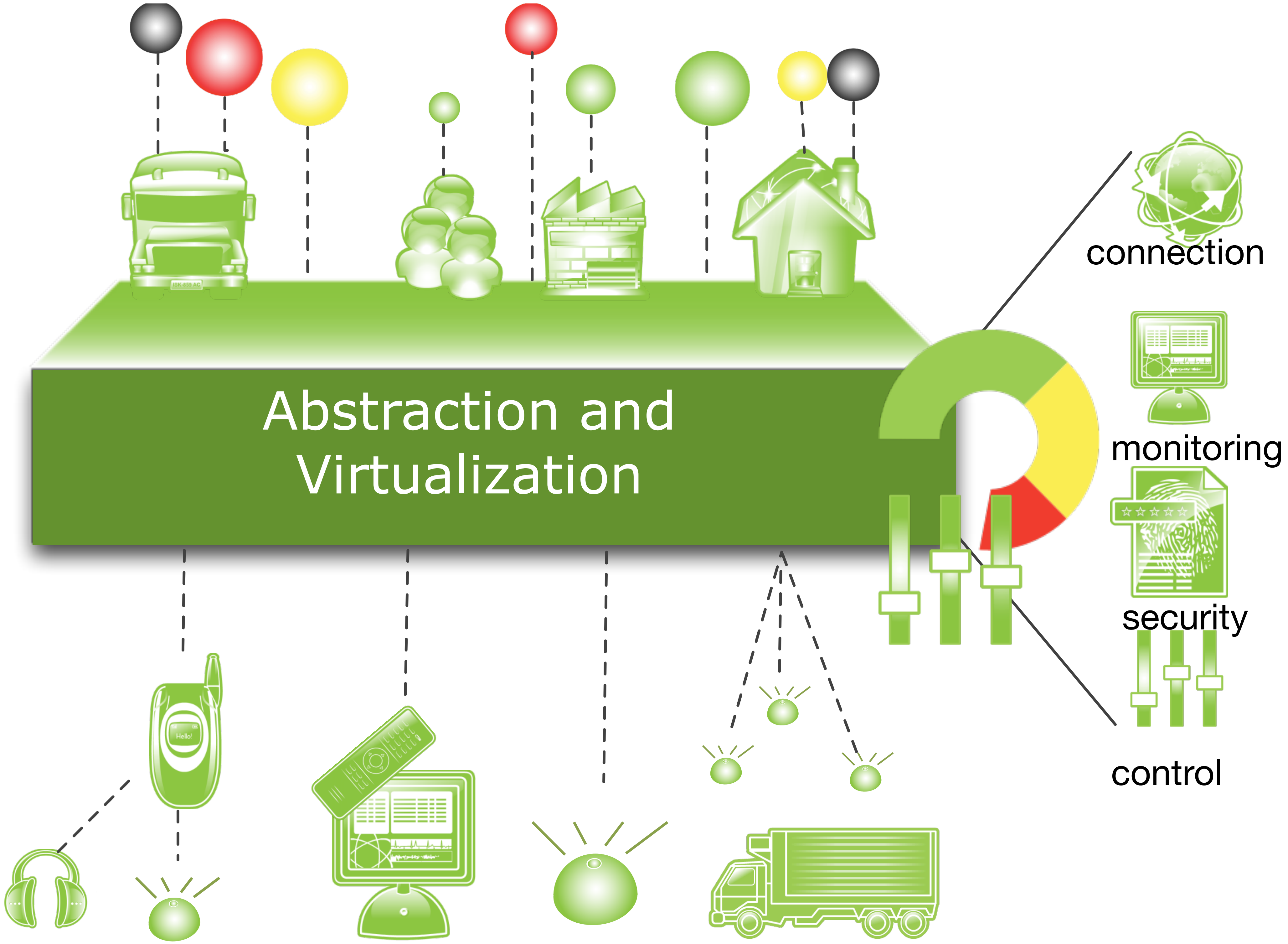
On Tuesday the E&P Information Management Association (EPIM) launched EPIM ReportingHub (ERH), an interesting semantic technology project in the field of oil and gas. According to the project website, ERH is "a very flexible knowledgebase for receiving, validating (using NPD's Fact Pages and PCA RDL), storing, analysing, and transmitting reports. The operators shall send XML schemas for DDR, DPR and MPR to ERH and ERH sends DDR and MPR as XML schemas to the NPD/PSA and all three reports as PDF to EPIM's License2Share (L2S). The partners may download all three reports and/or any data from one or more reports through flexible queries. Some parts of ERH will be in operation already in November 2011 and the rest as soon as the authorities and the industry are ready for it. ERH is owned and operated by EPIM."

"License to share"? - 0/1 - true/false

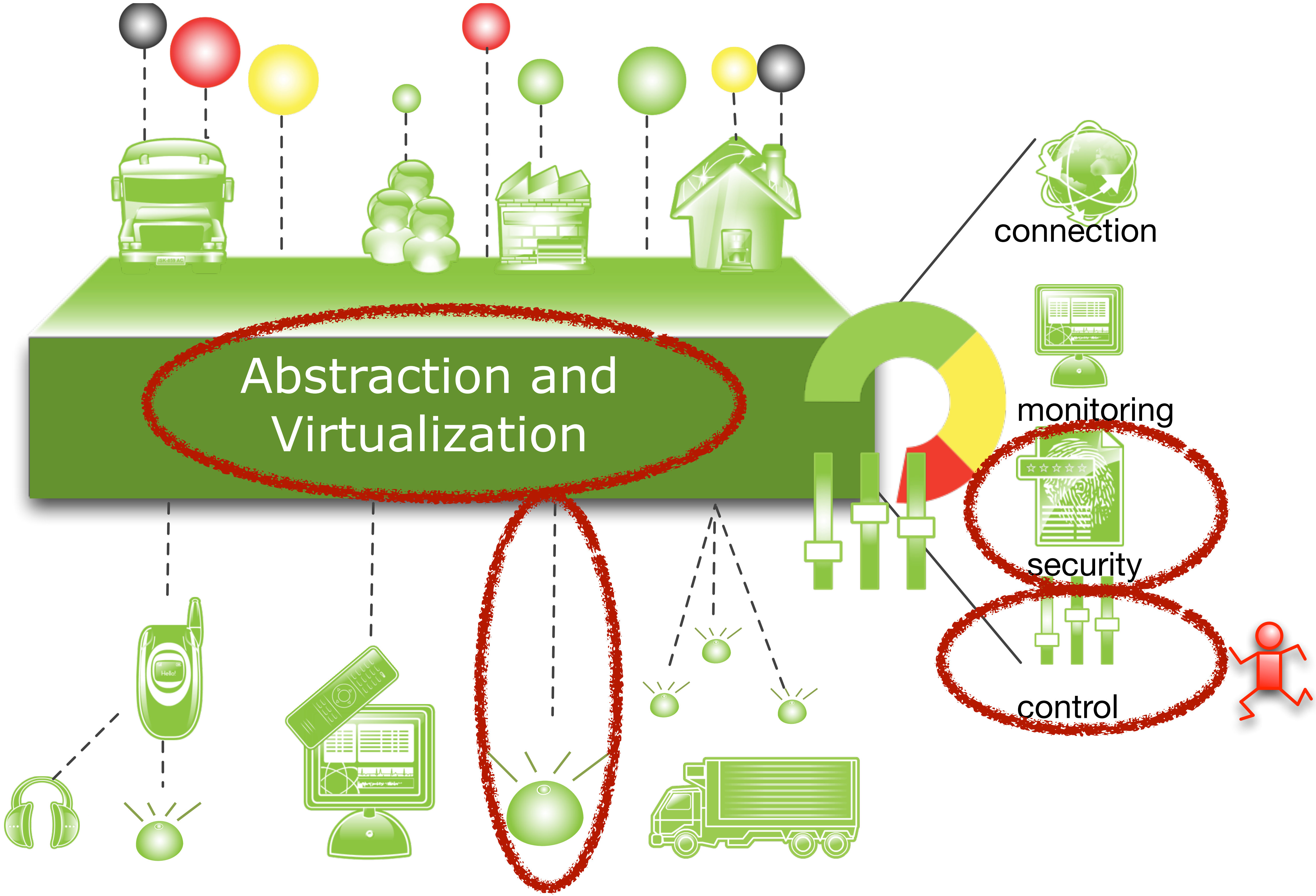
Measurable Security

- Insecure <-> Secure
  - IETF better-than-nothing-security (btns)
- Information distribution along 0/1 (false/true)?
  - “someone has stolen my identity” -> access granted
  - behaviour monitoring
  - change in partners/companies/hierarchies
- Data integration and weighting
  - integration of heterogeneous data: seismic, drilling, transportation
  - used across **systems**, disciplines, and organisations
- Automated processes
  - who contributes
  - **value** and **impact** of contribution
  - reasoning

Security areas in IoPTS



Security areas in IoPTS



Security challenges

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

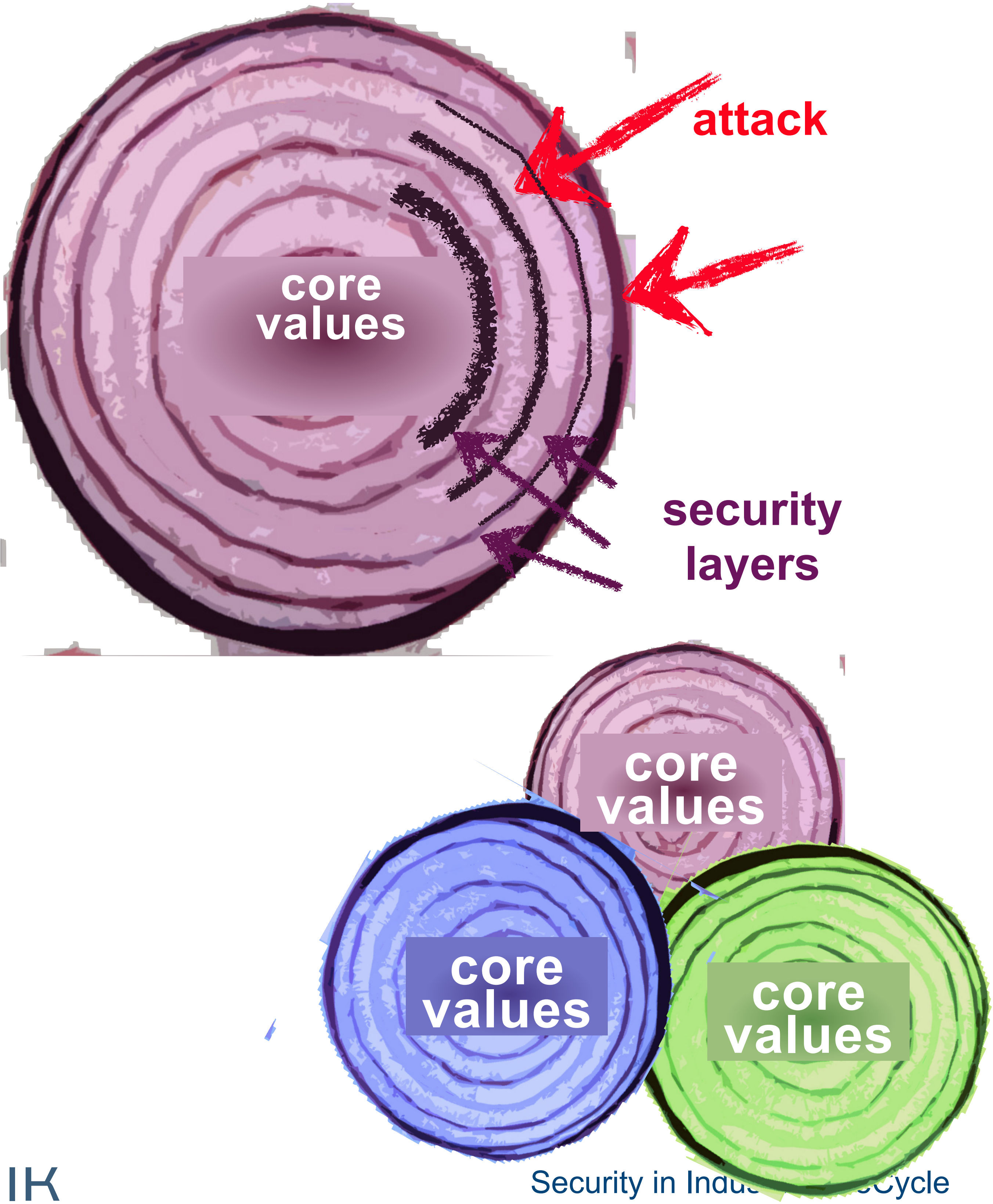
➡ you can't control

➡ concentrate on the core values

- Internet of People, Things and Service (IoPTS)
  - content aware: value to alarm
  - context aware: who has access - "we are not all friends"
  - attributes for security assessment

➡ Measure your values

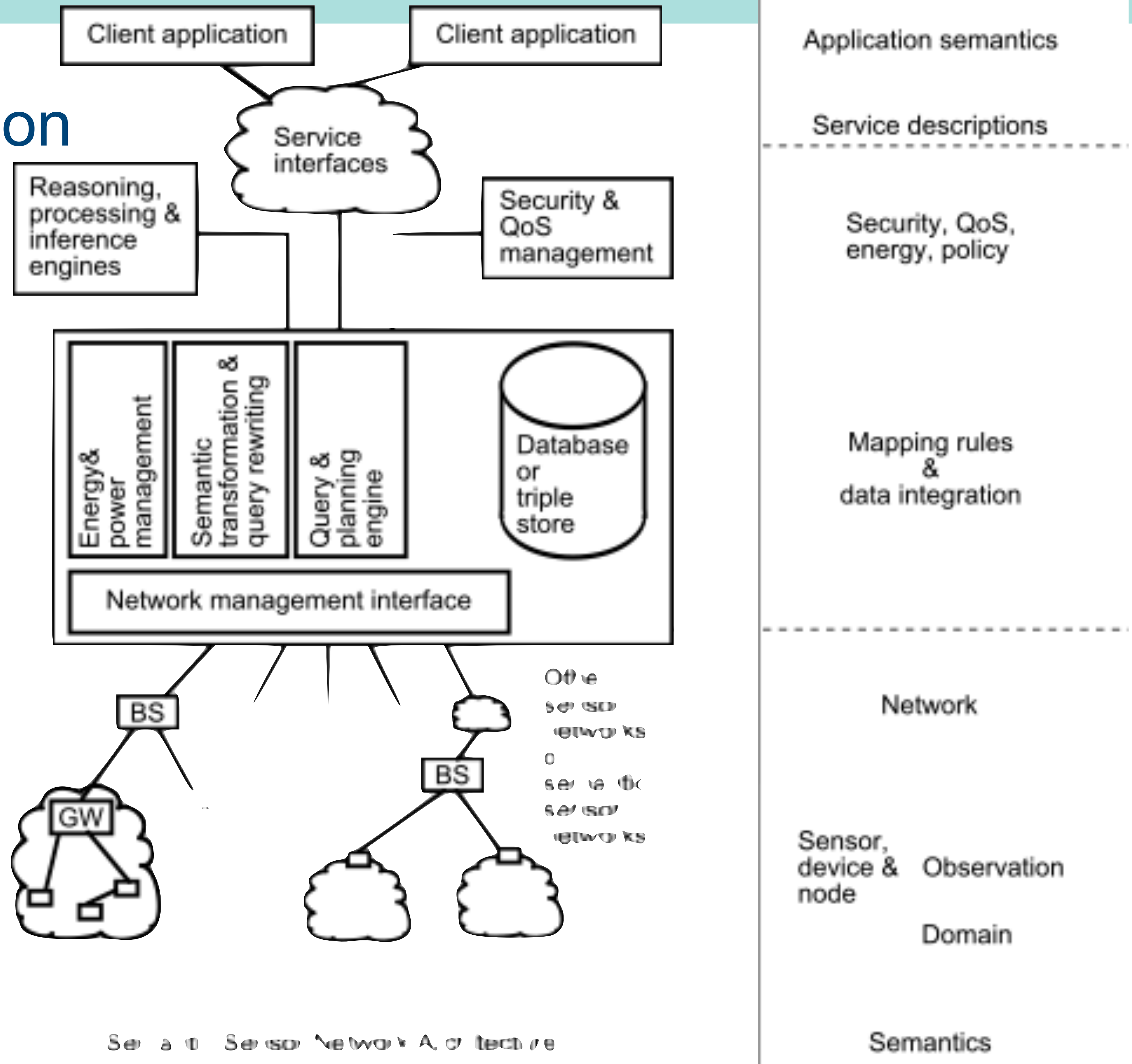
Attribute-based protection



- Demand
  - autonomy
  - context-/content-aware
- Adaptation
  - business environment
  - trust relation(?)
- Security, privacy
  - protect your core values
  - attribute-based access
  - monitor attack

Sensor Network Architecture

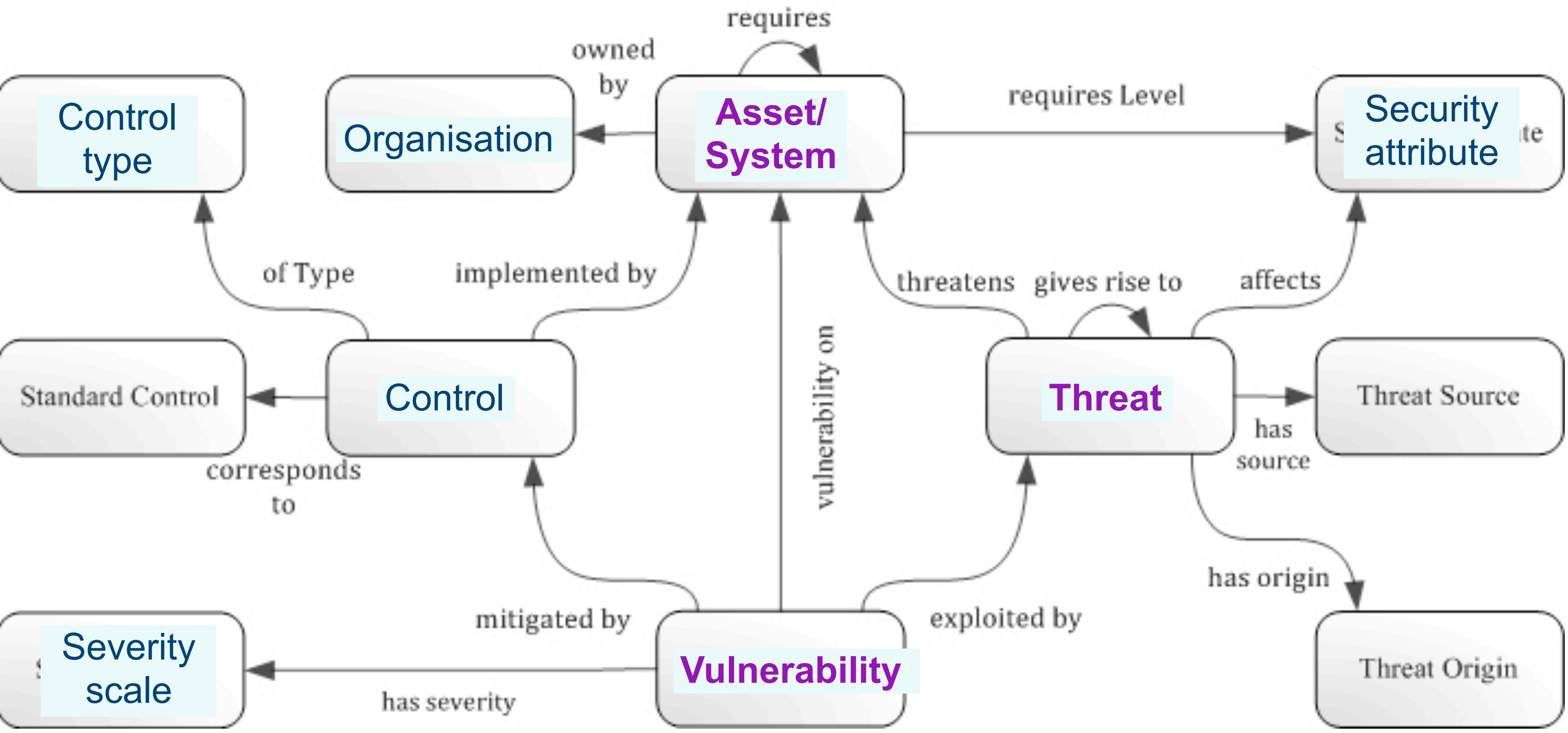
- Semantic dimension
  - Application
  - Services
  - Security, QoS,
  - Policies
  - mapping
- System
  - sensor networks
  - gateway
  - base station


Client application
Client application
Service interfaces
Reasoning, processing & inference engines
Security & QoS management
Energy& power management
Semantic transformation & query rewriting
Query & planning engine
Database or triple store
Network management interface
BS
BS
GW
Other sensor networks or semantic sensor networks
Application semantics
Service descriptions
Security, QoS, energy, policy
Mapping rules & data integration
Network
Sensor, device & node
Observation
Domain
Semantics

Semantic Sensor Network Architecture

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

Security assessment:
Traditional approach



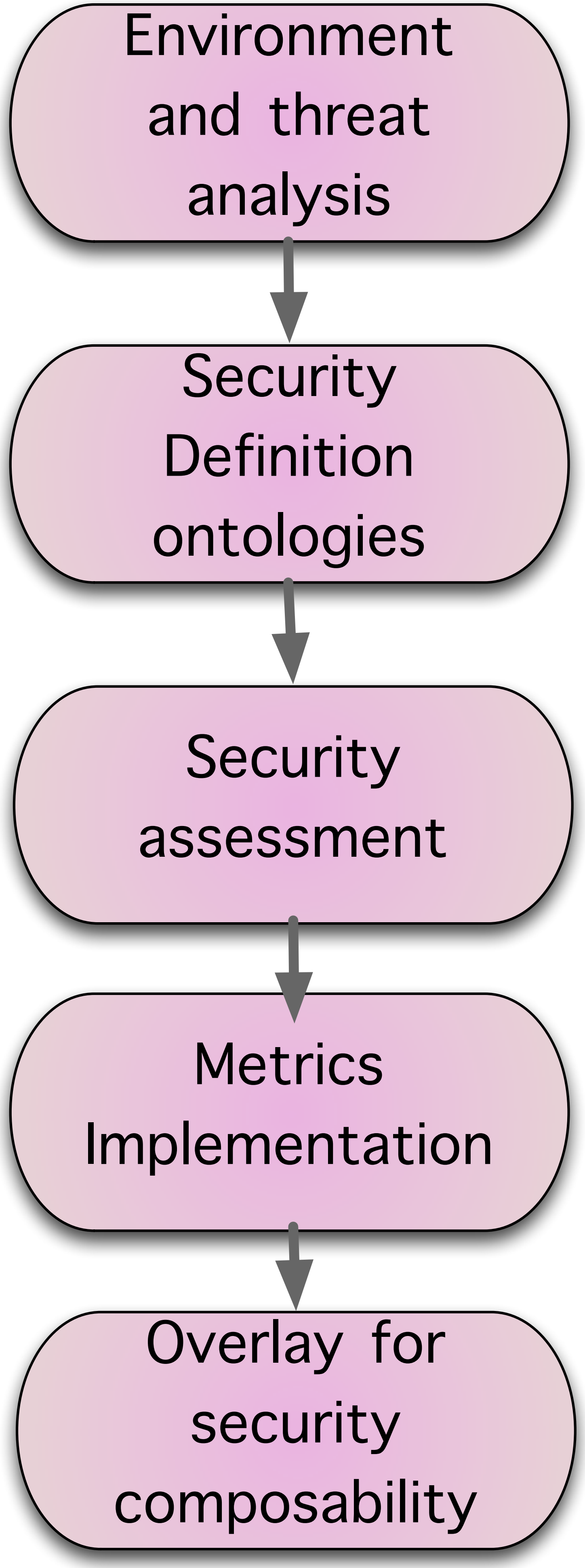
[source: http://securityontology.sba-research.org/]

The nSHIELD approach

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

Core concept

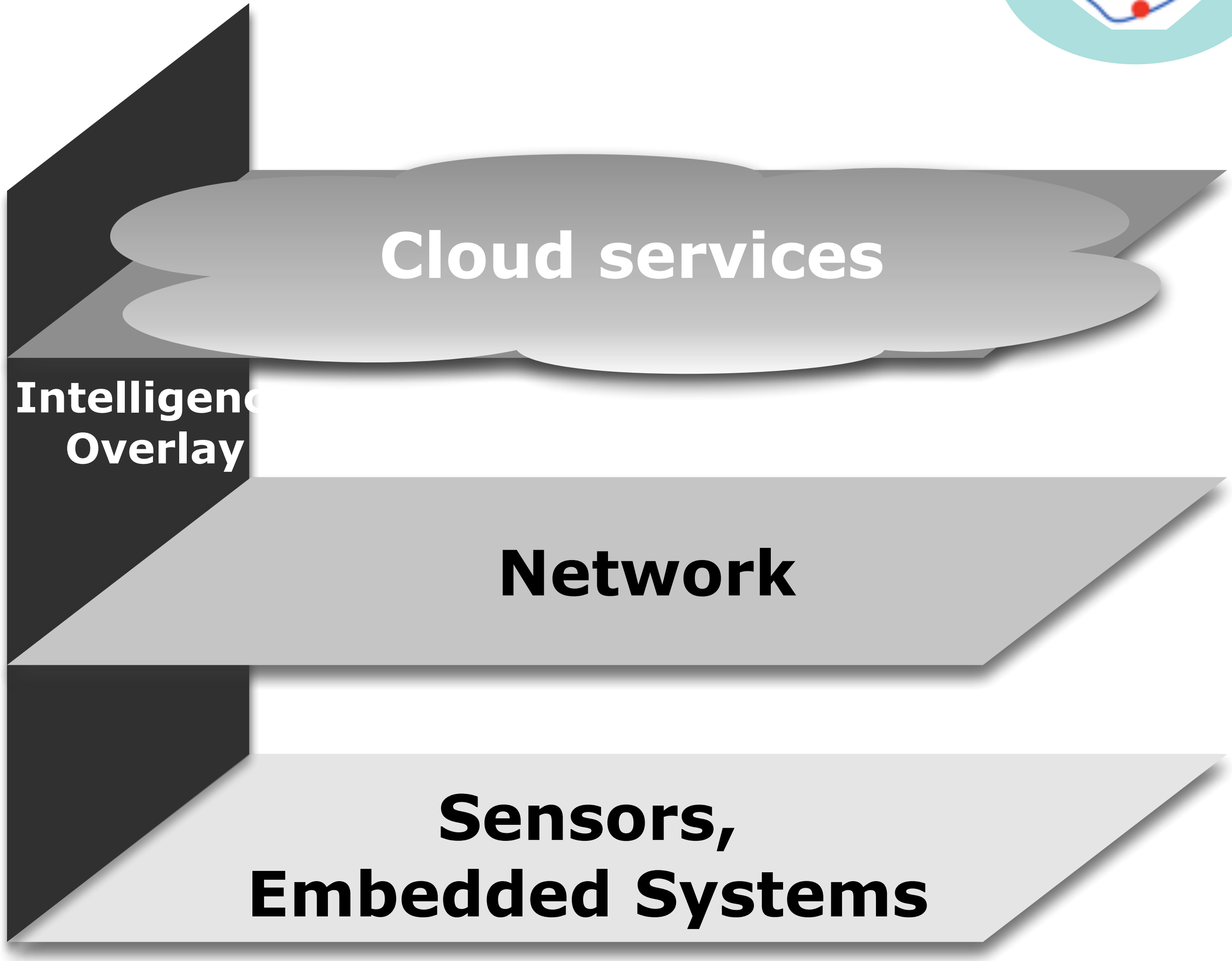
- Threat analysis
- Goal definition
- Semantic security description
- Semantic system description
- Security composability

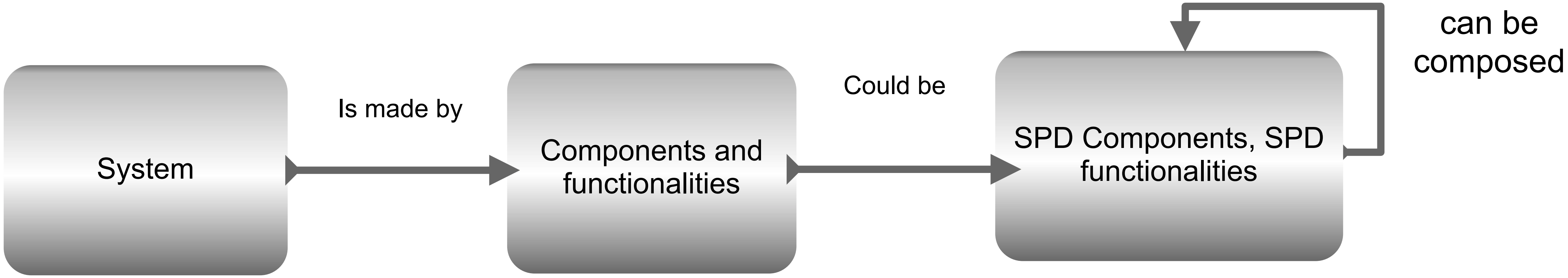

Environment and threat analysis
Security Definition ontologies
Security assessment
Metrics Implementation
Overlay for security composability

http://newSHIELD.eu

newSHIELD.eu approach

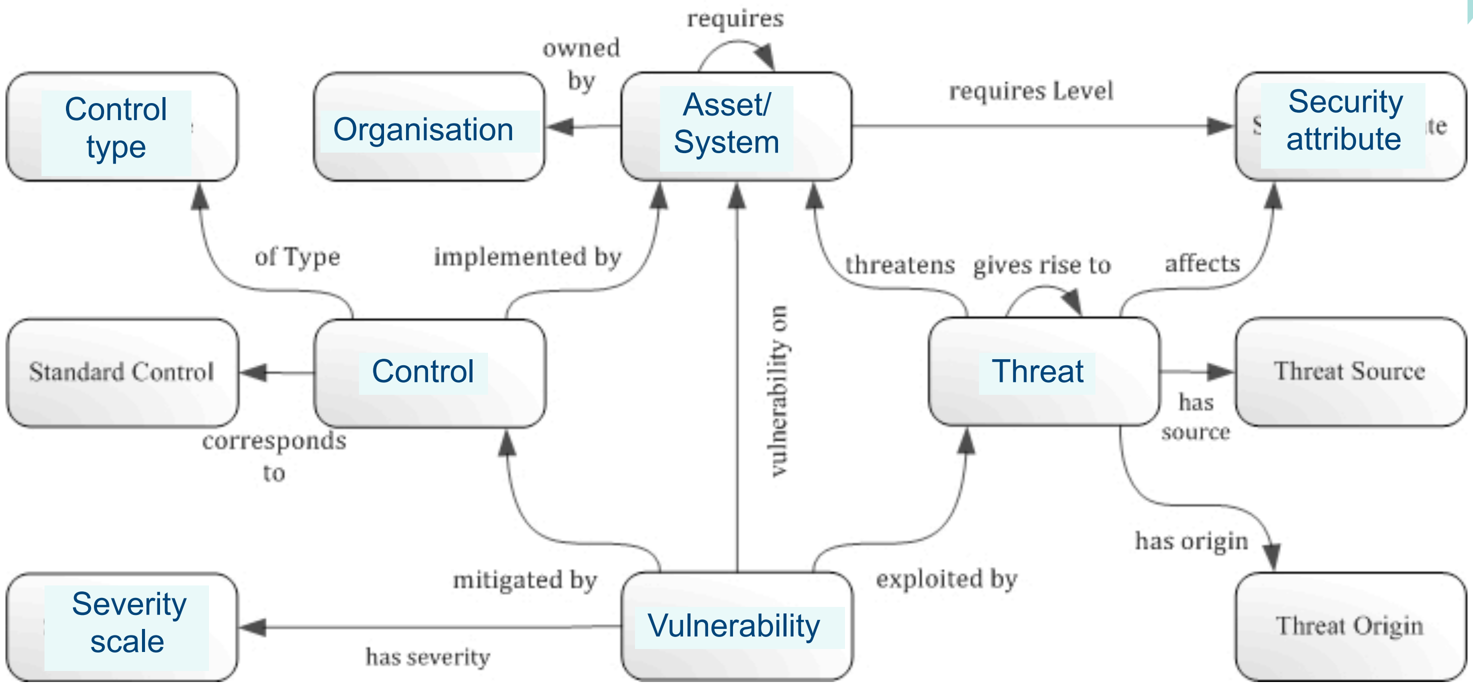
- Security, here
  - security (S)
  - privacy (P)
  - dependability (D)
- across the value chain
  - from sensors to services
- measurable security




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

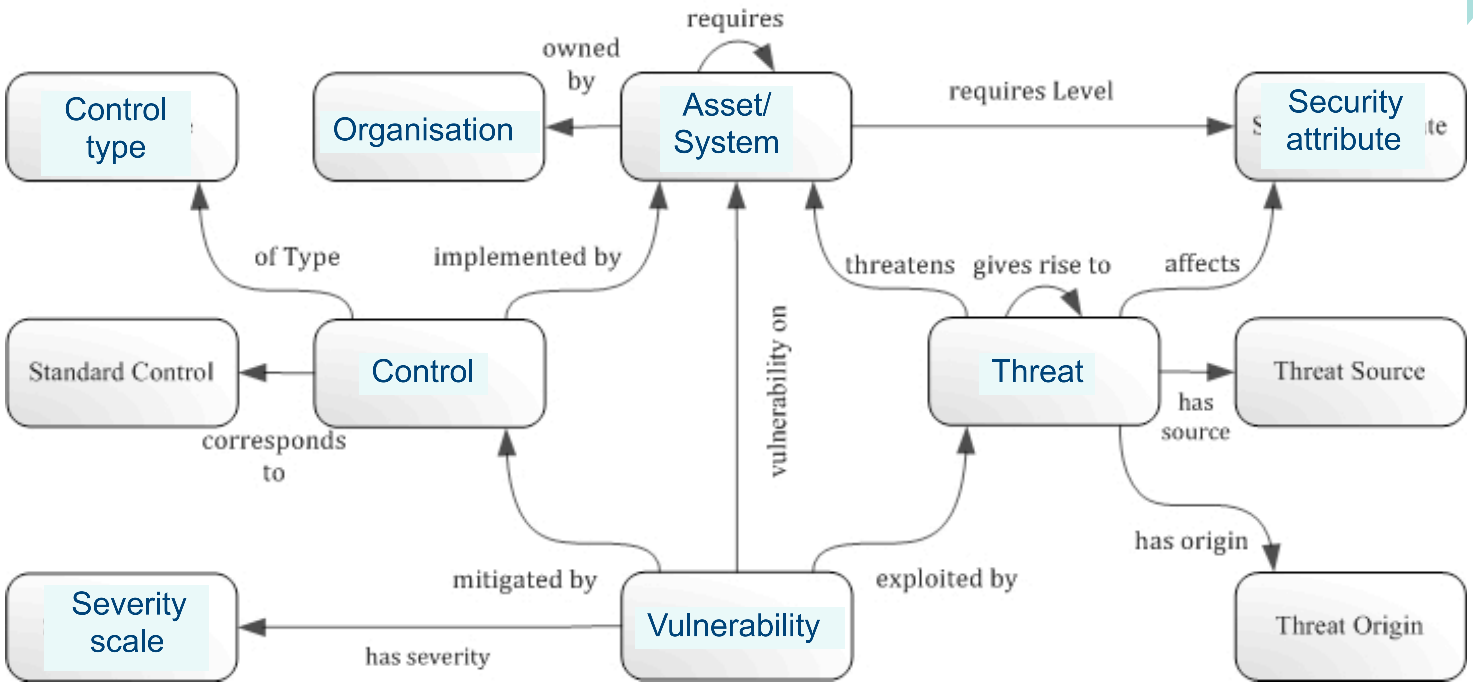
Limitations of the traditional approach

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



Limitations of the traditional approach

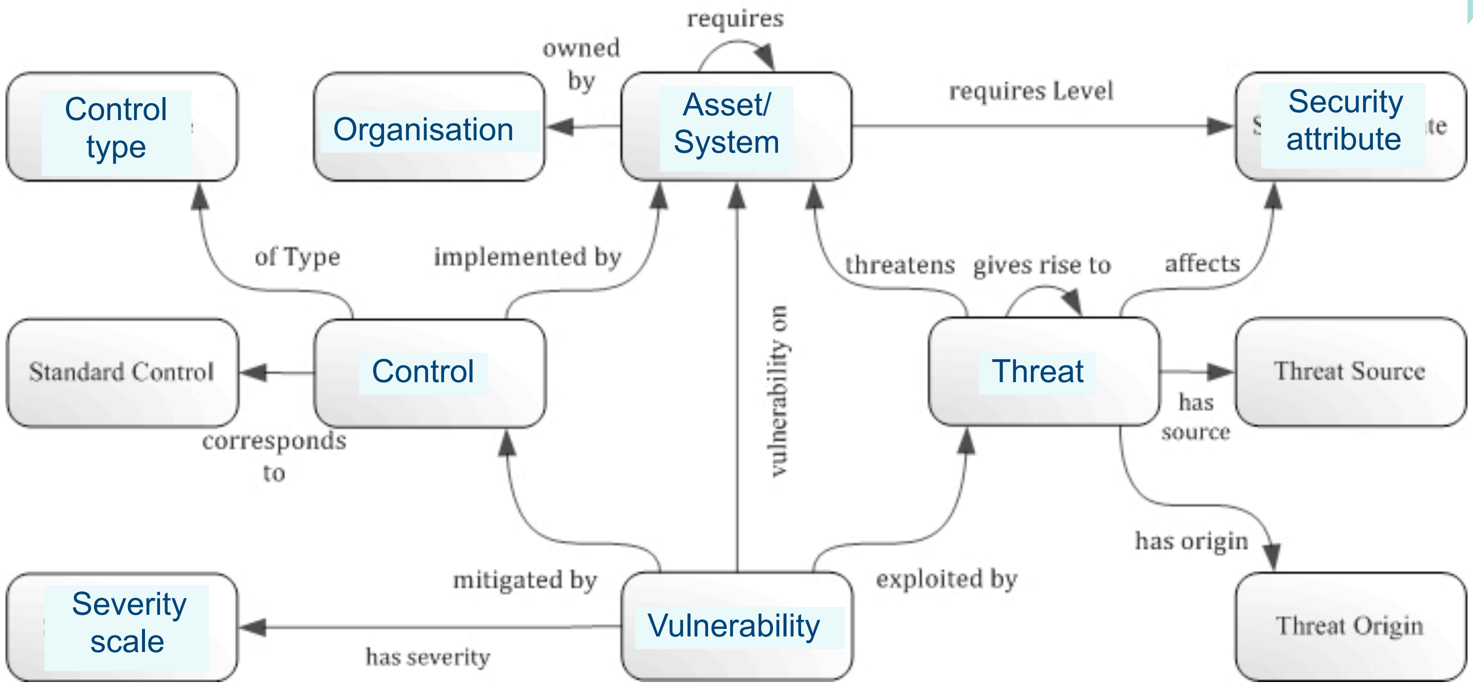
- Scalability
  - Threats
  - System
  - Vulnerability
- System of Systems
  - sensors
  - gateway
  - middleware
  - business processes



Recommendation:

Limitations of the traditional approach

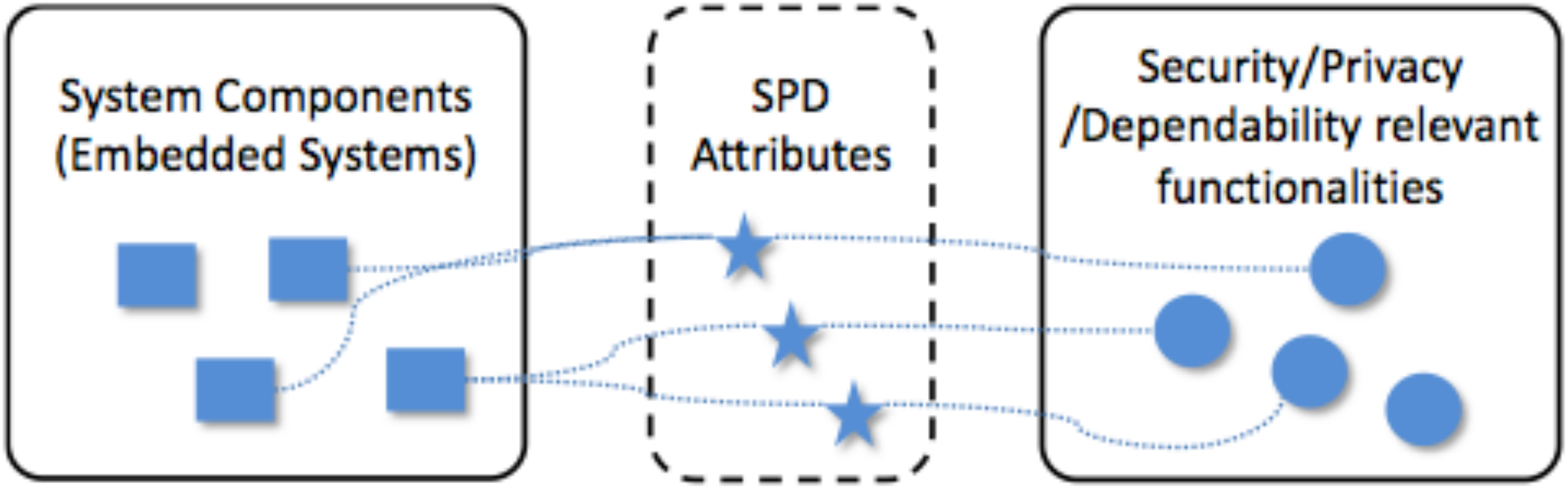
- Scalability
  - Threats
  - System
  - Vulnerability
- System of Systems
  - sensors
  - gateway
  - middleware
  - business processes

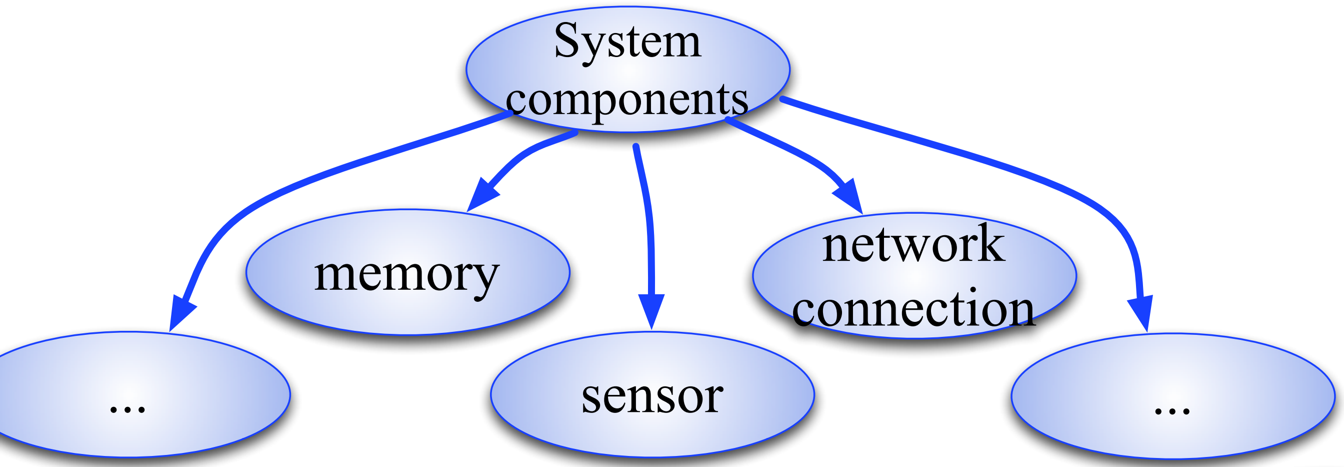


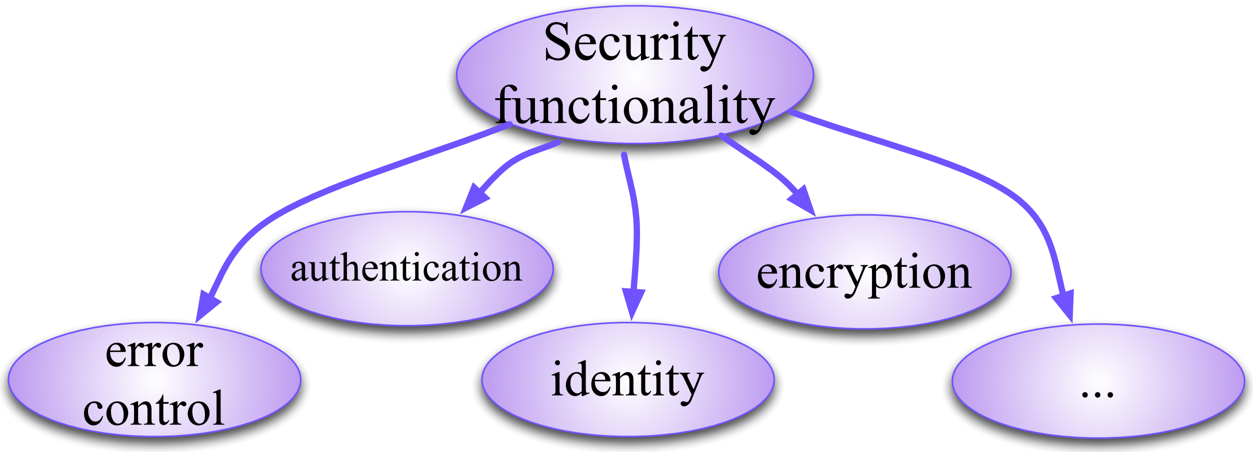
Recommendation:

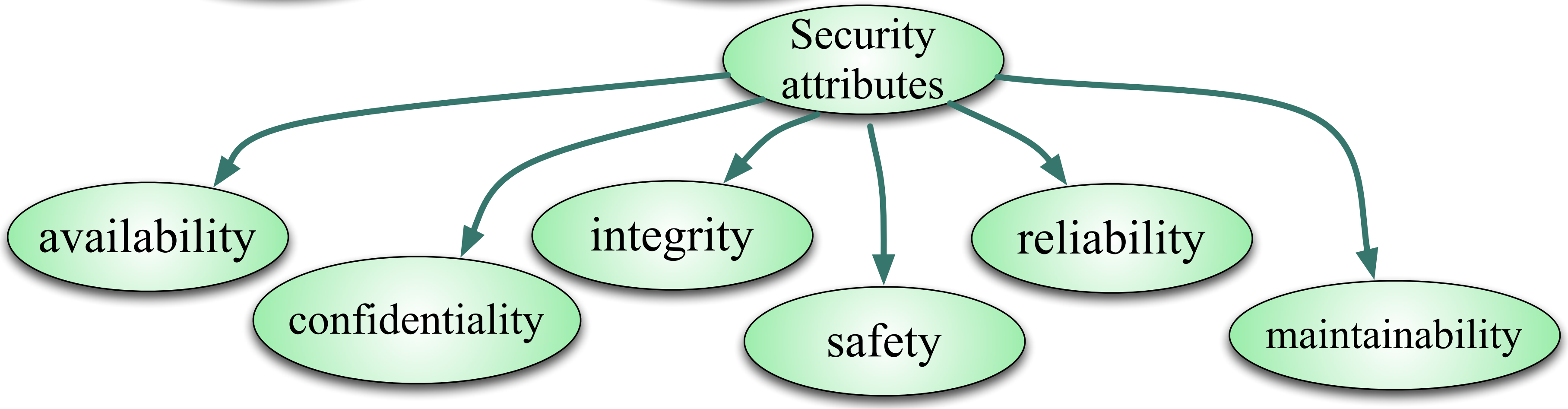
One ontology per aspect:
- security
- system
- threats
...

Security description

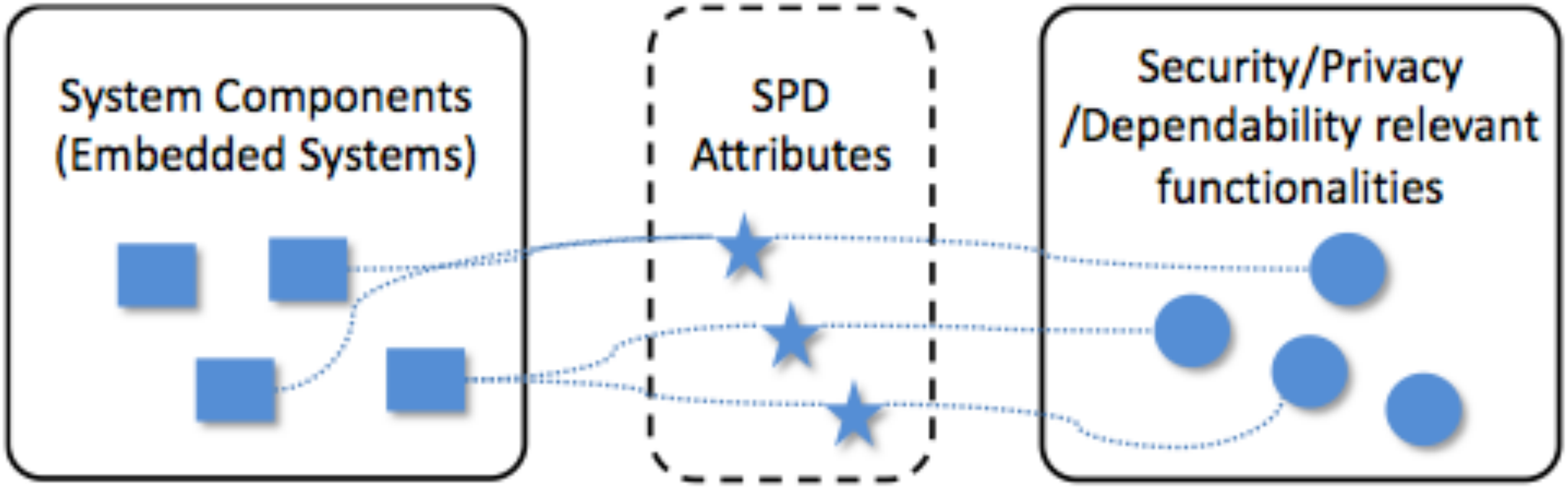








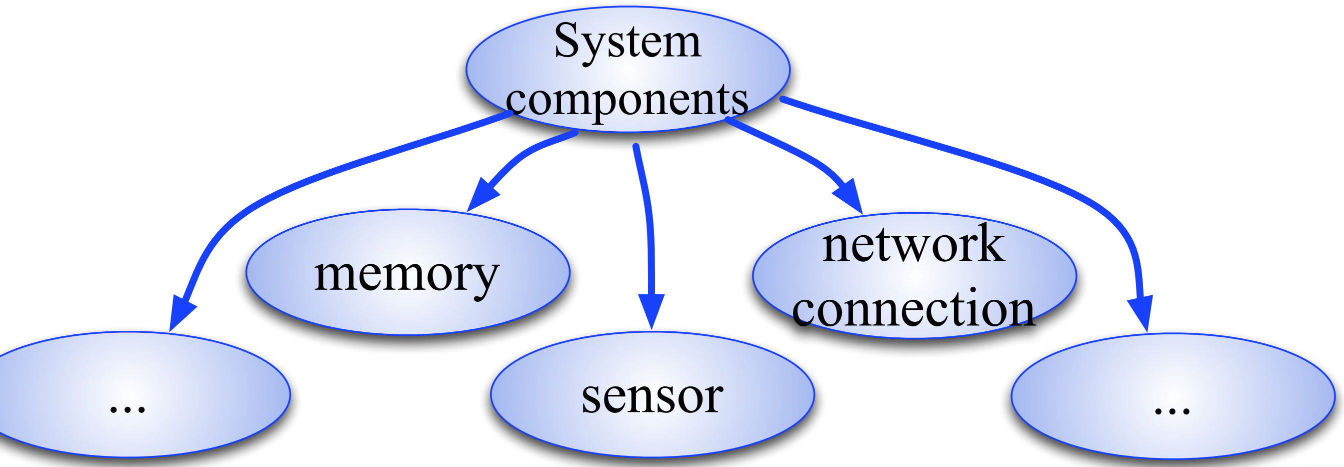
Security description



System Components (Embedded Systems)

SPD Attributes

Security/Privacy /Dependability relevant functionalities



System components

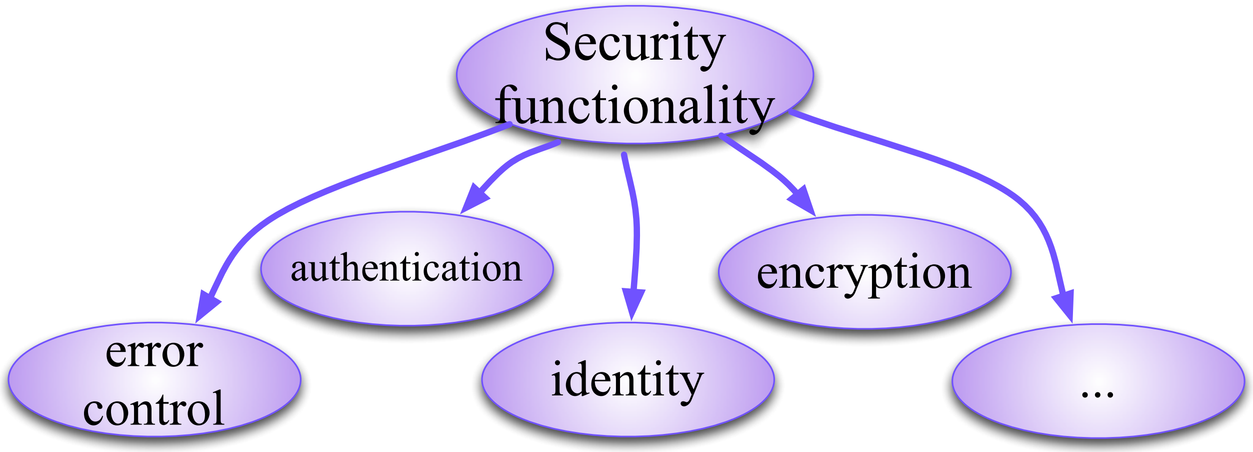
memory

sensor

network connection

...

...



Security functionality

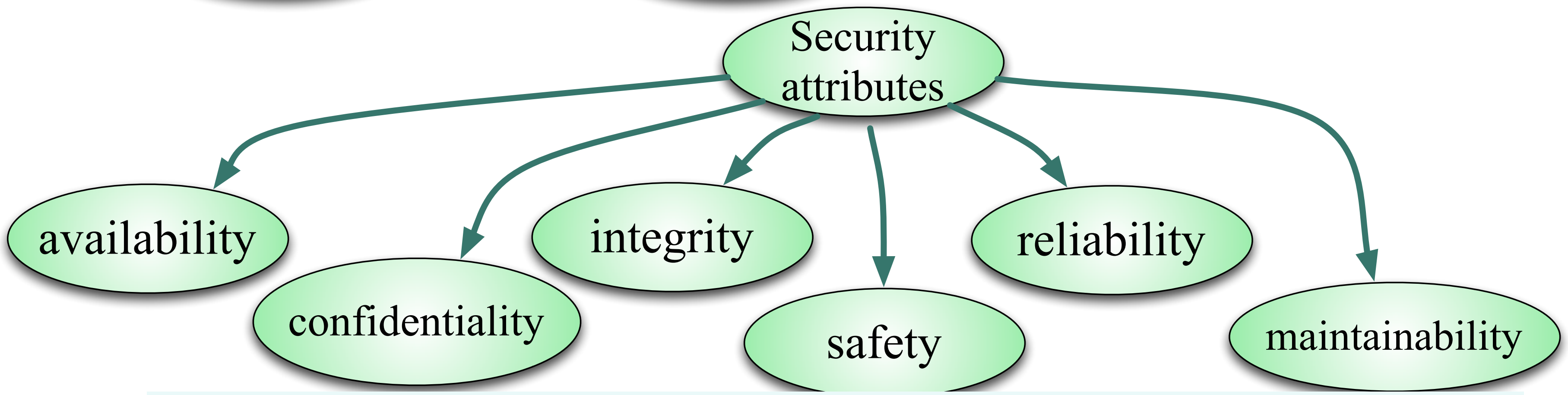
authentication

encryption

error control

identity

...



Security attributes

availability

integrity

reliability

confidentiality

safety

maintainability

Recommendation: One ontology per aspect

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”

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(?)

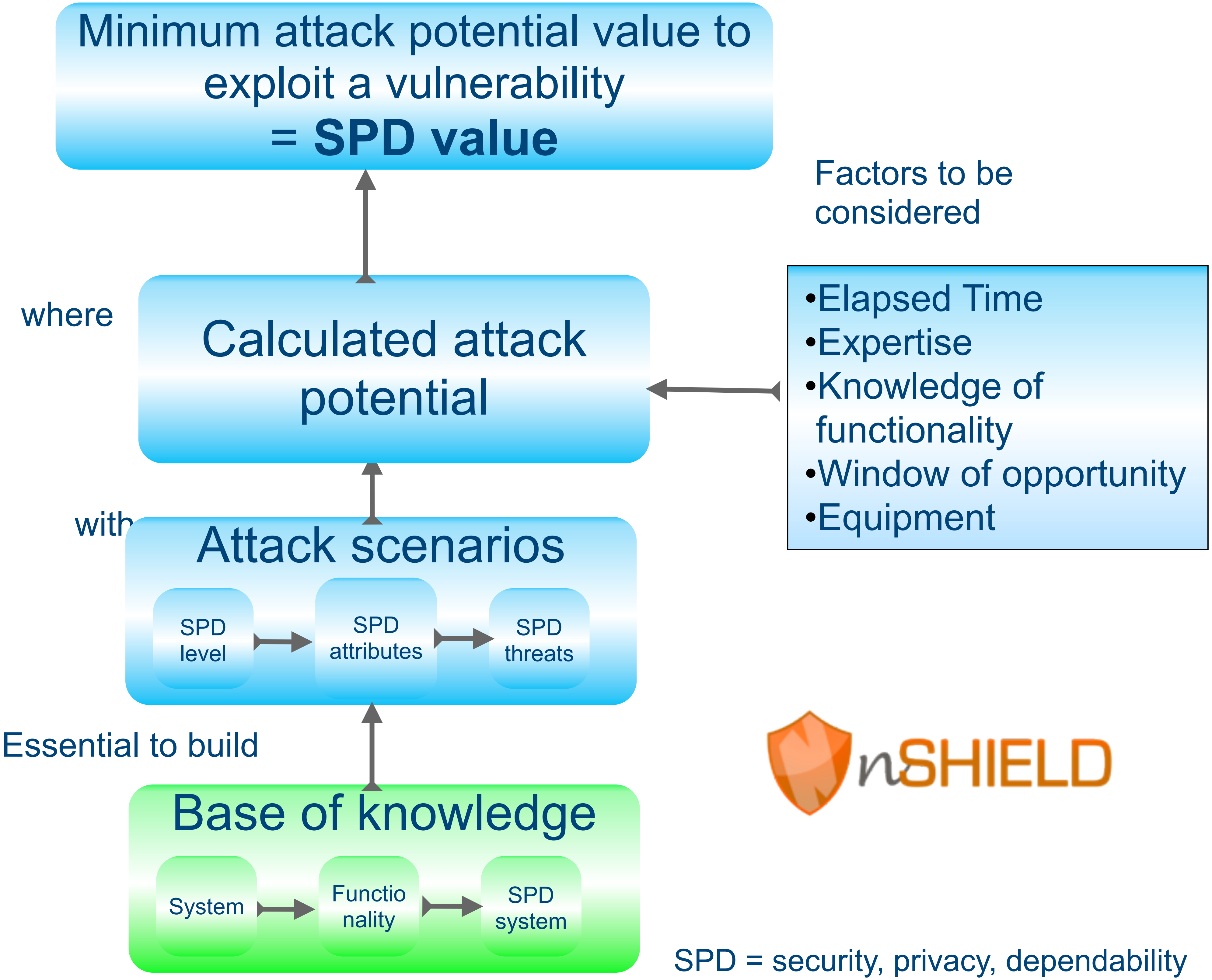
- Common approach?
  - SPD = level 4

that way?

- universal approach
  - code “red”

Open Issue - way on how to describe the security goal

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

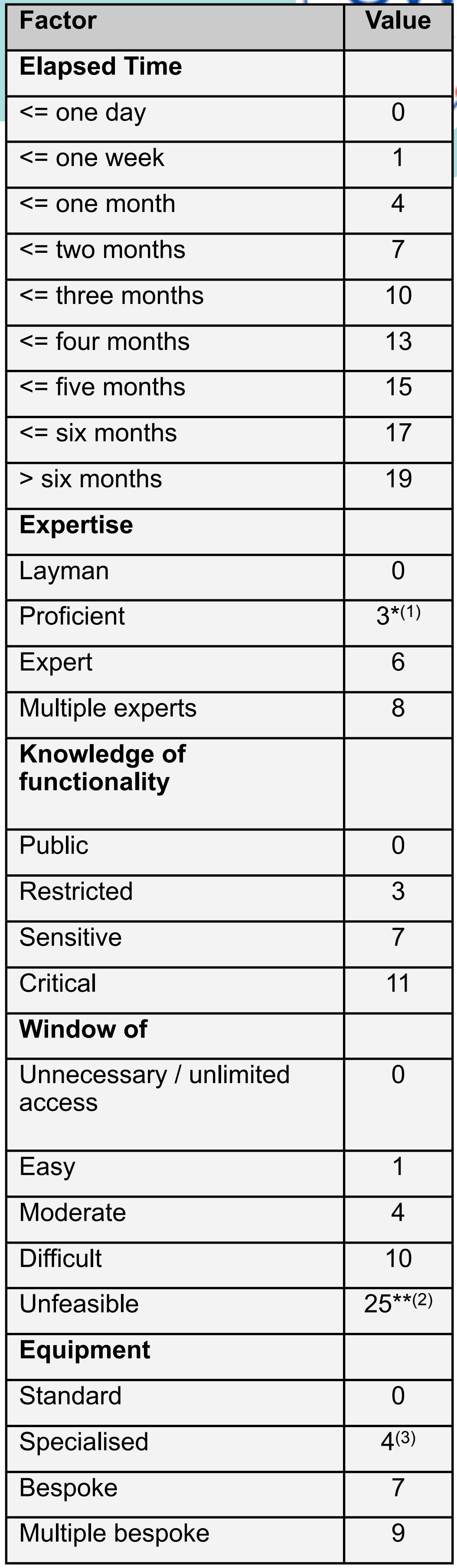
with

Attack scenarios

Essential to build

Base of knowledge

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

From security assessment to
Attribute-based access

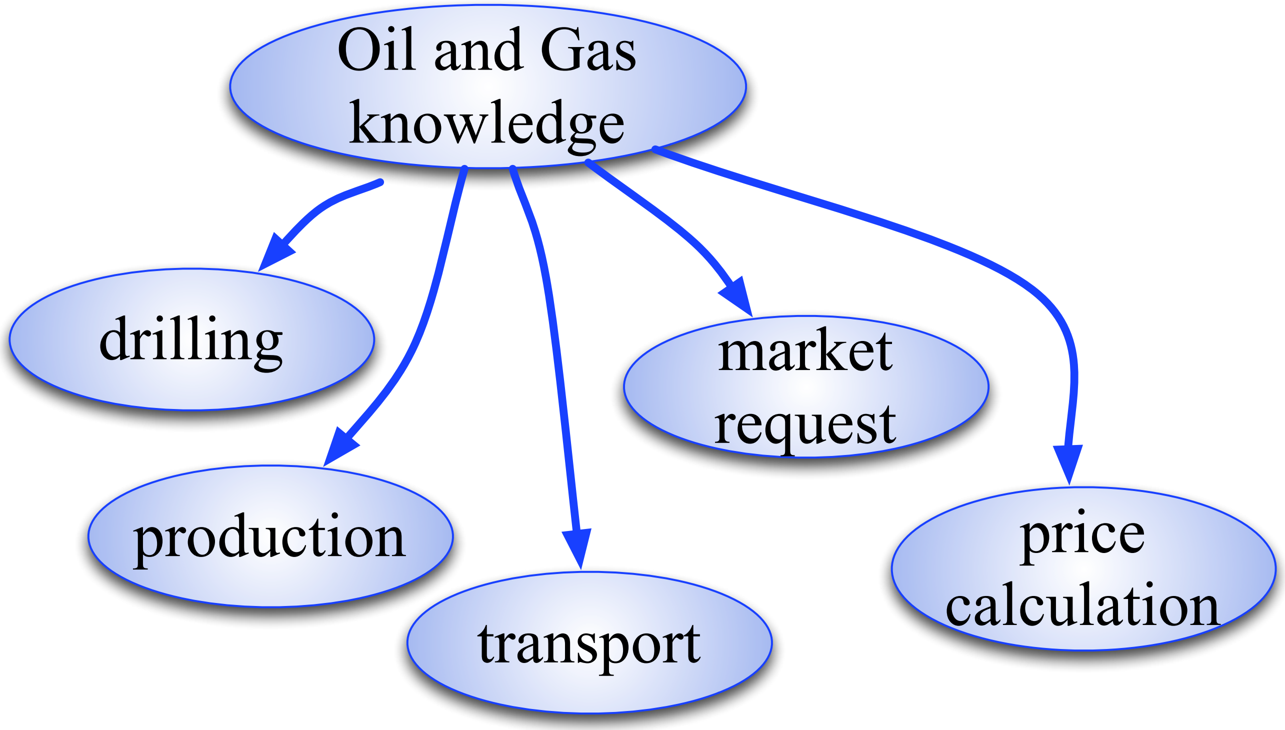
- Security assessment of the Internet of Things
  - Apply SHIELD methodology for SecPrivDep (SPD)
  - Describe functionalities in terms of security (ontologies)
  - Assess threats through Metrics
  - achieve a mean for SPD
- Access to information
  - who,
  - what kind of information
  - from where

- Attribute-based access
  - role (in project, company)
  - device, network
  - security tokens

Semantic attribute based (S-ABAC)

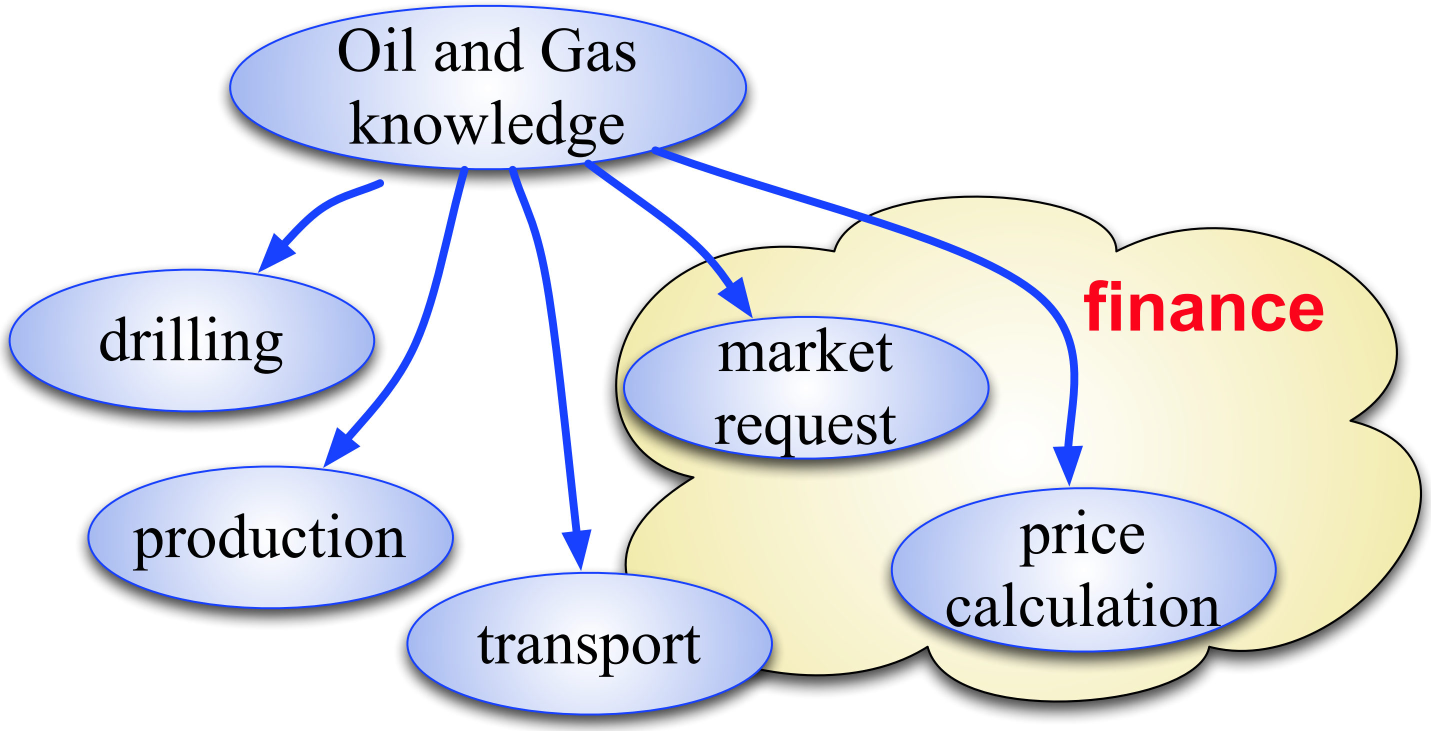
- Access to information
  - Sensor, Person, Service

- Attributes
  - roles
  - type of access
  - device
  - reputation
  - behaviour
  - ...



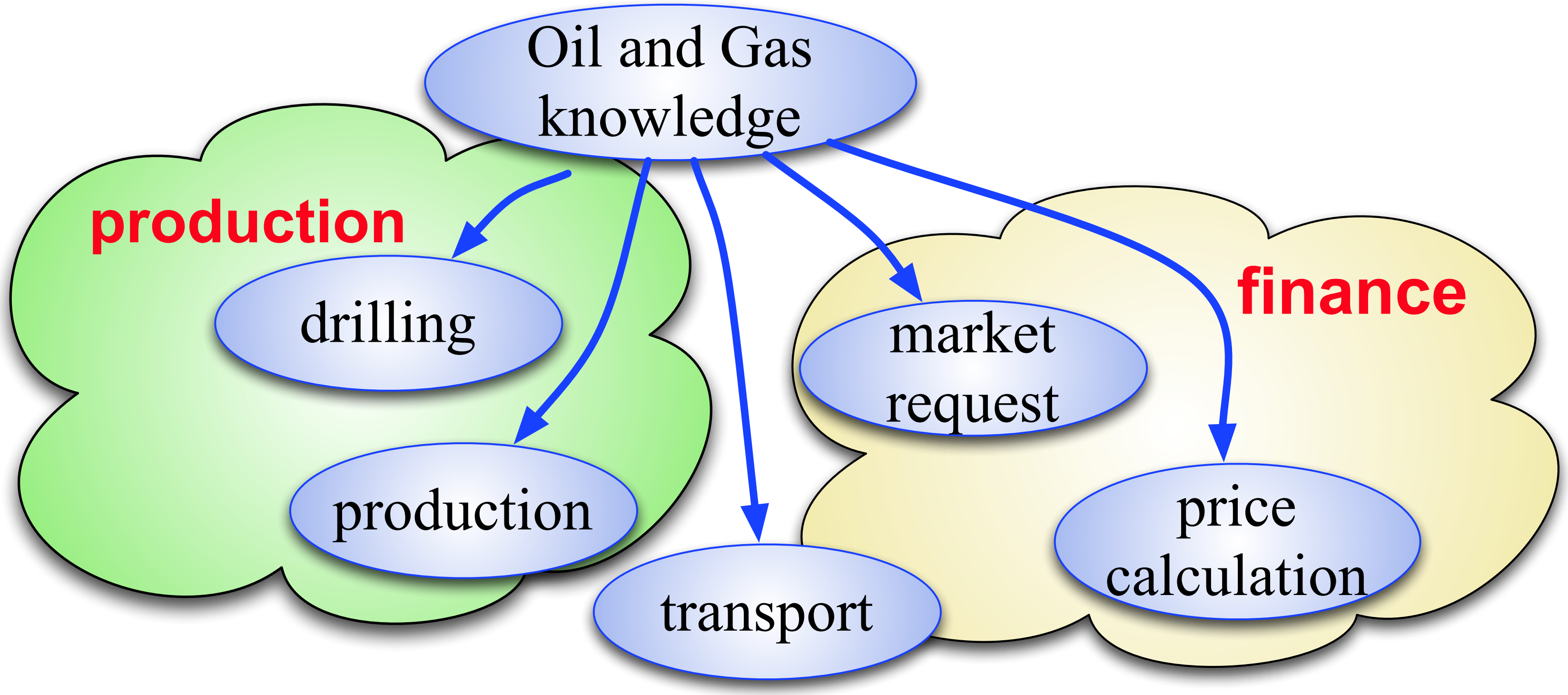
Semantic attribute based (S-ABAC)

- Access to information
  - Sensor, Person, Service
- Attributes
  - roles
  - type of access
  - device
  - reputation
  - behaviour
  - ...



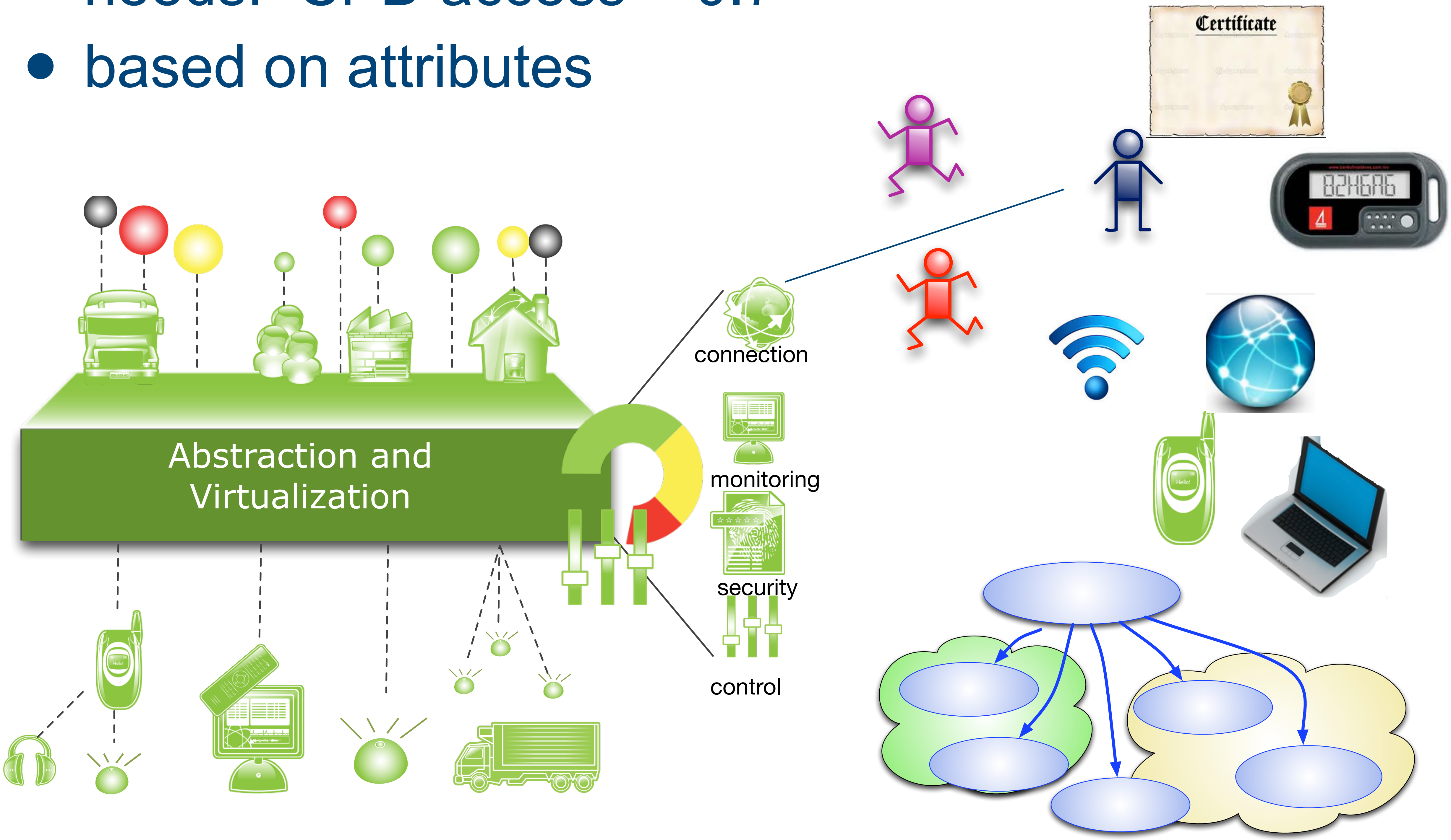
Semantic attribute based (S-ABAC)

- Access to information
  - Sensor, Person, Service
- Attributes
  - roles
  - type of access
  - device
  - reputation
  - behaviour
  - ...



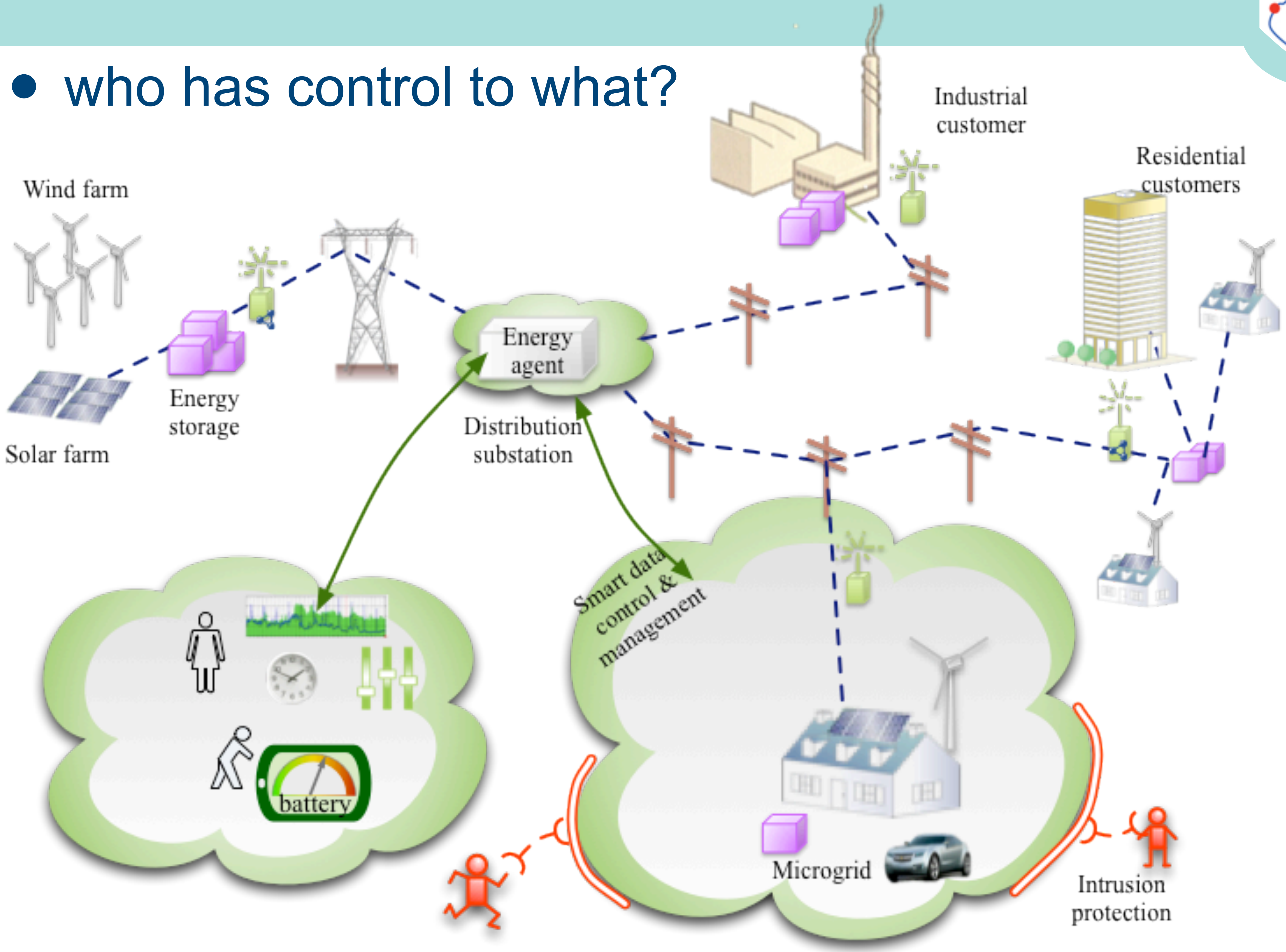
Bringing attributes to IoPTS

- Ontology-representation of access
- needs: “SPD access = 0.7”
- based on attributes



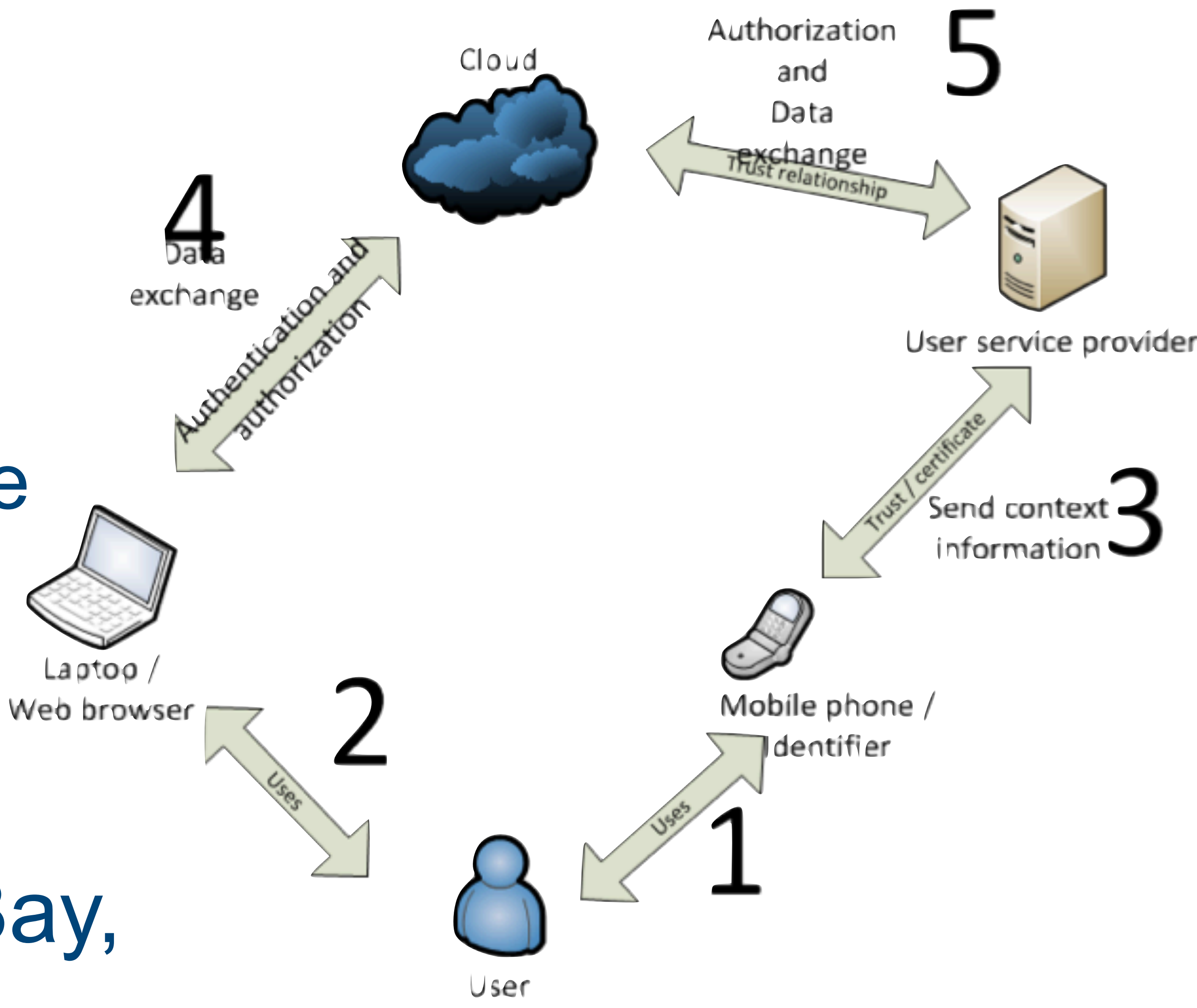
Example - Smart Energy Grid

- who has control to what?



ODATA - based ABAC

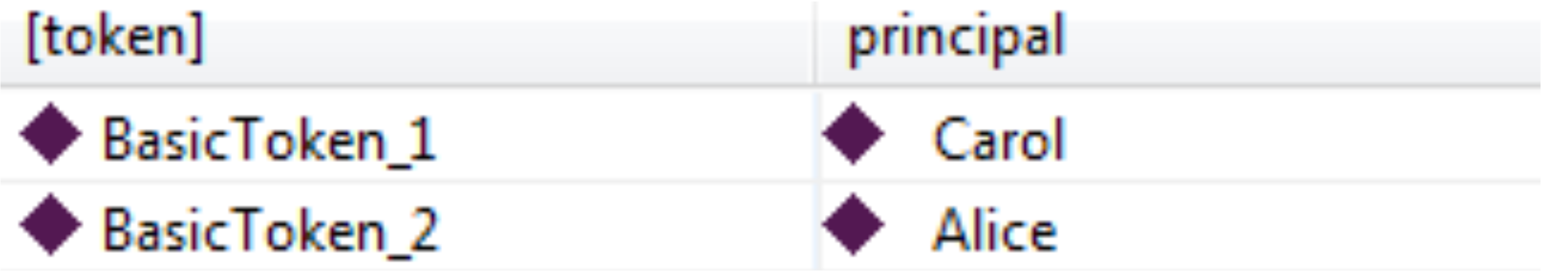
- ODATA,
  - released Feb2009
  - Entity Data Model (EDM)
  - Common Schema Definition Language (CSDL)
  - Entity Framework to infer the conceptual model
  - Query language LINQ
  - is a query language
- Used by: StackOverflow, eBay, TechEd, Netflix,...
- Microsoft’s approach for interworking



S-ABAC based access

- OWL & SWRL implementation
- Rules inferring security tokens

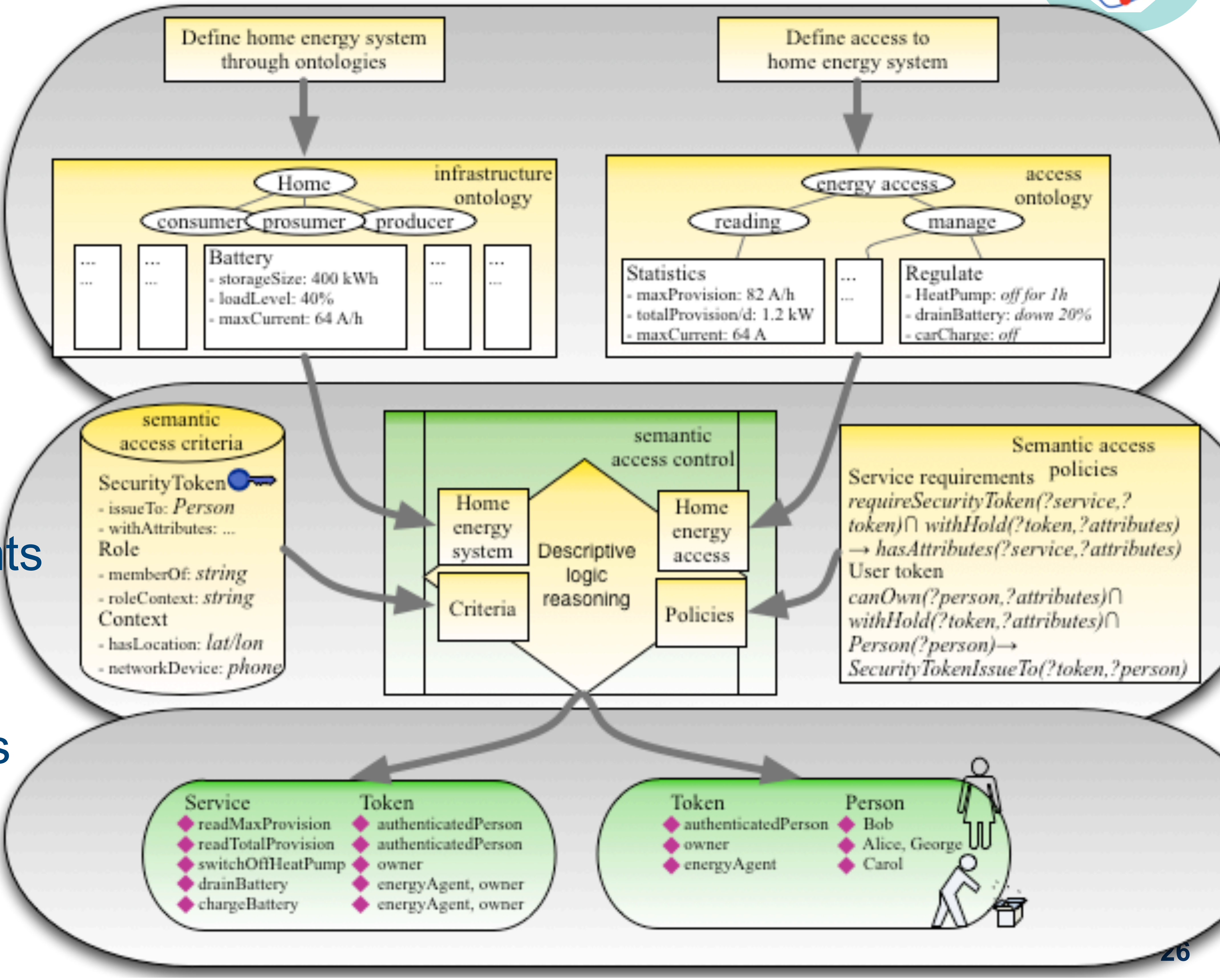
canOwn(?person,?attributes) ∩ withHold(?token,?attributes) ∩
(Person(?person) -> SecurityTokenIssueTo(?token, ?person)



[token]	principal
◆ BasicToken_1	◆ Carol
◆ BasicToken_2	◆ Alice

Application - Smart-grid

- Access criteria
  - Security token
  - role
  - context
- Policies
  - service requirements
  - service tokens
  - user tokens



Define home energy system through ontologies

Define access to home energy system

infrastructure ontology

Home

consumer prosumer producer

...
...

Battery
- storageSize: 400 kWh
- loadLevel: 40%
- maxCurrent: 64 A/h

access ontology

energy access

reading

manage

Statistics
- maxProvision: 82 A/h
- totalProvision/d: 1.2 kW
- maxCurrent: 64 A

Regulate
- HeatPump: *off for 1h*
- drainBattery: *down 20%*
- carCharge: *off*

semantic access criteria

SecurityToken
- issueTo: *Person*
- withAttributes: ...

Role
- memberOf: *string*
- roleContext: *string*

Context
- hasLocation: *lat/lon*
- networkDevice: *phone*

semantic access control

Home energy system

Criteria

Descriptive logic reasoning

Home energy access

Policies

Semantic access policies

Service requirements

requireSecurityToken(?service,?token)∩ withHold(?token,?attributes) → hasAttributes(?service,?attributes)

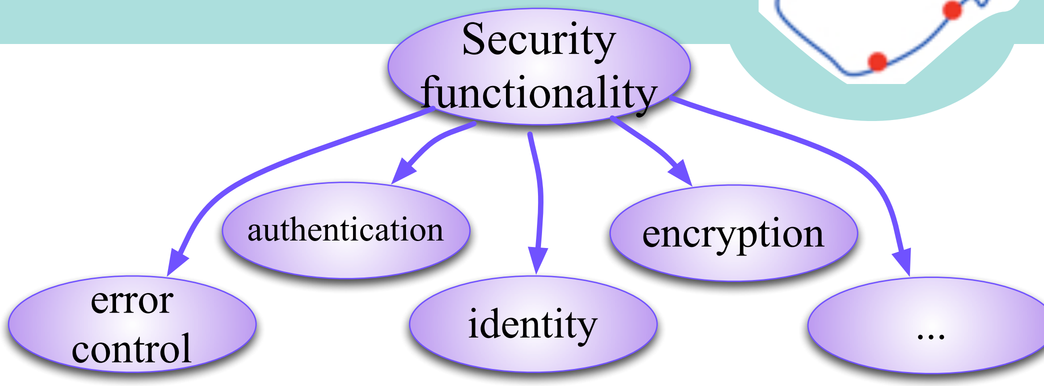
User token

canOwn(?person,?attributes)∩ withHold(?token,?attributes)∩ Person(?person)→ SecurityTokenIssueTo(?token,?person)

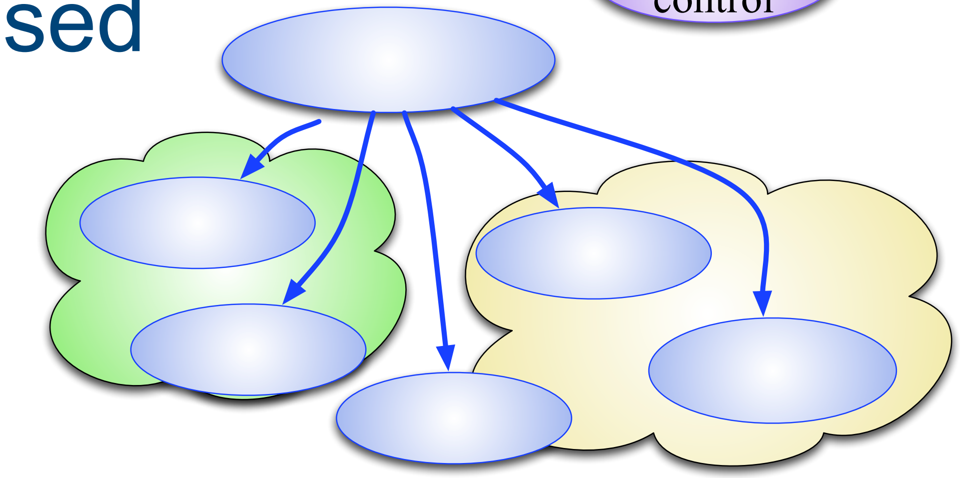
Service	Token
readMaxProvision	authenticatedPerson
readTotalProvision	authenticatedPerson
switchOffHeatPump	owner
drainBattery	energyAgent, owner
chargeBattery	energyAgent, owner

Token	Person
authenticatedPerson	Bob
owner	Alice, George
energyAgent	Carol

Conclusions & Recommendations



- Recommendations
  - one ontology per aspects
  - semantic attribute based access control



- Open Issues
  - description of security goals
  - metrics description of threat
  - sensor description

availability = 0.8, confidentiality=0.9, integrity=0.6

universal threat metrics?

SensorML

Semantic Sensor Network (SSN)

SenML

- Require “logic” in purchase process

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