Center for Wireless Innovation Norway
cwin.no

CWI
Norway

UNIK
UNIVERSITY GRADUATE CENTER

Semantic Days, Stavanger, May 2013
"Business Intelligence and Semantics"

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 for Business Intelligence
  - Application in the IoT
  - Access, Authentication,... for People, Things And Services (IoPTS)
  - threat, goal, architecture
- Semantic Approach
  - Ontologies for security, system, component functionality
  - Metrics based assessment
  - context-aware security - for people, things and services
  - Semantic attribute based access
- Experiences and challenges
  - Specific ontologies for each threat
  - Sensor/device standardisation
  - distributed or universal metrics
- Conclusions

The Semantic Dimension of the Internet of Things (IoT)

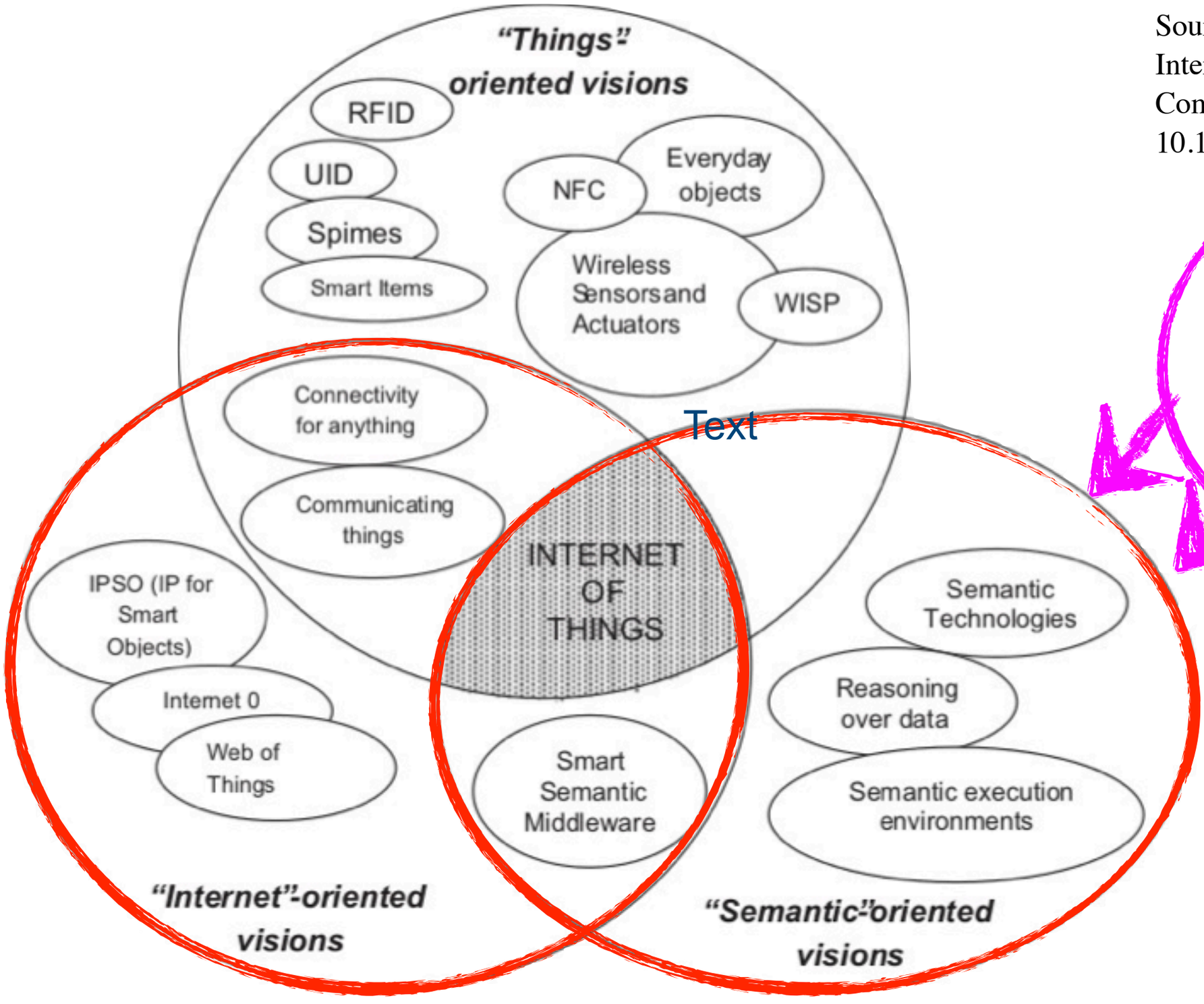
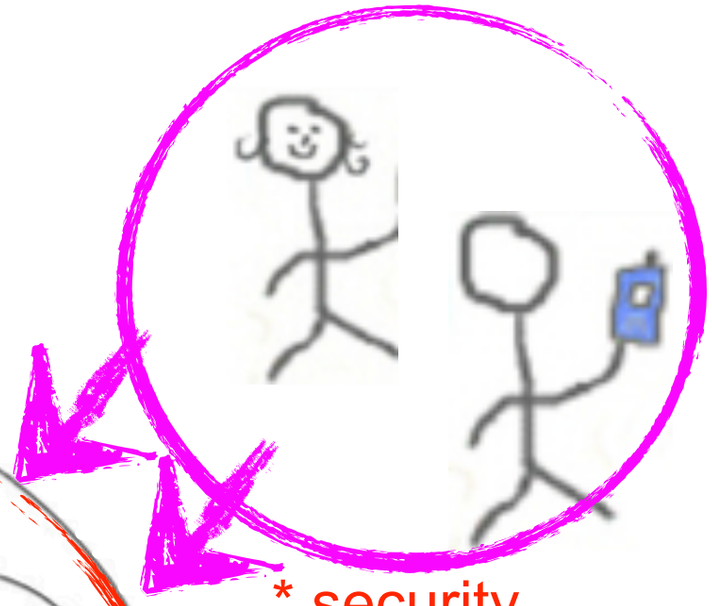


Fig. 1. "Internet of Things" paradigm as a result of the convergence of different visions.

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

Text

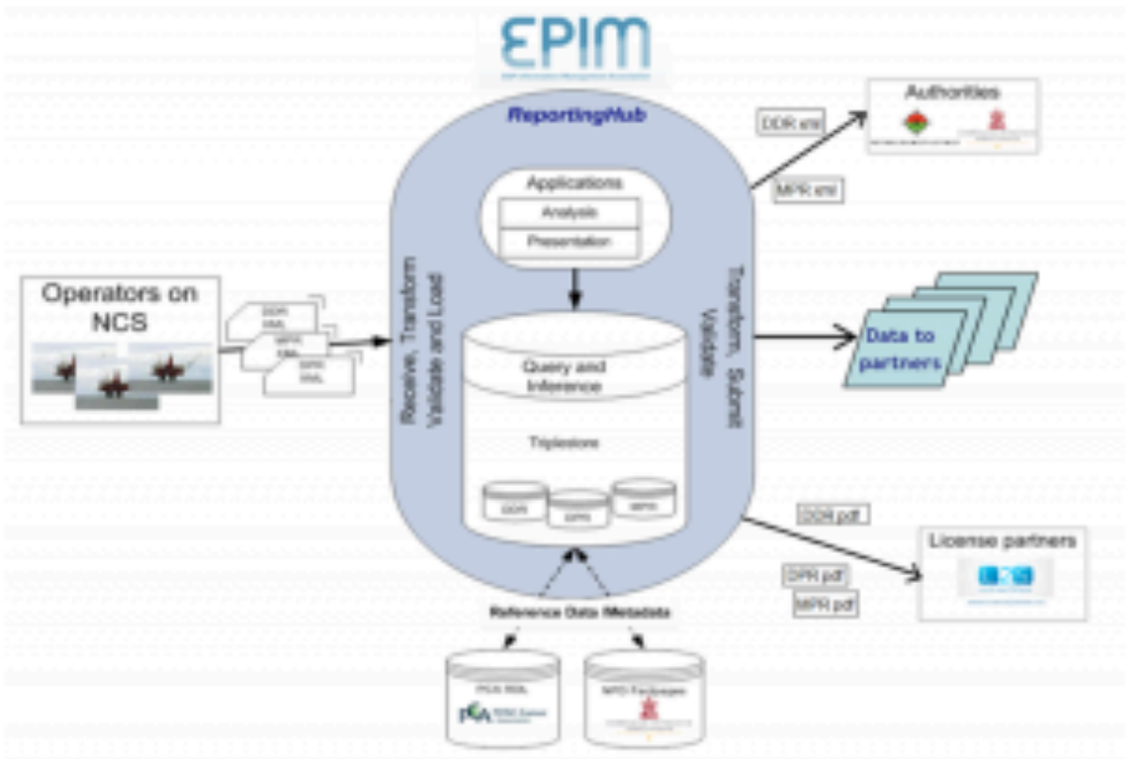


* security
* privacy
* dependability
  - context
  - content
* personalised

IoT application in Oil and Gas

Semantic Case Study: EPIM ReportingHub

By Angela Guess on February 12, 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

Business Intelligence

- Information distribution along 0/1 (false/true)?
  - “someone has stolen my identity” -> access granted
  - shades of grey
  - behaviour monitoring
- 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 challenges

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

➡ you can't control

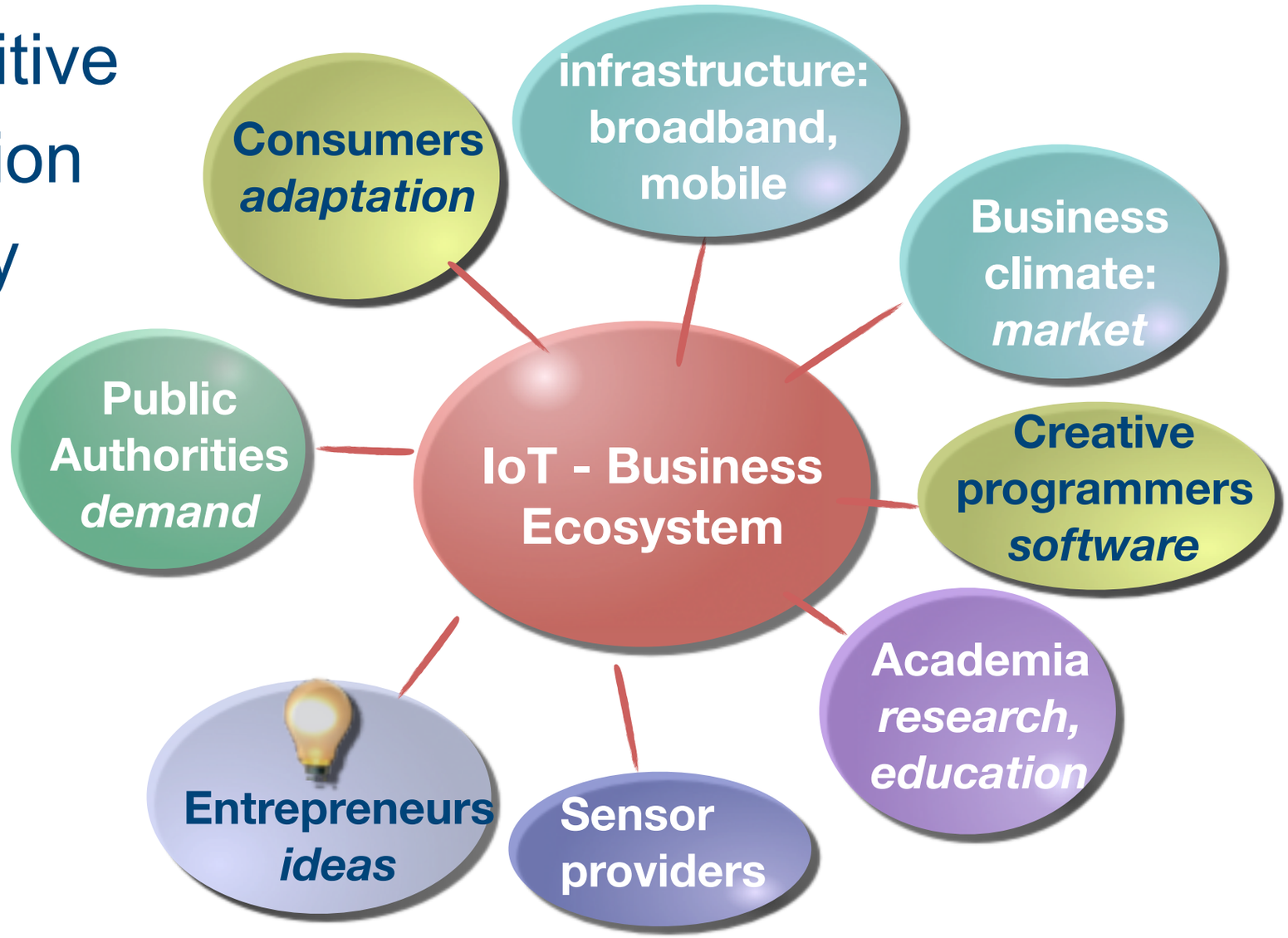
➡ concentrate on the core values

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

➡ Measure your values

IoT success, more than technology

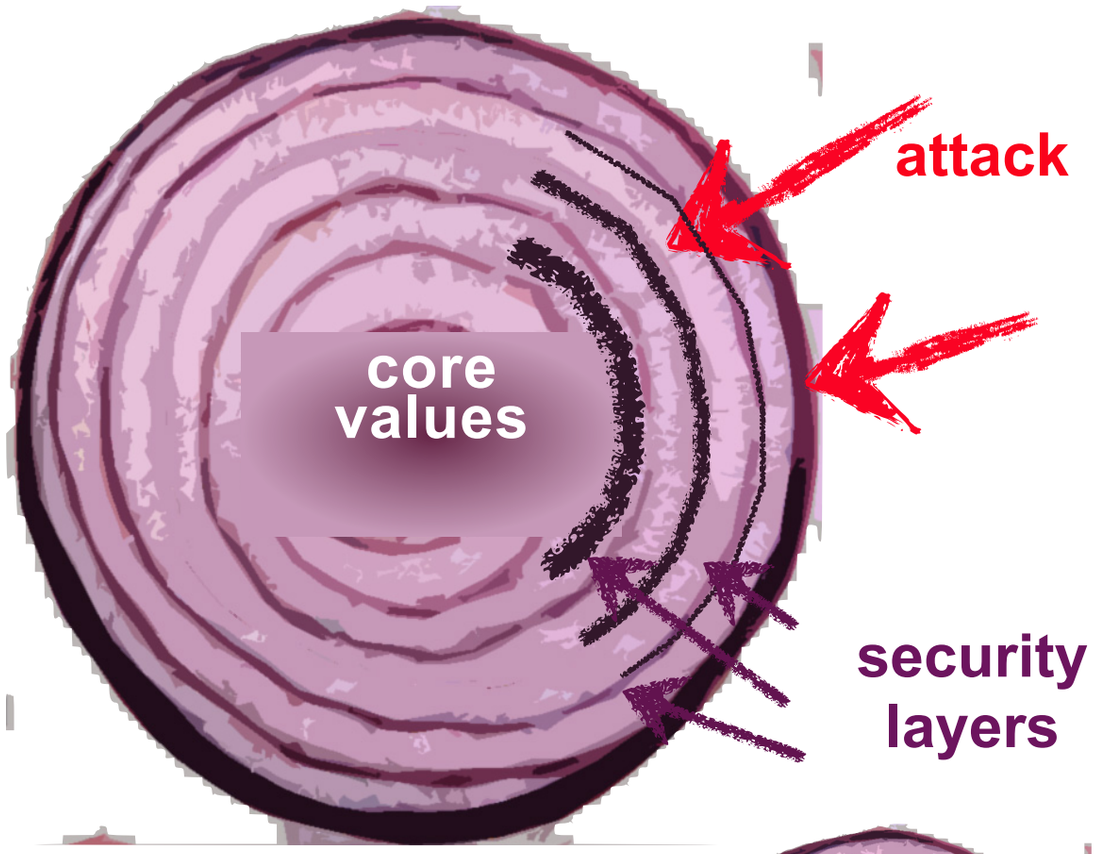
- Creating business
  - openness, competitive
  - climate for innovation
  - IoT data availability
- Trust authorities
  - trust, confidence
  - specific demand
- Scalability
  - (early) adapters
  - education

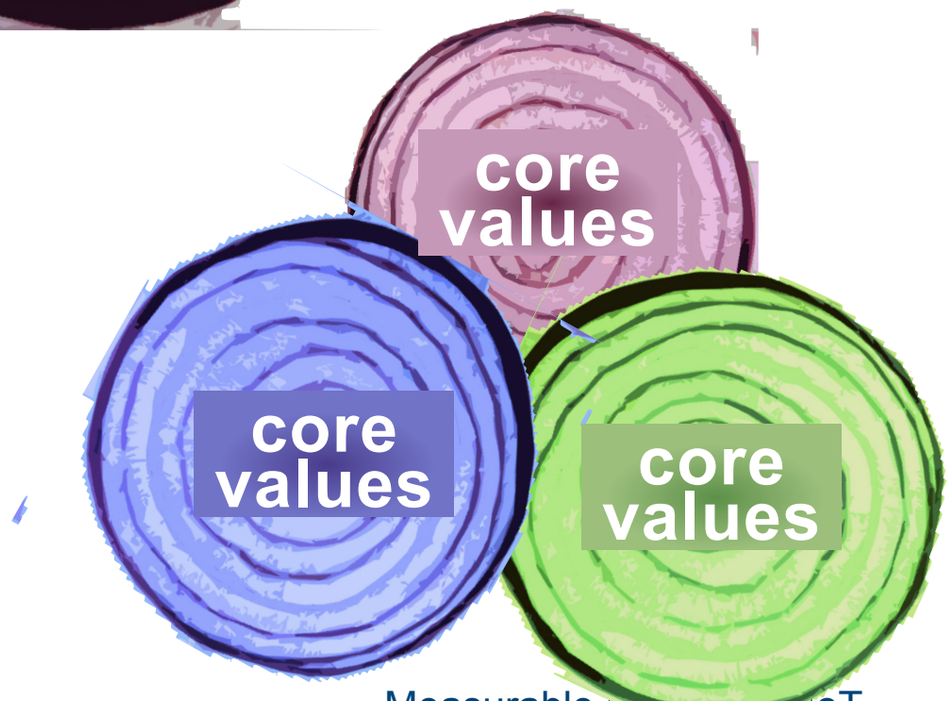


IoT success, more than technology

- Creating business
  - openness, competitive
  - climate for innovation
  - IoT data availability
- Trust authorities
  - trust, confidence
  - specific demand
- Scalability
  - (early) adapters
  - education

Create a successful ecosystem





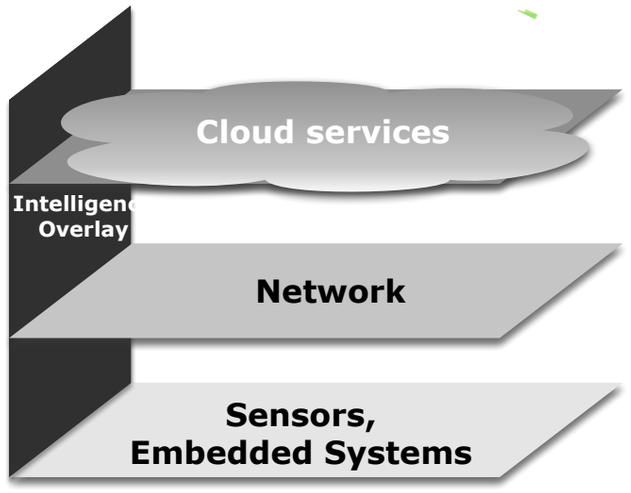
- Demand
  - autonomy
  - context-/content-aware
- Adaptation
  - infrastructure
  - business environment
  - trust
- Security, privacy
  - protect your core values
  - share as much as possible
  - monitor attack

Two dimensions of Internet of Things
for oil and gas

- Identification and protection of values
  - security evaluation
  - attack monitoring

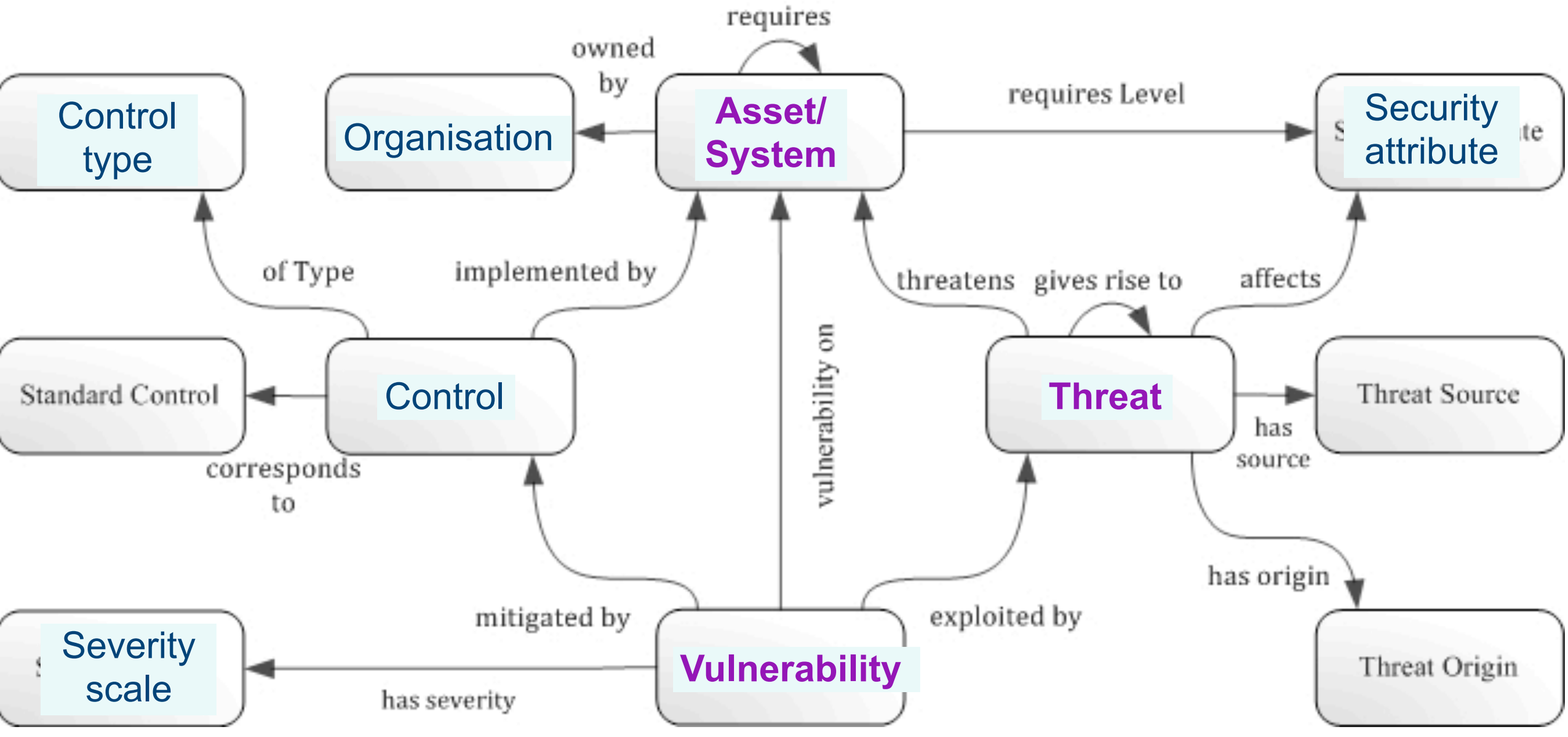
Architecture for

- Internet of Things (IoT)



- (semantic attribute-based) Access Control

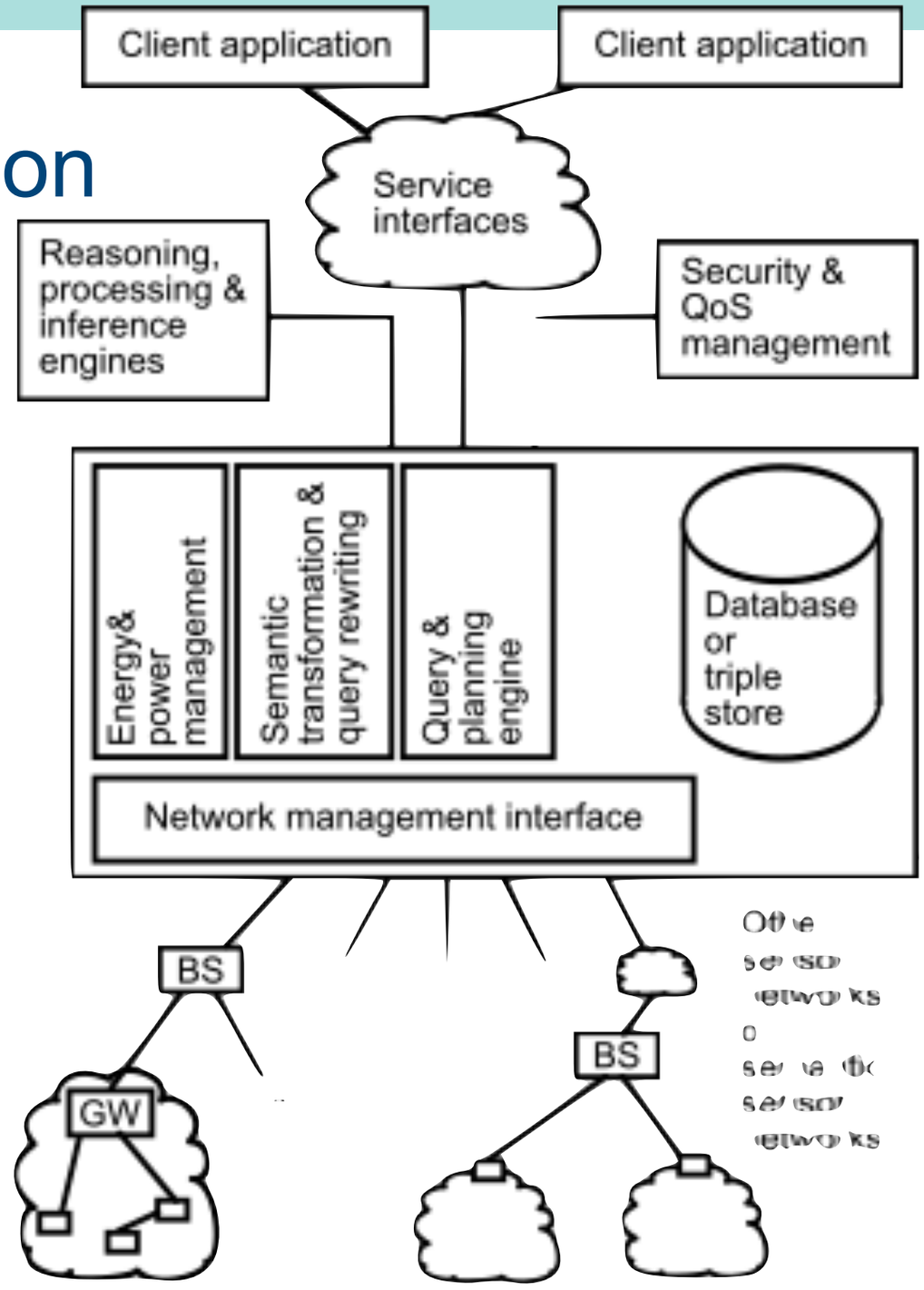
Traditional approach



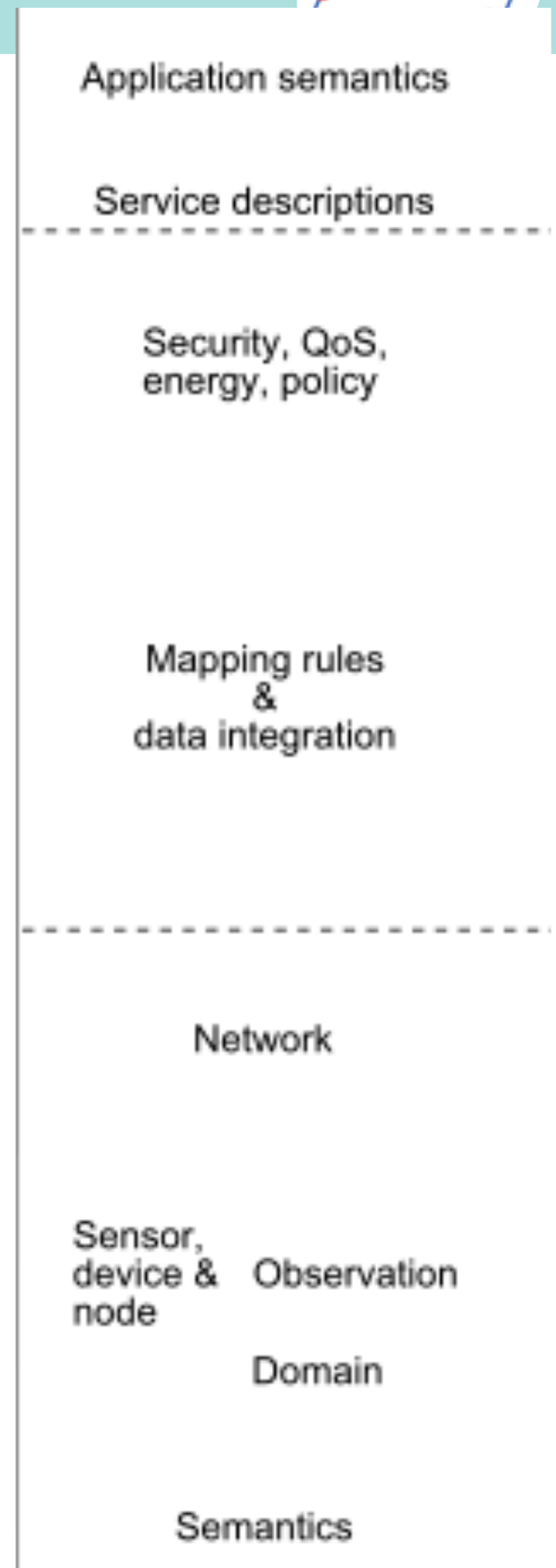
[source: http://securityontology.sba-research.org/]

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

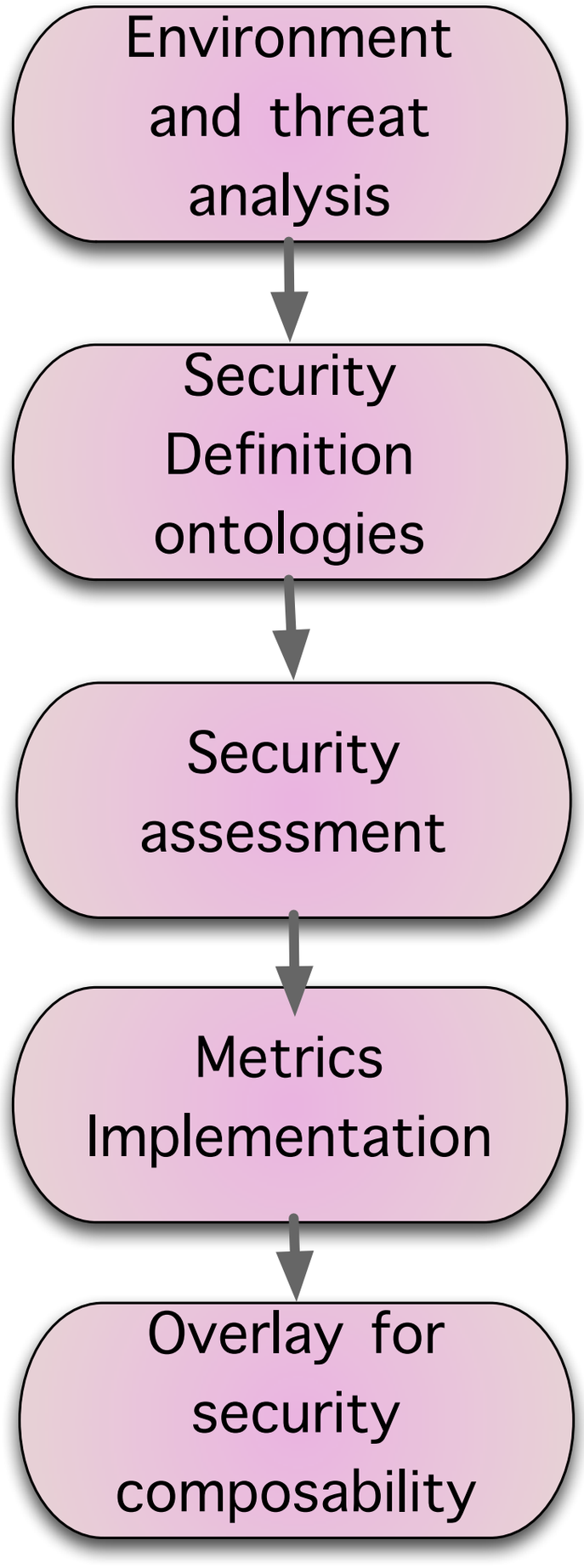


The nSHIELD approach

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

Core concept

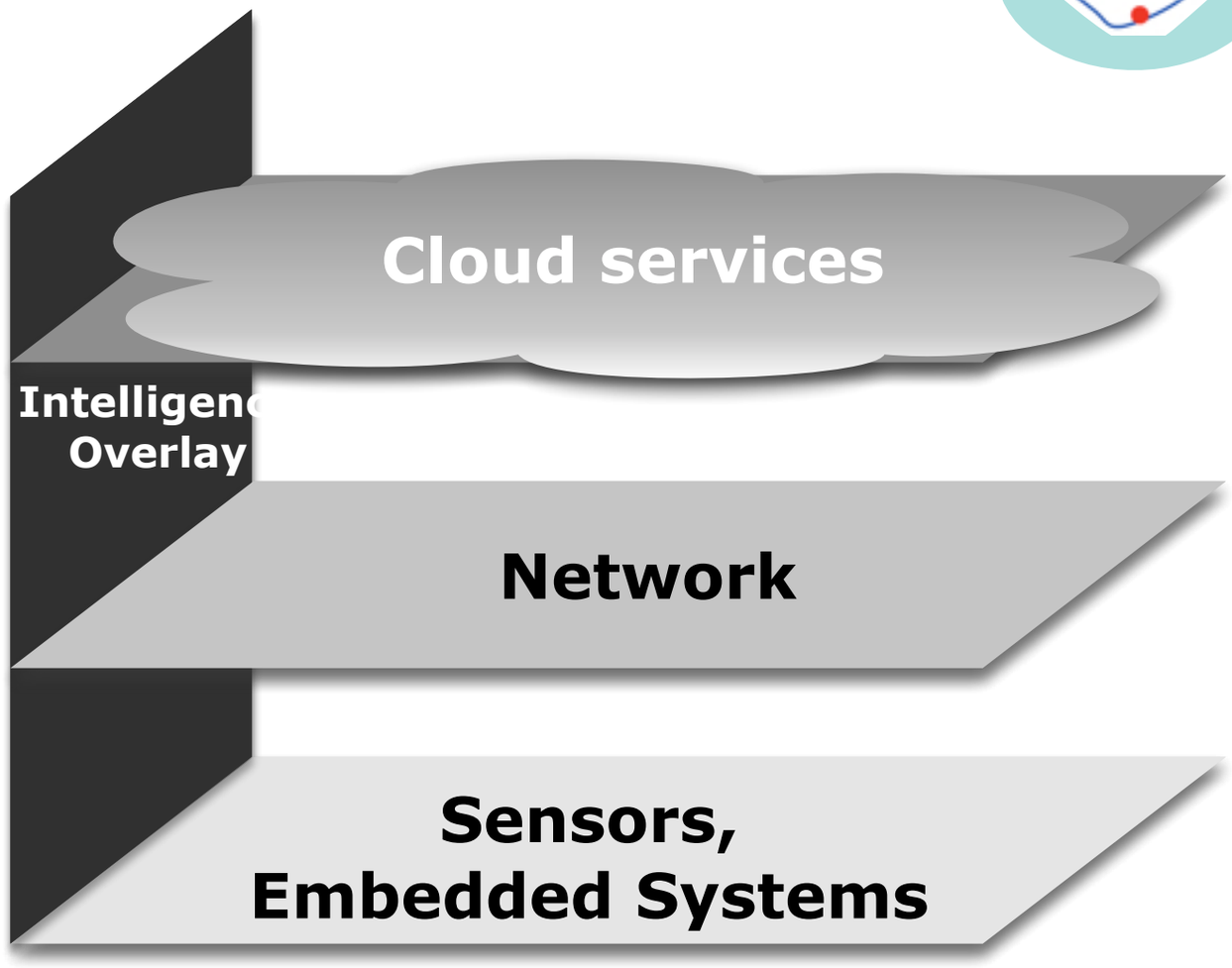
- Threat analysis
- Goal definition
- Semantic security description
- Semantic system description
- Security composability

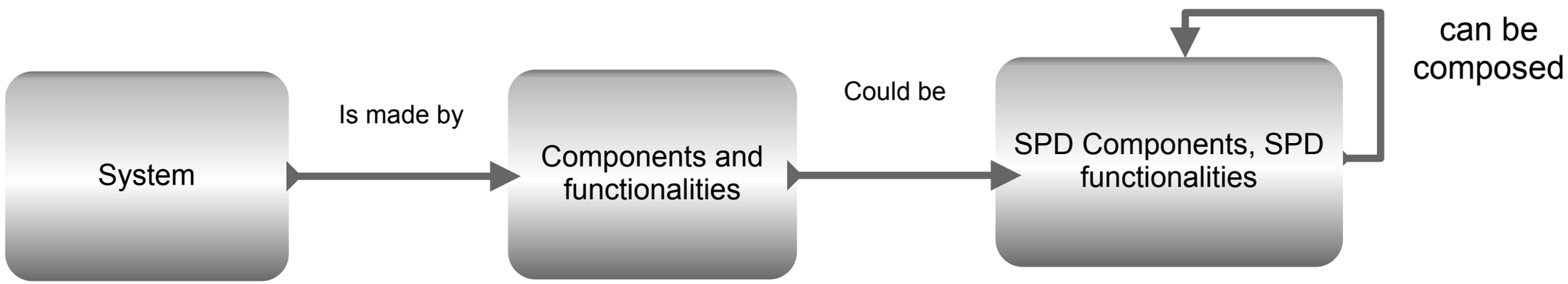


http://newSHIELD.eu

newSHIELD.eu approach

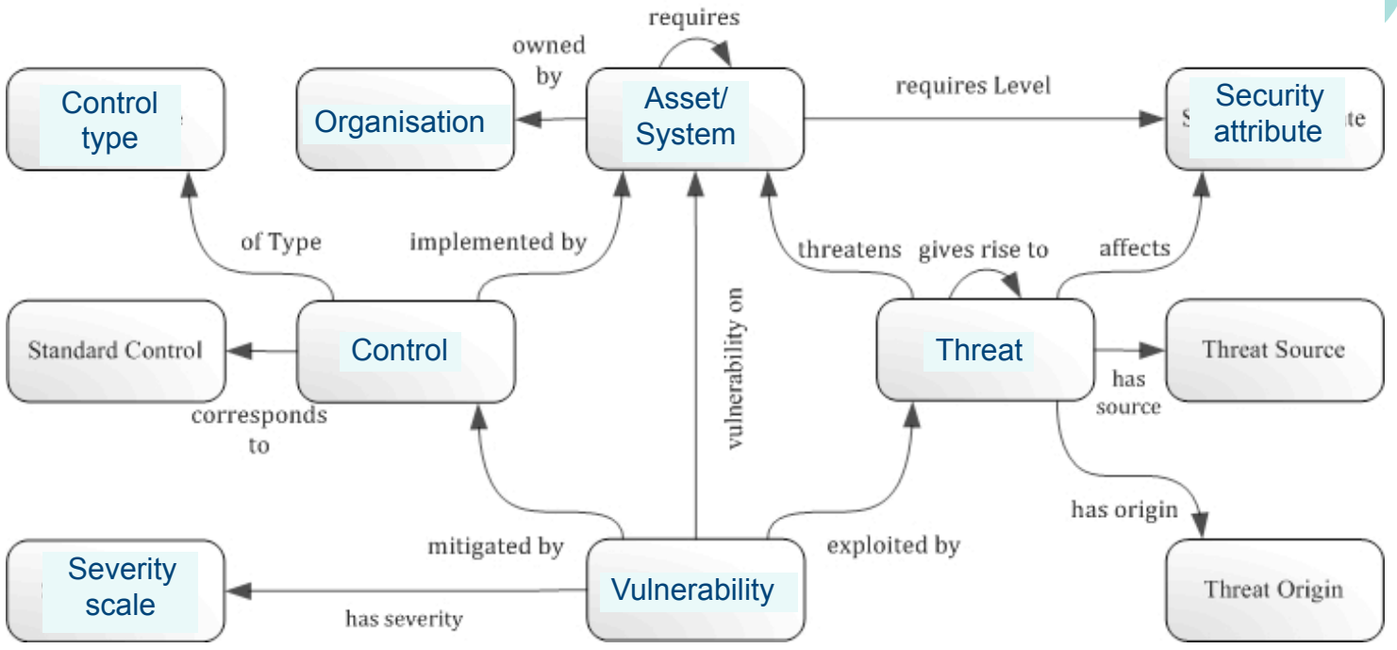
- Security, here
  - security (S)
  - privacy (P)
  - dependability (D)
- across the value chain
  - from sensors to services
- measurable security





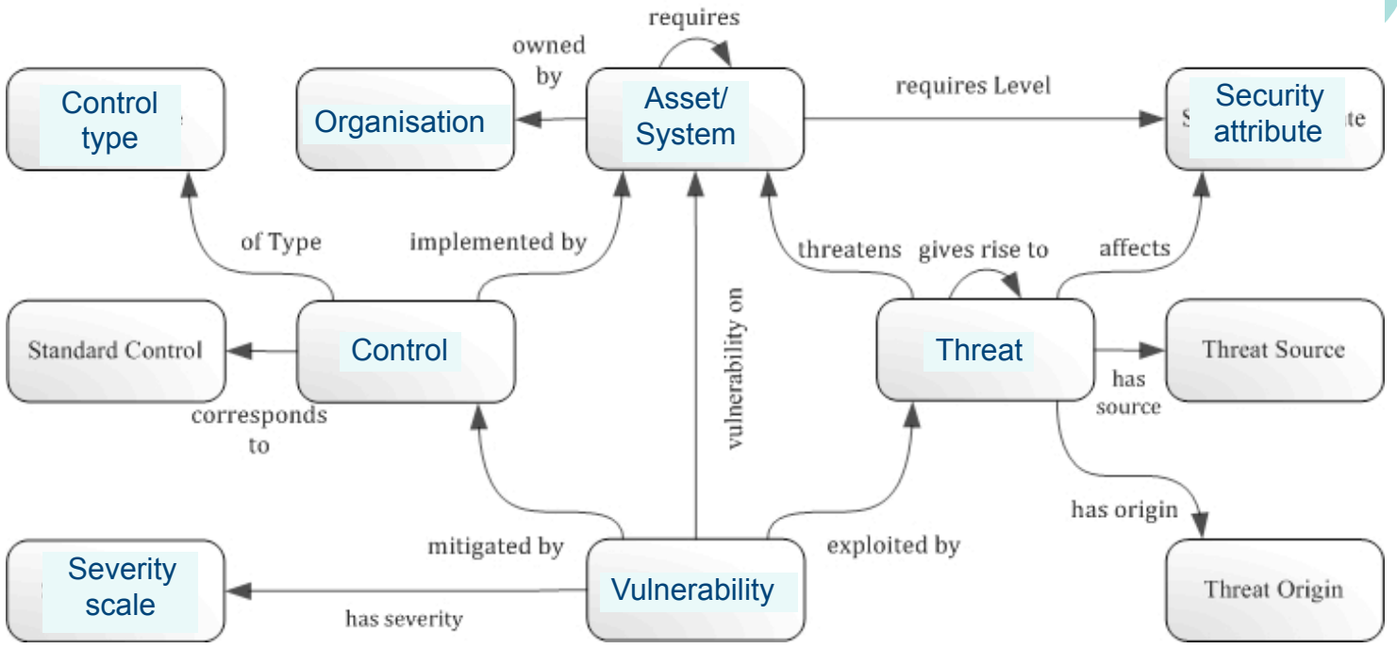
Limitations of the traditional approach

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



Limitations of the traditional approach

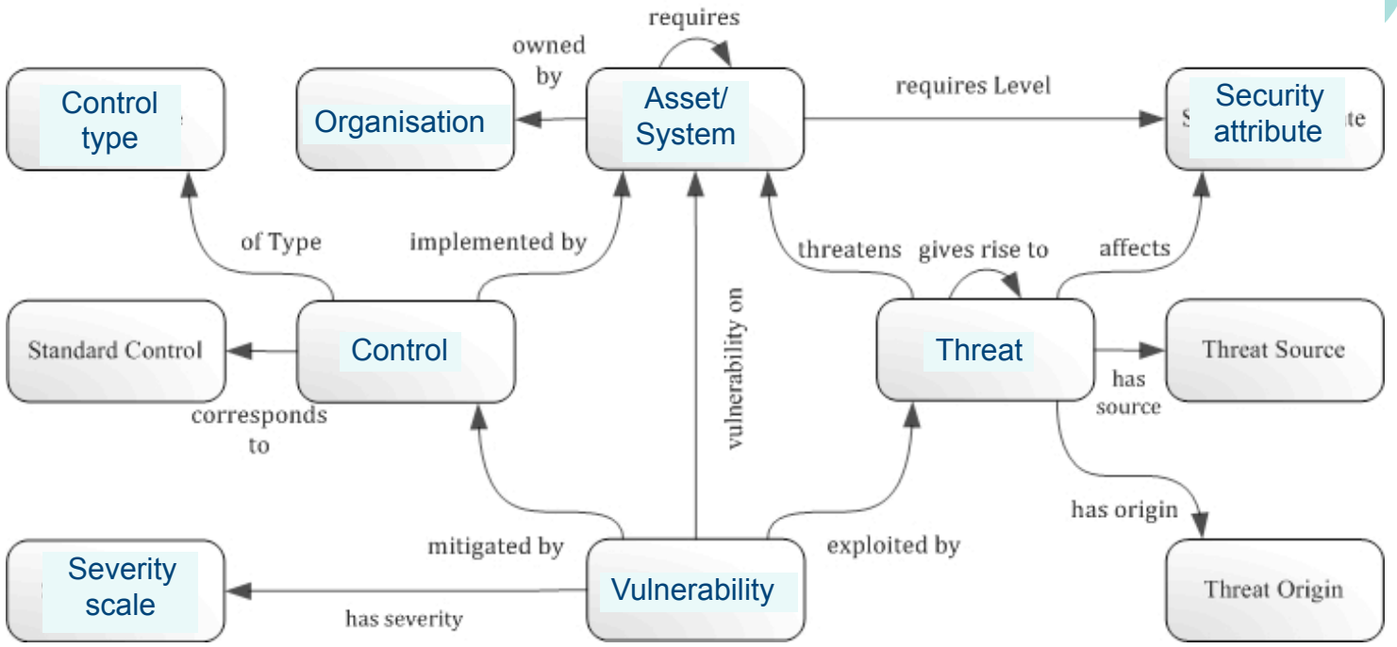
- Scalability
  - Threats
  - System
  - Vulnerability
- System of Systems
  - sensors
  - gateway
  - middleware
  - business processes



Recommendation 1:

Limitations of the traditional approach

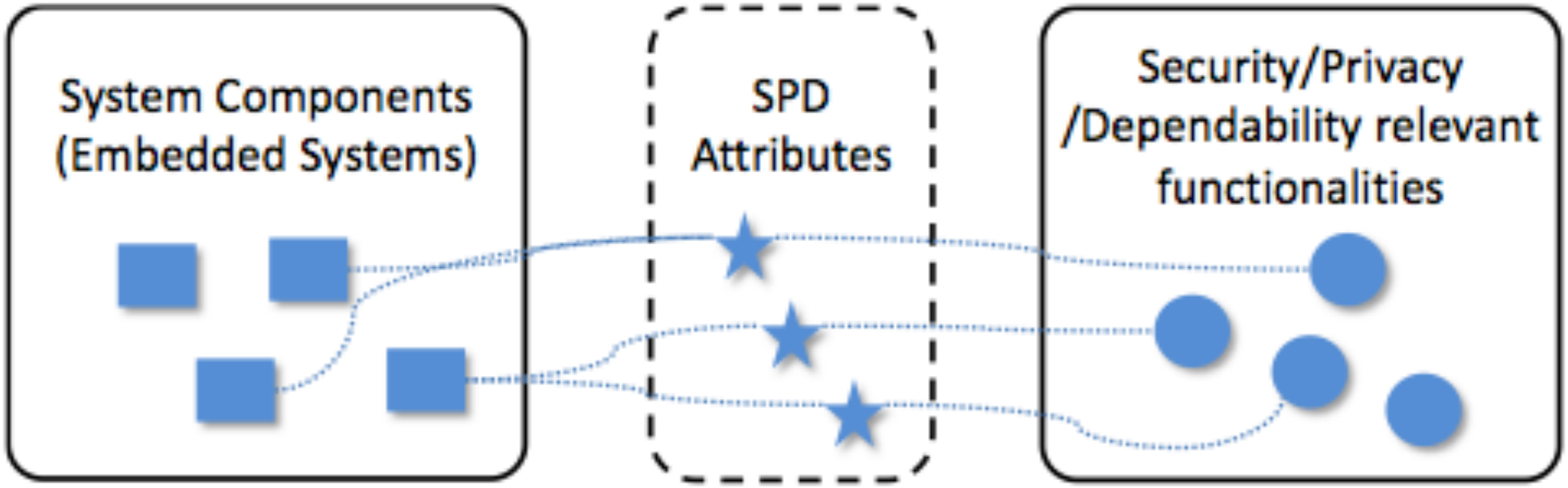
- Scalability
  - Threats
  - System
  - Vulnerability
- System of Systems
  - sensors
  - gateway
  - middleware
  - business processes

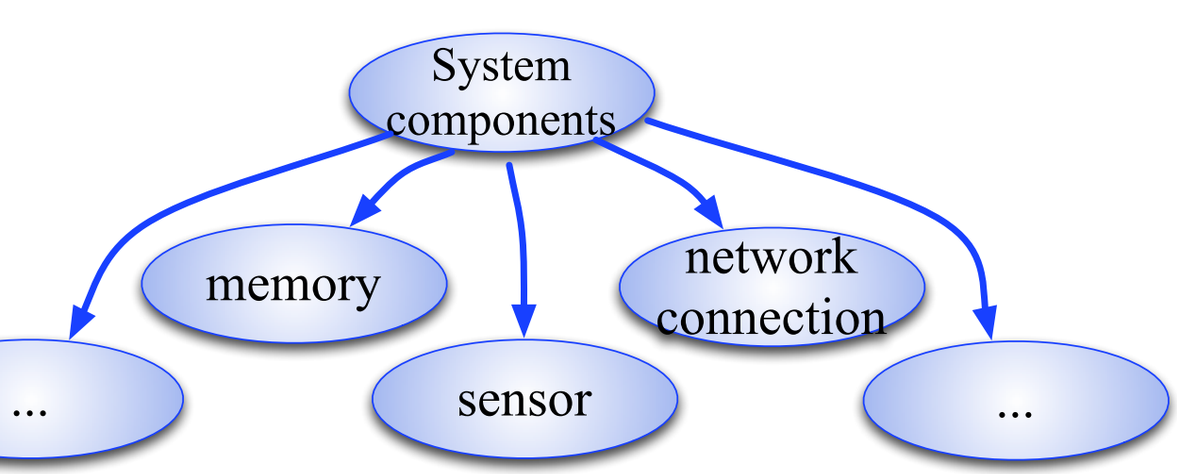


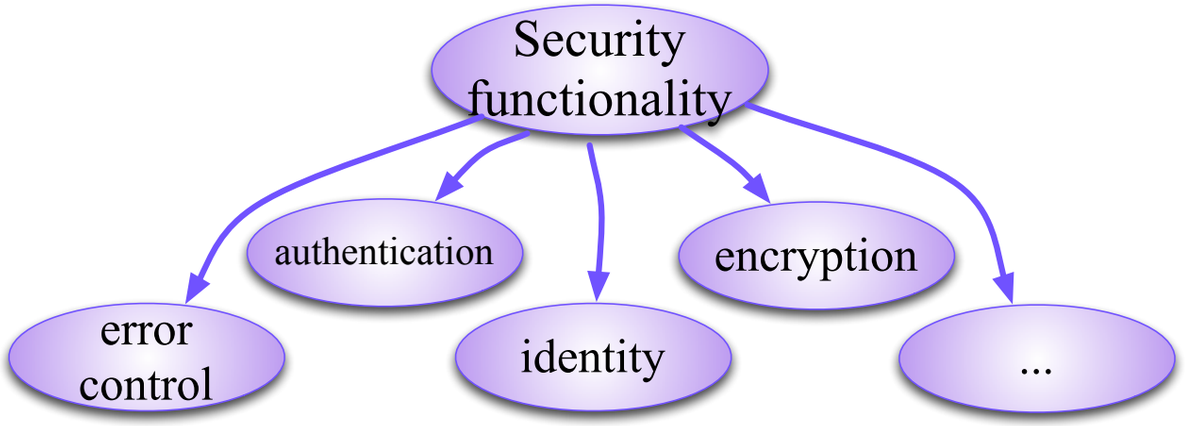
Recommendation 1:

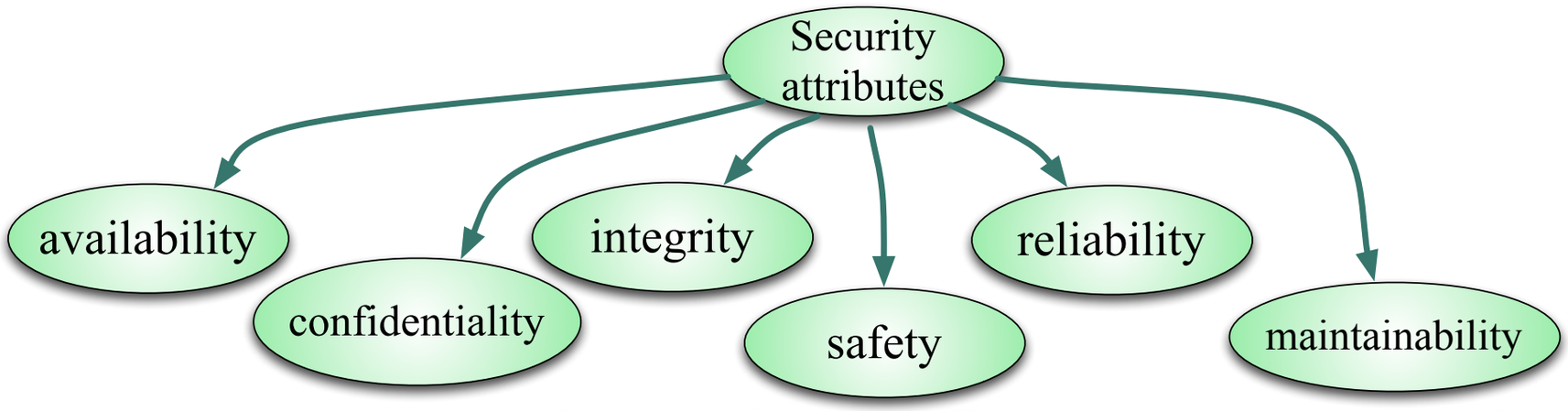
One ontology per aspect:
- security
- system
- threats
...

Security description

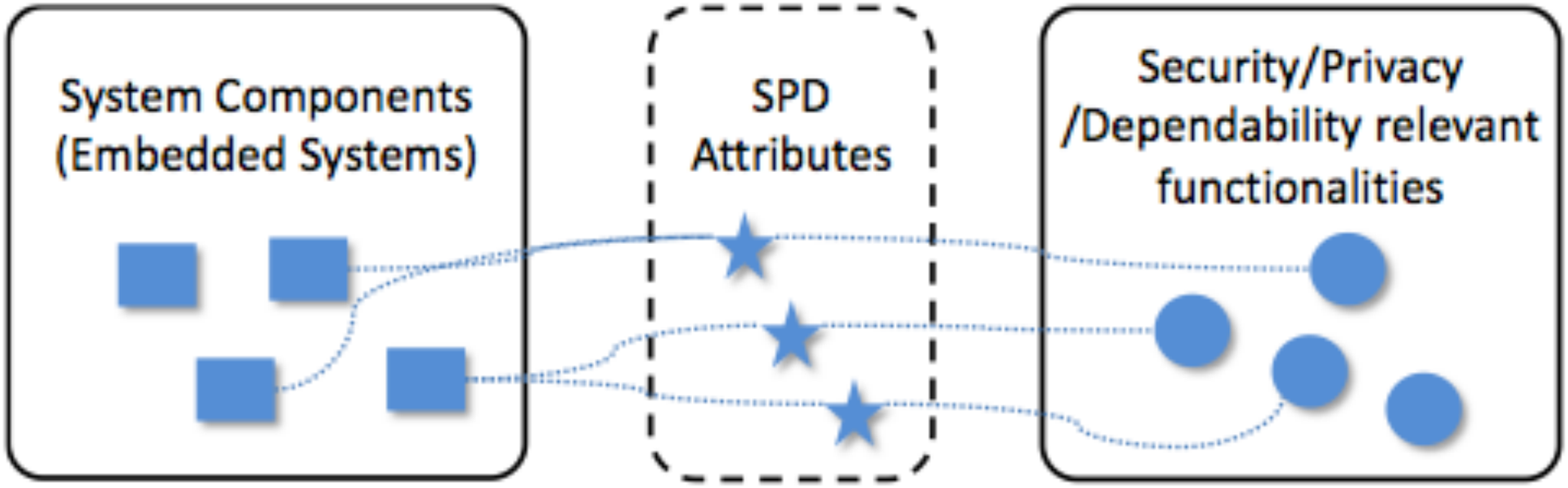


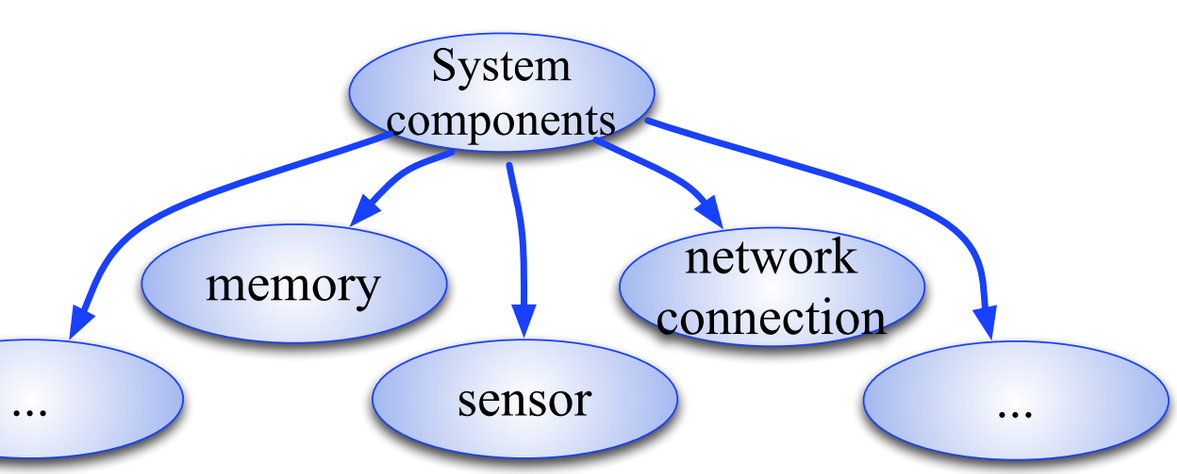


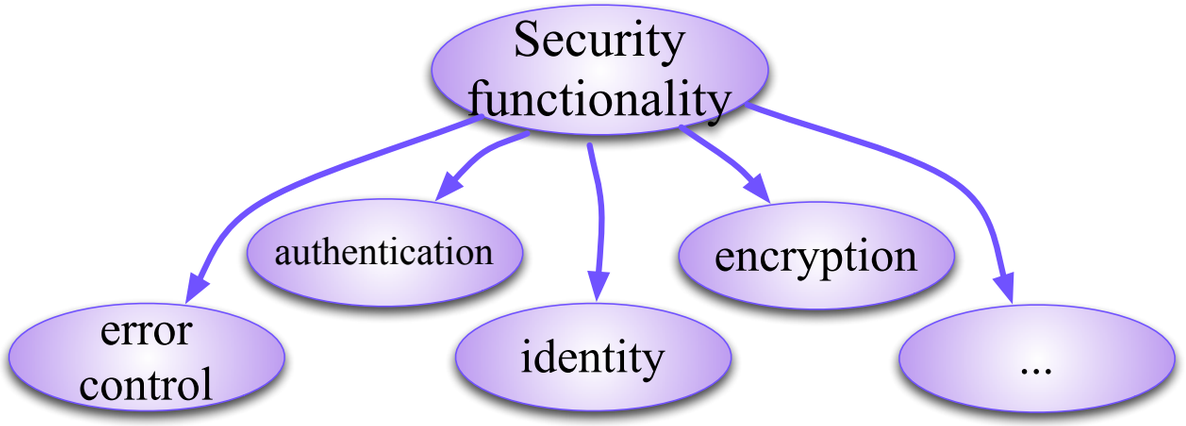


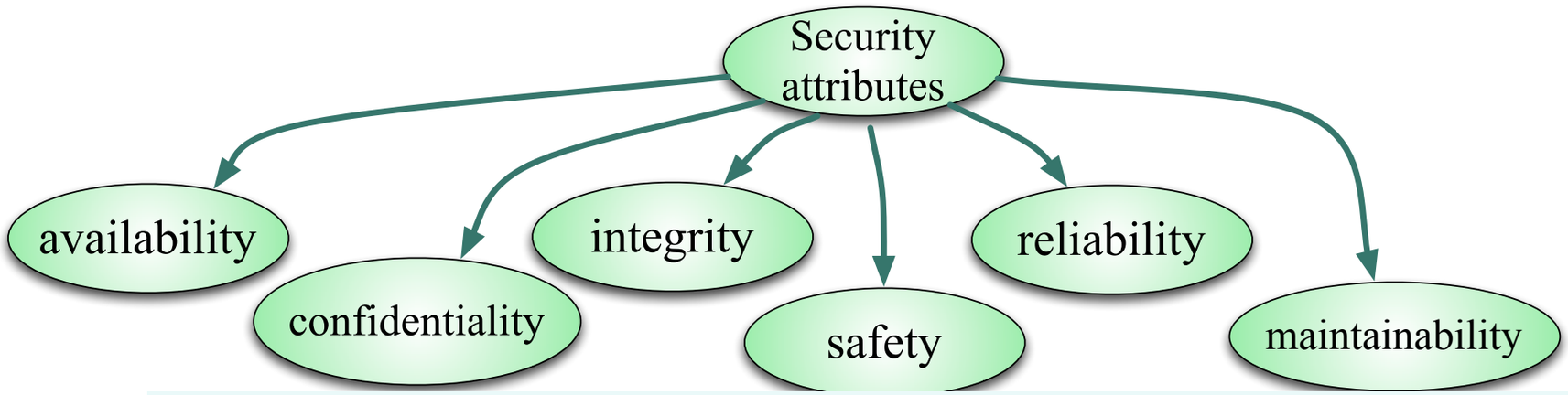


Security description









Recommendation 1: 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 1 - 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

SPD level → SPD attributes → SPD threats

Essential to build

Base of knowledge

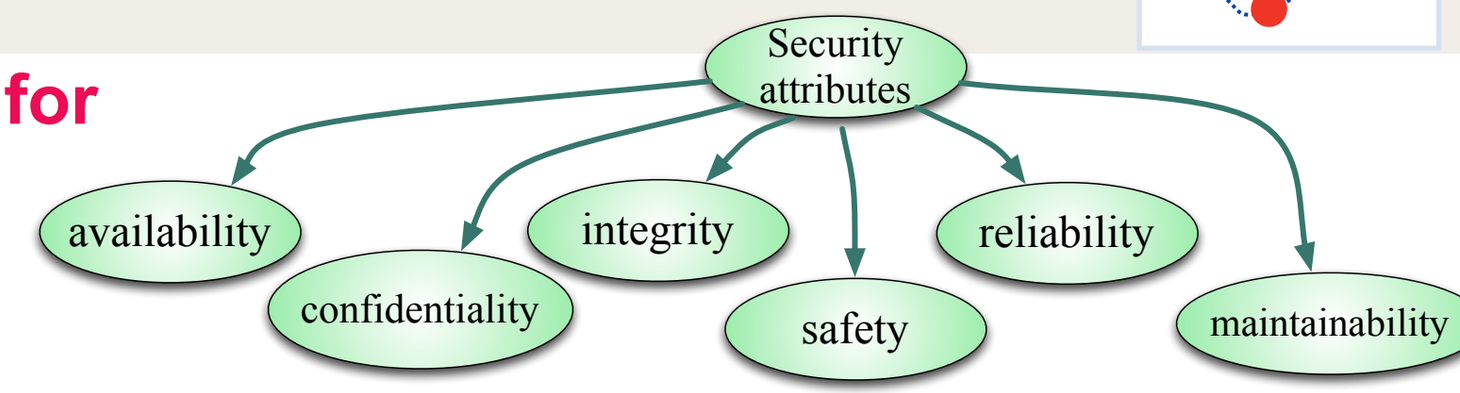
System → Functionality → SPD system

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

SPD = security, privacy, dependability

Semantic Security for Business Intelligence in Oil & Gas

Recommendation 1: ontologies for security, systems, functionality



Open Issue 1: way on how to describe the security goal

availability = 0.8, confidentiality=0.9, integrity=0.6 ⟷ security class = “green”

Open Issue 2: metrics description for threat

universal threat metrics? ⟷ selection of metrics due to application?

Open Issue 3: sensor description

Sensor/Device System description?

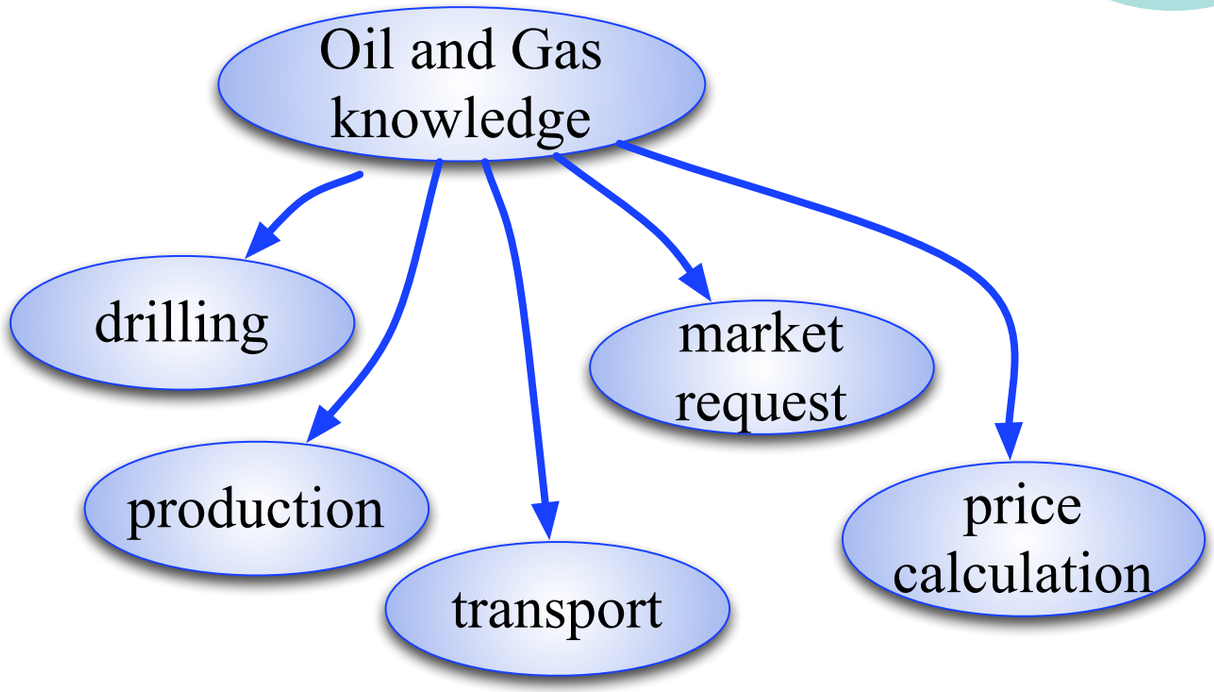
SensorML

Semantic Sensor Network (SSN) ontology

SenML

Semantic attribute based (S-ABAC)

- Access to information
  - Sensor, Person, Service
- OWL & SWRL implementation
- Rules inferring security tokens



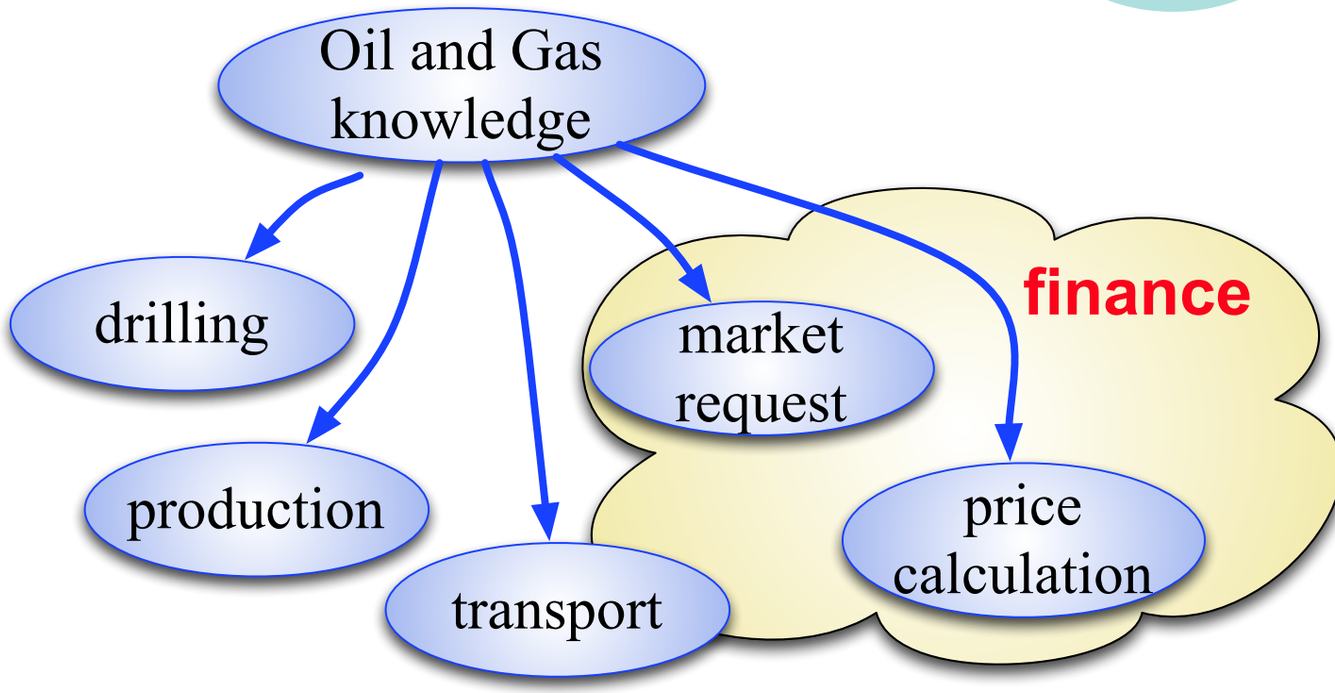
Attributes: roles, access, device, reputation, behaviour, ...

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

[token]	principal
BasicToken_1	Carol
BasicToken_2	Alice

Semantic attribute based (S-ABAC)

- Access to information
  - Sensor, Person, Service
- OWL & SWRL implementation
- Rules inferring security tokens



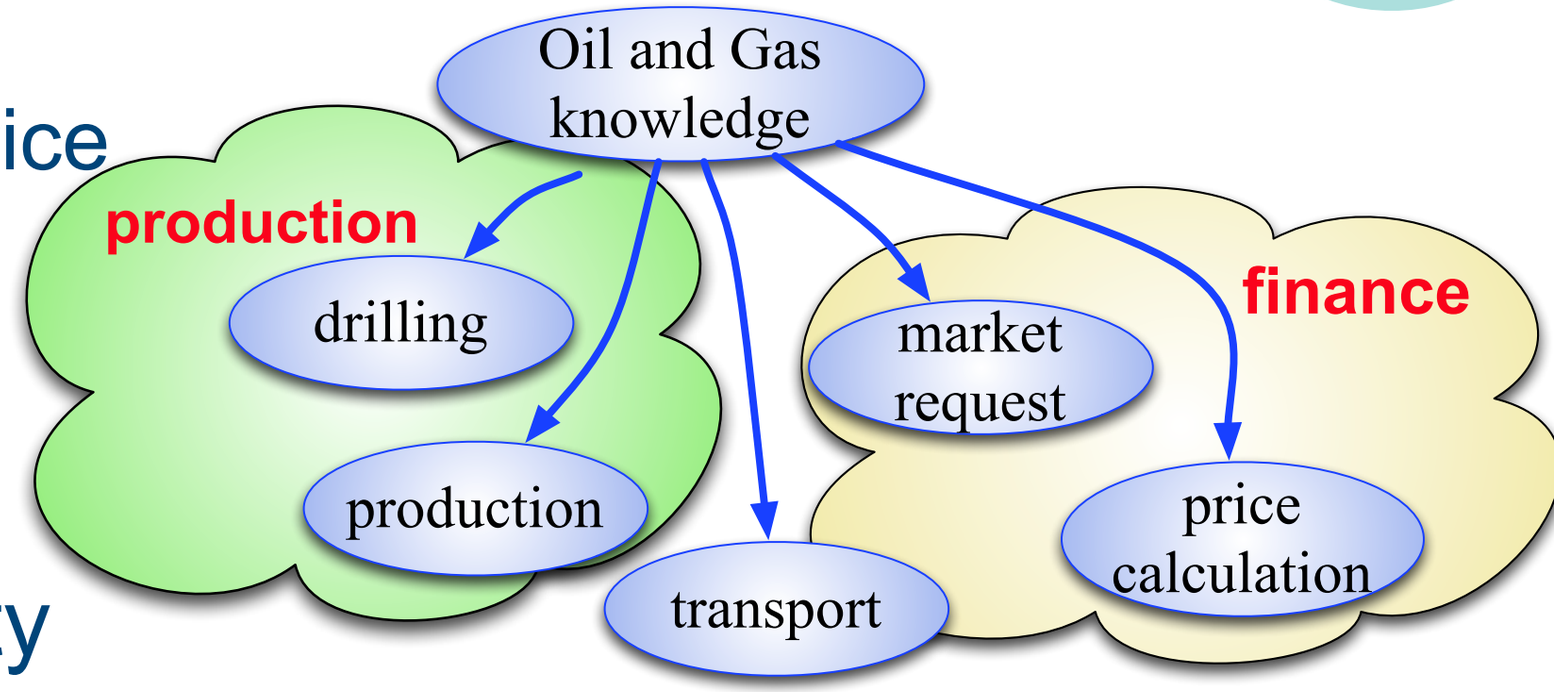
Attributes: roles, access, device, reputation, behaviour, ...

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

[token]	principal
BasicToken_1	Carol
BasicToken_2	Alice

Semantic attribute based (S-ABAC)

- Access to information
  - Sensor, Person, Service
- OWL & SWRL implementation
- Rules inferring security tokens



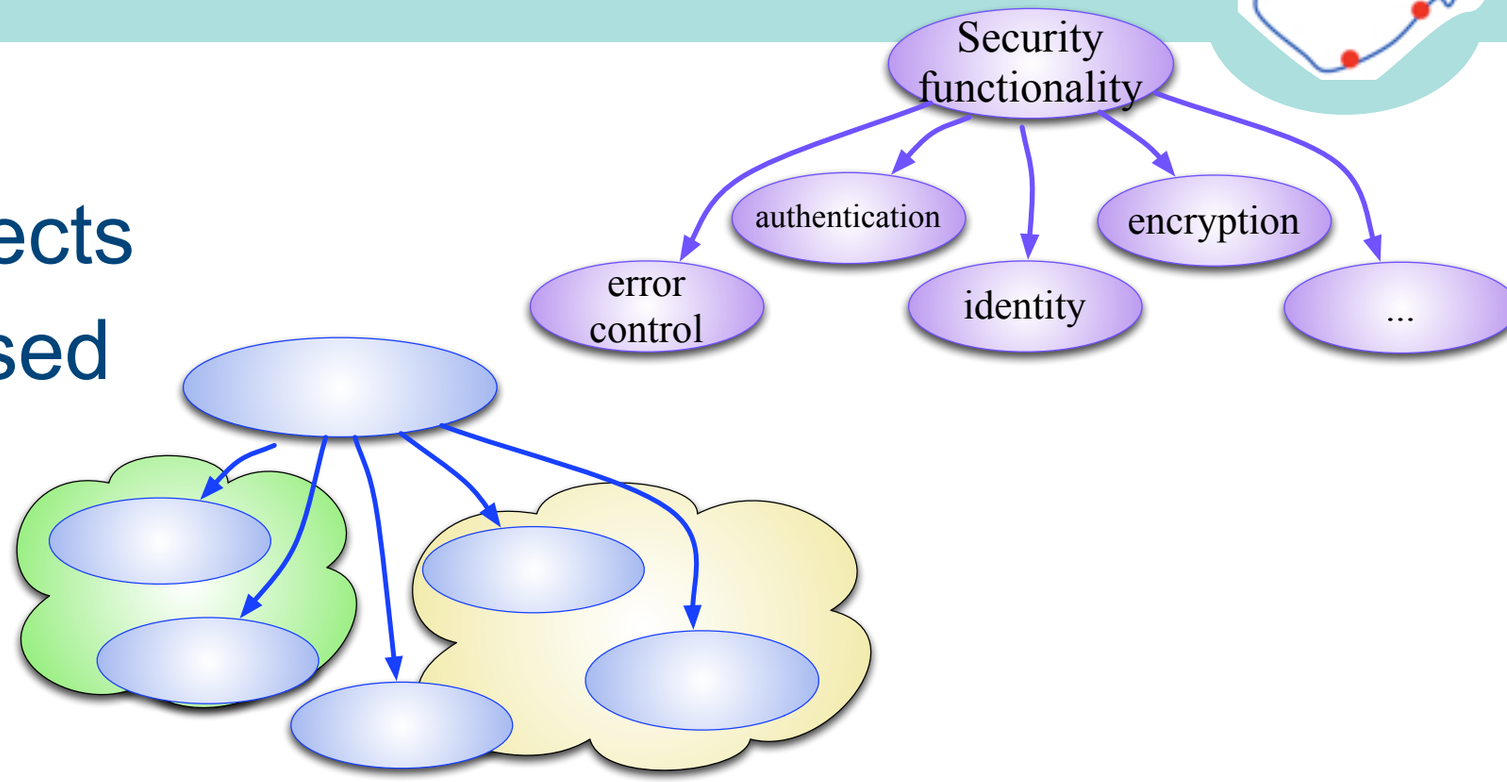
Attributes: roles, access, device, reputation, behaviour, ...

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

[token]	principal
BasicToken_1	Carol
BasicToken_2	Alice

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?

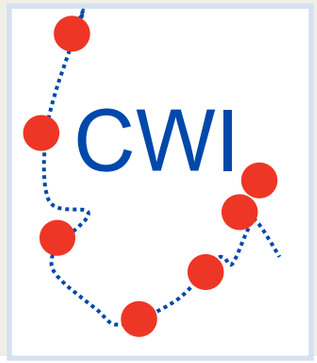
SensorML

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

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