Center for Wireless Innovation Norway
cwin.no

CWI
Norway

UNIK
UNIVERSITY GRADUATE CENTER

FFI IKT seminar - Jeløya - April 2013

Measurable Security - a discussion of potential approaches

Josef Noll,
Prof. at University of Oslo/UNIK
Member of CWI Norway
josef@unik.no

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~~

The Semantic Dimension

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

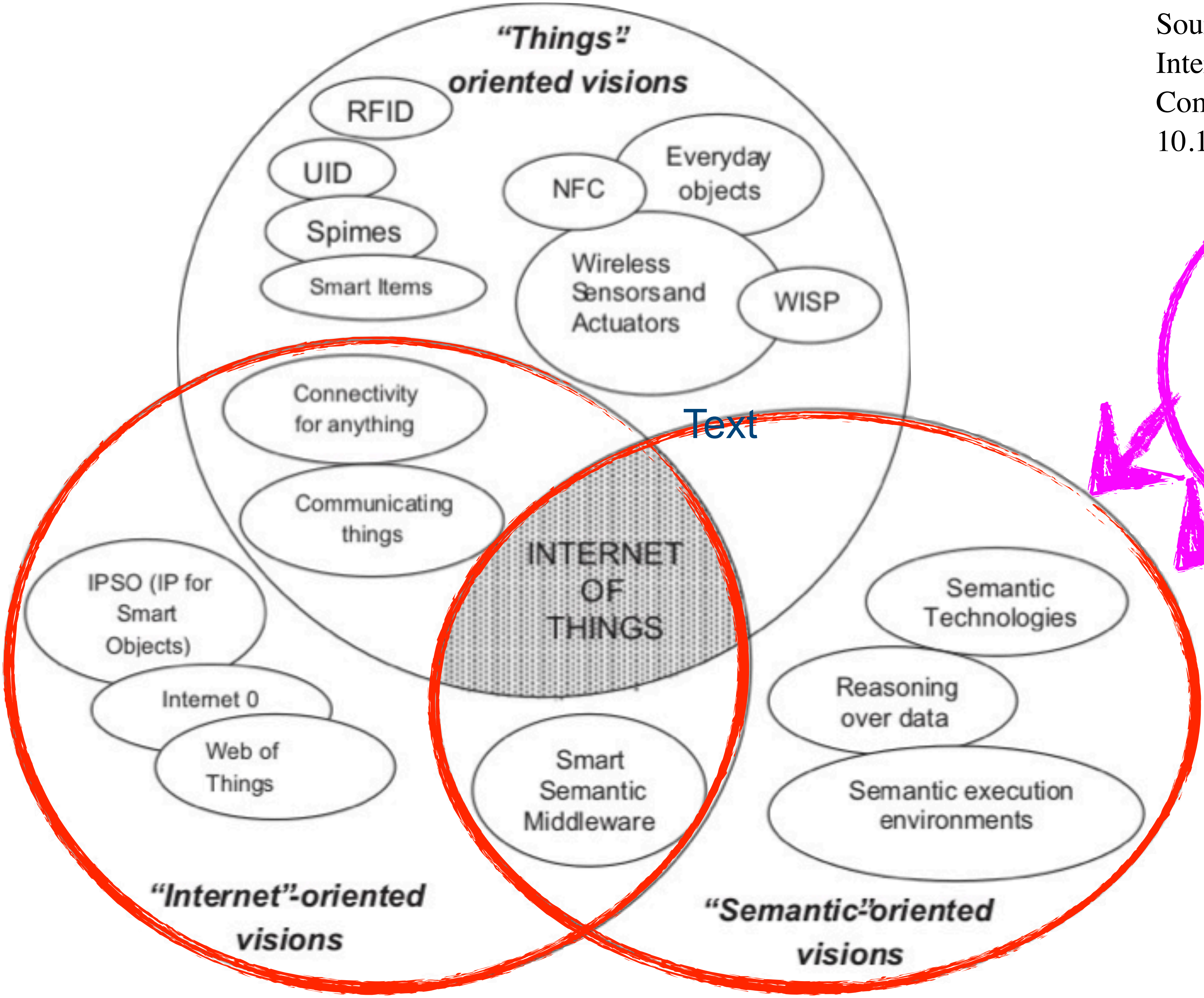
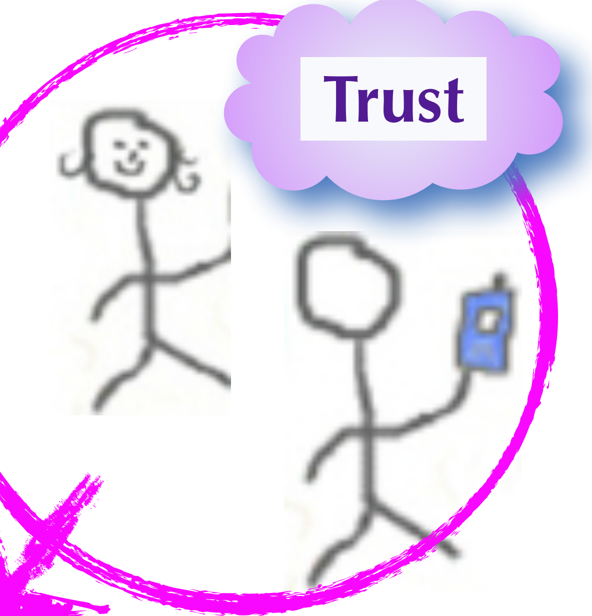
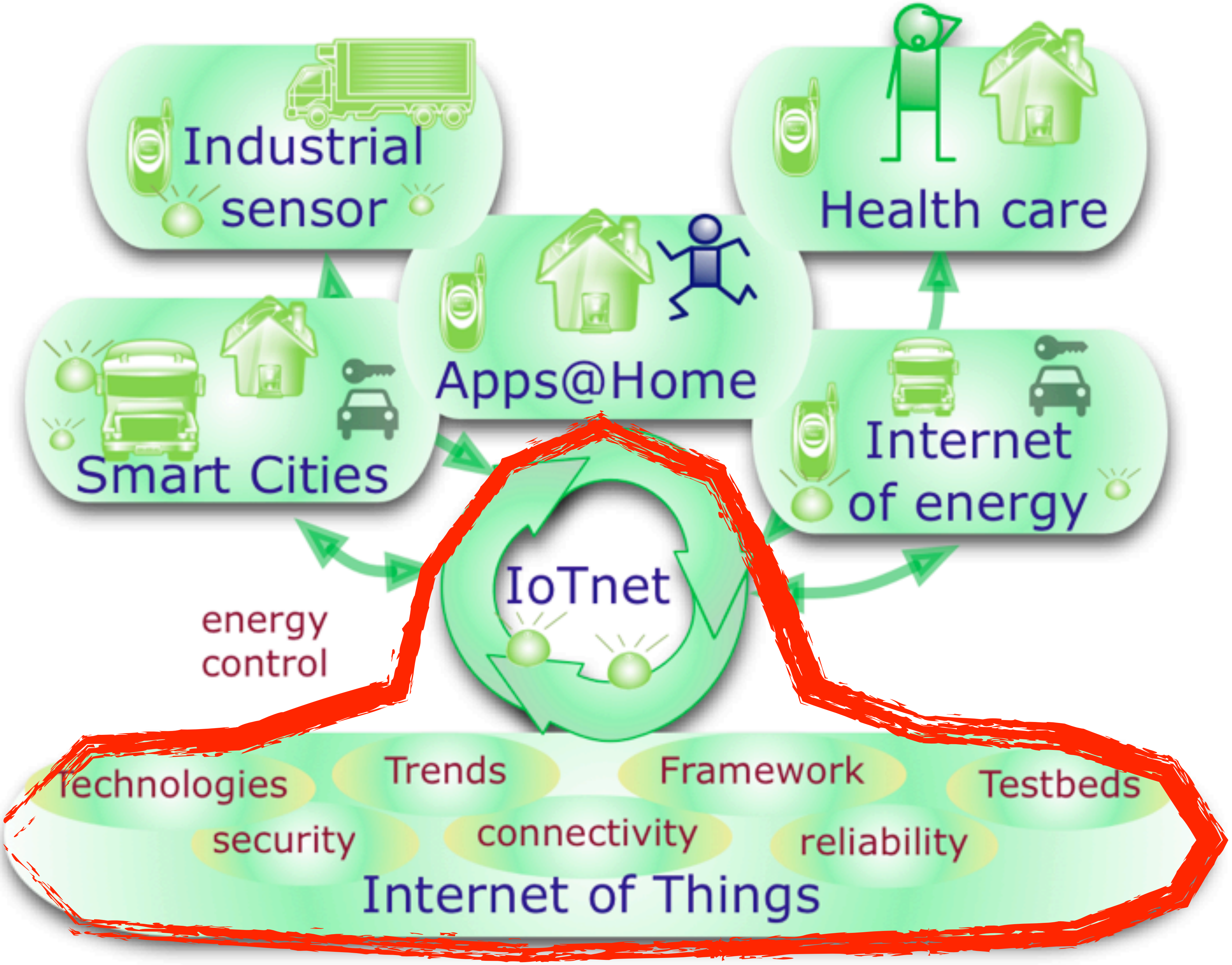

"Things" oriented visions
RFID
UID
Spimes
Smart Items
NFC
Everyday objects
Wireless Sensors and Actuators
WISP
Connectivity for anything
Communicating things
Text
INTERNET OF THINGS
IPSO (IP for Smart Objects)
Internet 0
Web of Things
Smart Semantic Middleware
Semantic Technologies
Reasoning over data
Semantic execution environments
"Internet"-oriented visions
"Semantic"-oriented visions

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



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

The IoT technology and application domain

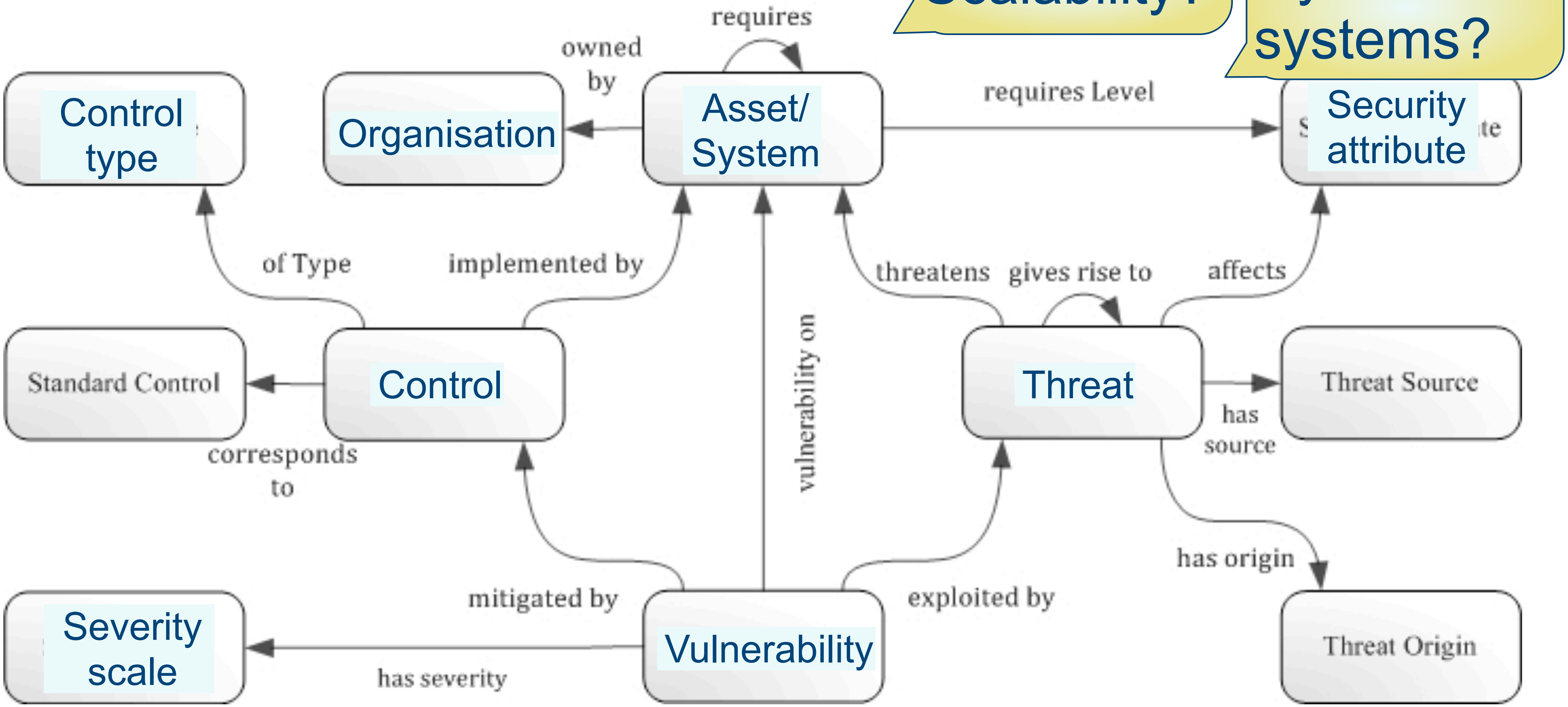


Traditional approach

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

Scalability?

System of systems?



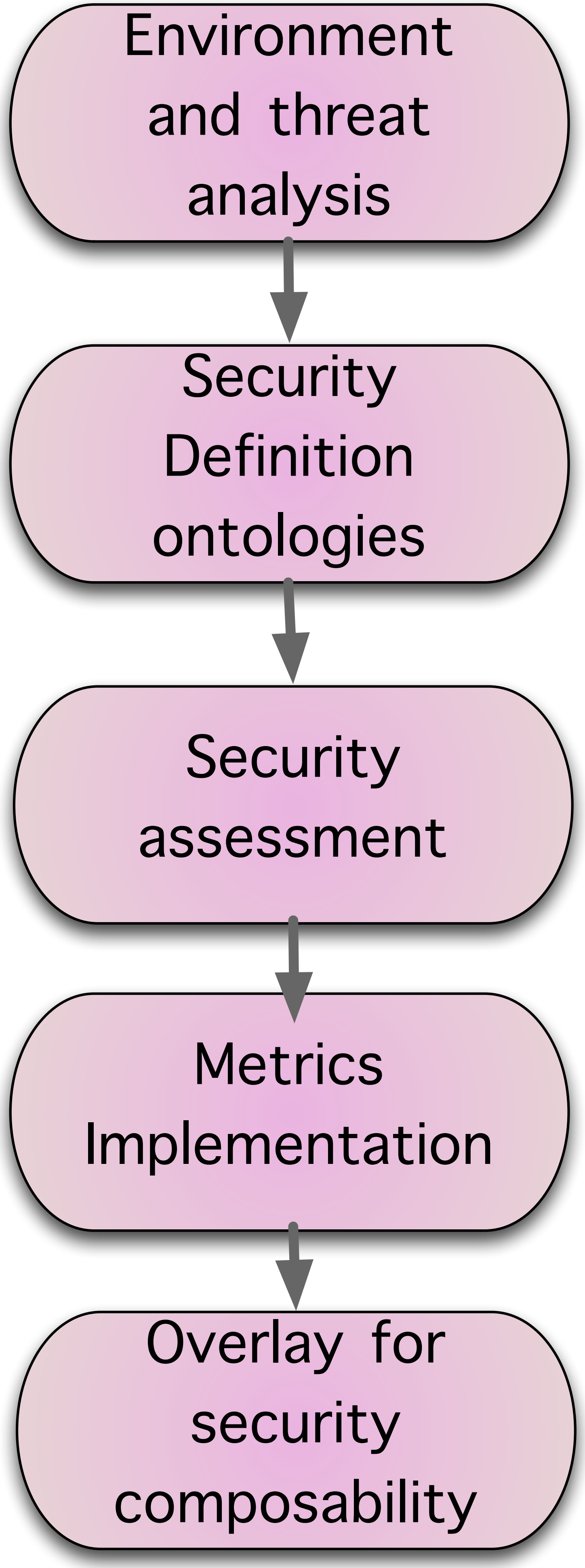
[source: http://securityontology.sba-research.org/]

The nSHIELD approach

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

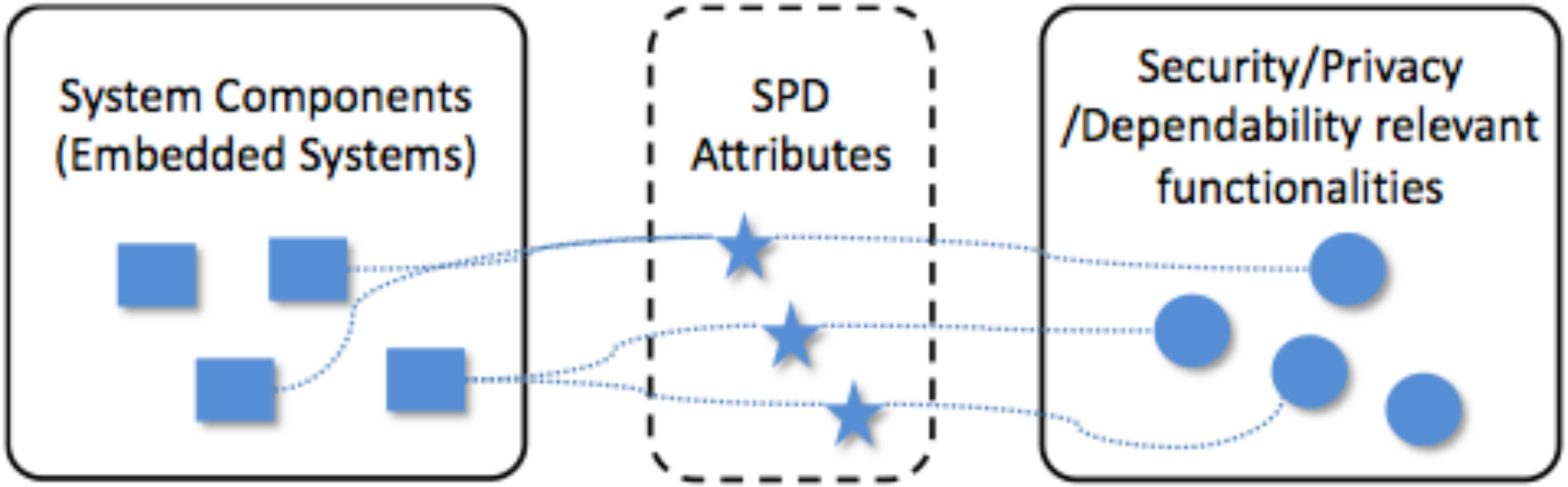
Core concept

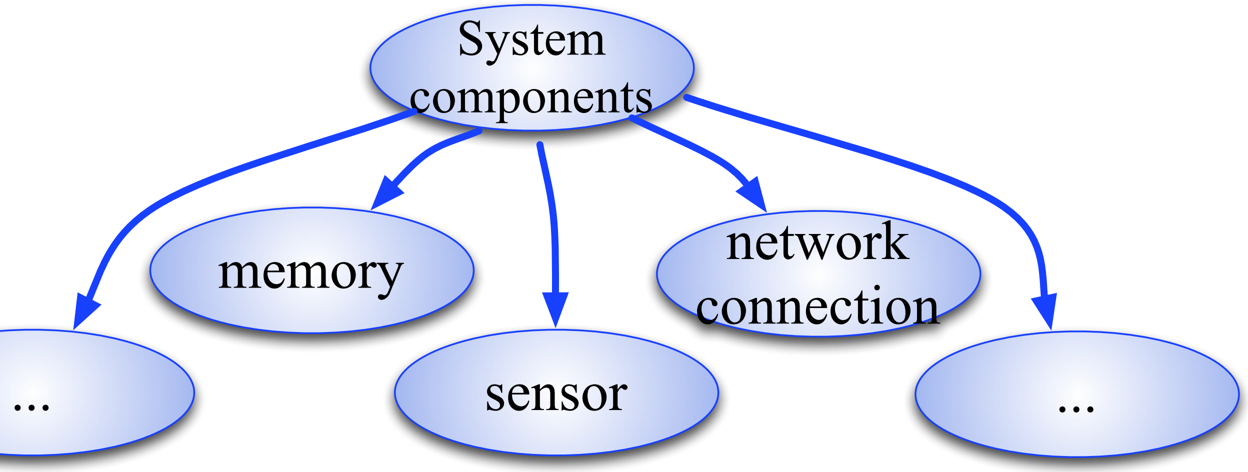
- Threat analysis
- Goal definition
- Semantic security description
- Semantic system description
- Security composability


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

http://newSHIELD.eu

Security description


System Components (Embedded Systems)
SPD Attributes
Security/Privacy /Dependability relevant functionalities


System components

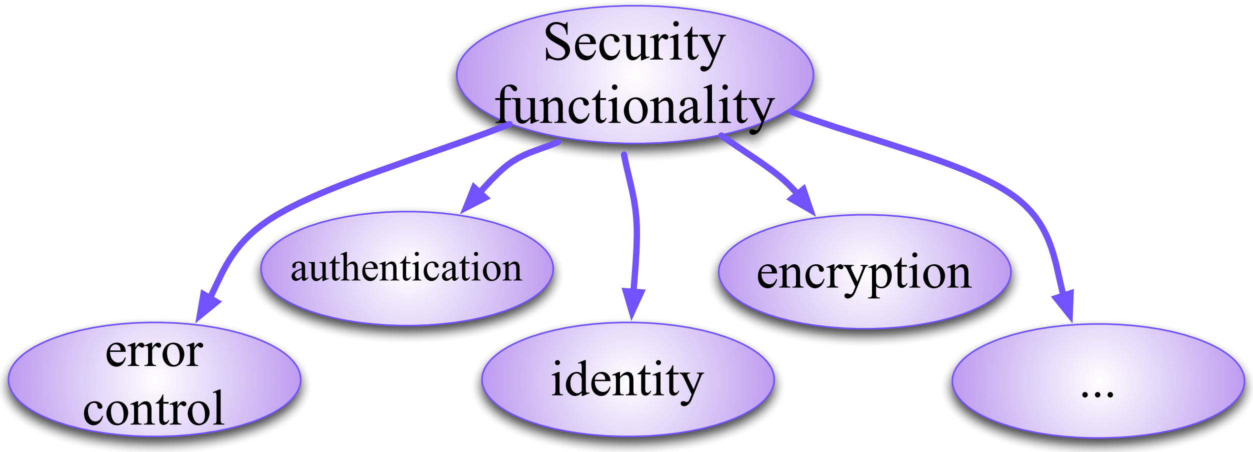
memory

sensor

network connection

...

...


Security functionality

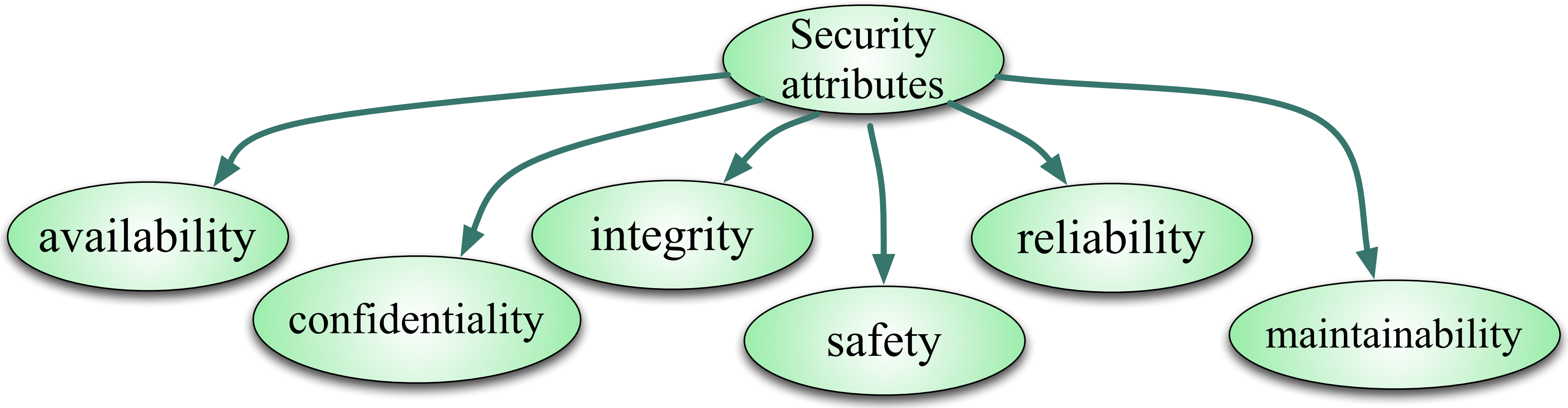
error control

authentication

identity

encryption

...


Security attributes

availability

confidentiality

integrity

safety

reliability

maintainability

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?

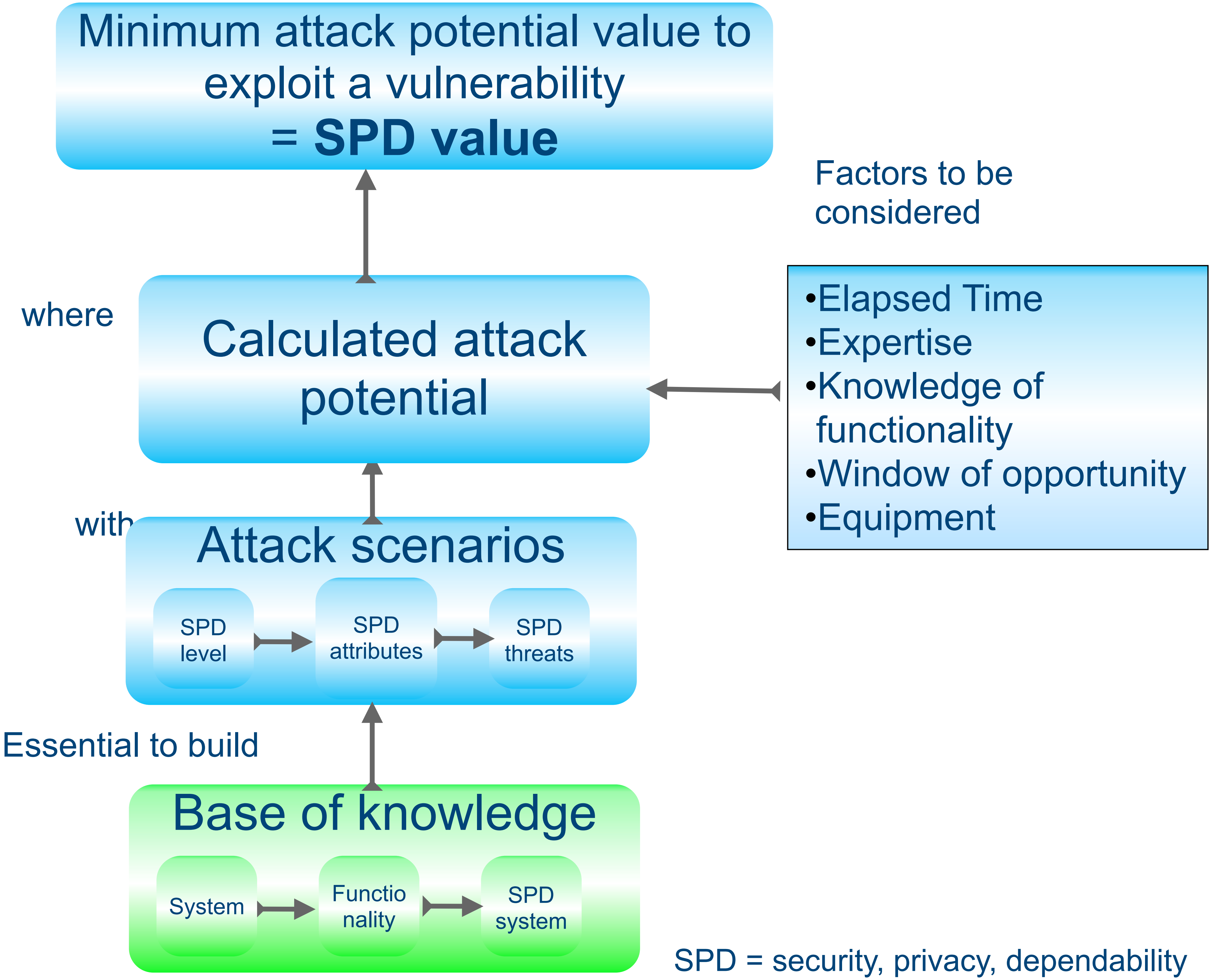
- more specific
- easier to understand(?)

- 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 ajor topics

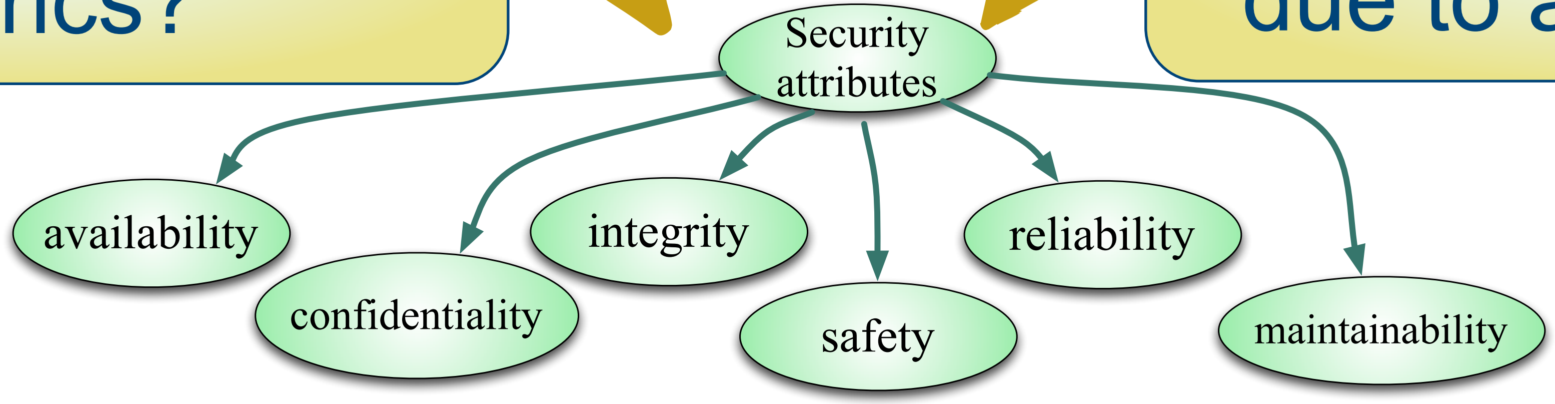
I need your help

specific application ontologies?

ontologies for security, systems, functionality

universal threat metrics?

selection of metrics due to application?



Sensor/Device System description?

SensorML

Semantic Sensor Network (SSN) ontology

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
- 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