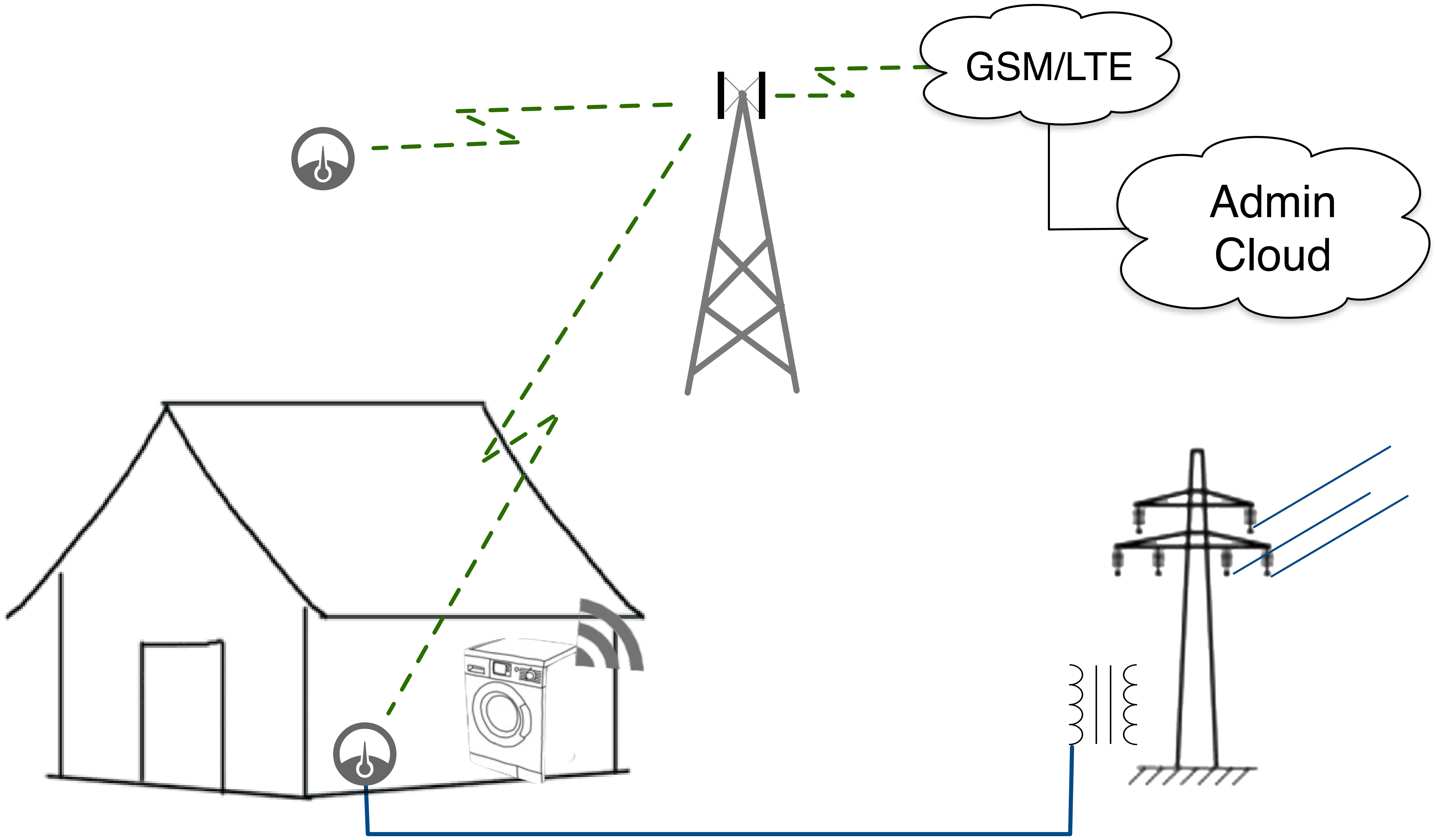
UNIVERSITY OF OSLO

TEK5530 Measurable Security for the Internet of Things

L4 Security Semantics



Josef Noll
Professor
Department of Technology Systems

Overview

- Learning outcomes
- Recap: technology mapping
- Service requirements
  - Functional Requirements
  - Non-functional requirements
  - Security requirements
- Semantic technologies
  - why Semantics
  - elements of semantics
  - examples
- Security Ontologies
  - traditional view
  - Application-oriented view
- Map Security, Privacy, Dependability
- Conclusions

Expected Learning outcomes

Having followed the lecture, you can

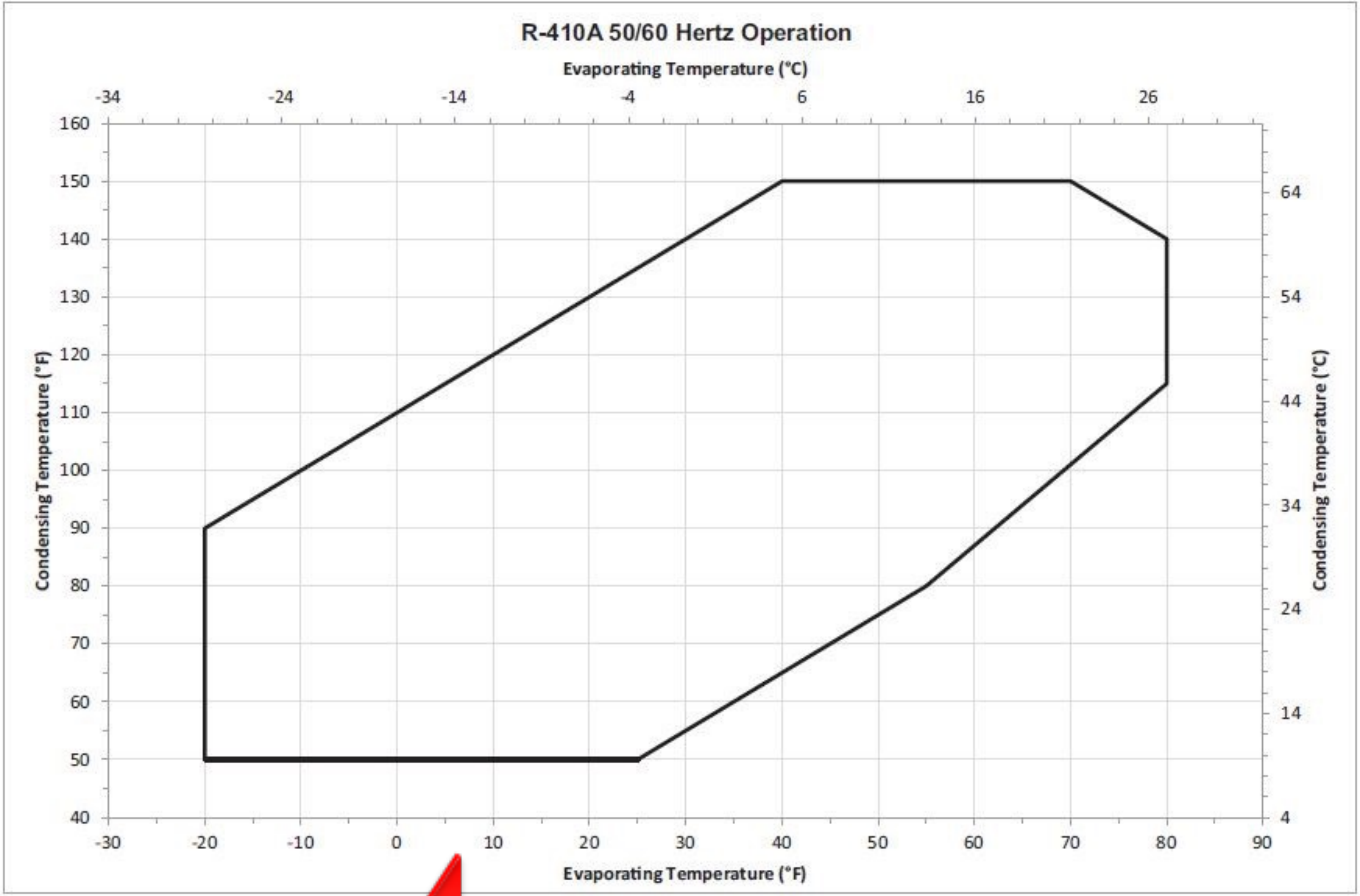
- explain components of the Smart Grid (AMS) System of Systems
- can explain the difference between functional, non-functional and security components
- provide examples of security challenges in IoT
- explain the difference between the web, the semantic web, web services and semantic web services
- explain the core elements of the Semantic Web
- apply semantics to IoT systems
- provide an example of attribute based access control
- discuss the shortcomings of the traditional threat-based approach
- list the main elements of the semantic descriptions of s,p,d functionalities
- perform a semantic mapping of s,p,d attributes

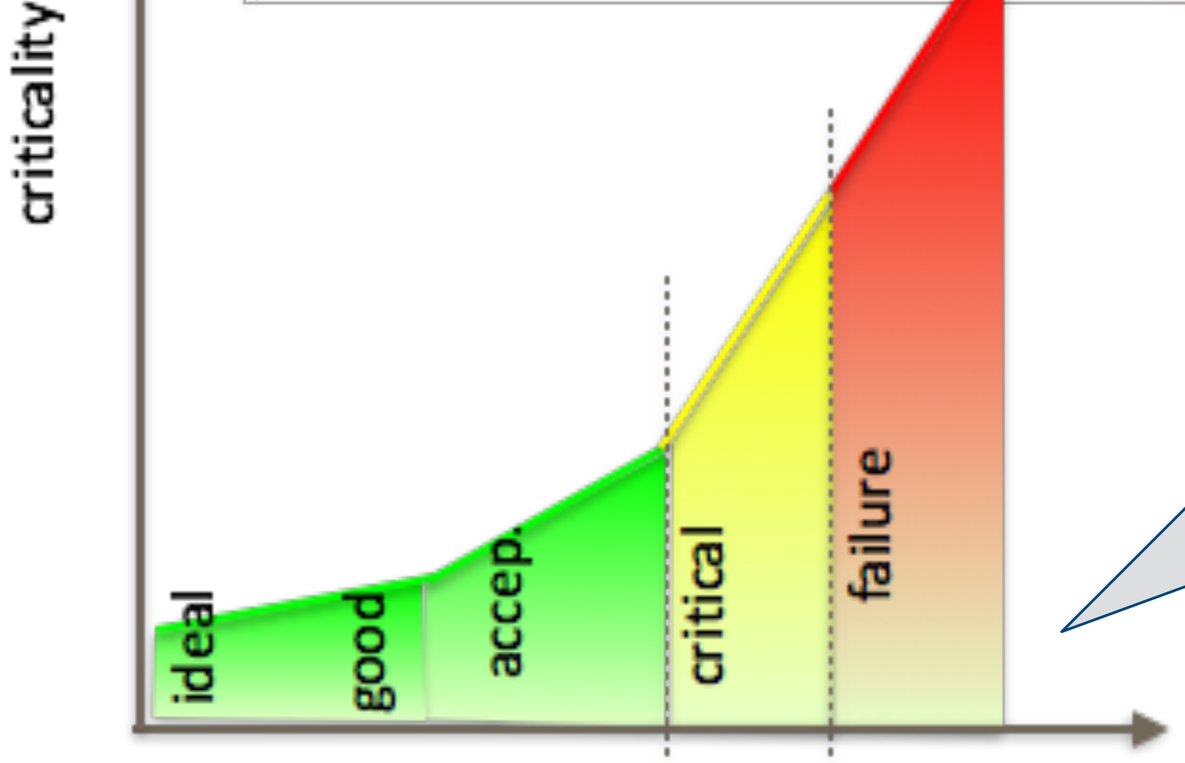
Service Requirements

- Functional Requirements,
  - e.g. report a value
- Non-functional requirements,
  - e.g. perform the operation in less than 0,5s
- Security requirements
  - e.g. ensure the confidentiality of the data

Recap: Conversion and operating envelope

- Operating envelope: the operational parameters where our network can work “well”, depends on the technology and on the task
- For traffic estimation we need it in ”communication” QoS
  - Bandwidth, delay, jitter, (redundancy)
- Often can be done with simple arithmetic with a certain confidence level

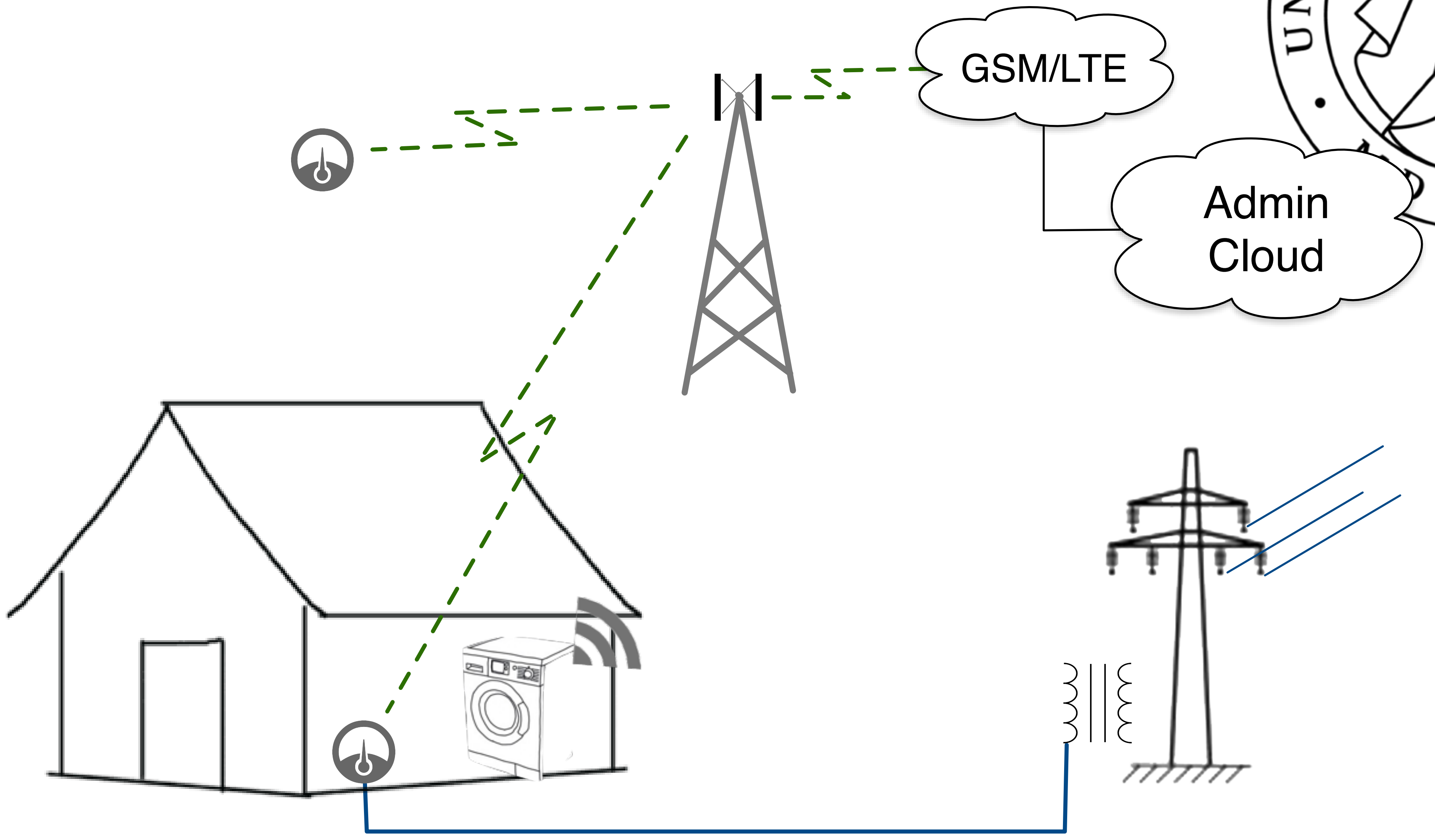


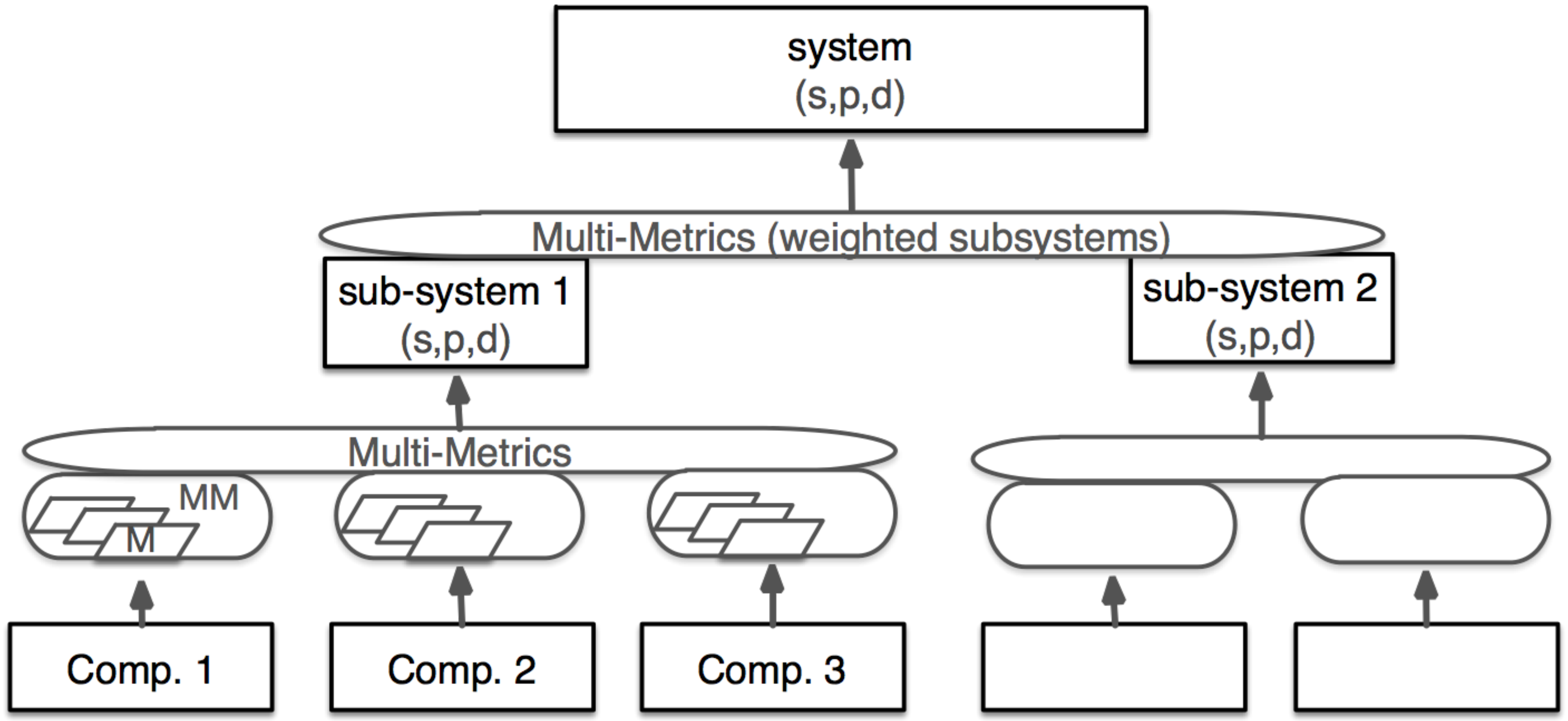


1) How does he Operating Envelope look like applying criticality?
2) How can the criticality be applied for SPD?

Example:
System of Systems

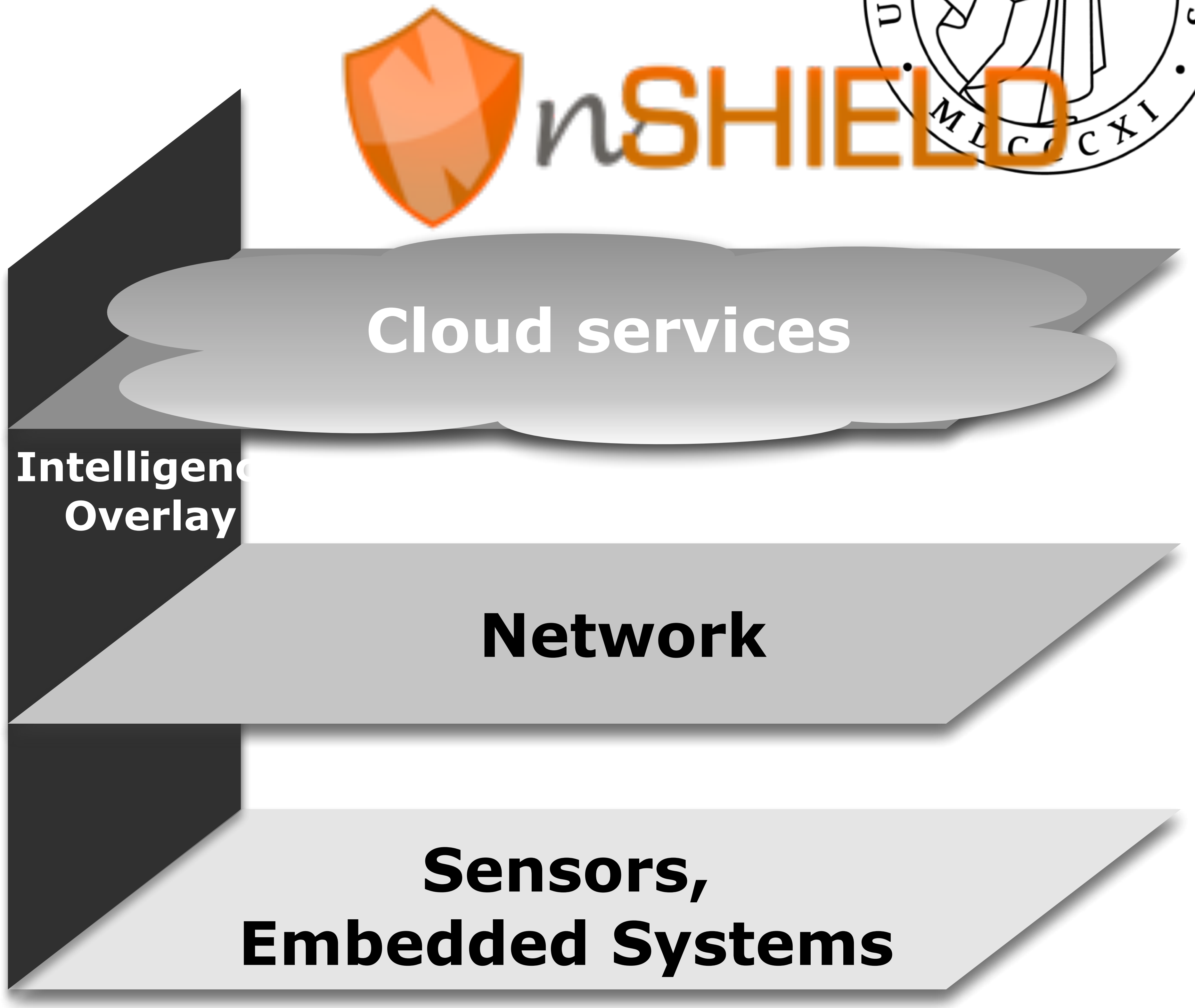
- A system consists of sub-systems
  - Example: Automatic Meter System (AMS) consists of reader (AMR), aggregator, communications, storage, user access
- A sub-system consists of sub-…-system
  - Example: AMR consists of power monitor, processing unit, communication unit
- A sub-….-system consists of components
  - Ex: AMR communication contains of a baseband processing, antenna, wireless link
- Components have parameters
  - Wireless link component: f=868 MHz, output power=?, Encryption=?

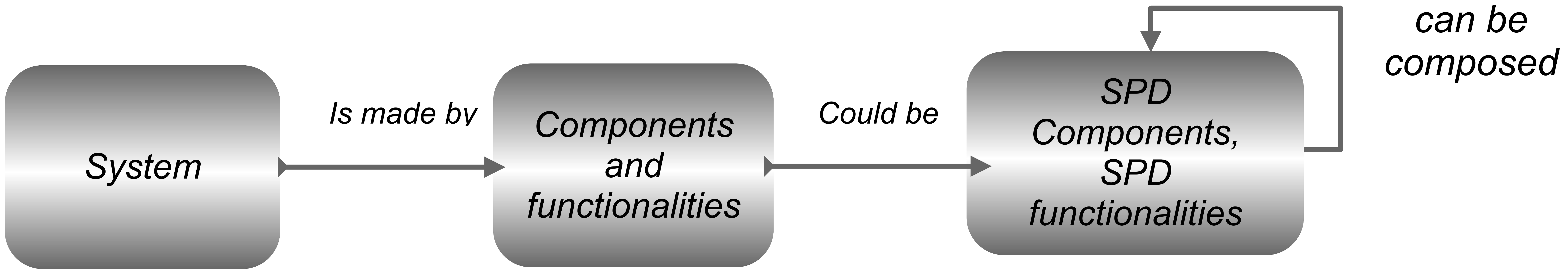




newSHIELD.eu approach

- ➡ Security approach by JU Artemis
  - Industry, National and EU supported (JU) activities
  - special focus on sensor systems
- ➡ 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

Examples of
Security challenges in the IoT

- **System**: Intrusion awareness, fault-tolerance, data redundancy and diversity
- **Platform**: Auto start up on power failure, Auto reconfigurable on software failure, Auto synchronization on software failure, End-to-end secure communication, Mal-user detection, Access control for accessing sensor data
- **Middleware**: SPD Audit, Cryptographic Support, Identification and Authentication, Protection of the SPD functionalities, Security Management
- **Hardware**: SPD metrics, Self-recovery from hardware transient faults (through fault-injection), Auto-reconfiguration, Data encryption, Provision of security and privacy services, data encryption/decryption
- **Radio**: Threats tolerant transmission

System components

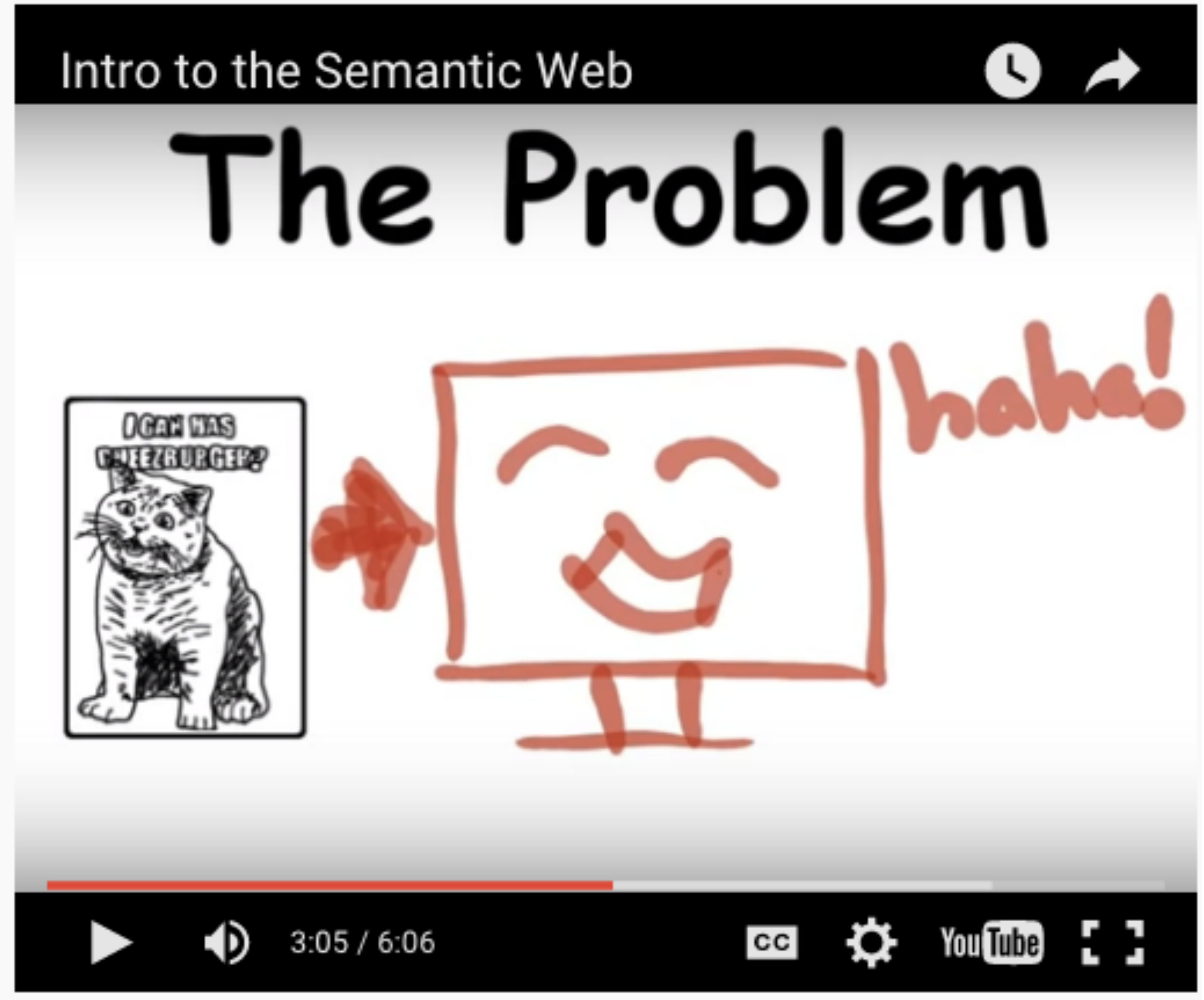
classified after objective

- Functional components
  - input component (sensors, keyboard, mouse,..)
  - output component (alarm, screen, actuator,..)
  - processing component
  - Storing component (data base, files,)
  - Connection (wireless connection, wired connection)
- Security, Privacy, Dependability (SPD) components:
  - Encryption: Encryption algorithm, keys,..
  - Protocols
  - Authentication(mechanism (fingerprint, password, password complexity,.....) .
  - Authorization (privileges, ..)
- Management components (OS, Web server, data server)
- Human component (admin, user, ..).
- Physical component, car being a component in a car factory. (if treated as "sub-system)

Semantic technologies

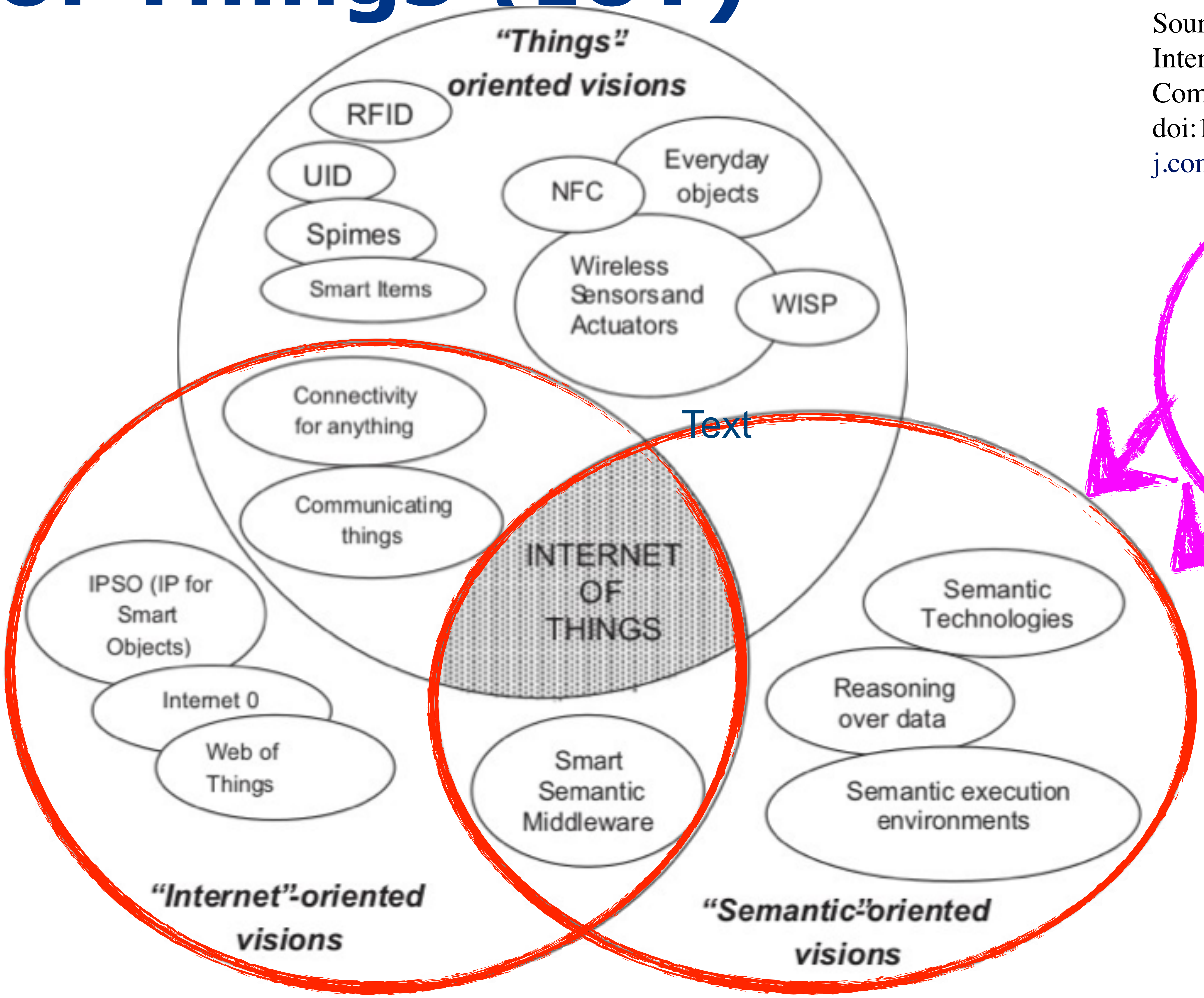
- ➡ why Semantics?
- ➡ Elements of semantics
  - https://youtu.be/OGg8A2zfWKg

- ➡ Watch the video (6 min) then we discuss your impressions



The Semantic Dimension of the Internet of Things (IoT)

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
Text
Smart Semantic Middleware
Semantic Technologies
Reasoning over data
Semantic execution environments
"Internet"-oriented visions
"Semantic"-oriented visions

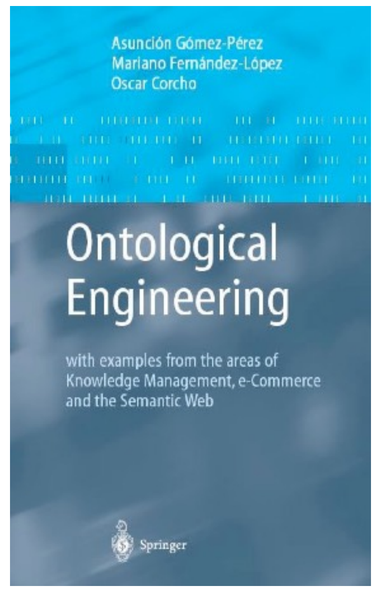
* security
* privacy
* dependability
  - context
  - content
* personalised

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

Why Semantics?

- Syntax vs. Semantics

Arab



الاسم: الهندسة فعلم التطو ر

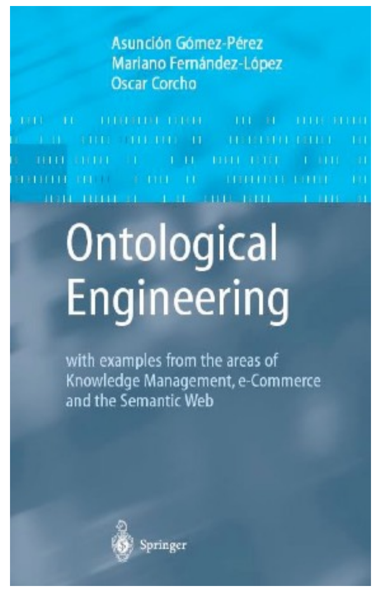
المؤلّفون: آسنسيون غومزبرز

السّعر: $74.95

الكتاب **:المنتج**

```
الاسم>الهندسة فعلم التطو ر </الاسم>>
<<المؤلّفون>آسنسيون غومزبرز </المؤلّفون
السّعر>$74.95</السّعر>>
<<الكتاب>المنتج </الكتاب
```

English



Title: Ontological Engineering
Authors: Asunción Gómez-Pérez...
Price: $74.95
Product: Book

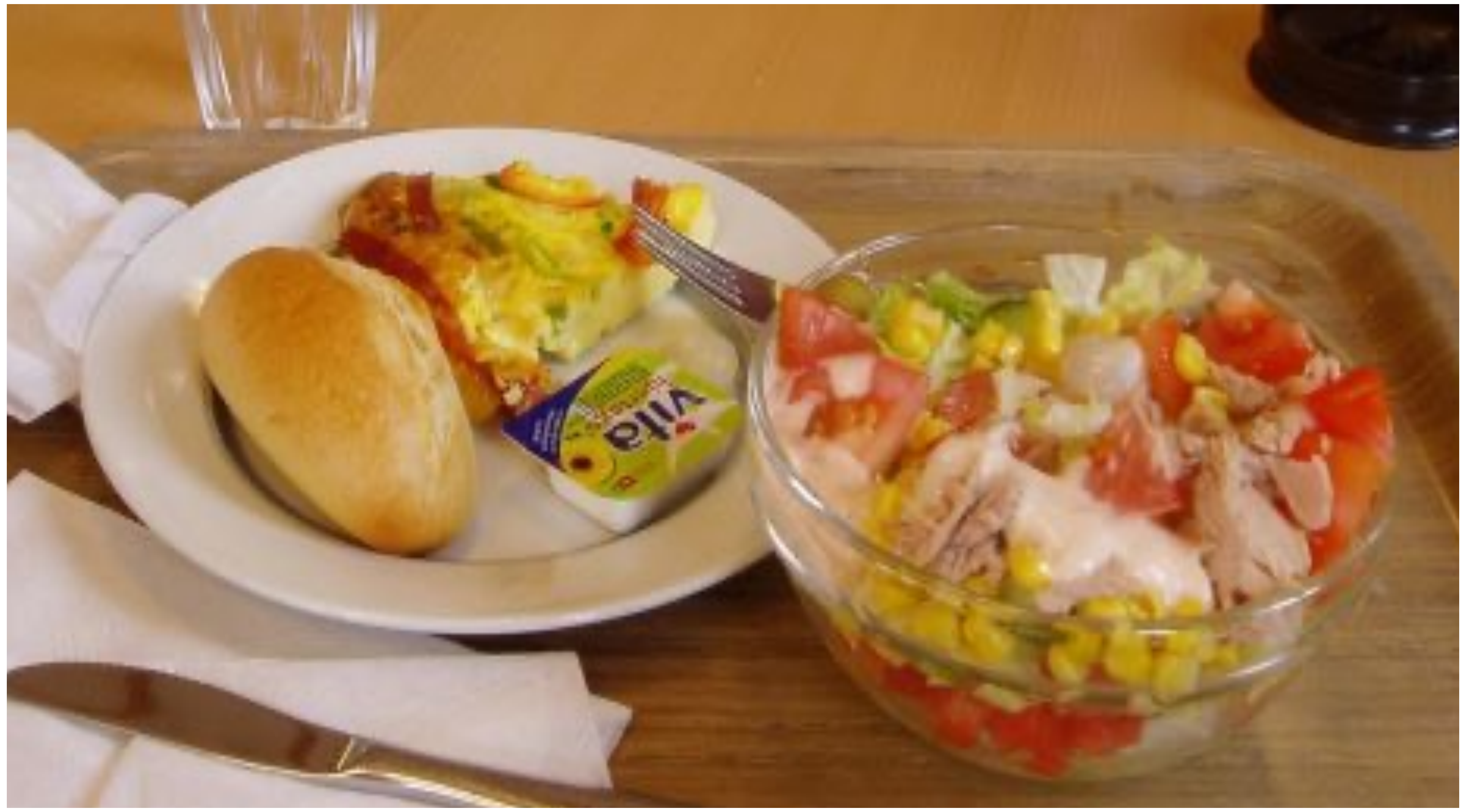
```
<Title>Ontological Engineering</Title>
<Author>Asunción Gómez-Pérez...</Author>
<Price>$74.95</Price>
<Product>Book</Product>
```

What do the tags mean for the machine?

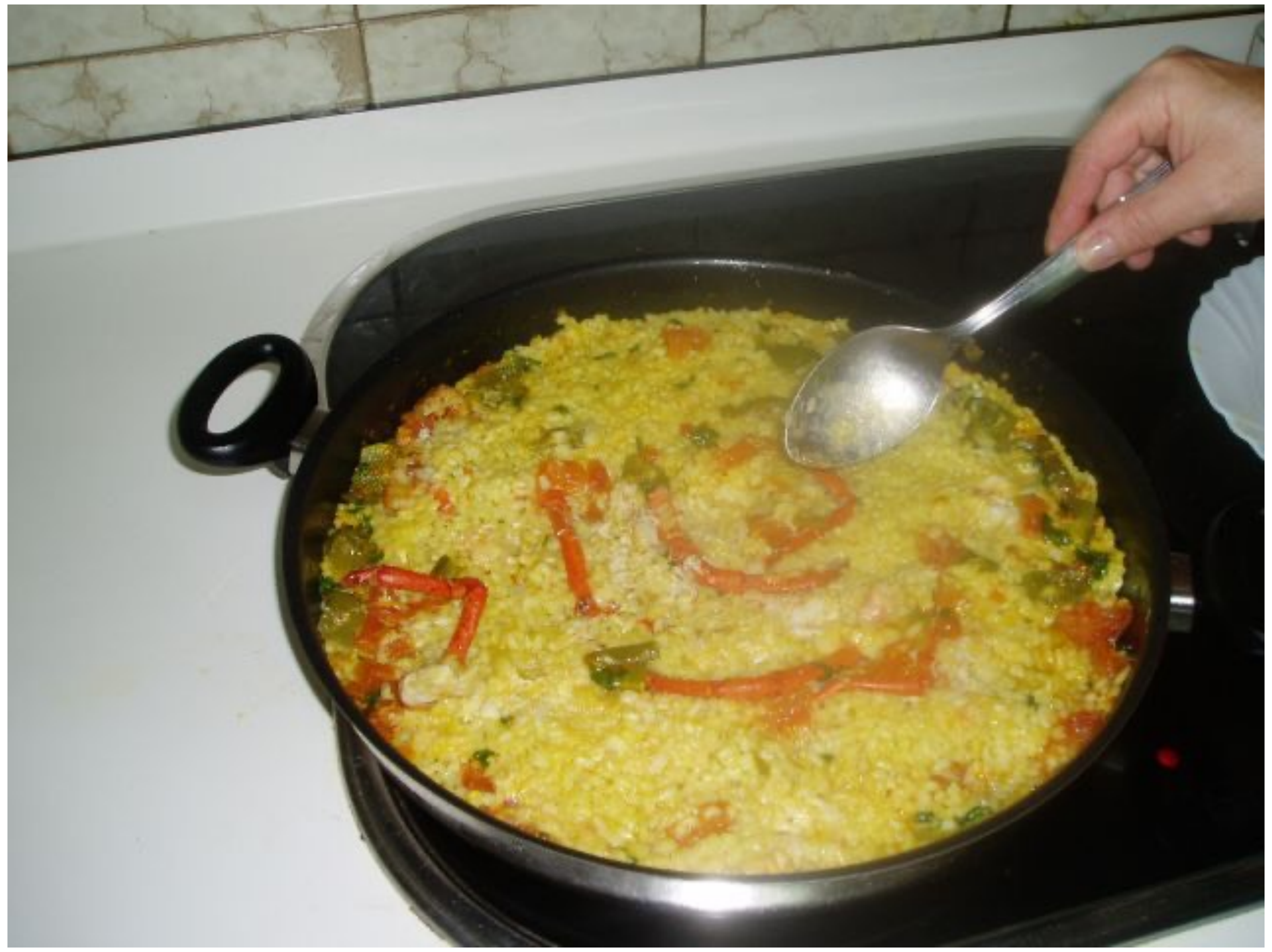
Source: Juan Miguel Gomez, University Carlos III de Madrid

Why Semantics?

- Conceptual Level



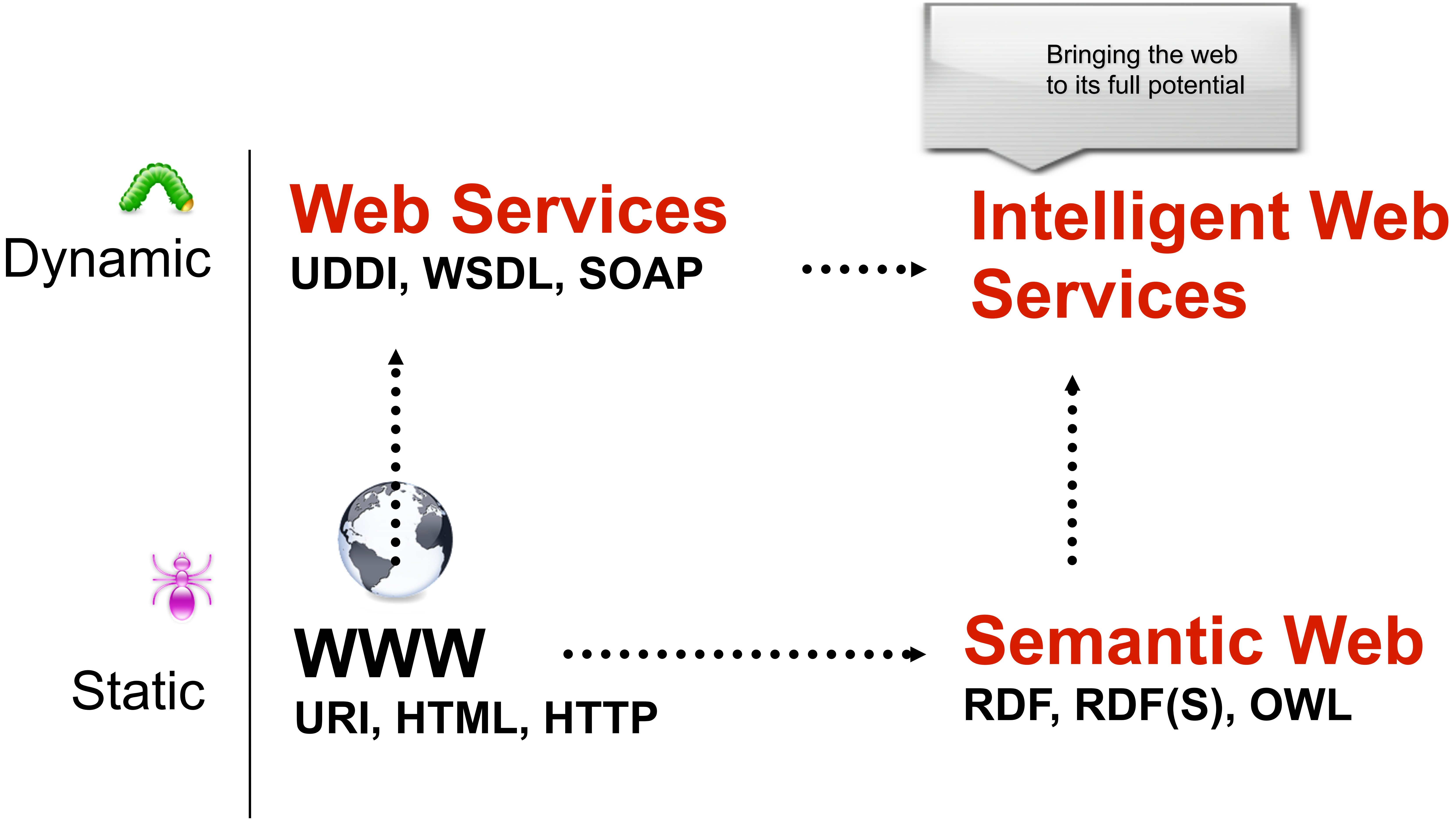
lunch (.no)



lunch (.es)

Source: Juan Miguel Gomez, University Carlos III de Madrid

Semantic Web Services



Bringing the web to its full potential

Source: Juan Miguel Gomez, University Carlos III de Madrid

Requirements for Service Evolution

Web services

- Fixed service set, Static service composition, Low degree of automation
- Poor reliability
- Fixed Service Level Agreement

Semantic Web Services

- Flexible services, easy new services
- Alternative service provision
- Global, dynamic services

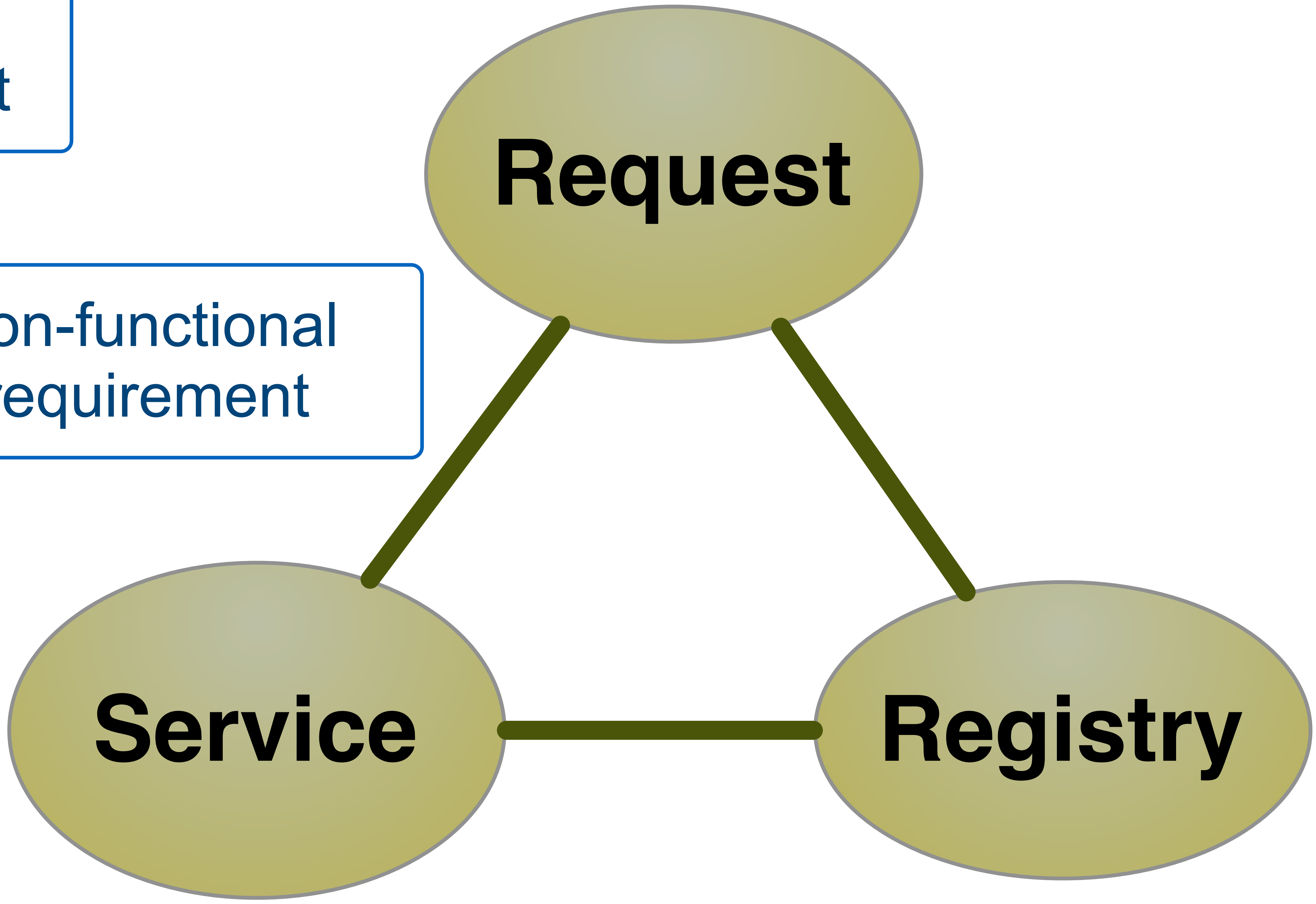
Elements of Web Services

functional requirement

- Service Request
  - want to come to Barcelona University

non-functional requirement

- Services
  - buy a flight ticket (cheap, direct, …)
  - buy a metro/bus ticket



- Service registry
  - link to ticket ordering at norwegian.no

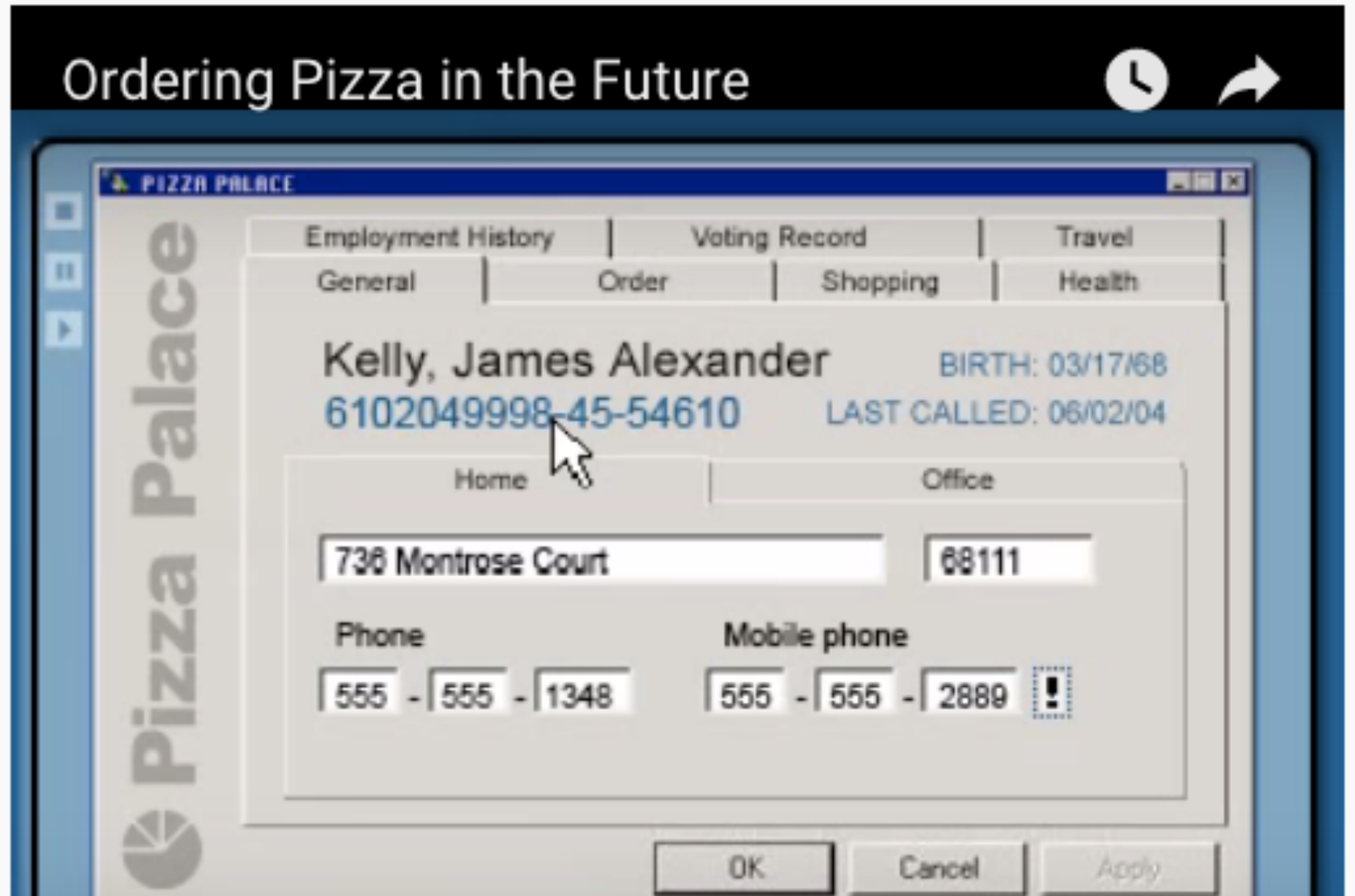
s,p,d requirement

- (Security) - Privacy attribute
  - only use company which does not sell my data

Elements in Semantic Technologies

[Source: Wikipedia]

- Extensible Markup Language (XML) is a markup language that defines a set of rules for encoding documents in a format which is both human-readable and machine-readable.
- RDF - Formal semantics is built upon a W3C XML standard for objects called the Resource Description Framework (RDF)
- OWL - The Web Ontology Language (OWL) is a family of knowledge representation languages for authoring ontologies.
- A semantic reasoner, reasoning engine, rules engine, or simply a reasoner, is a piece of software able to infer logical consequences from a set of asserted facts or axioms.
- Classes (concepts) are abstract groups, sets, or collection of objects (example: human, woman)
- Individuals (instances) are the specific objects, e.g. Josef is a Father
- Attributes (properties) describing objects (individual and classes) in the ontology. Example: Human hasName, Josef has name Josef Noll



Ordering Pizza in the Future

PIZZA PALACE

Pizza Palace

Employment History | Voting Record | Travel
General | Order | Shopping | Health

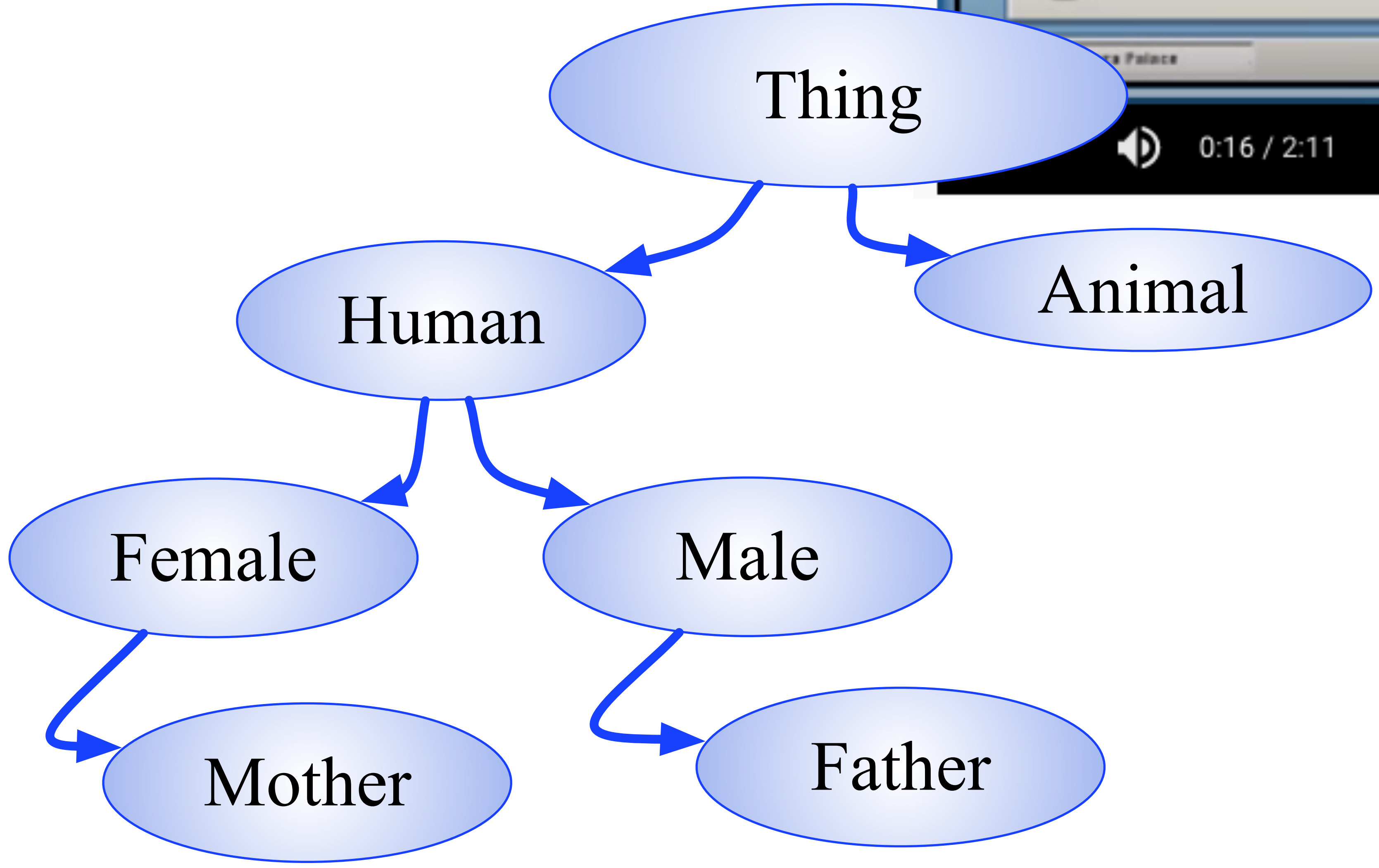
Kelly, James Alexander
BIRTH: 03/17/68
6102049998-45-54610
LAST CALLED: 06/02/04

Home: 736 Montrose Court
Office: 68111

Phone: 555 - 555 - 1348
Mobile phone: 555 - 555 - 2889

OK | Cancel | Apply

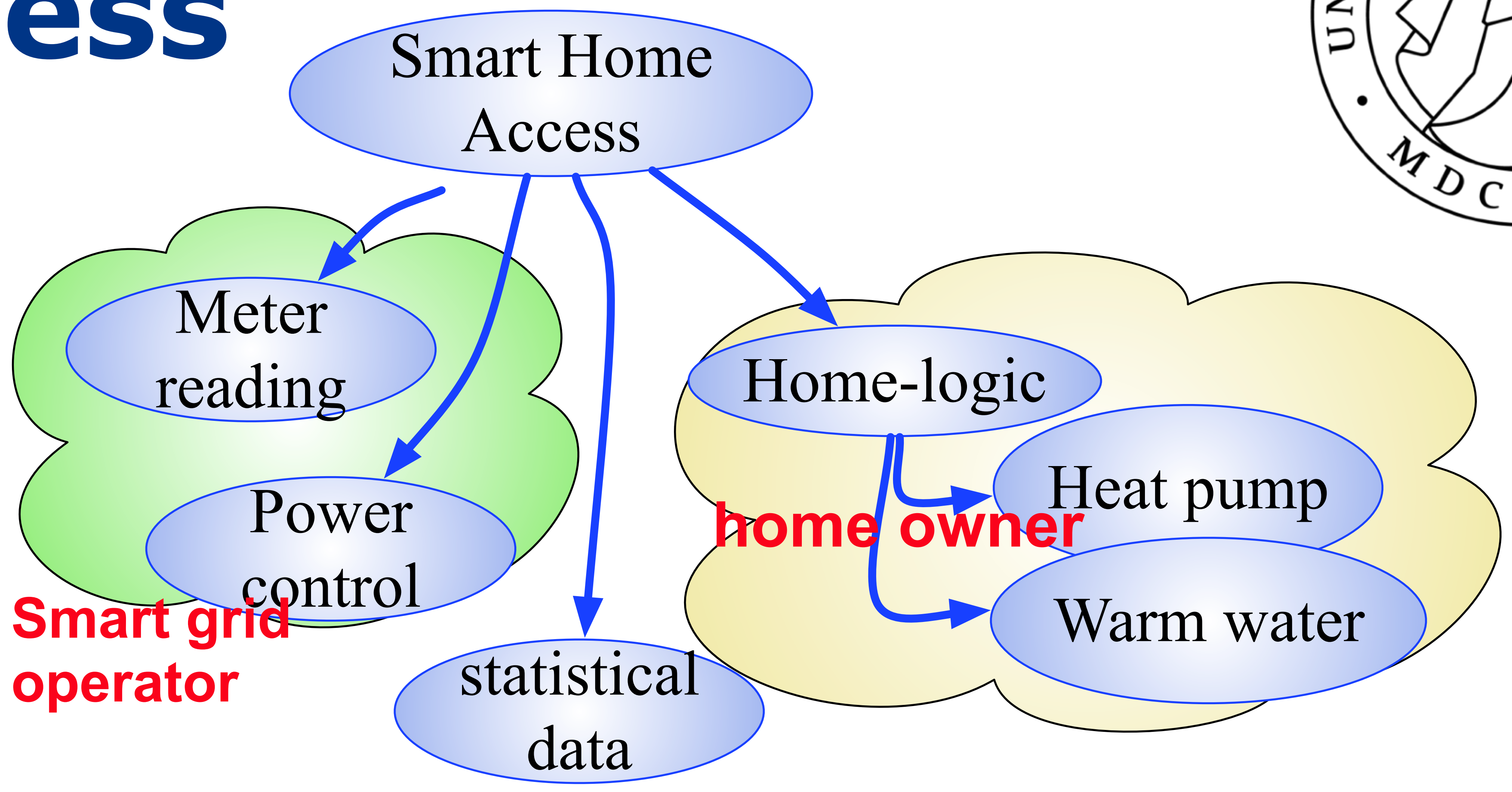
0:16 / 2:11



further reading:
https://www.slideshare.net/marinasantini1/09-semantic-webontologies?qid=8b178746-ea3c-48db-b4f6-6bc9b0923d9b

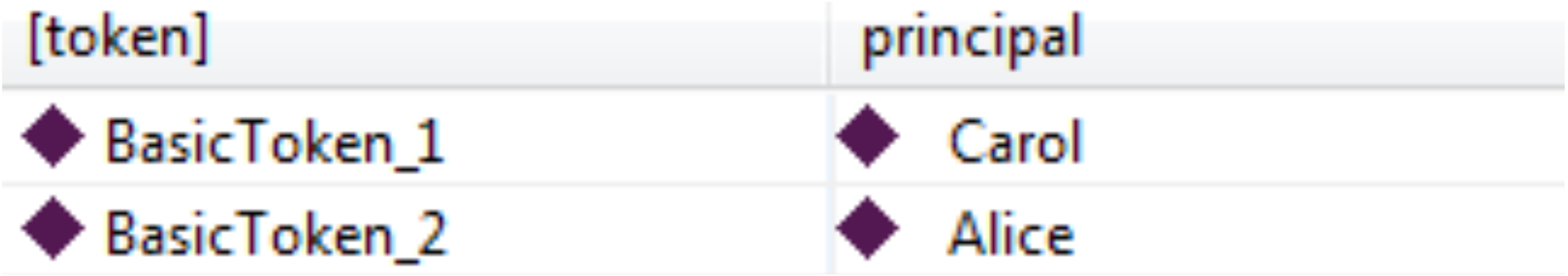
Semantic attribute based access control (S-ABAC)

- ➡ Access to information
  - who (sensor, person, service)
  - what kind of information
  - from where
- ➡ Attribute-based access
  - role (in organisation, home)
  - device, network
  - security tokens
- ➡ OWL & SWRL implementation
- ➡ Rules inferring security tokens



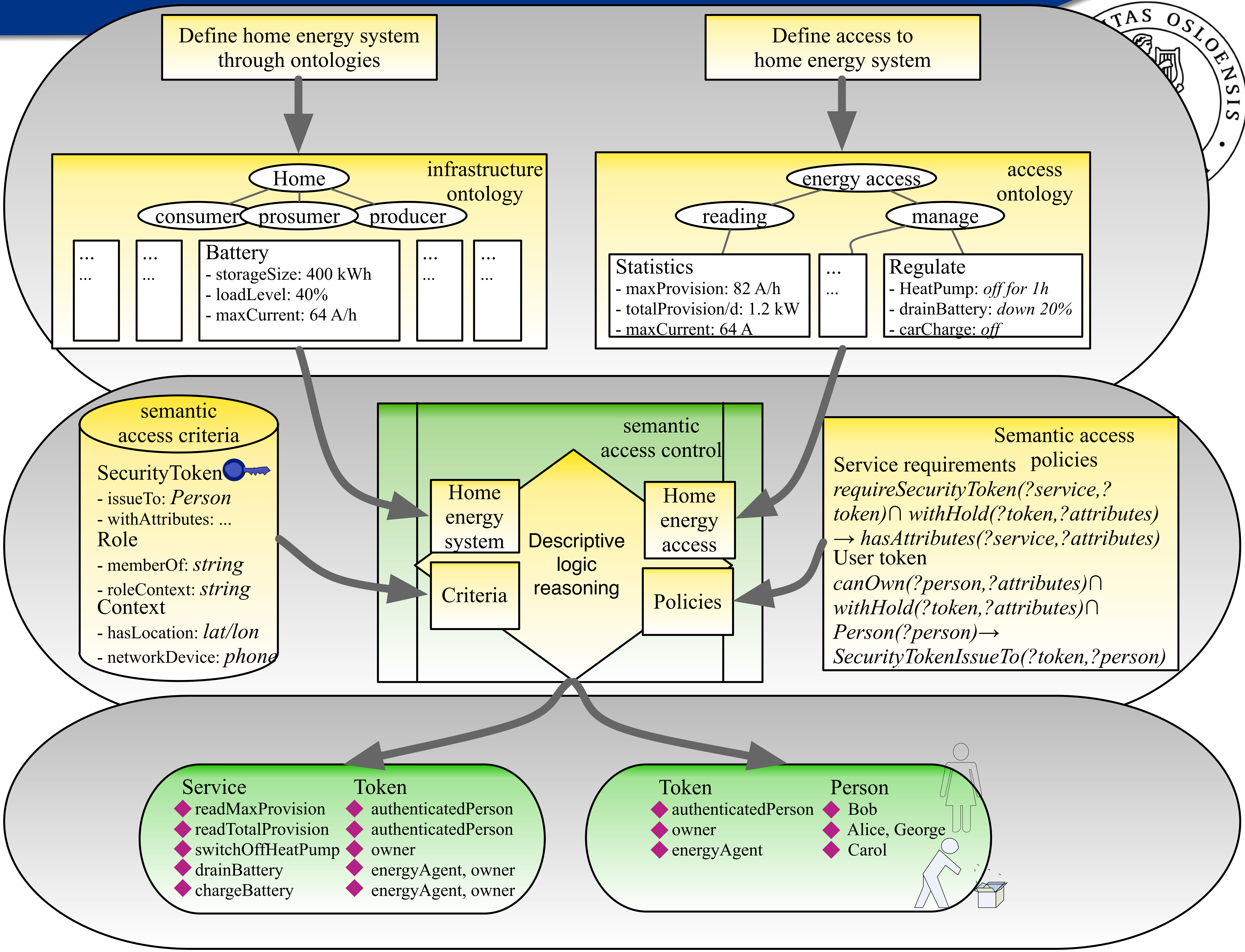
Attributes: roles, access, device, reputation, behaviour, ...

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



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

Smart Home: Complex access



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)

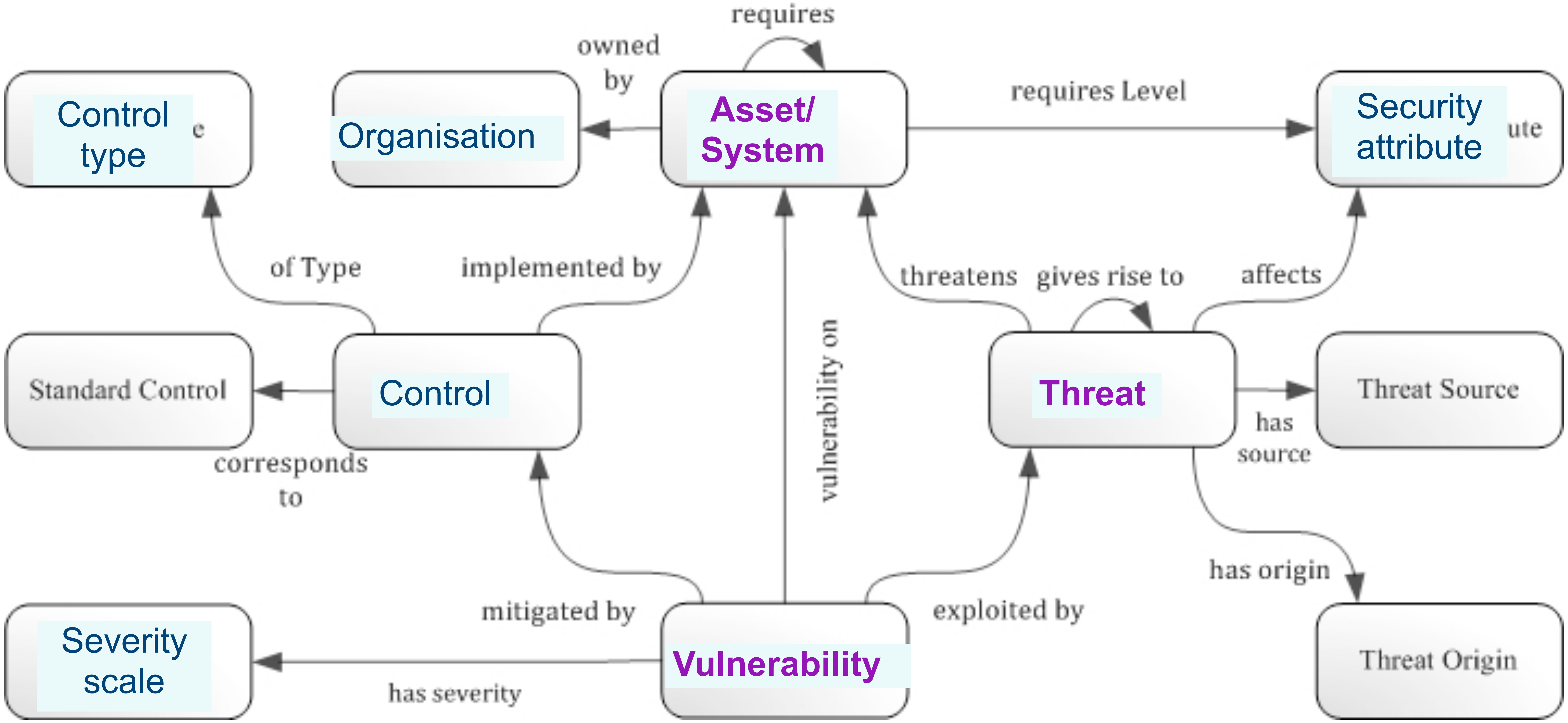
Service	Token
readMaxProvision	authenticatedPerson
readTotalProvision	authenticatedPerson
switchOffHeatPump	owner
drainBattery	energyAgent, owner
chargeBattery	energyAgent, owner

Token	Person
authenticatedPerson	Bob
owner	Alice, George
energyAgent	Carol

Security Ontologies
- traditional view
- Application-oriented view

Traditional approach

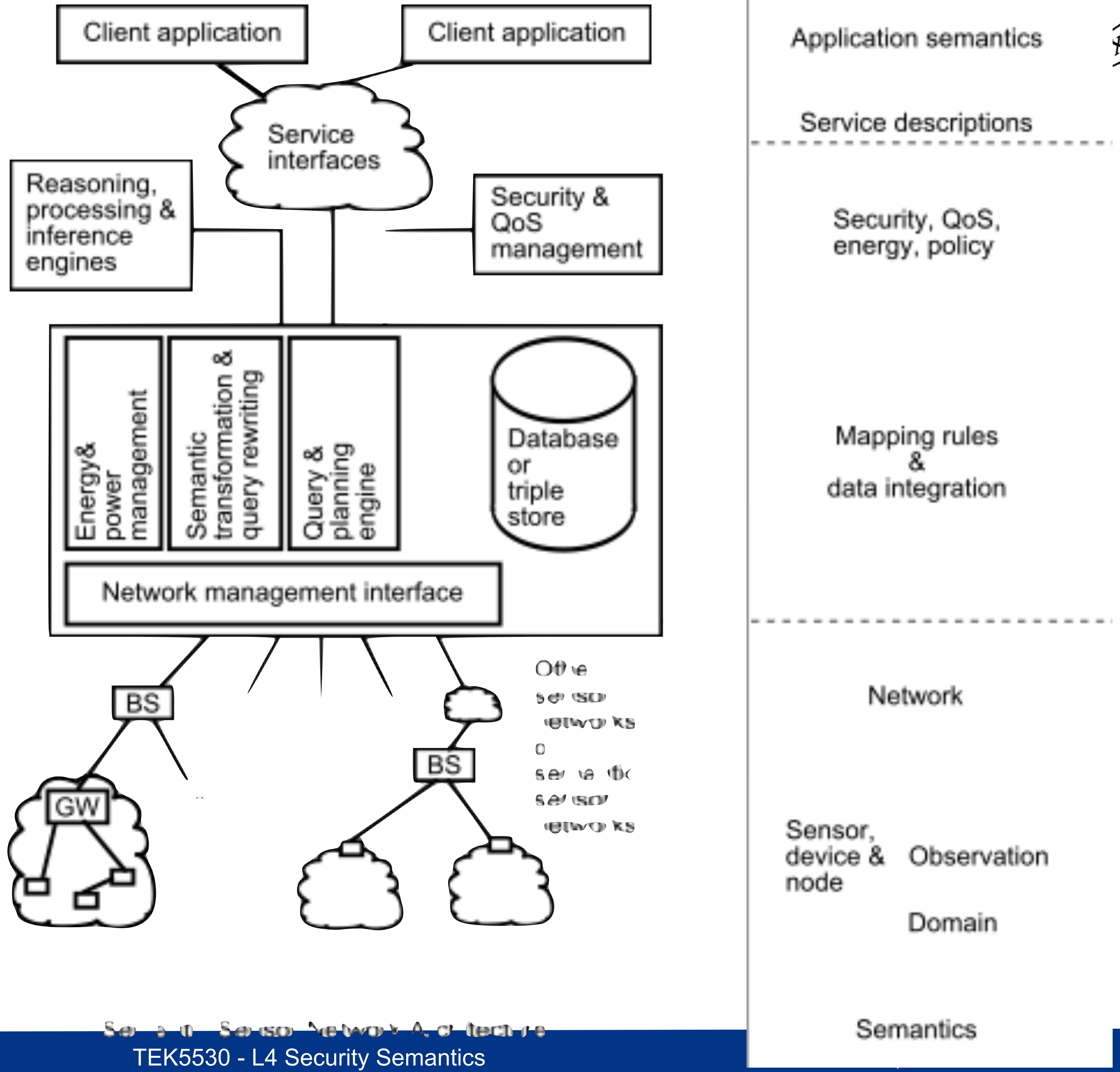
- Combined approach, addressing threat, vulnerability, system impact and control



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

Sensor Network Architecture

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

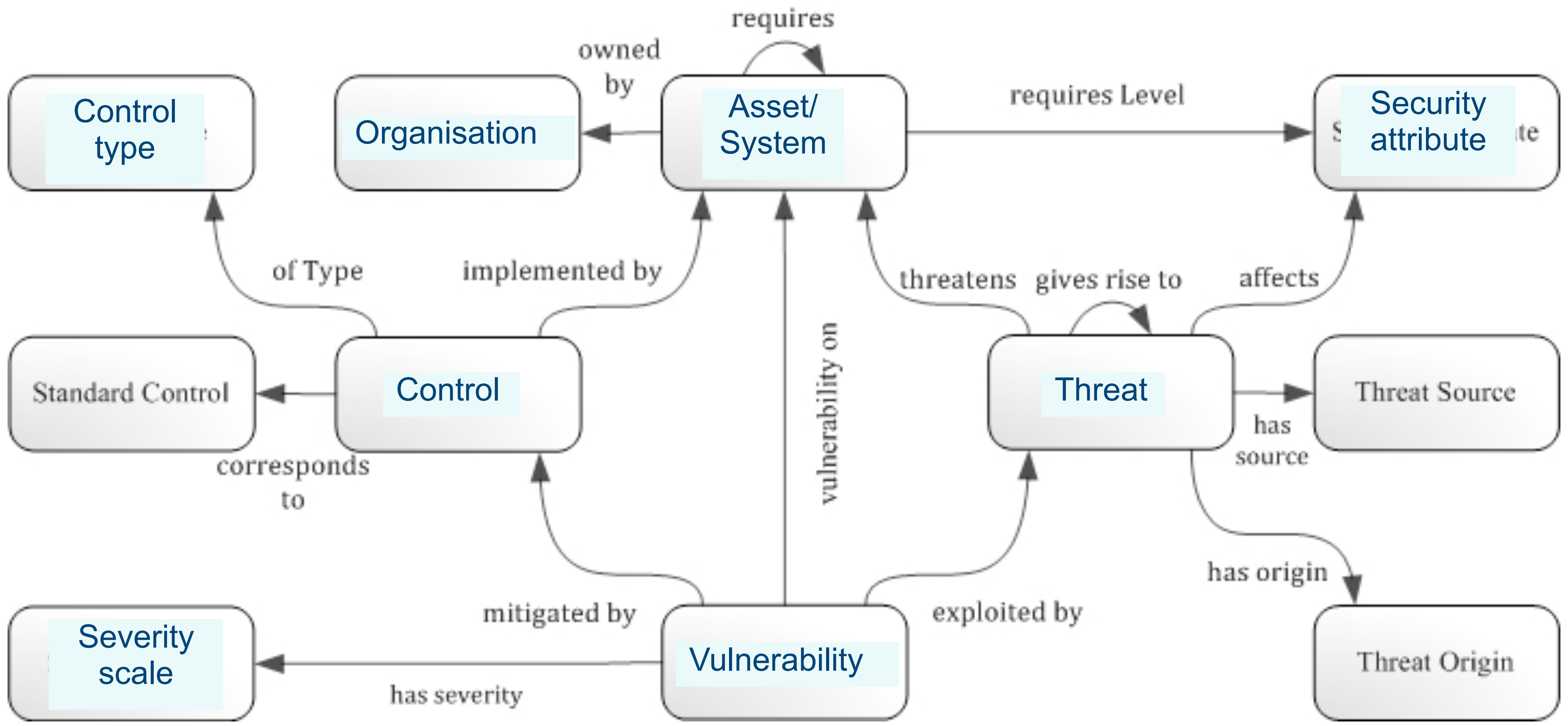

Client application
Client application
Service interfaces
Reasoning, processing & inference engines
Security & QoS management
Energy& power management
Semantic transformation & query rewriting
Query & planning engine
Database or triple store
Network management interface
BS
GW
BS
Other sensor networks 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

Limitations of the traditional approach

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

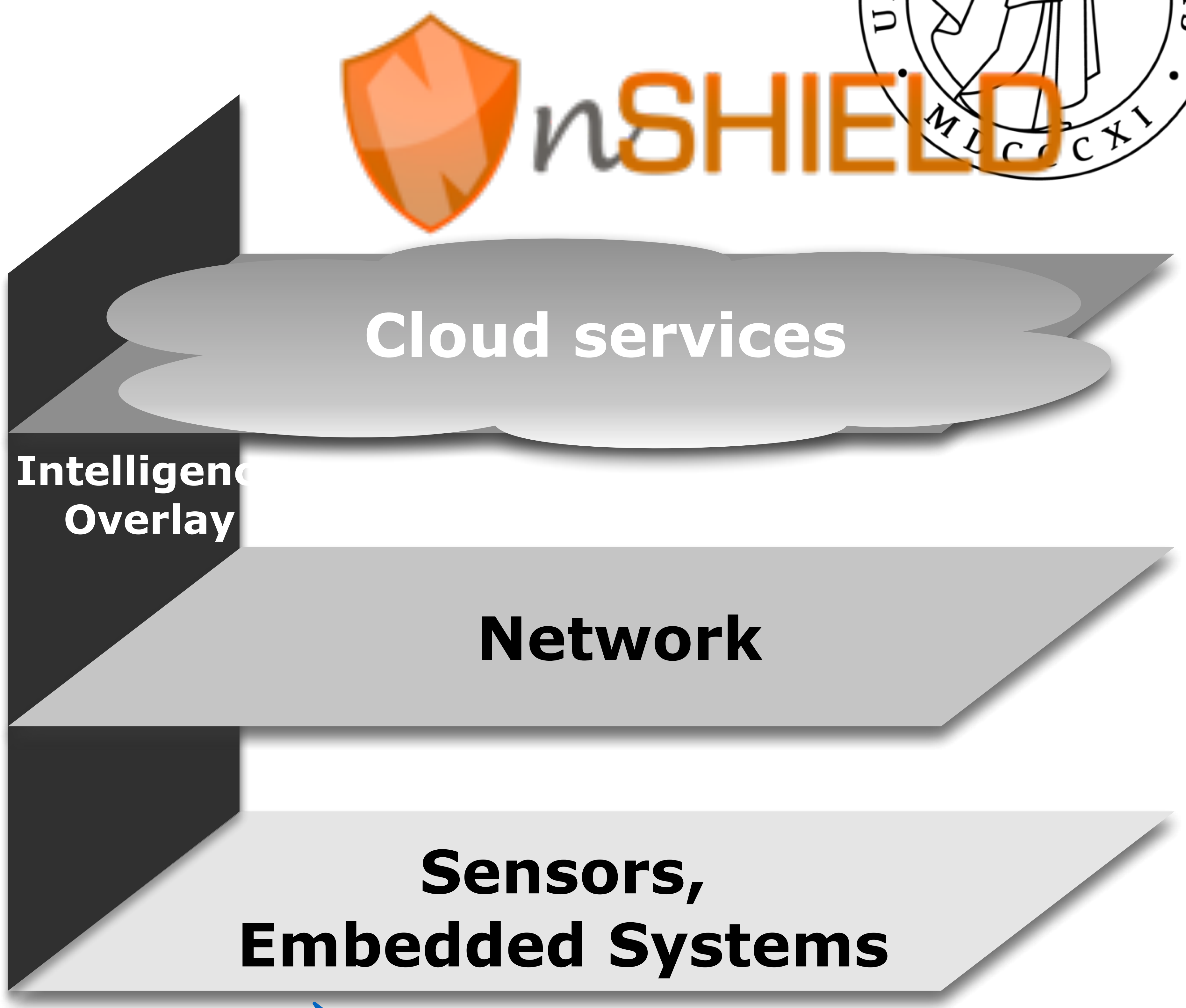


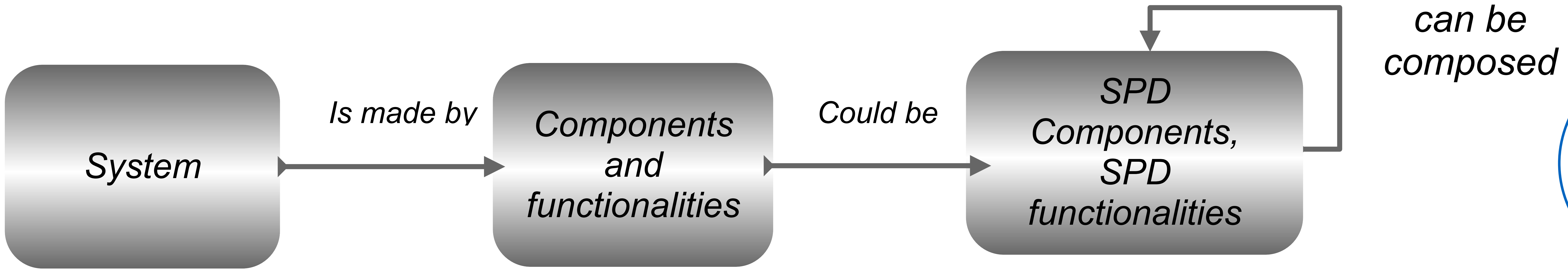
Recommendation:

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

Applied security

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



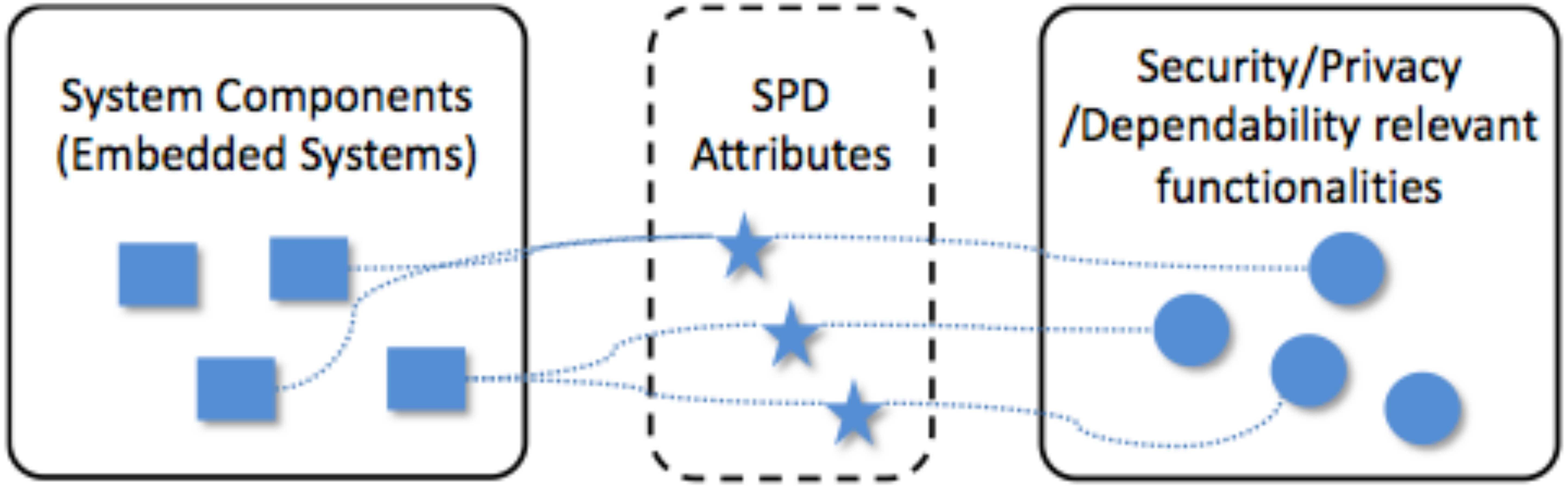


System
Is made by
Components and functionalities
Could be
SPD Components, SPD functionalities
can be composed

What ontologies are needed?

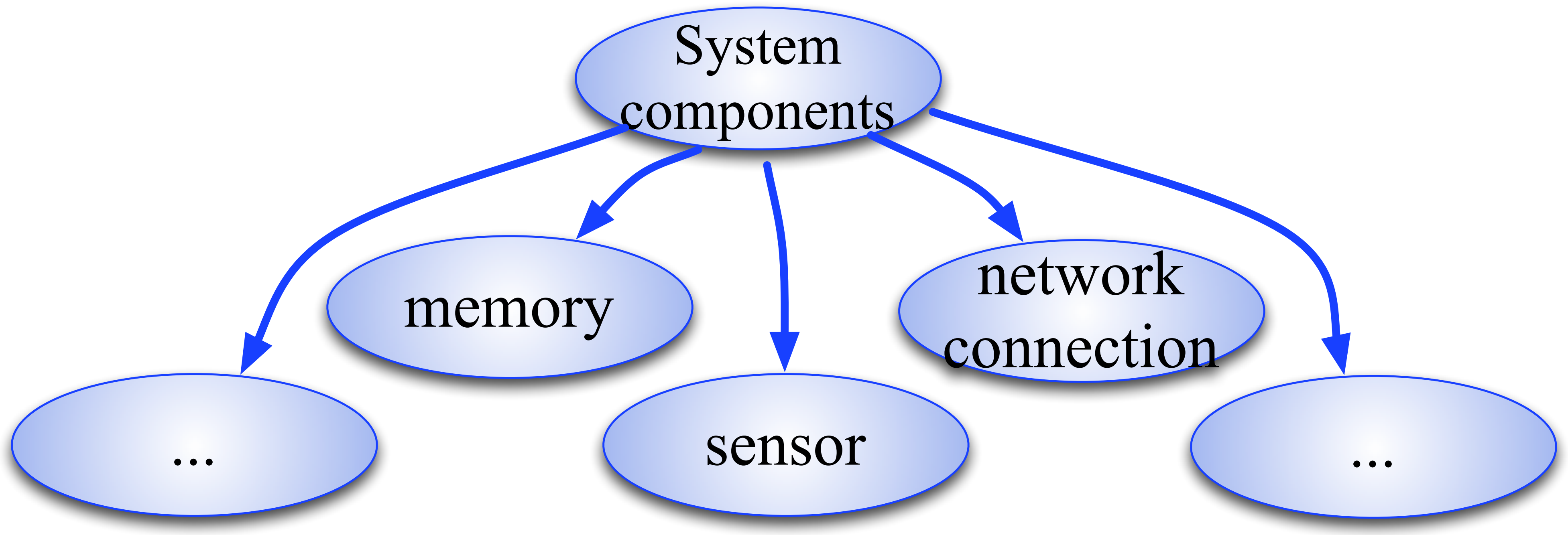
Security description

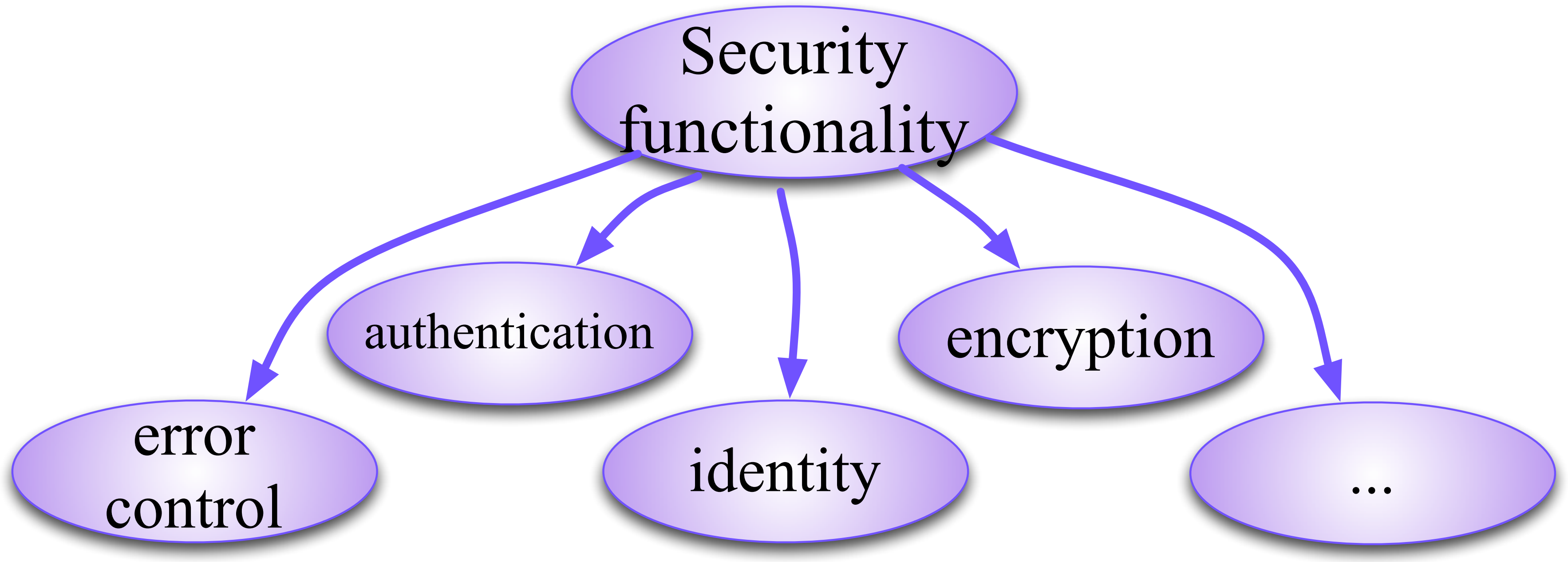
- Ontologies for system, security attributes, security functionality


System Components (Embedded Systems)

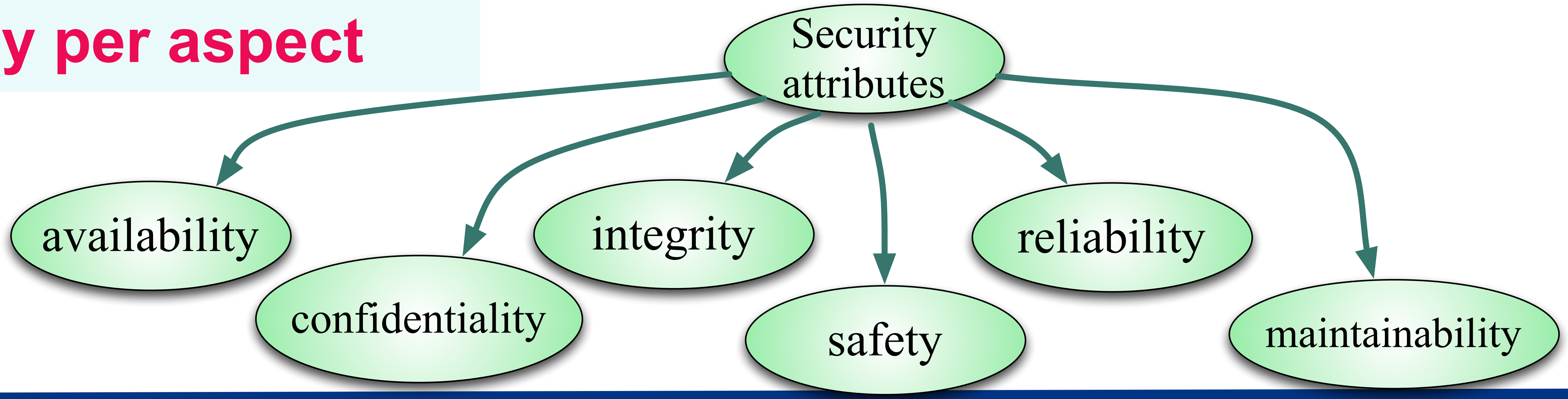
SPD Attributes

Security/Privacy /Dependability relevant functionalities



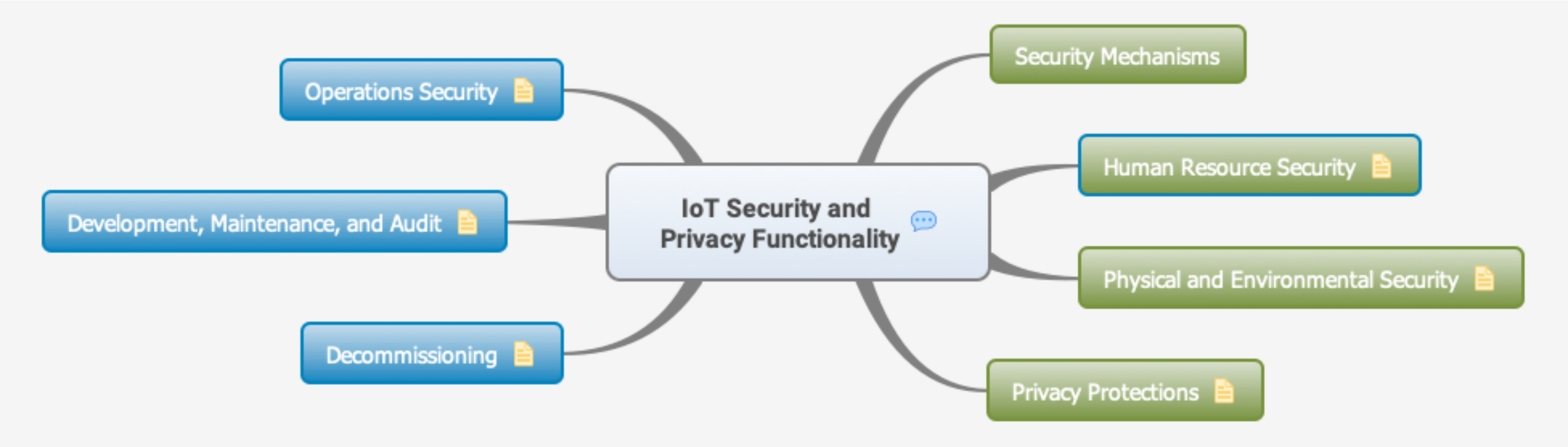


Recommendation: One ontology per aspect



IoT Security & Privacy Lifetime Security

see: SPF.IoTSec.no



IoT Security and Privacy Functionality

Operations Security

Development, Maintenance, and Audit

Decommissioning

Security Mechanisms

Human Resource Security

Physical and Environmental Security

Privacy Protections

[Source: Elahe Fazeldehkordi https://its-wiki.no/images/d/d0/IoT_SecPrivFunc_LifeMap_v2.pdf]

IoT Security - Access control

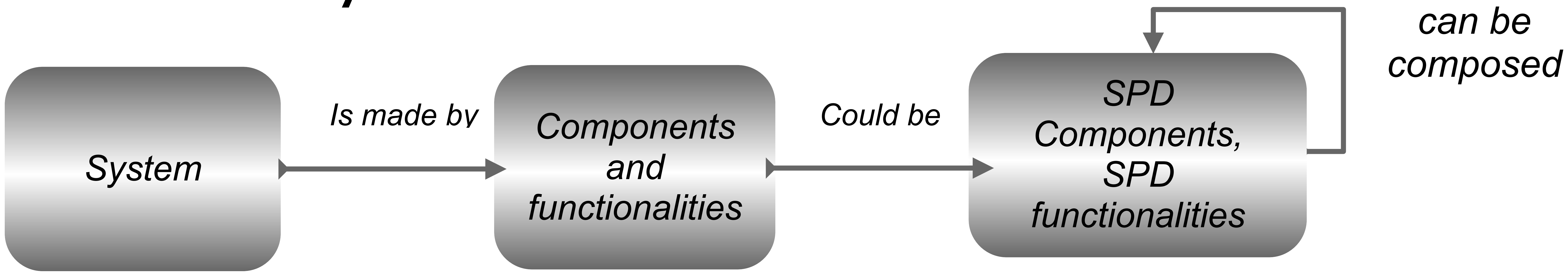
see: SPF.IoTSec.no

Security Mechanisms

- Access Control
  - Accessing Only Authorized Individuals to Collected Personal Information
  - Consider Measures to Keep Unauthorized Users from Accessing a Consumer's Device, Data, or Personal Information Stored on the Network.
  - Secure Authentication/ Authorization/Access Control
    - Requiring Strong Passwords
    - Implementing two-factor Authentication (2FA)
    - Use Personal Identification Numbers (PINs)
    - Use Multi-factor Authentication (MFA)
    - Securing Password Recovery Mechanisms
    - Option to Force Password Expiration After a Specific Period
    - Option to Change the Default Username and Password
    - Using Certificates for Authentication
    - Considering Biometrics for Authentication
    - Considering Certificate-Less Authenticated Encryption (CLAE)
    - User Managed Access (UMA)
    - OAuth 2.0
    - Ensure default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed.
    - Authentication credentials including but not limited to user passwords shall be salted, hashed and/or encrypted.
    - Protect against 'brute force' and/or other abusive login attempts. This protection should also consider keys stored in devices.
    - Ensure password recovery or reset mechanism is robust and does not supply an attacker with information indicating a valid account. The same applies to key update and recovery mechanisms.

Upcoming lectures

- L5: Paper presentation
- L6: Multi-Metrics Method for measurable Security



System

Is made by

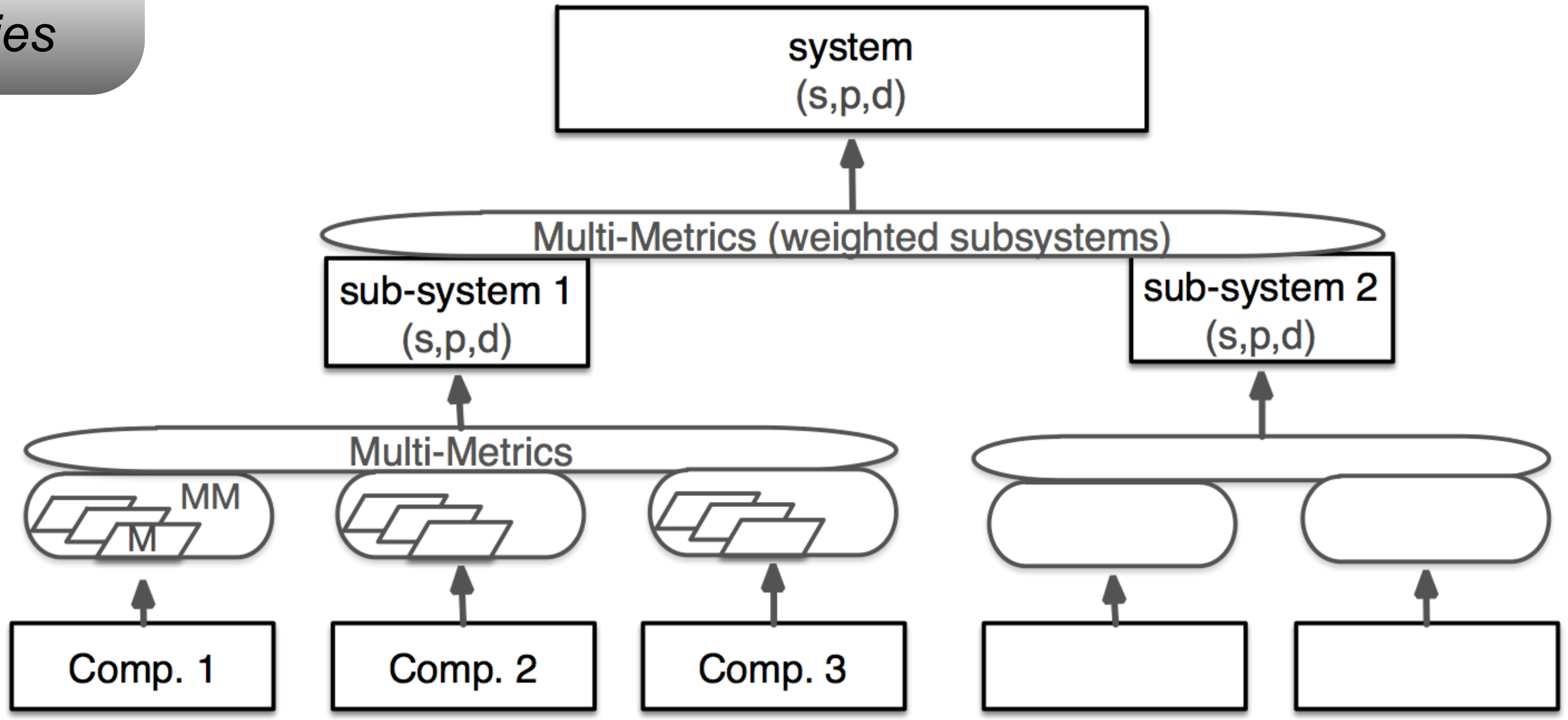
Components and functionalities

Could be

SPD Components, SPD functionalities

can be composed

- …. applying Multi-Metrics



system (s,p,d)

Multi-Metrics (weighted subsystems)

sub-system 1 (s,p,d)

sub-system 2 (s,p,d)

Multi-Metrics

Comp. 1

Comp. 2

Comp. 3

Learning outcomes

Having followed the lecture, you can

- explain components of the Smart Grid (AMS) System of Systems
- can explain the difference between functional, non-functional and security components
- provide examples of security challenges in IoT
- explain the difference between the web, the semantic web, web services and semantic web services
- explain the core elements of the Semantic Web
- apply semantics to IoT systems
- provide an example of attribute based access control
- discuss the shortcomings of the traditional threat-based approach
- list the main elements of the semantic descriptions of s,p,d functionalities
- perform a semantic mapping of s,p,d attributes *(future work)*