MŰEGYETEM 1782

Kiberfizikai rendszerek

Dr. Péceli Gábor egyetemi tanár
Kocsis Imre tanársegéd
Dr. Pataricza András egyetemi tanár
Vörös András tud. segédmunkatárs

Oktatók





Kiberfizikai rendszerek (Cyber-Physical Systems - CPS)

- A tantárgy célkitűzése
- Az internethez integrált beágyazott rendszerek
  - a felhő szolgáltatások → számítási lehetőségek
  - Interneten keresztül elérhető tudás és szolgáltatások
  - felhasználói igények által vezérelt
  - adaptív/átkonfigurálható
  - internetes infrastruktúra megbízhatatlansága

Követelmények

- 1 db zárthelyi okt.26. 16-18 óráig
    - pótZH szorgalmi időszakban,
    - pót-pótZH pótlási héten
- 1 db házi feladat
    - Részbeadások:
        - szept.28. (specifikáció),
        - okt.26. (rendszerterv),
        - dec.7. (védés)
    - Pótlás a pótlási héten
- Szóbeli vizsga
    - Csak aláírással
        - ZH + házi feladat
    - Megajánlott jegy
        - jeles ZH és jeles házi feladat alapján

MŰEGYETEM 1782

Challenges in Cyber-Physical Systems

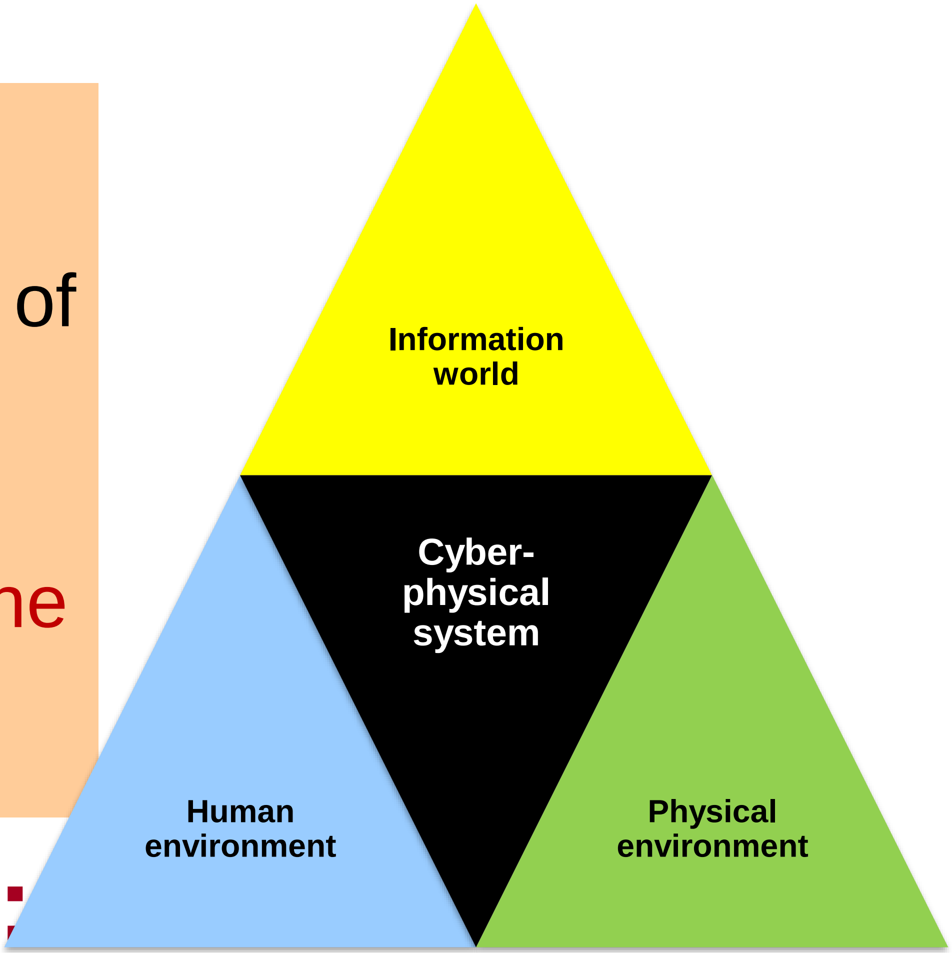
András Pataricza

Budapest University of Technology and Economics

pataric@mit.bme.hu

Let's reach an unlimited intelligence by the synergy of

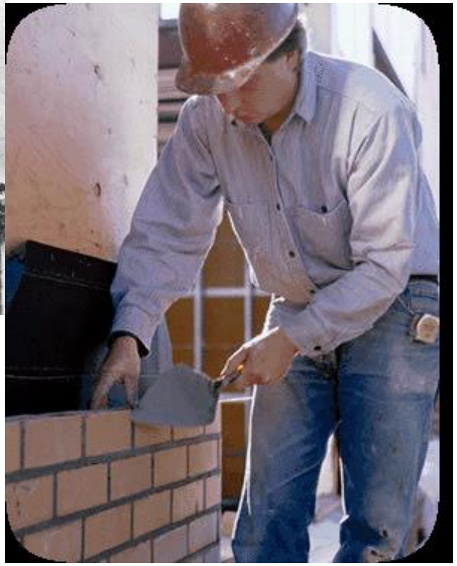
- intelligence in the cyber space and
- ES interfacing them to the physical world



THE NEW ERA: INTERNET OF THINGS AKA CYBER-PHYSICAL SYSTEMS

ES paradigm shift

Traditional



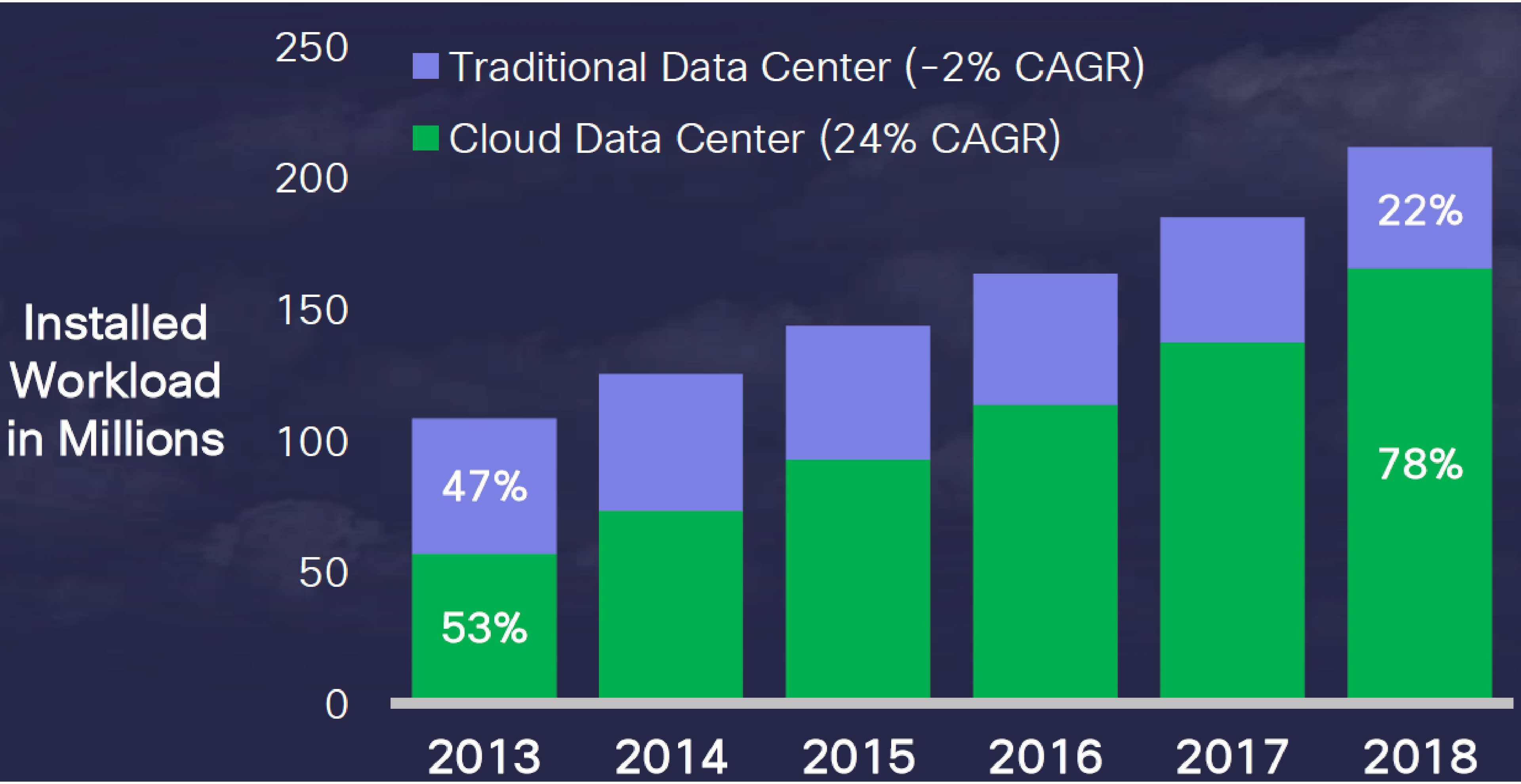
Industrialized

- Best component technologies
- Standardized components
- Automated system design

Local vs. remote data

Data integration

Cloud computing around the globe



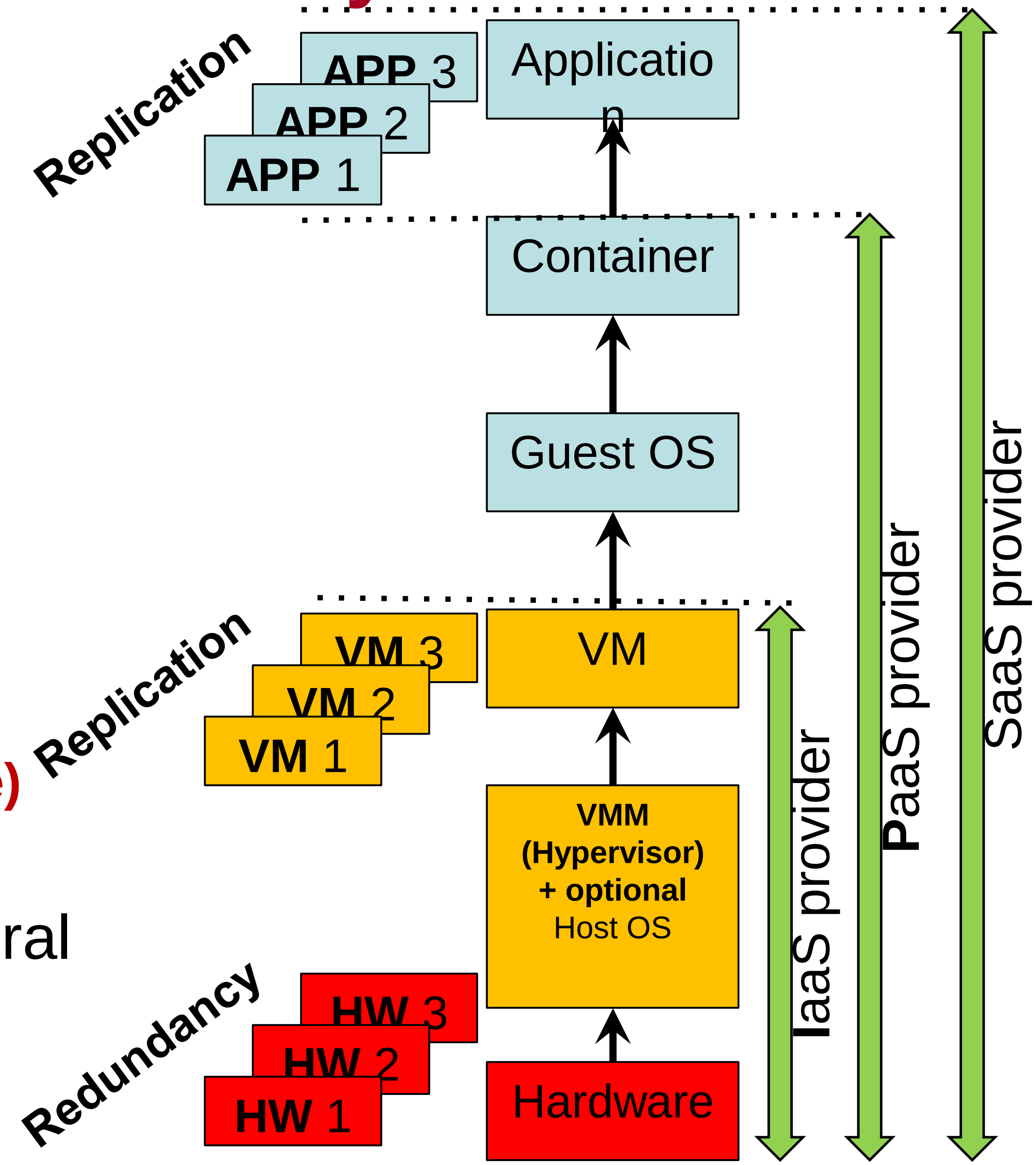
Source: Cisco Global Cloud Index: Forecast and Methodology 2013–2018

Mission critical cloud computing

- August 31, 2015
  - Federal aviation administration
  - 108$ million now, $1 billion in 10 years
  - Source: CSC news
- Network Functions Virtualization
  - The „telco” cloud
  - Source: NFV

Critical services over ordinary clouds?

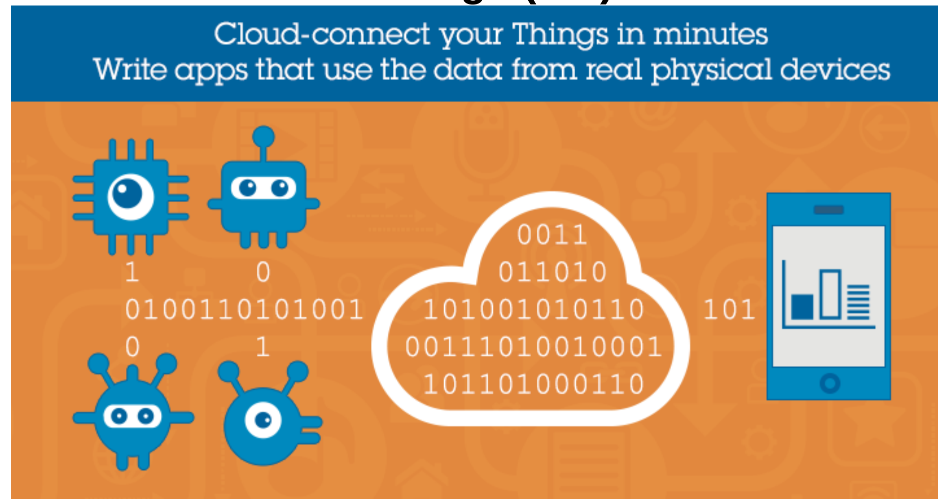
- Environment
  - HW/SW stack
  - Cloud service models
- Research objective
  - Scope
    - **Carrier grade IaaS**
    - SDN
  - Objective
    - **Availability (downtime)**
    - **Cost**
  - Redundancy architectural pattern
    - HW,VM, App, else



Appearance of cloud-based semantic services

- "Drag-and-drop" application prototyping
- Uniformization
  - Meta-algorithms
    - Data
      - COMPUTED
      - SENSED

IBM Internet of Things (IoT) Foundation



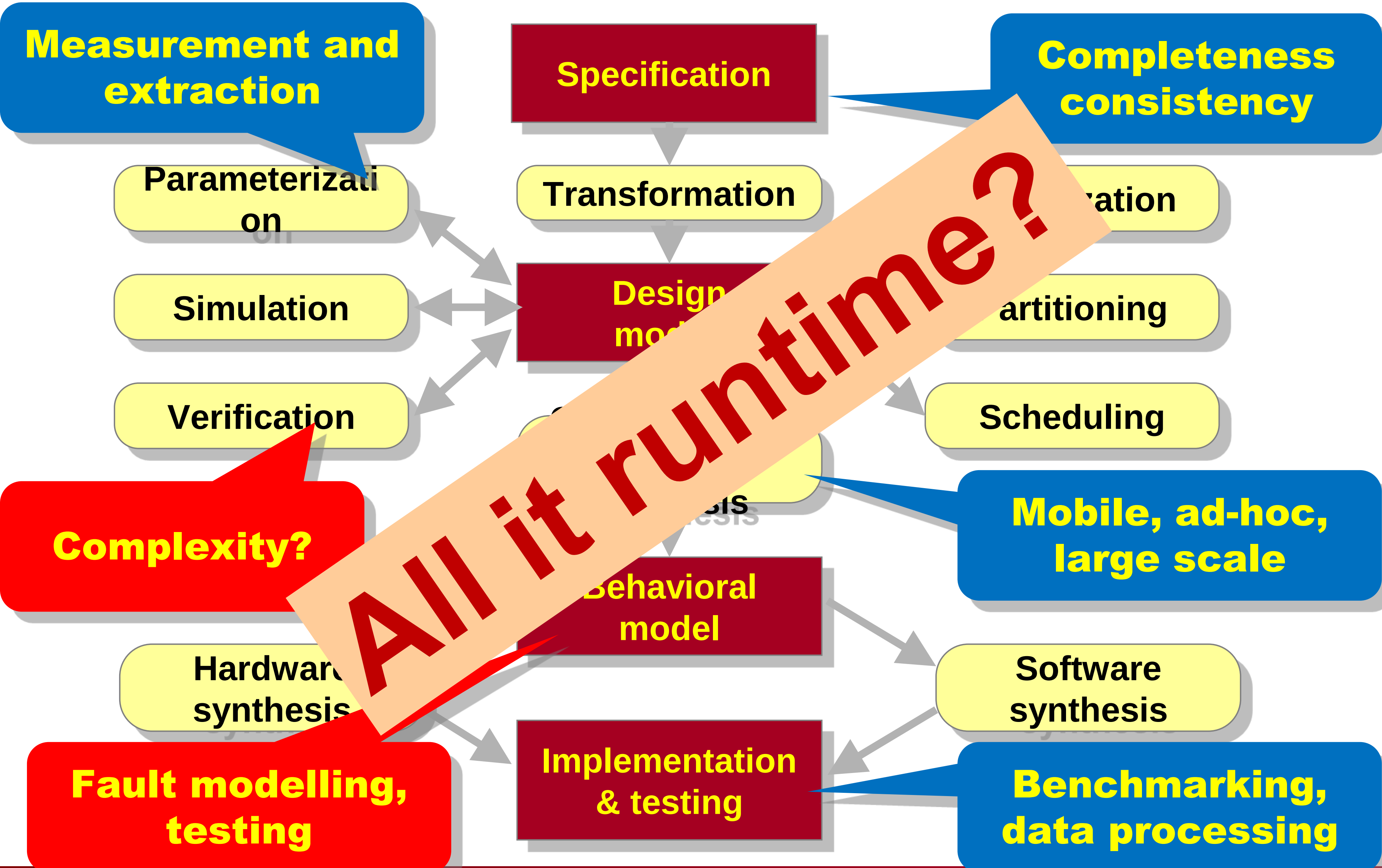
Wolfram Connected Devices Project

Example

- Cameras on riverside
- Different applications concurrently using the same primary information
- Tasks can change according to time/season/requirements
  - Identification of ships
  - Monitoring the break-up of ice
  - Monitoring the water level
  - Monitoring the speed of flood
  - Pollution check
  - Supervision of hostile entrance to the ship

On-demand Cyber Physical Systems

Critical CPS design and challenges



Service Oriented Approach

- Embedded systems provide services
  - Information of sensors
  - information of Internet
  - high level information derived
  - actuation possibility (limited)
- Services in a database
- Upon a new task: solution derived based on design patterns and available resources
- new solution deployed with no interference with the already running ones

Case study: supervising a server room

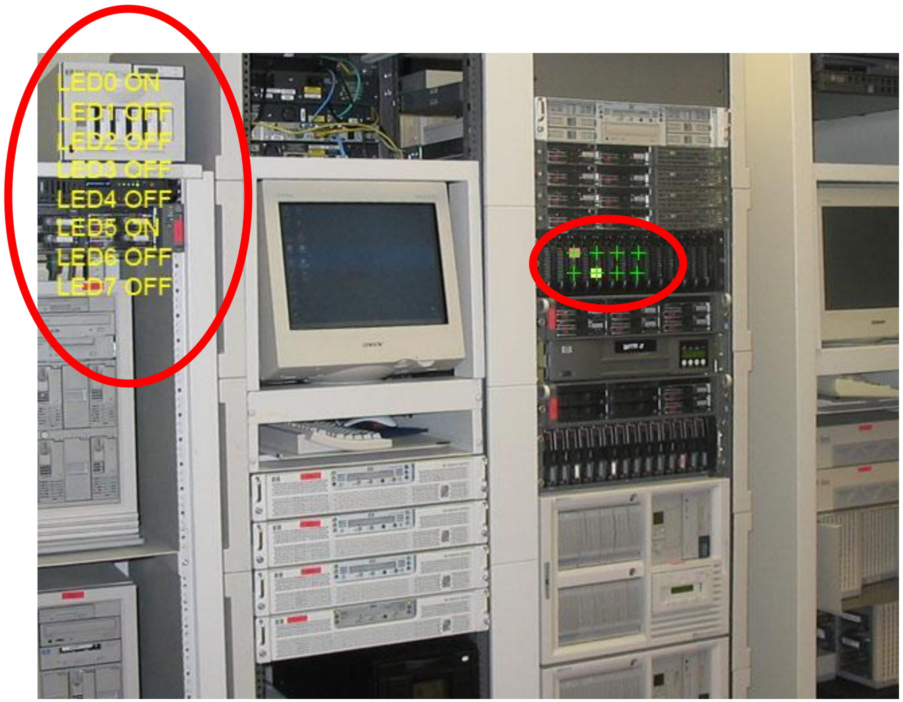
- Observations
  - temperature
  - humidity
  - state of doors/windows
  - monitoring the power consumption weather (temp./humidity)
  - temperature of outflow air of air conditioning
  - state of server computers/switches (video based)

Sensor platform

- Beagleboard-XM embedded SBC
- Sensors
  - temperature
  - humidity
  - web camera
  - power meters
  - microswitches to windows/doors
- Information from the web
  - weather status
  - weather forecast

3.25’”×
3.25”

Processing the camera pictures in the Cloud

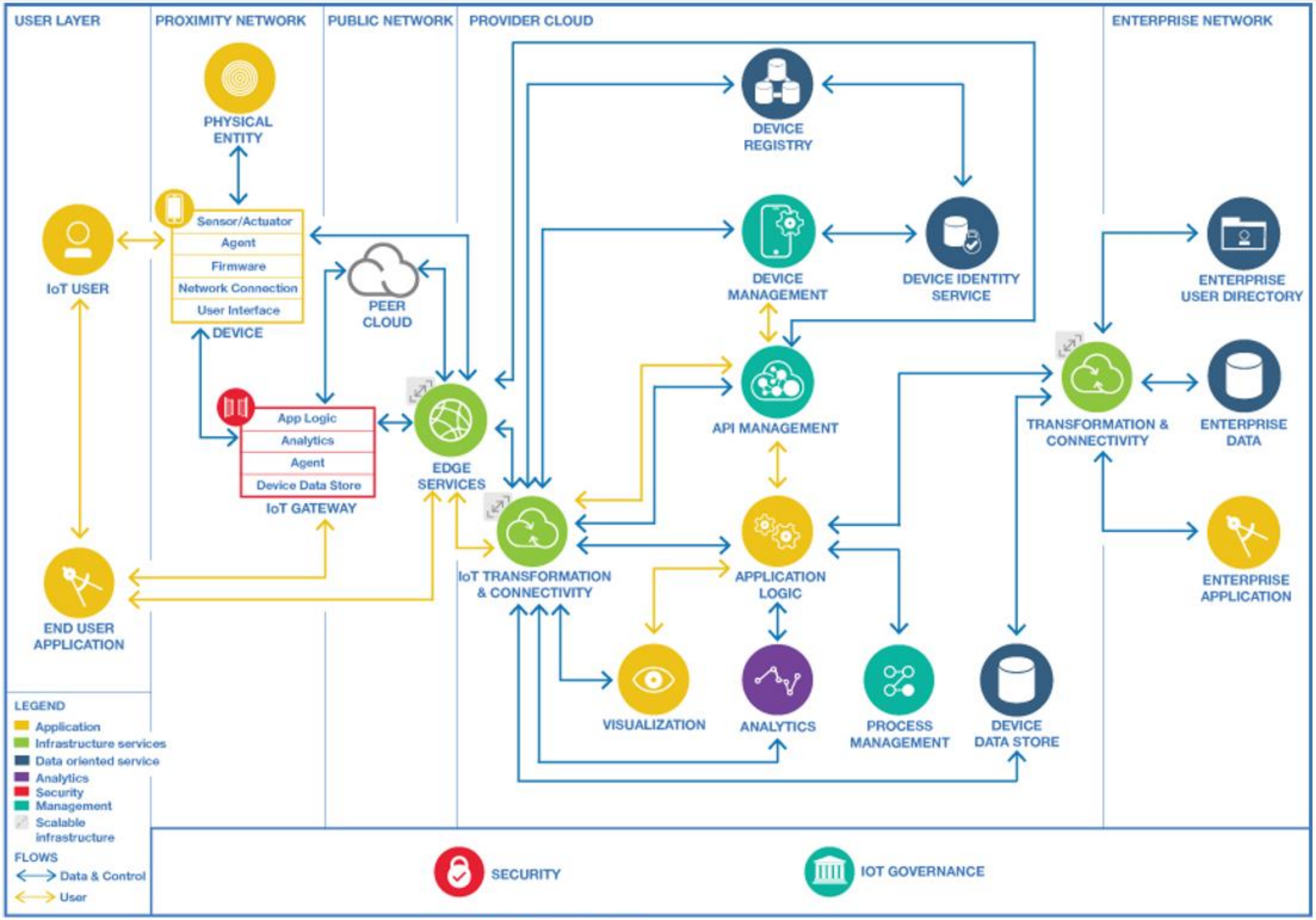


- Motion JPEG stream
  - available on the Internet
- Threshold

- Virtualization for sensor drivers

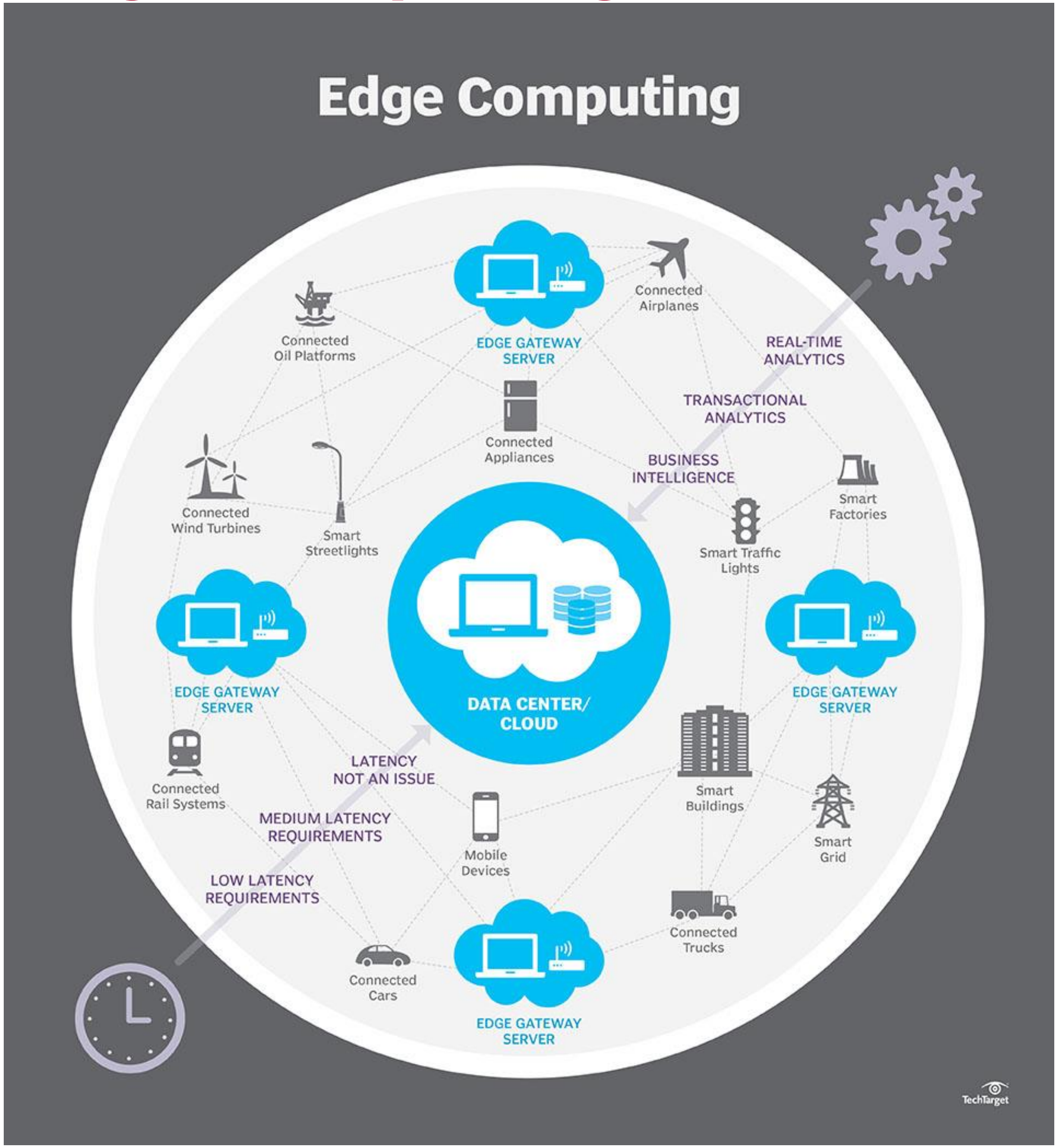
Cloud Customer Architecture for IoT

- http://www.cloud-council.org/deliverables/CSCC-Cloud-Customer-Architecture-for-IoT.pdf



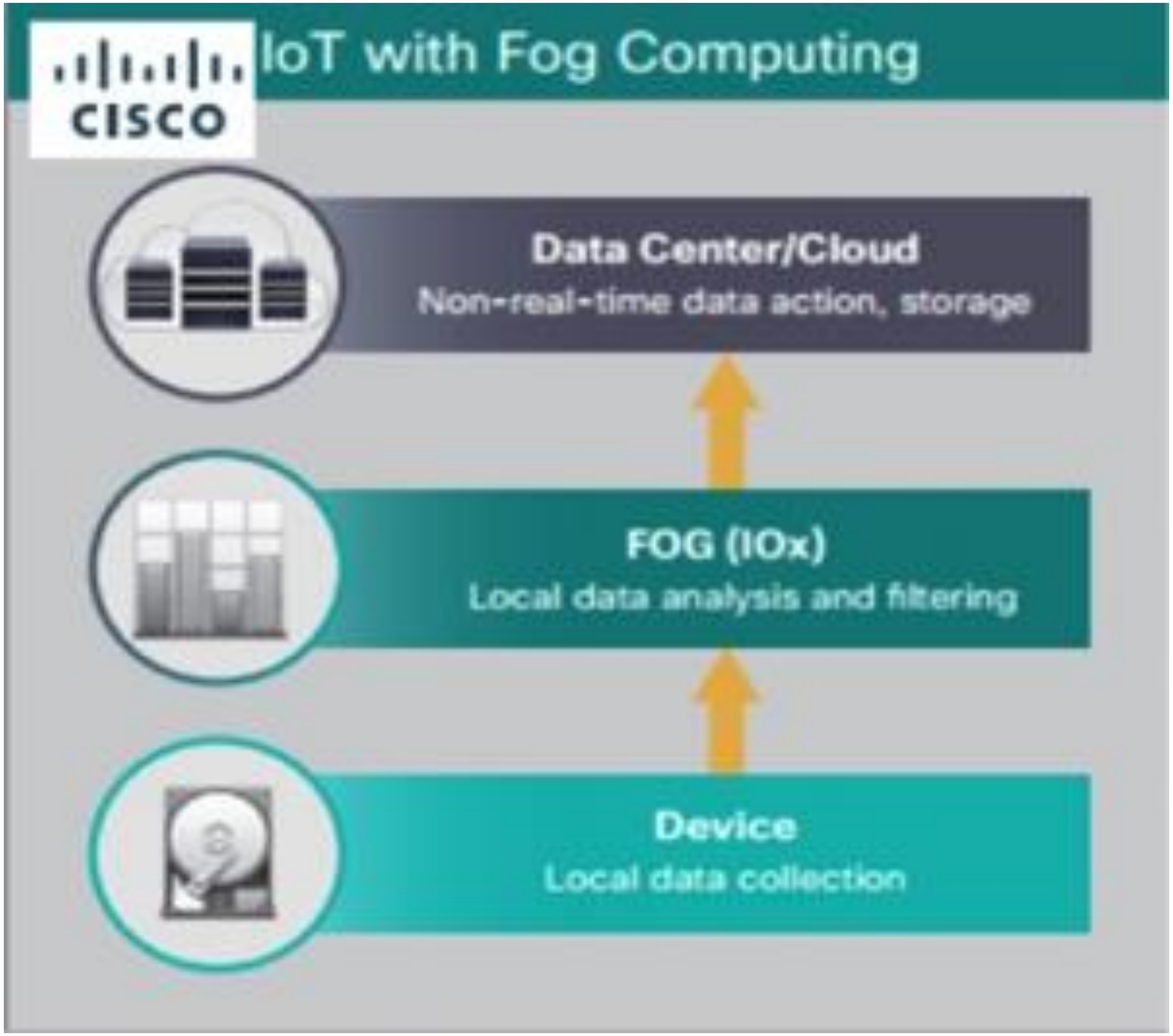
 6

Edge computing

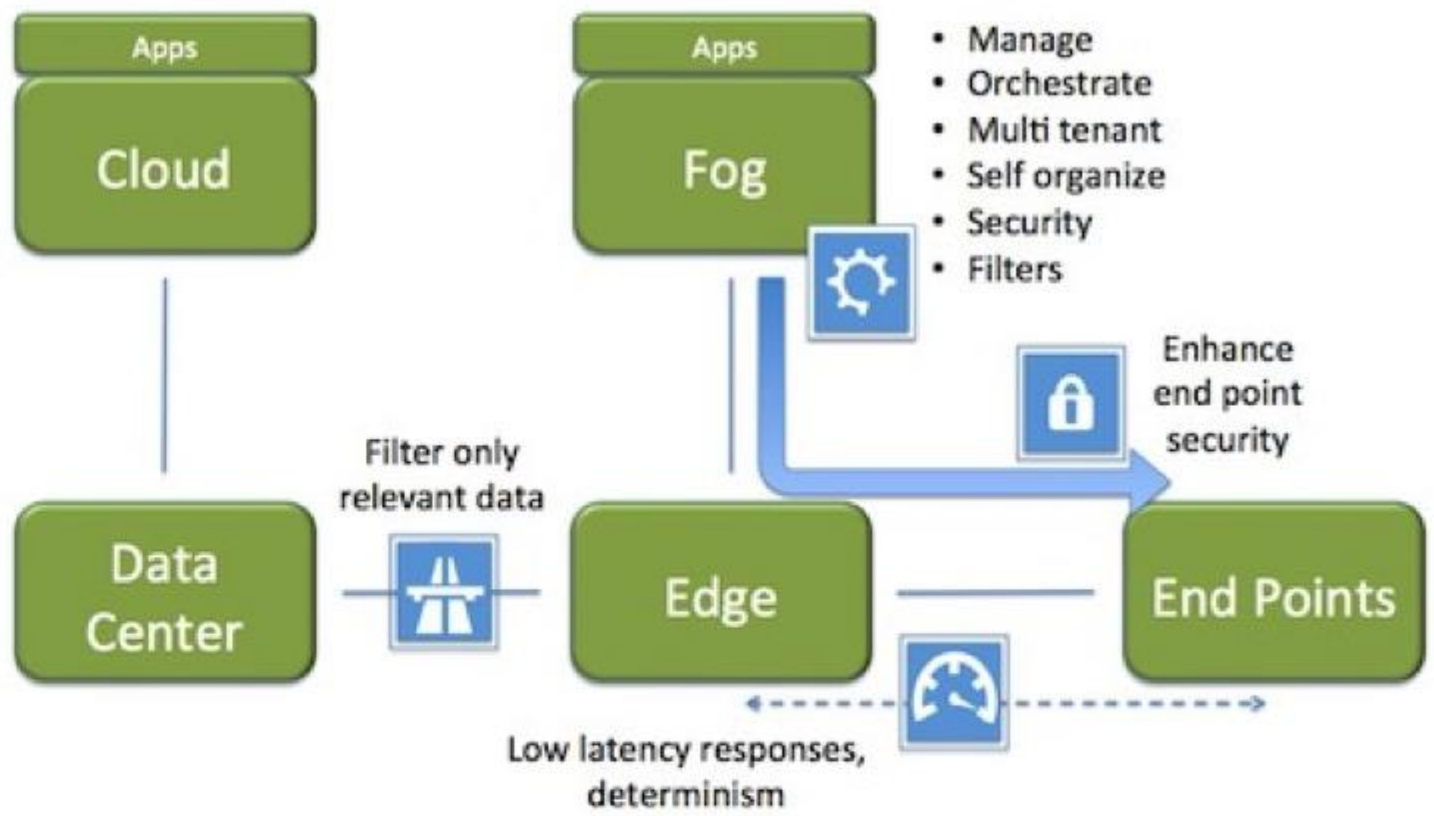


- Techtarget: Edge computing definition

Fog computing



Edge and fog computing



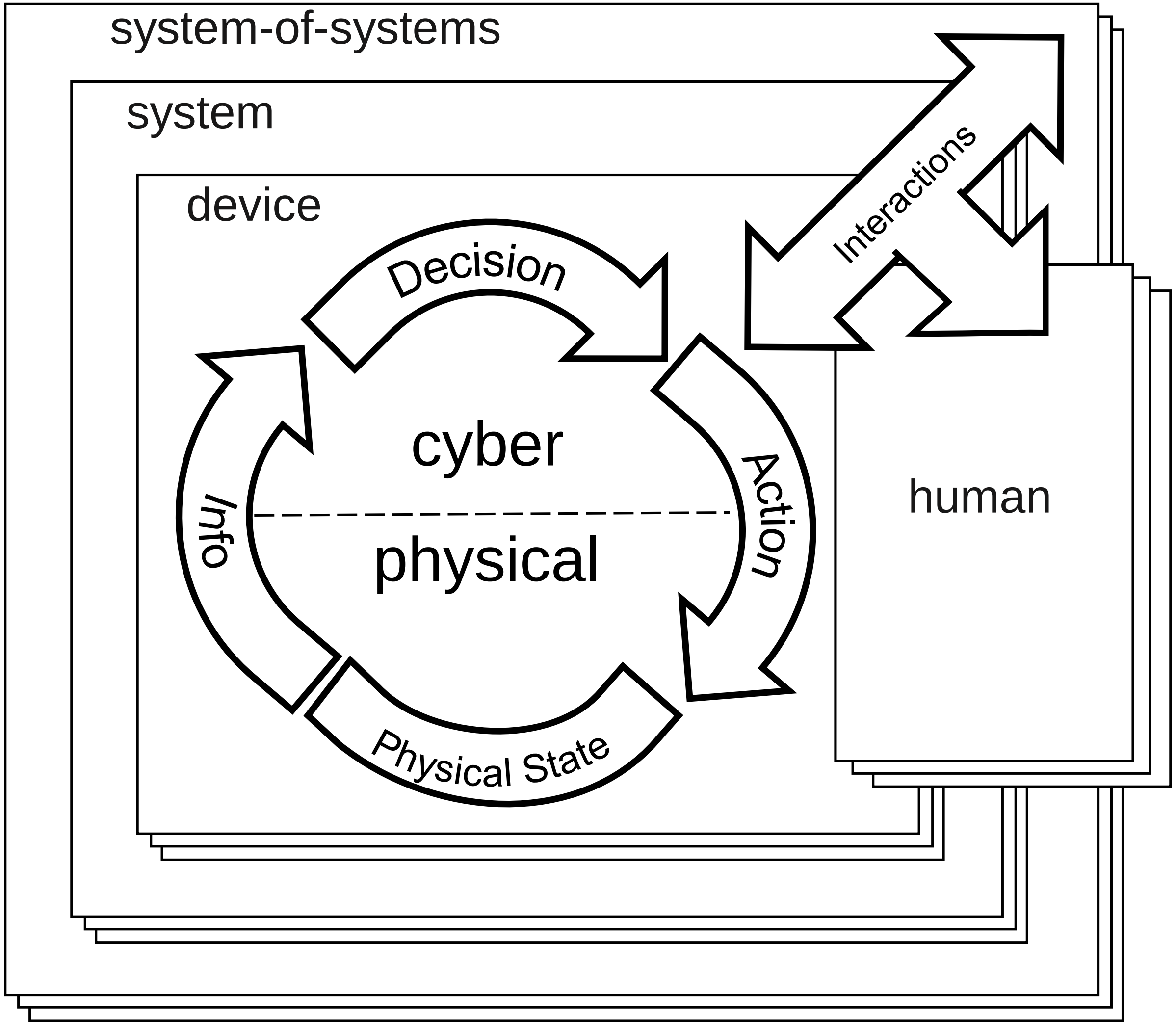
End of lecture #1

Cost impact estimation

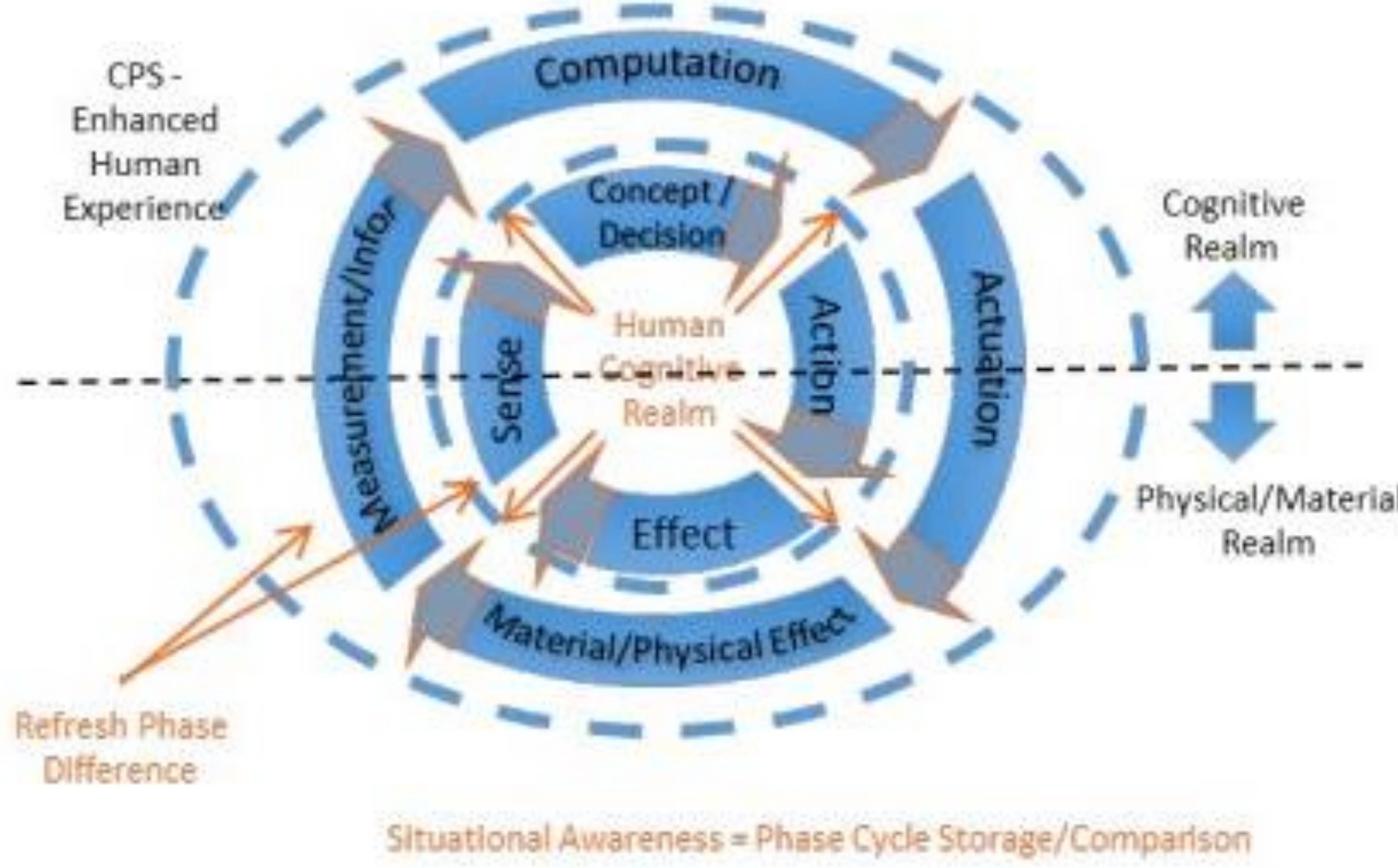
# of System Requirements	Easy	Nom.	Diff.
# New	0,5	1,0	5,0
# Design For Reuse	0,7	1,4	6,9
# Modified	0,3	0,7	3,3
# Deleted	0,3	0,5	2,6
# Adopted	0,2	0,4	2,2
# Managed	0,1	0,2	0,8

1. Quality and stability Modification: ~ 70% !
2. Requirement set complexity reduction
   - 4 similar problems
     - Separate solution: $4 \times New = \mathbf{400\%}$
     - Global solution: $1 \times Reuse + 4 \times Adopt = \mathbf{300\%}$

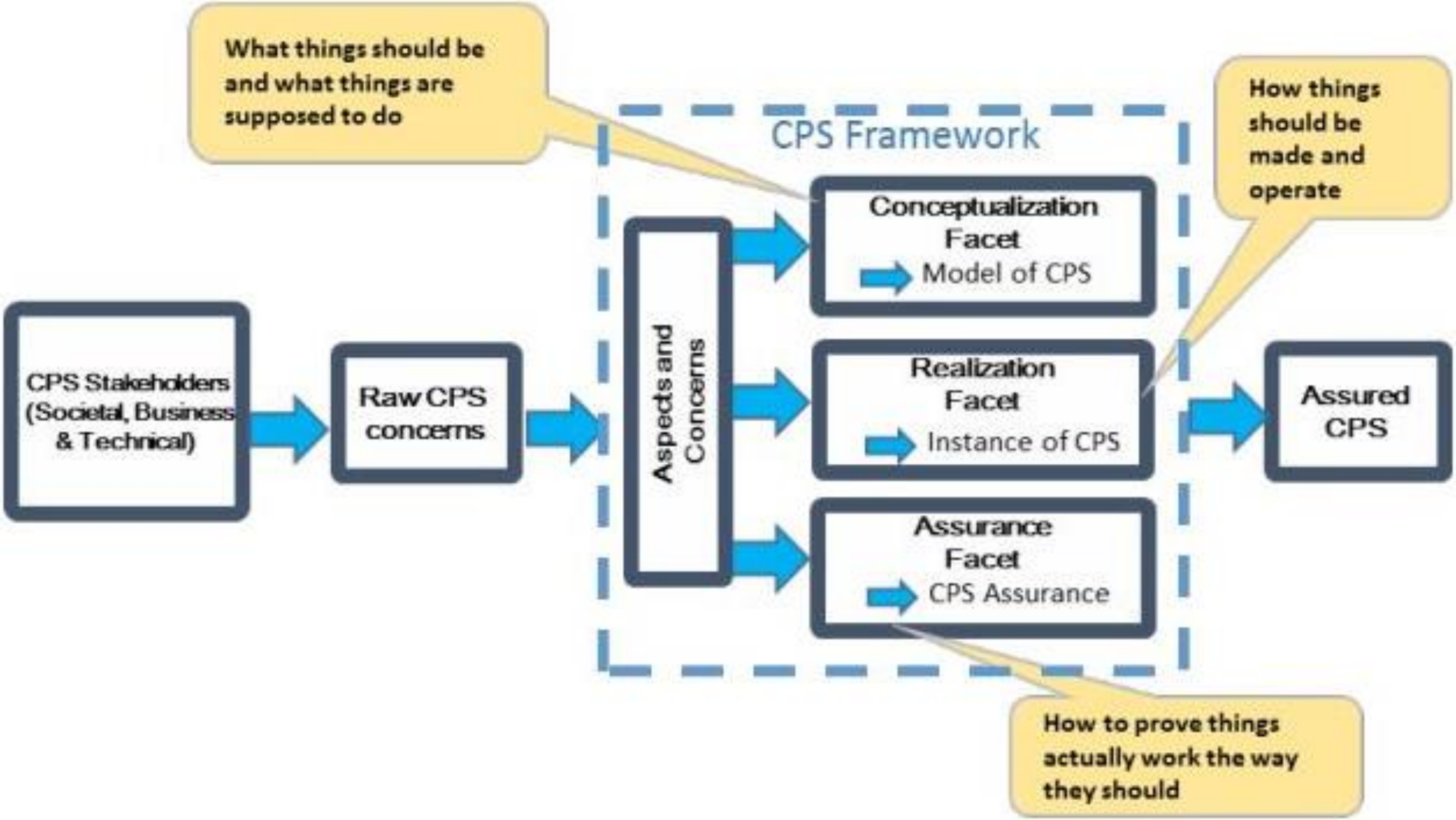
NIST CPS Framework



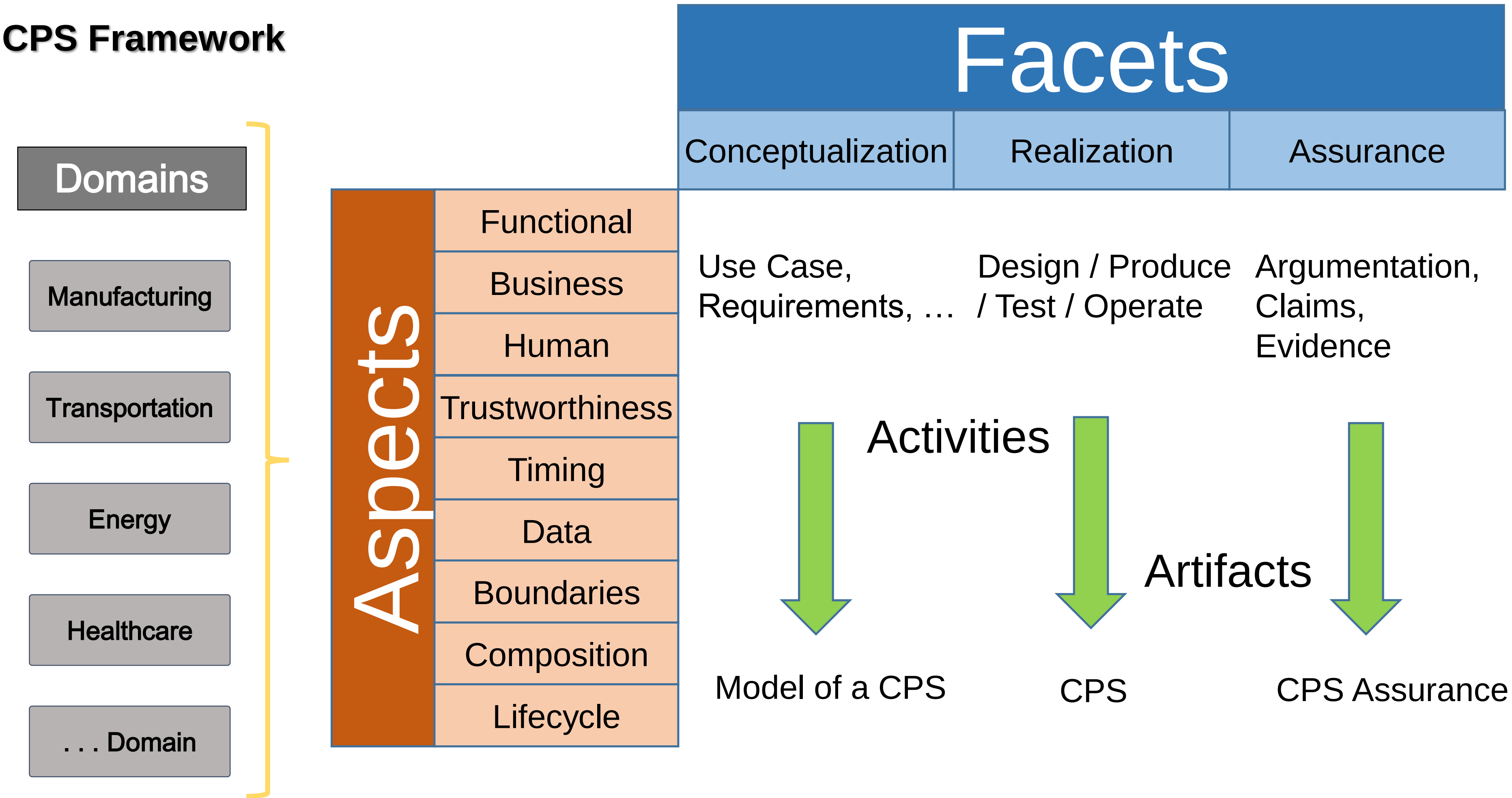
NIST CPS Cognitive Cycle



NIST CPS Framework for System Design



CPS Framework



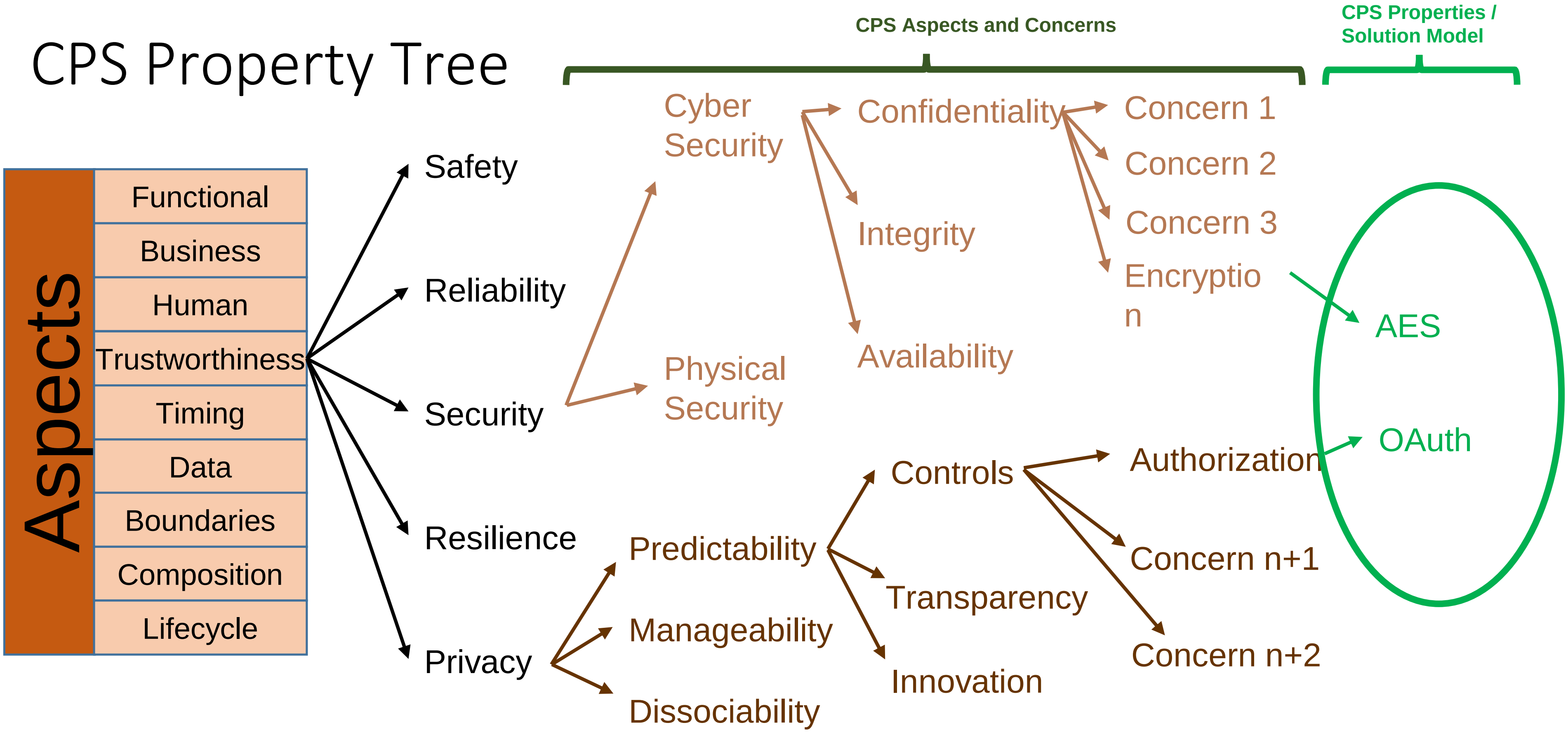
Aspects

Aspect	Description
Functional	Concerns about function including sensing, actuation, control, communications, physicality, etc.
Business	Concerns about enterprise, time to market, environment, regulation, cost, etc.
Human	Concerns about human interaction with and as part of a CPS.
Trustworthiness	Concerns about trustworthiness of CPS including security, privacy, safety, reliability, and resilience.
Timing	Concerns about time and frequency in CPS, including the generation and transport of time and frequency signals, timestamping, managing latency, timing composability, etc.
Data	Concerns about data interoperability including fusion, metadata, type, identity, etc.
Boundaries	Concerns related to demarcations of topological, functional, organizational, or other forms of interactions.
Composition	Concerns related to the ability to compute selected properties of a component assembly from the properties of its components. Compositionality requires components that are composable: they do not change their properties in an assembly. Timing composability is particularly difficult.
Lifecycle	Concerns about the lifecycle of CPS including its components.

Concerns

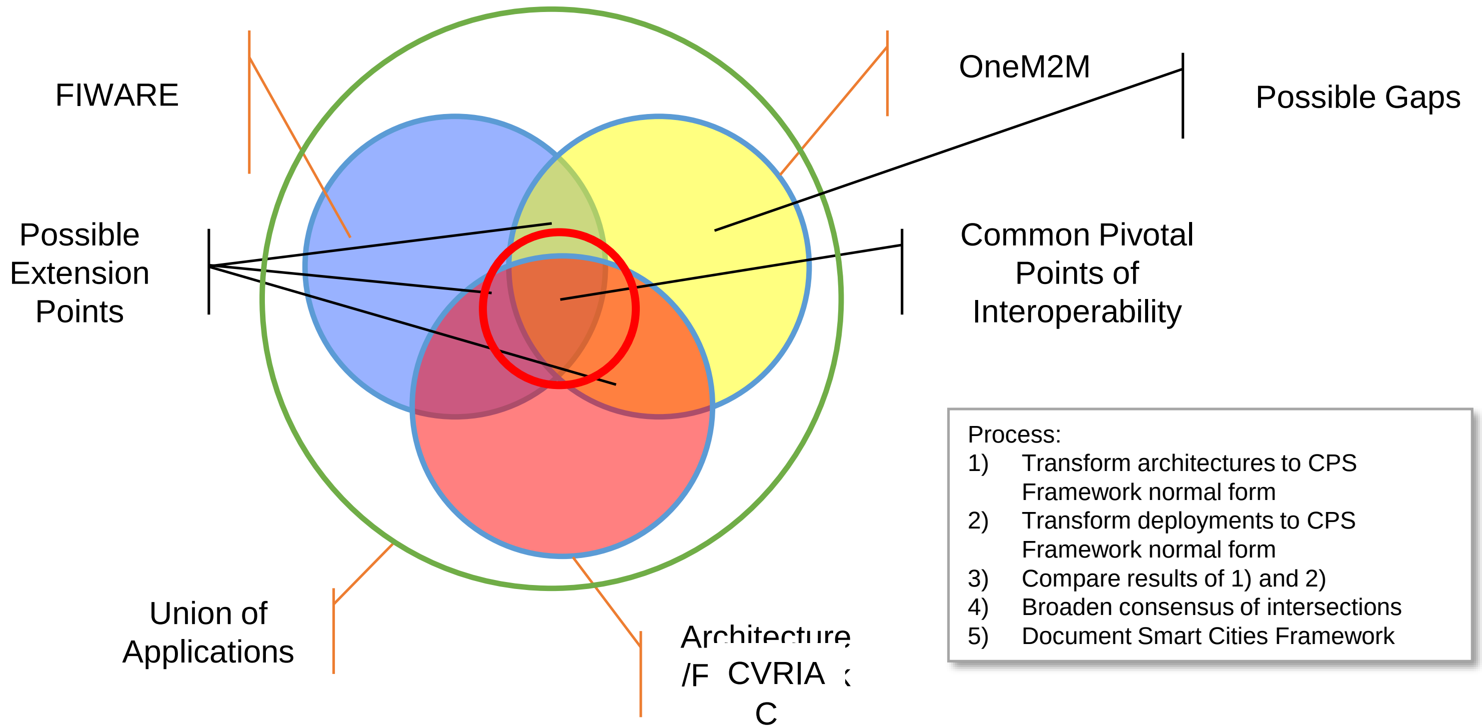
Aspect	Concern	Description
		the ability to modify a CPS or its function, if necessary.
Functional	**functionality**	Concerns related to the function that a CPS provides.
Functional	**manageability**	Concerns related to the management of CPS function. For example, Managing Timing in complex CPS or SoS is a new issue with CPS that did not exist before. It is being developed with new standards
Functional	**measurability**	Concerns related to the ability to measure the characteristics of the CPS.
Functional	**monitorability**	Concerns related to the ease and reliability with which authorized entities can gain and maintain awareness of the state of a CPS and its operations. Includes logging and audit functionality.
Functional	**performance**	Concerns related to the ability of a CPS to meet required operational targets.
Functional	**physical**	Concerns about purely physical properties of CPS including seals, locks, safety, and EMI.
Functional	**physical context**	Concerns relating to the need to understand a specific observation or a desired action relative to its physical position (and uncertainty.) While this information is often implied and not explicit in traditional physical systems, the distributed, mobile nature of CPS makes this a critical concern.
Functional	**sensing**	Concerns related to the ability of a CPS to develop the situational awareness required to perform its function.

CPS Property Tree



A secure, privacy protected message exchange might consist of the simultaneous (set of) properties:
{Trustworthiness.Security.Cybersecurity.Confidentiality.Encryption.AES, Trustworthiness.Privacy.Predictability.Controls.Authorization.OAuth}

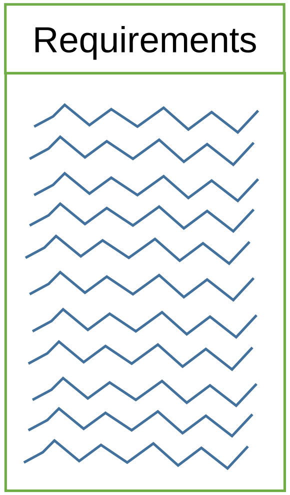
How to Discover Consensus



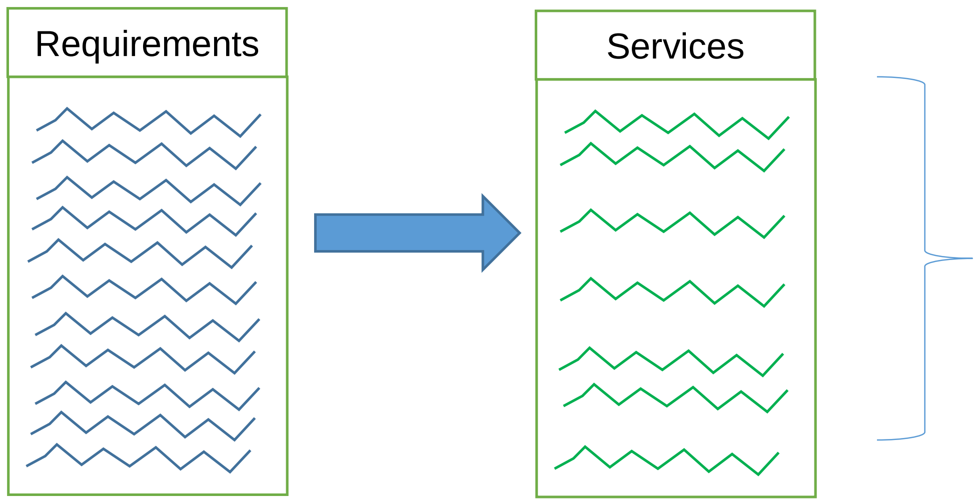
Process:
1) Transform architectures to CPS Framework normal form
2) Transform deployments to CPS Framework normal form
3) Compare results of 1) and 2)
4) Broaden consensus of intersections
5) Document Smart Cities Framework

Specs to Pivotal Points of Interoperability

Technology level (Device, System, System of Systems) Technology scope description (text) Zone of Concerns (text -- Enterprise, Field, Mobile, Premises)	Is a Solution Provided?		
Aspect/Concern	CVRIA	FIWARE	
Functional	yes		
physical actuation	yes	yes	no
communication	yes	yes	yes
Syntactic Interoperability	see nest 3		yes
OSI-Application	yes		yes
OSI-Presentation	yes		
Network Interoperability	see nest 3		
OSI-Session	yes	yes	
OSI-Transport	yes		no
OSI-Network	yes		no
Basic Connectivity	see nest 3	no	no
OSI-Data Link	yes		no
OSI-Physical	yes		no



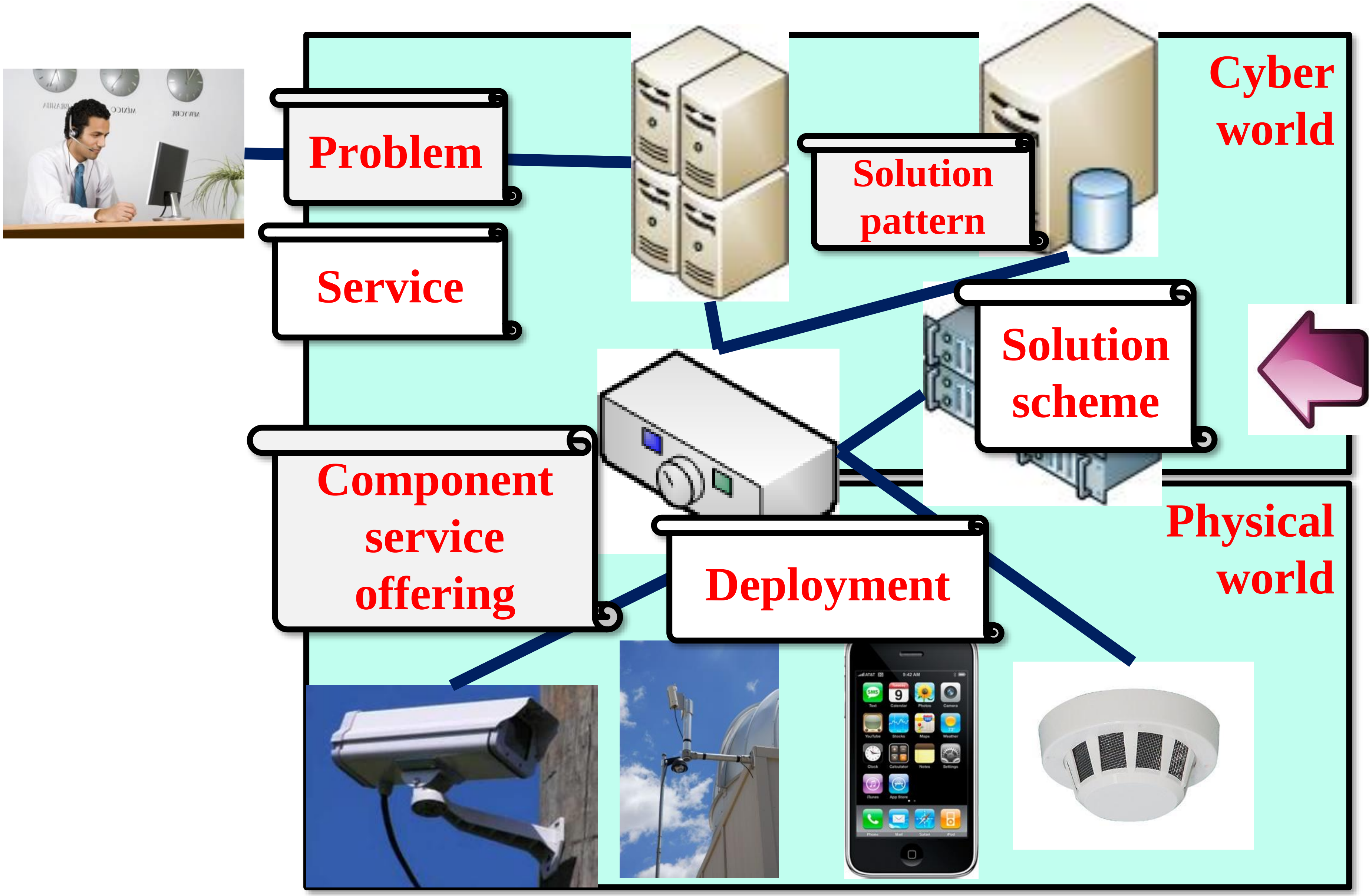
Zones of Concern: From Requirements To Services



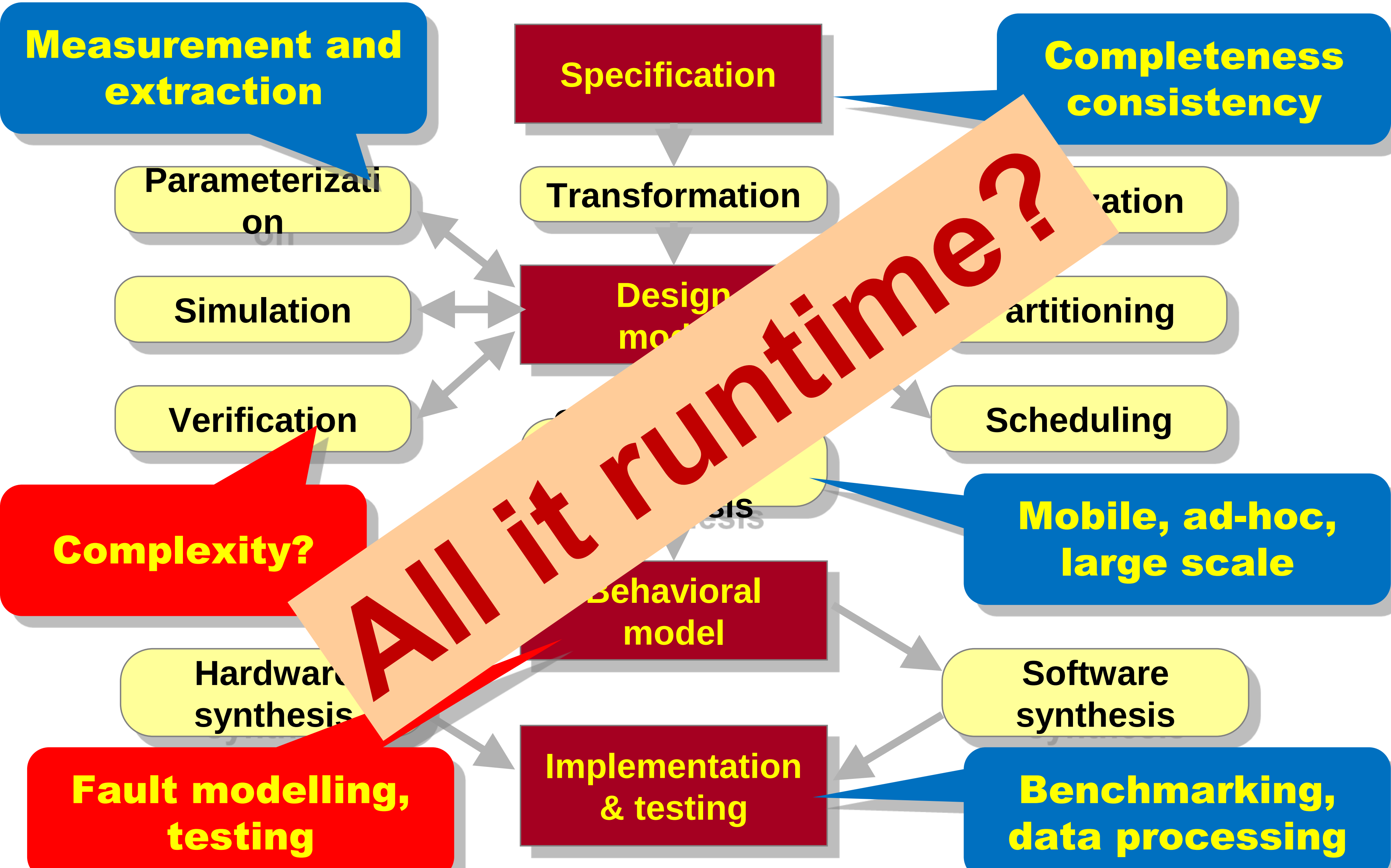
Zone of Concerns = bundles of services that address a “vector” of concerns

E.g. CyberSecurity Zone of Concerns: Authorization service + Confidentiality Service

COMPOSITION OF CYBER-PHYSICAL SYSTEMS


Problem
Service
Solution pattern
Cyber world
Solution scheme
Component service offering
Deployment
Physical world

Critical CPS design and challenges



Development Process for Critical Systems

Unique Development Process (Traditional V-Model)

Critical Systems Design

- requires a certification process
- to develop justified evidence
- that the system is free of flaws

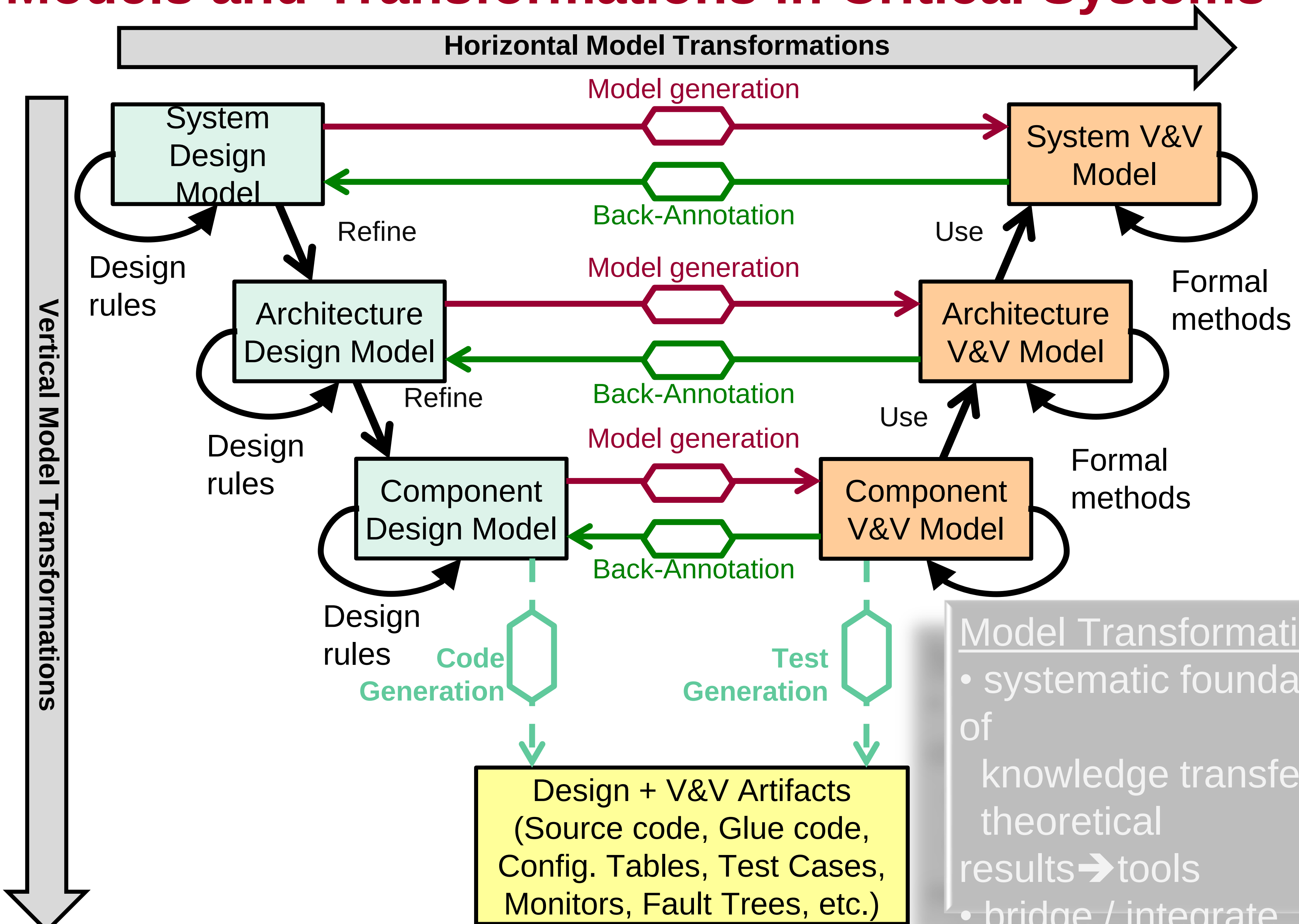
Software Tool Qualification

- obtain certification credit
- for a software tool
- used in critical system design

Innovative Tool → Better System

Qualified Tool → Certified Output

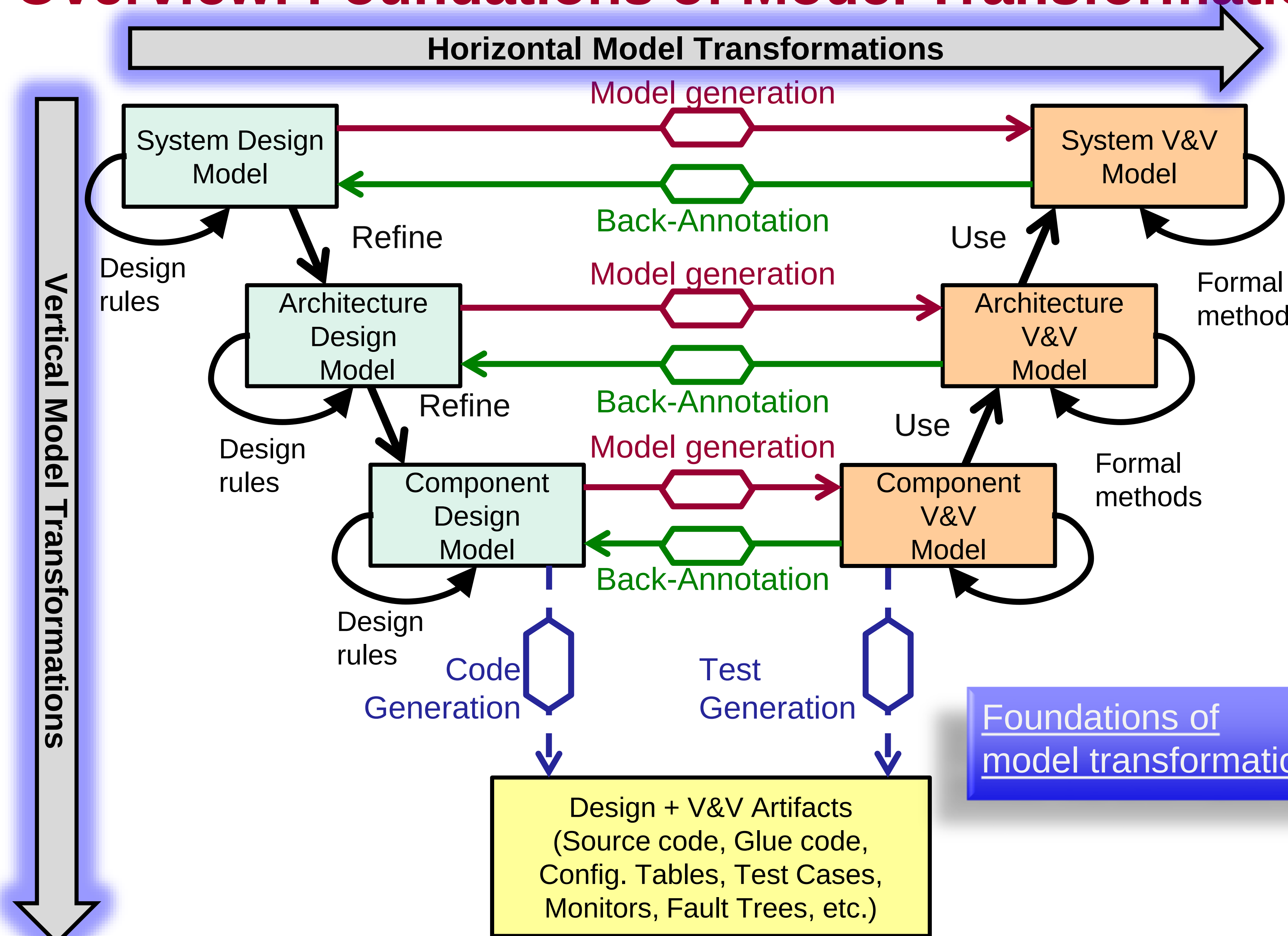
Models and Transformations in Critical Systems



Model Transformations

- systematic foundation of knowledge transfer: theoretical results→tools
- bridge / integrate existing

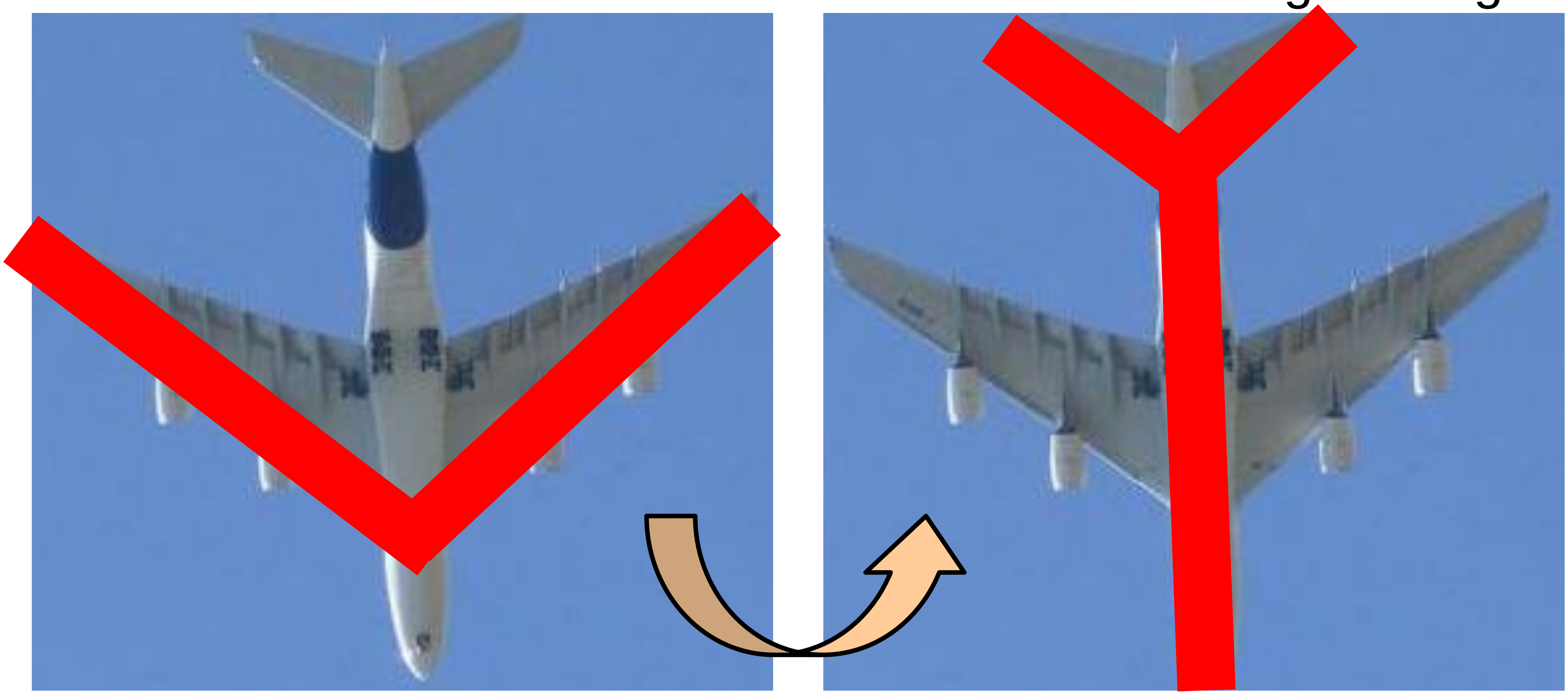
Overview: Foundations of Model Transformations



[Foundations of model transformations]

Model-Driven Engineering of Critical Systems

Traditional V-Model | Model-Driven Engineering



- DO-178B/C: Software Considerations in Airborne Systems and Equipment Certification (RTCA, EUROCAE)
- Steven P. Miller: Certification Issues in Model Based Development (Rockwell Collins)

<u>Main ideas of MDE</u>

- early validation of system models
- automatic source code generation

➔ quality++ tools ++ development cost--

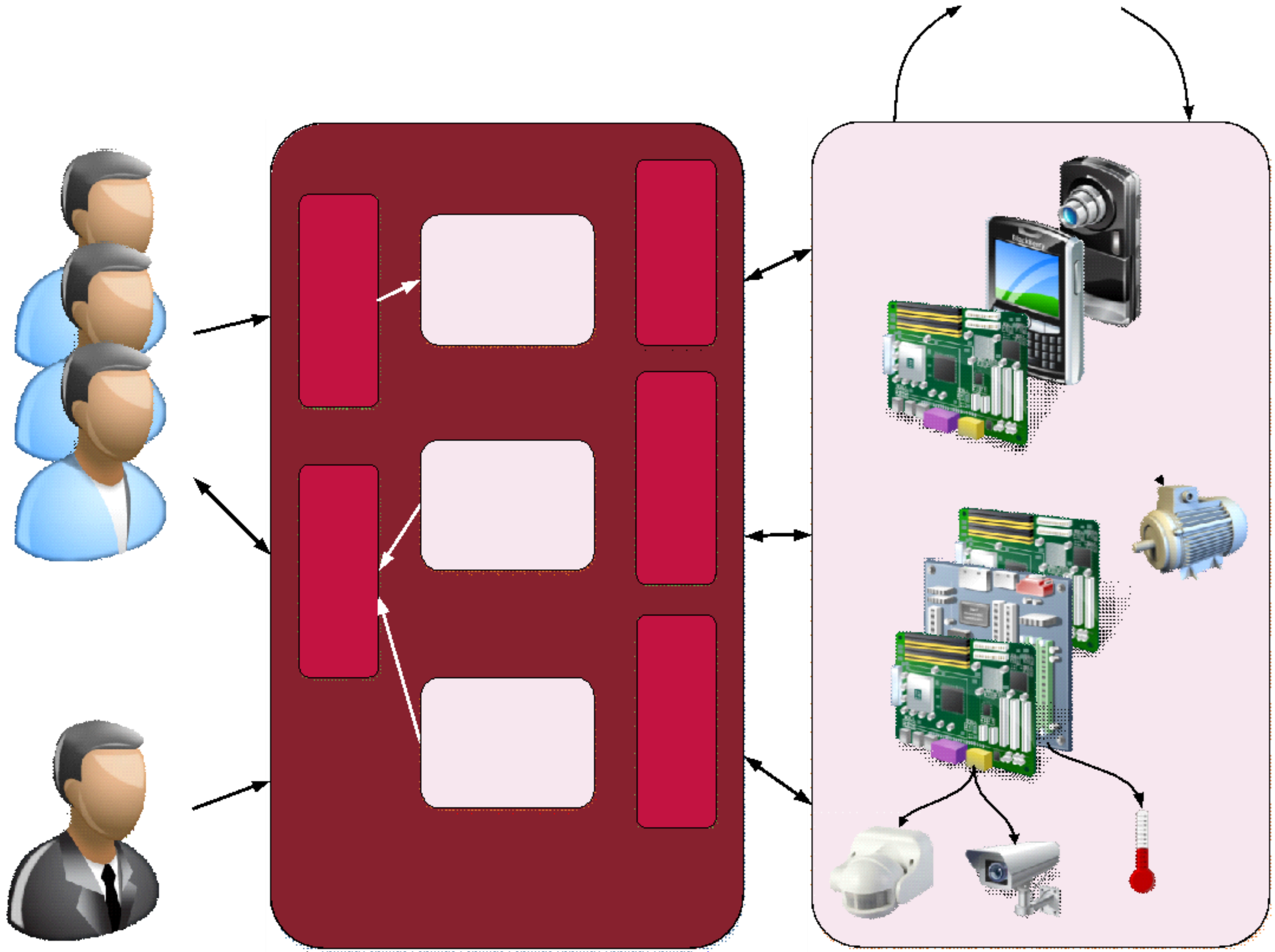
Design schemes

- Detecting changes in system state
- Detecting changes in environment
- Reconfiguration
  - Resource allocation
    - generation of new application/middleware
    - replacement of sensors
    - new information fusion etc.
  - Design space exploration
    - Qualitative
    - Quantitative

Composability

- System design principle:
  - recombinant components
  - can be assembled in various combinations
- Meaningful fusion of self-contained services
- Provide interoperability of devices
  - Bridging the gap between different
    - physical,
    - computational and
    - communication capabilities

Dynamic composition of cyber-physical systems



Requirements of composability

- User interface for describing domain specific constraints
- Abstract interfaces between cooperating nodes
  - Embedded systems connected to sensors and actuators
  - Mobile devices
  - Conventional computing devices,
  - cloud resources
- Automated system maintenance,
- Fault tolerance, redundancy

Composability through abstraction

- Finding a conceptual domain where devices are homogeneous
  - Possibly the lowest level of such domains
- Abstraction of computing capabilities
  - Virtualization (QEMU, Java, Python)
- Abstraction of physical capabilities
  - Sensor virtualization (SOS),
  - Feature discovery
- Abstraction of communication capabilities
  - Self-describing communication interface (SOS)

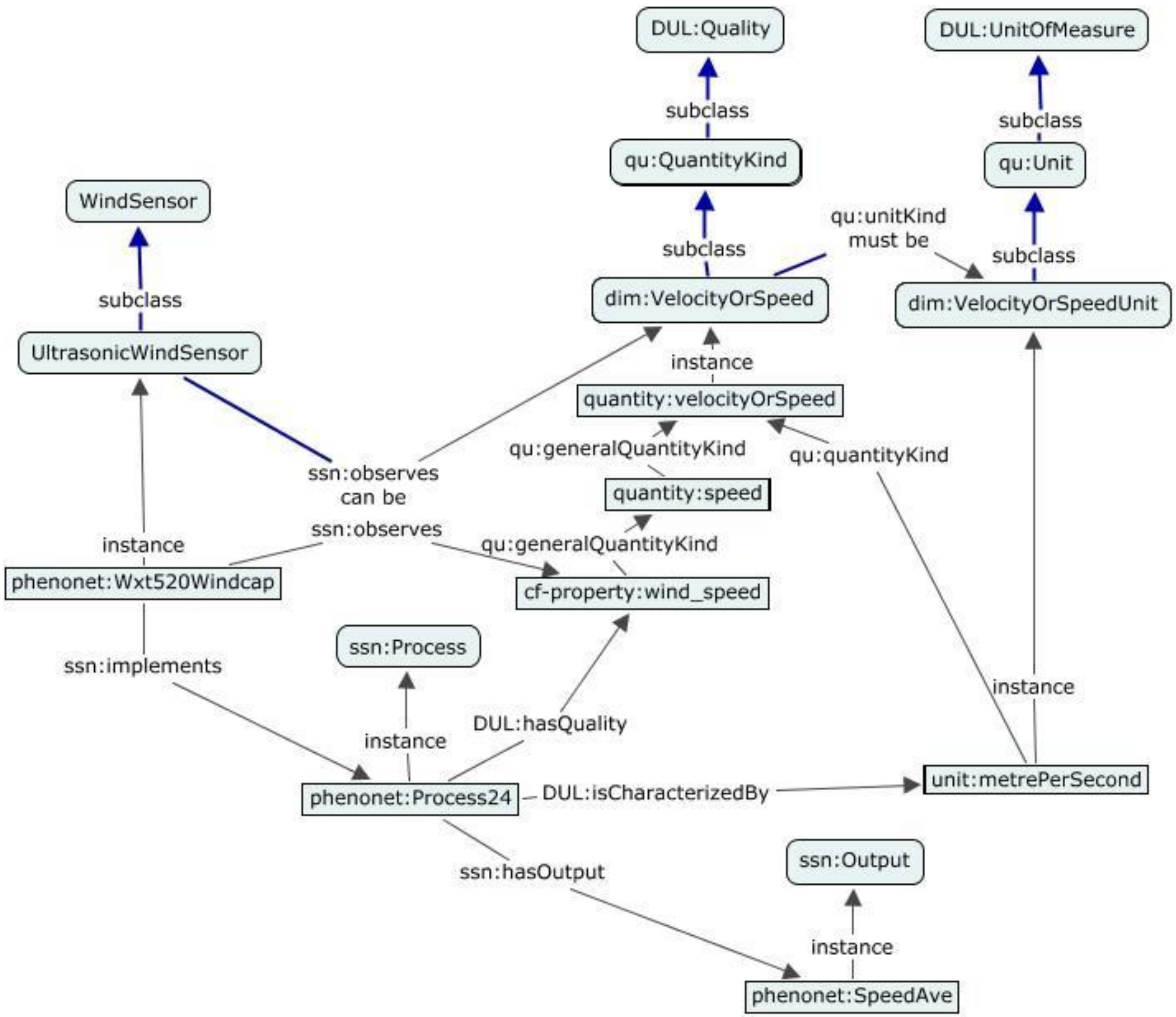
Sensor Observation Service (SOS)

- Abstracts sensor data and communication
  - Self-describing sensor information database
  - Stores sensor data with geographic relevance
  - Efficient data queries
    - temporal or spatial filters
- Members of the CPS
  - direct communication with the SOS

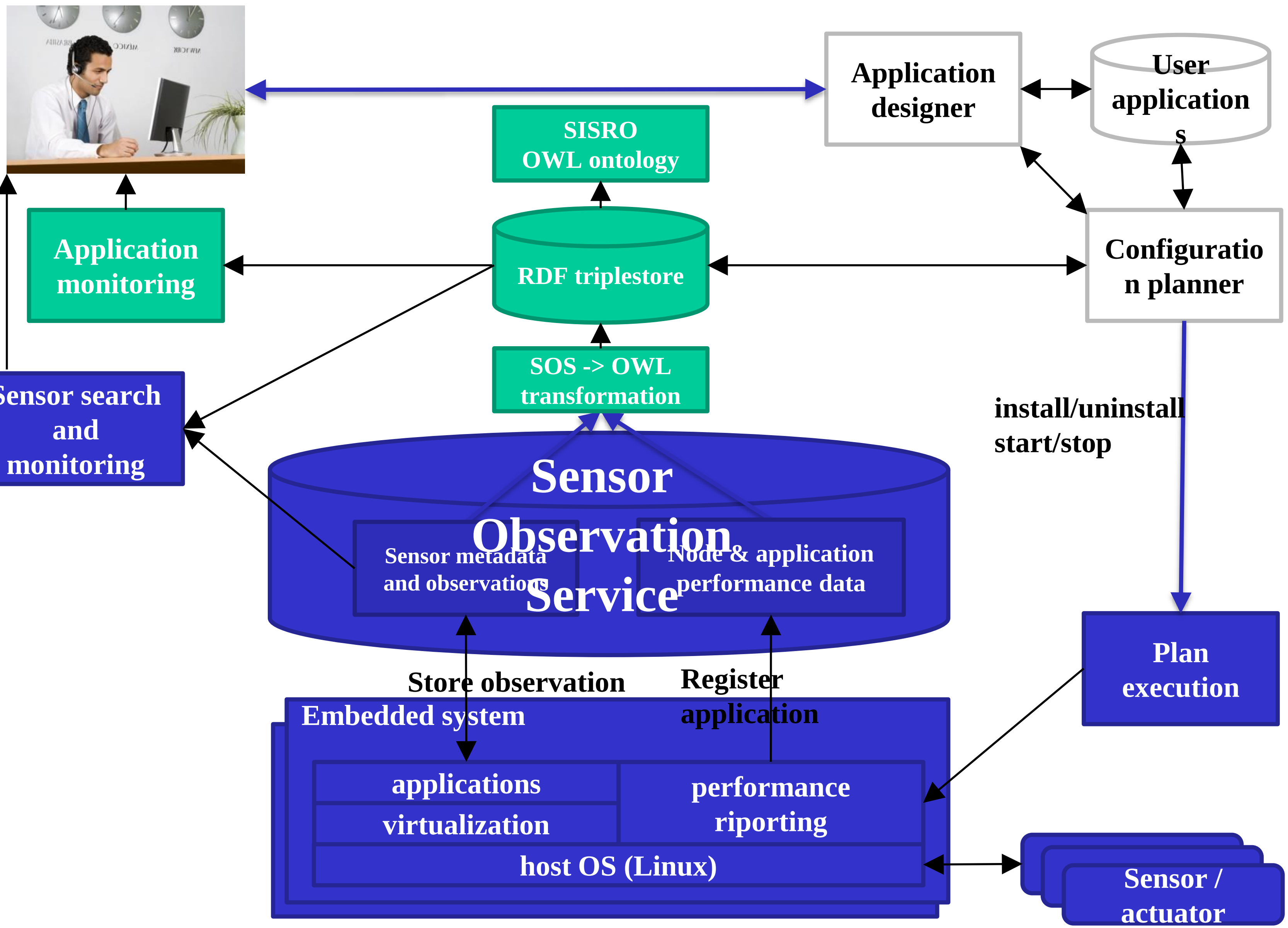
Semantic Sensor Network (SSN) ontology

- W3C Incubator Group (2009-2011)
- Capabilities of sensors and sensor networks
  - Formal ontology
- Covers:
  - system, deployment, sensing device, process
  - observed phenomenon (e.g. wind)
    - sensor type (e.g. ultrasonic wind sensor)
    - property (e.g. wind direction)
    - meaning (e.g. blows from direction)
    - unit of measure (e.g. radian)
  - operating range (e.g. temperature, humidity, ...)

SSN example: wind sensor



Architecture



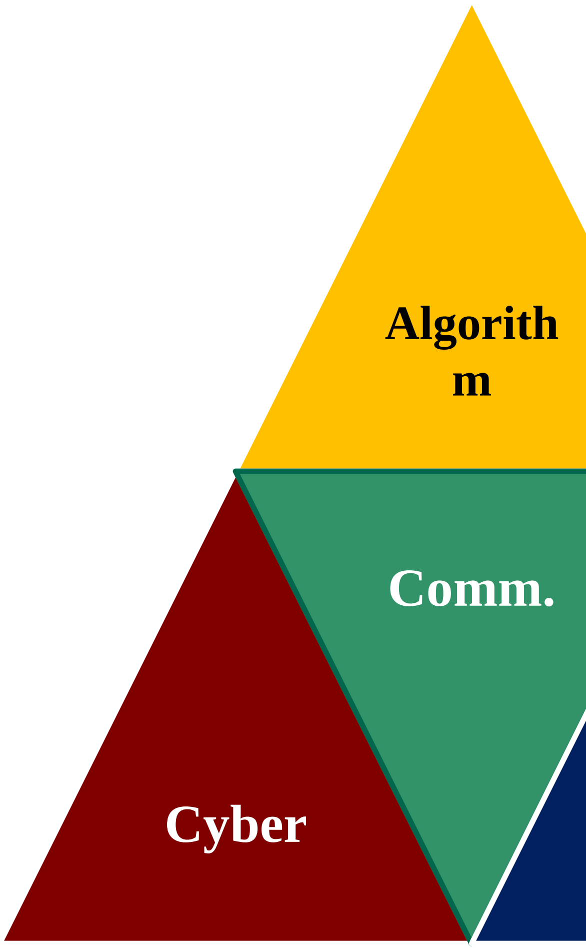
Opportunities and threats in the cps paradigm

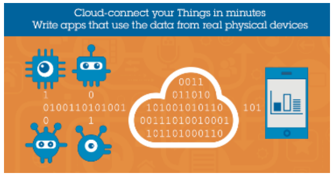
RESILIENCE

Self-* properties – dynamic challenges and solutions

Opportunities-algorithmic diversity

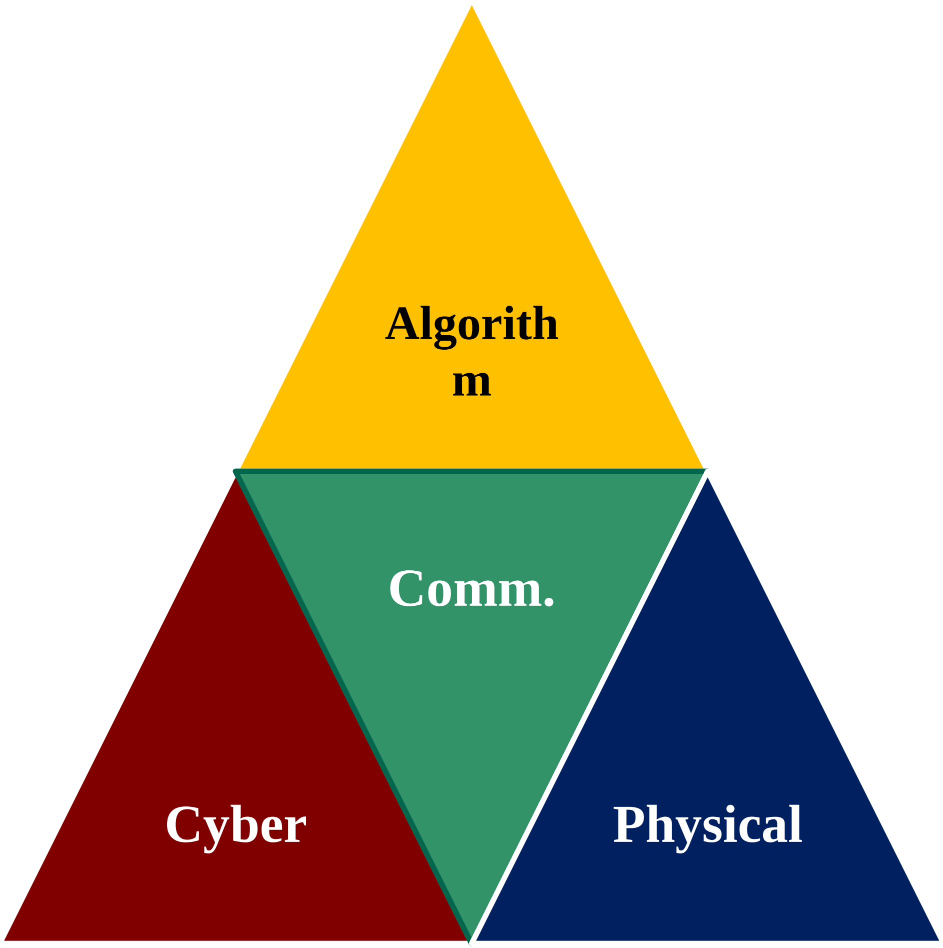
- "Meta-algorithms'
- Different principles
  - Speed control in Italy:
    - Radar
    - Laser
    - TUTOR
  - Resource requirements
- External providers
  - Aaas – algorithm as a service
  - External validator





Opportunities- resource redundancy

- Cheap computational redundancy, but
  - Depends on the reservation policy
- Virtualized network (SDN)
  - Fast failover
- Cheap sensors
  - Multitude of sensors



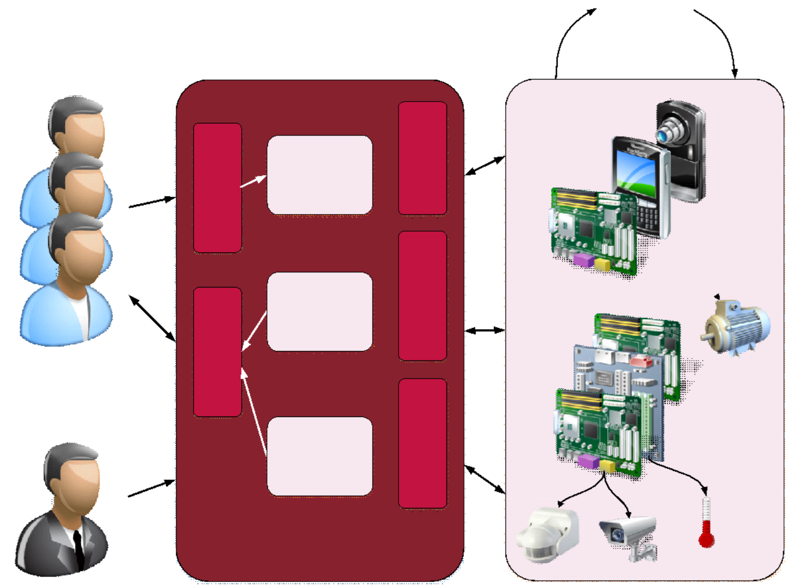
Dynamic reconfiguration of resources

User applications describe observational and processing constraints

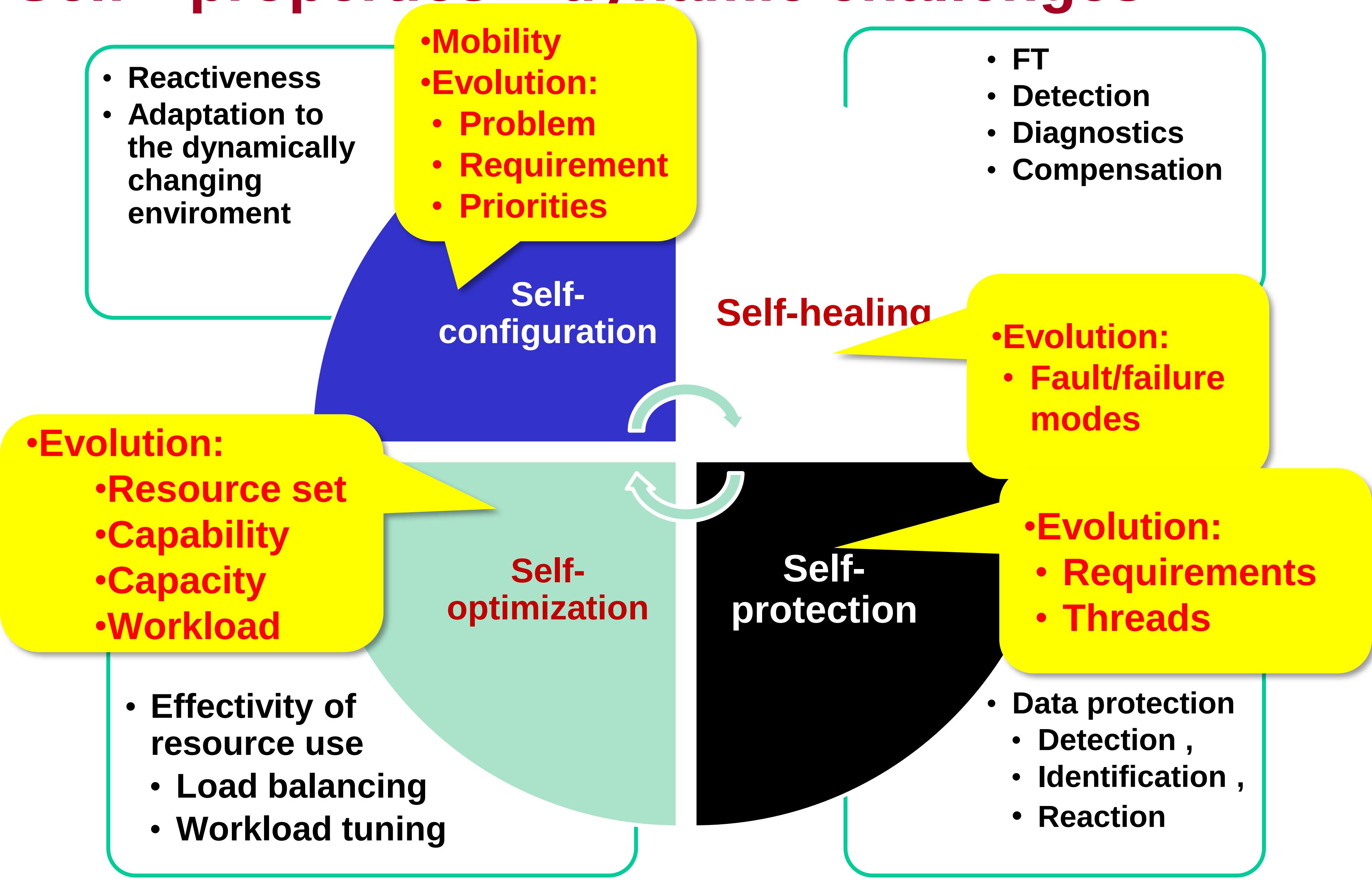
System state monitoring

Design space exploration

Performance monitoring Deployment



Self-* properties – dynamic challenges



Self-* properties – dynamic challenges

- Reactiveness
- Adaptation to the dynamically changing enviroment

•Mobility
•Evolution:
- Problem
- Requirement
- Priorities

- FT
- Detection
- Diagnostics
- Compensation

•Evolution:
- Fault/failure modes

•Evolution:
- •Resource set
- •Capability
- •Capacity
- •Workload

•Evolution:
- Requirements
- Threads

- Effectivity of resource use
  - Load balancing
  - Workload tuning

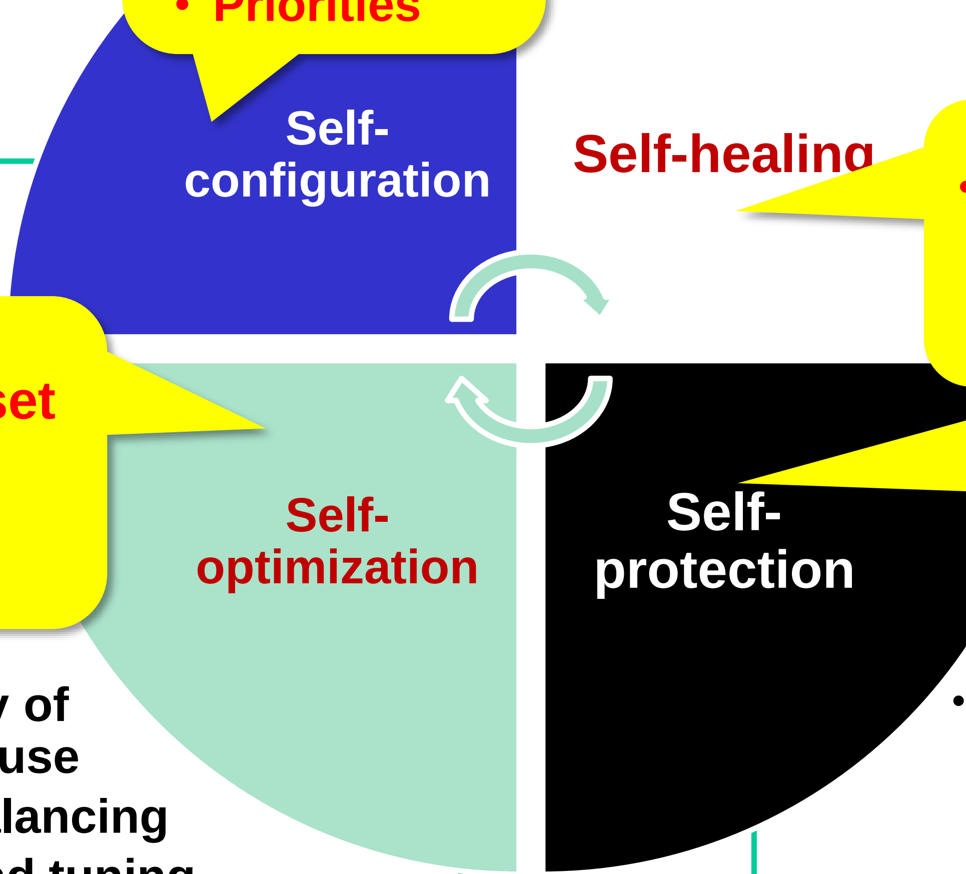
- Data protection
  - Detection ,
  - Identification ,
  - Reaction

Self-* properties – dynamic challenges

- Reactiveness
- Adaptation to the dynamically changing enviroment

•Mobility
•Evolution:
- Problem
- Requirement
- Priorities

- FT
- Detection
- Diagnostics
- Compensation



•Evolution:
- Fault/failure modes

•Evolution:
- •Resource set
- •Capability
- •Capacity
- •Workload

•Evolution:
- Requirements
- Threads

- Effectivity of resource use
  - Load balancing
  - Workload tuning

- Data protection
  - Detection ,
  - Identification ,
  - Reaction

Safety-critical systems are

- protected against worst-case technical faults, but
- unprotected against malicious attacks

THE HORRIBLE MOTIVATION - NEW DANGERS ARE HERE…

Polish teen derails tram after hacking train network

A 14-year-old Polish boy turned the tram system in the city of Lodz into his “train set”.

- a modified TV remote control to change track points, and derailed four vehicles.
- Twelve people injured.

Past ES products in service without the full spectrum of extrafunctional properties as design aspects

The Telegraph

Malware implicated in fatal Spanair plane crash

Authorities investigating the 2008 crash of Spanair flight 5022 have discovered a central computer system used to monitor technical problems in the aircraft was infected with malware.

An internal report issued by the airline revealed the infected computer failed to detect three technical problems with the aircraft, which if d[illegible]tected, may have prev[illegible] off...

ES: long life span

Security: evolving threats

Flight 5022 [illegible] takeoff from Madrid-Barajas International Airport two years ago today, killing 154 and leaving only 18 survivors.

msnbc.com

Safety contra security?

Safe, but not secure

- **People may escape danger from inside**

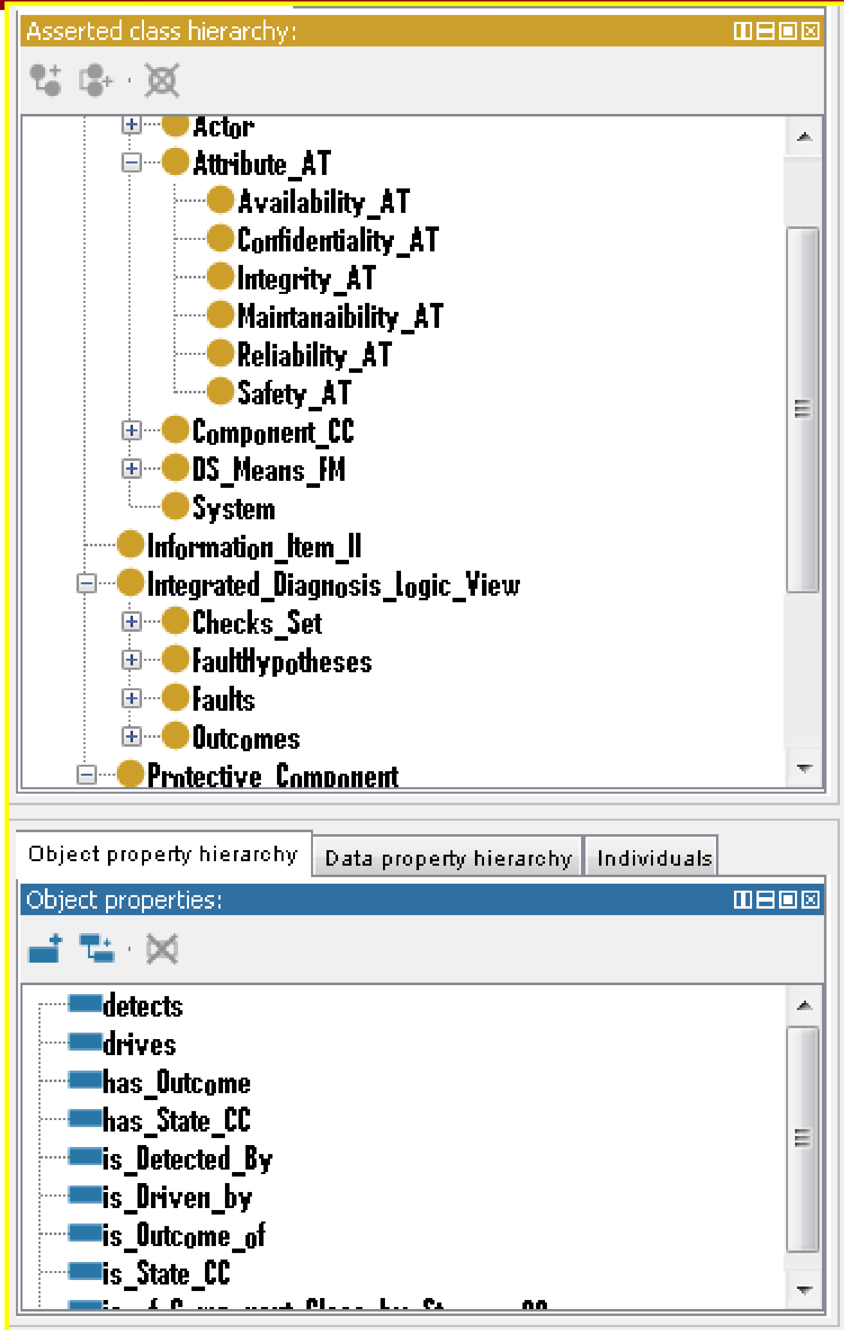
Secure, but not safe

- **No intruder can enter the gate**

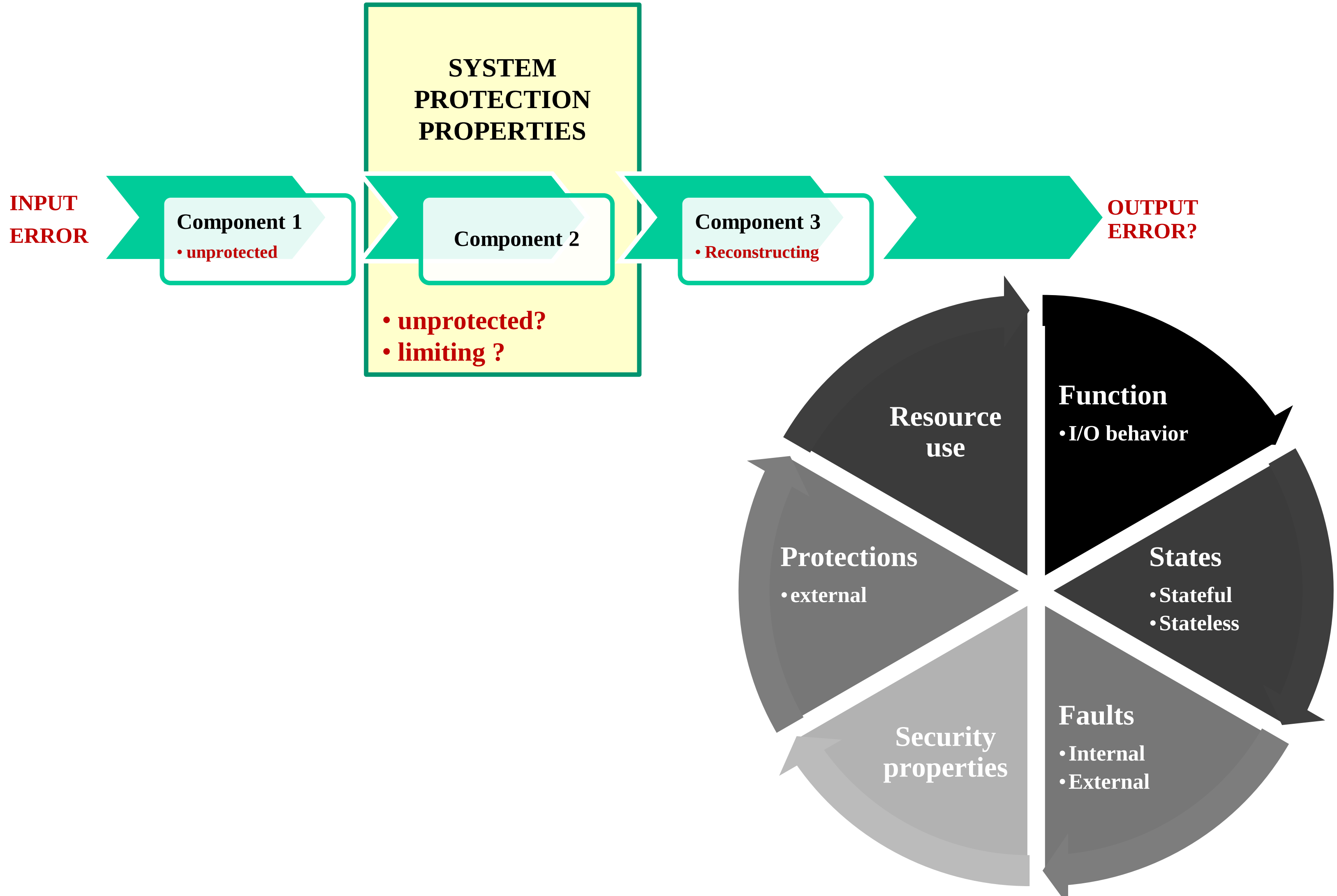
Specialization: error propagation/ protection

Introduces:

- Security aspects
- Protection profiles
- Error propagation attributes



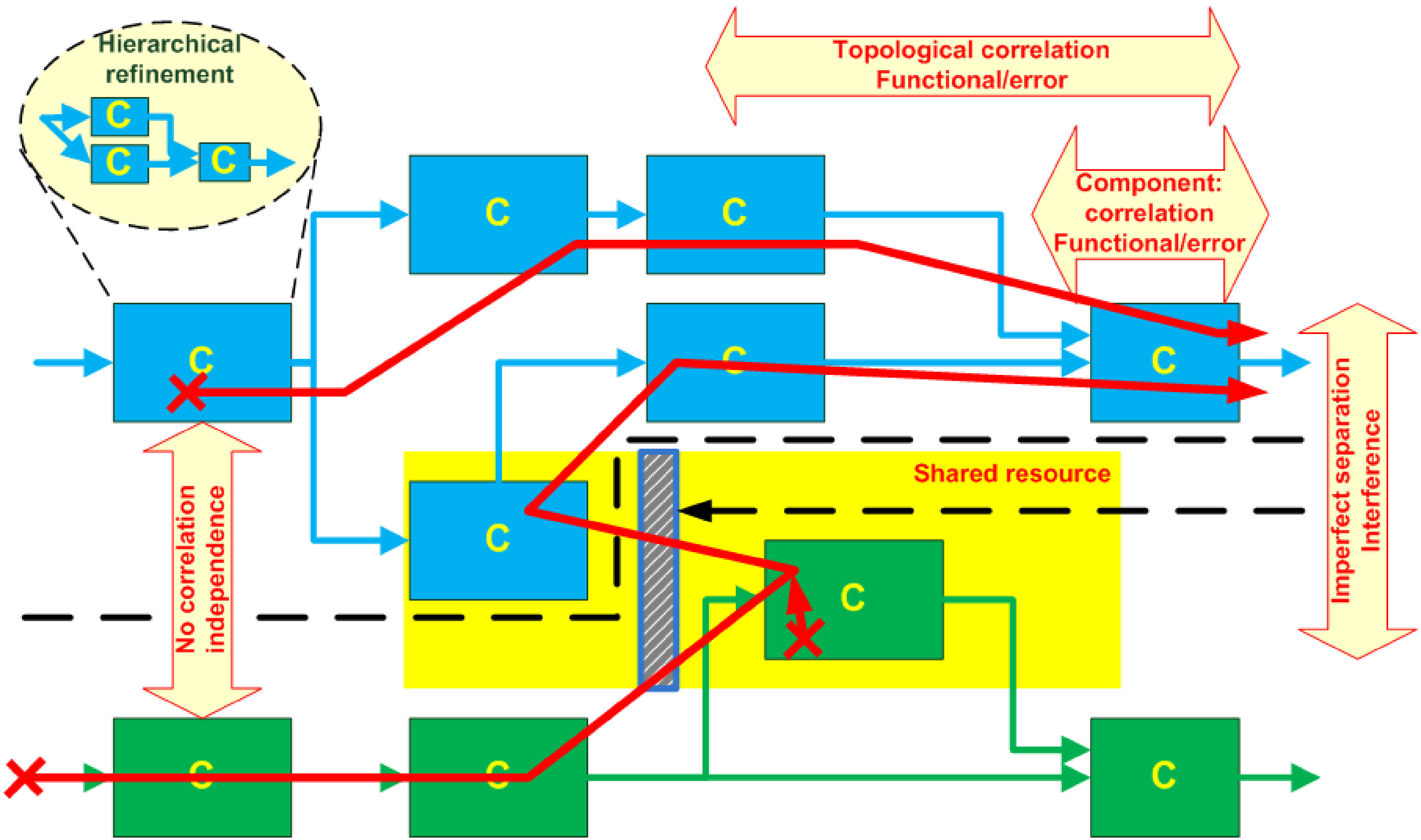
System level fault impact analysis



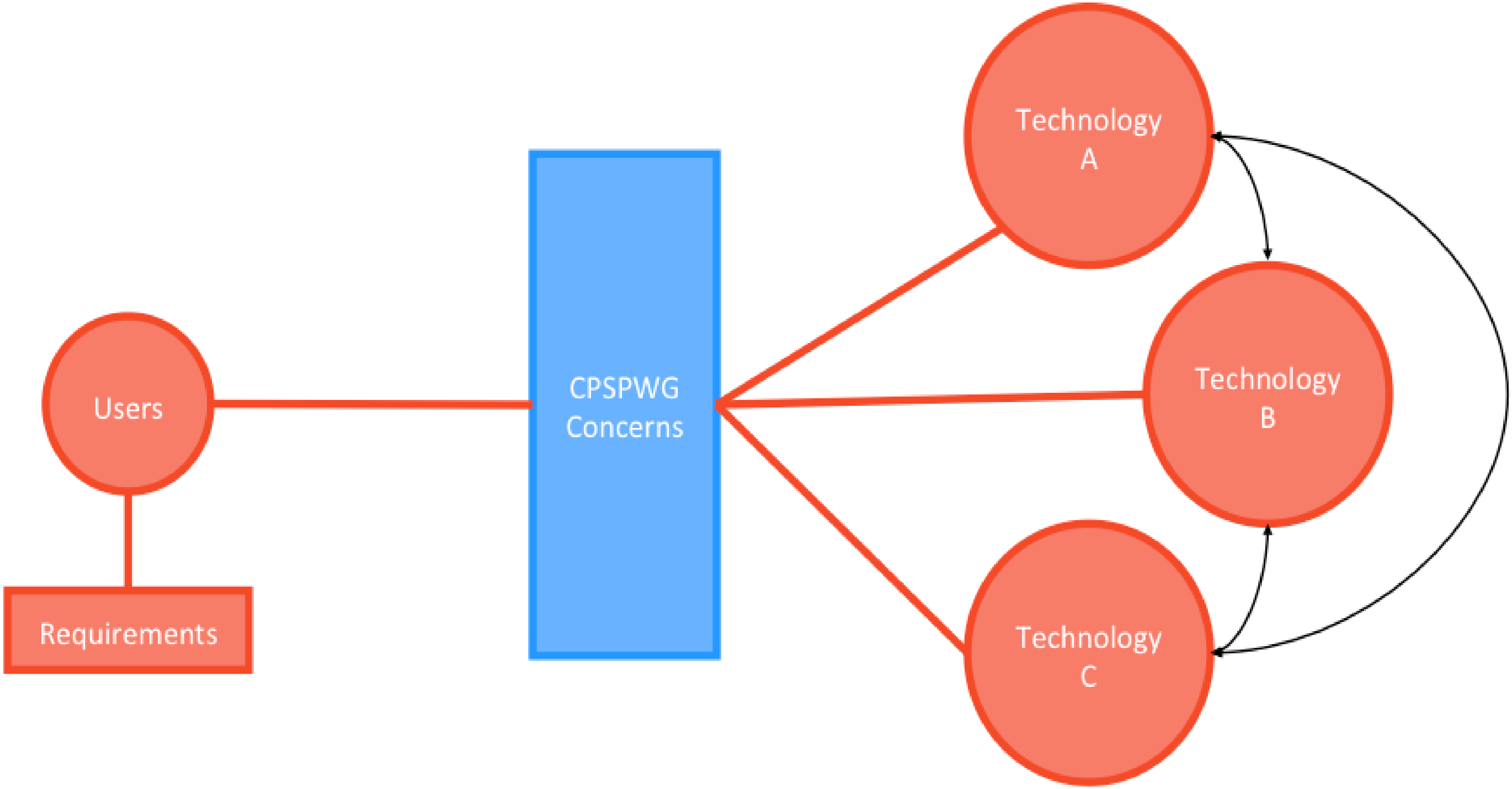
Safety vs. security analysis

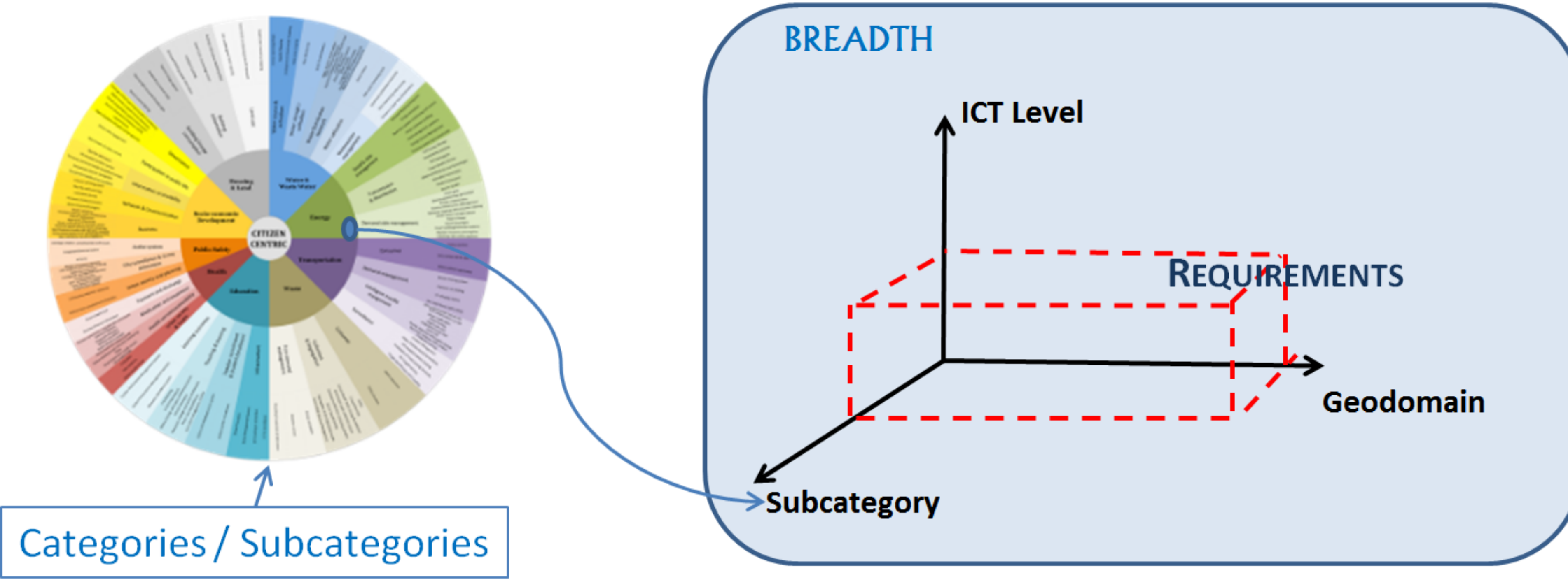
	Safety	Security
Fault	HW/SW Unintentional defects LIMITED FAULTS	Intrusion
Error	Distorted values/states	
Failure	Critical failure	
Propagation model	Funtional/ architectural	Functional/ architectural + attack surface

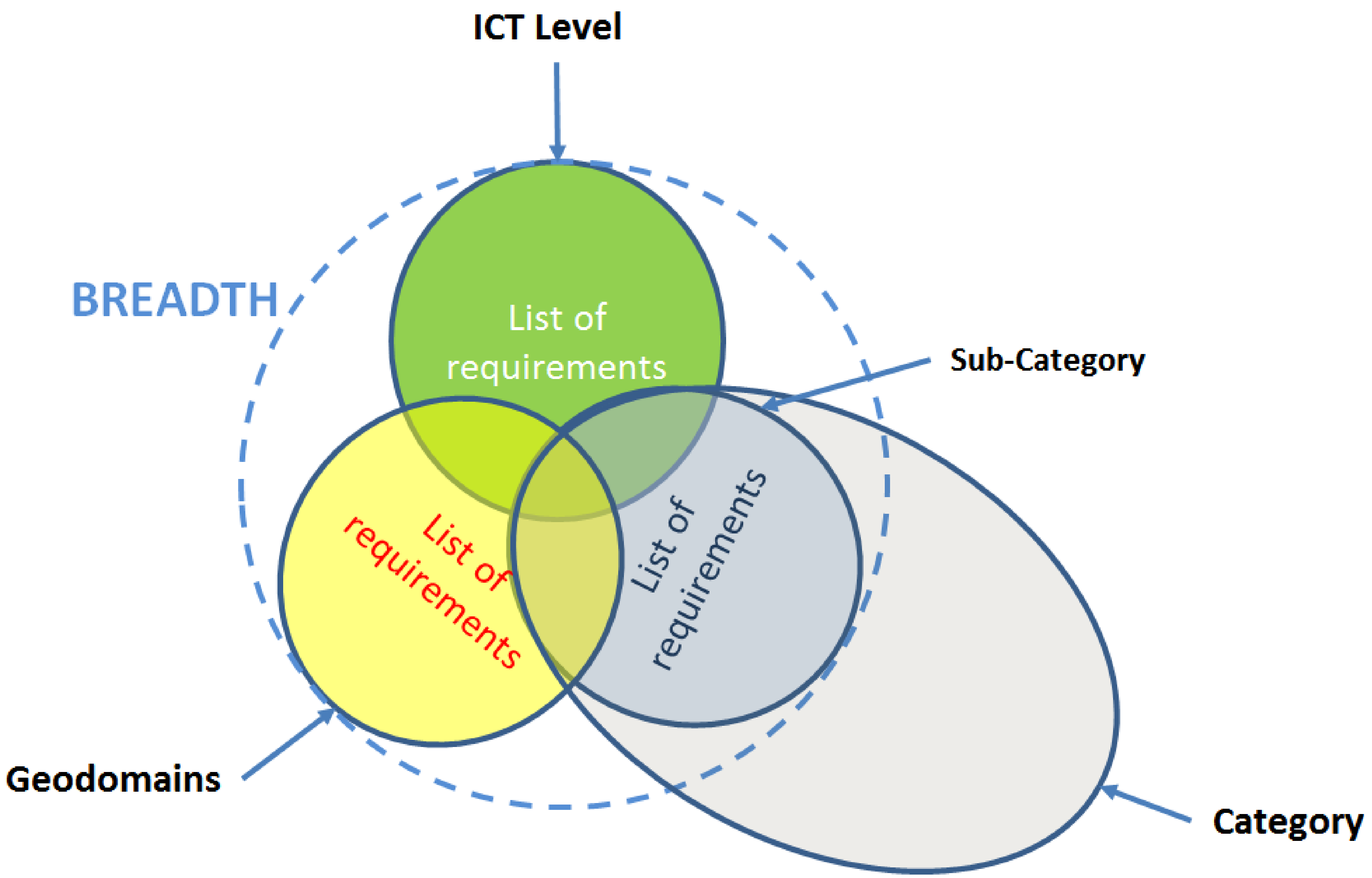
Dependability/security problems and analysis

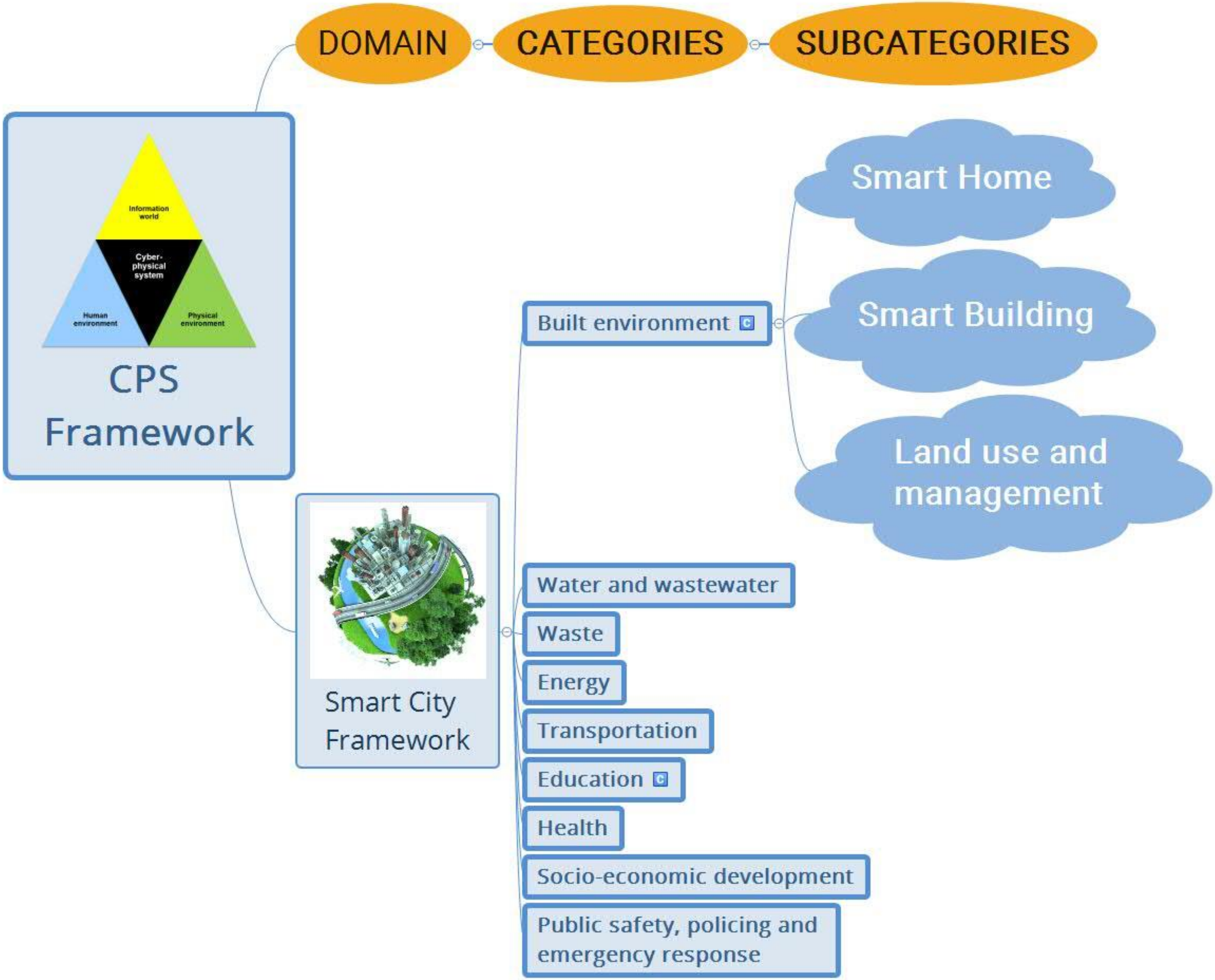


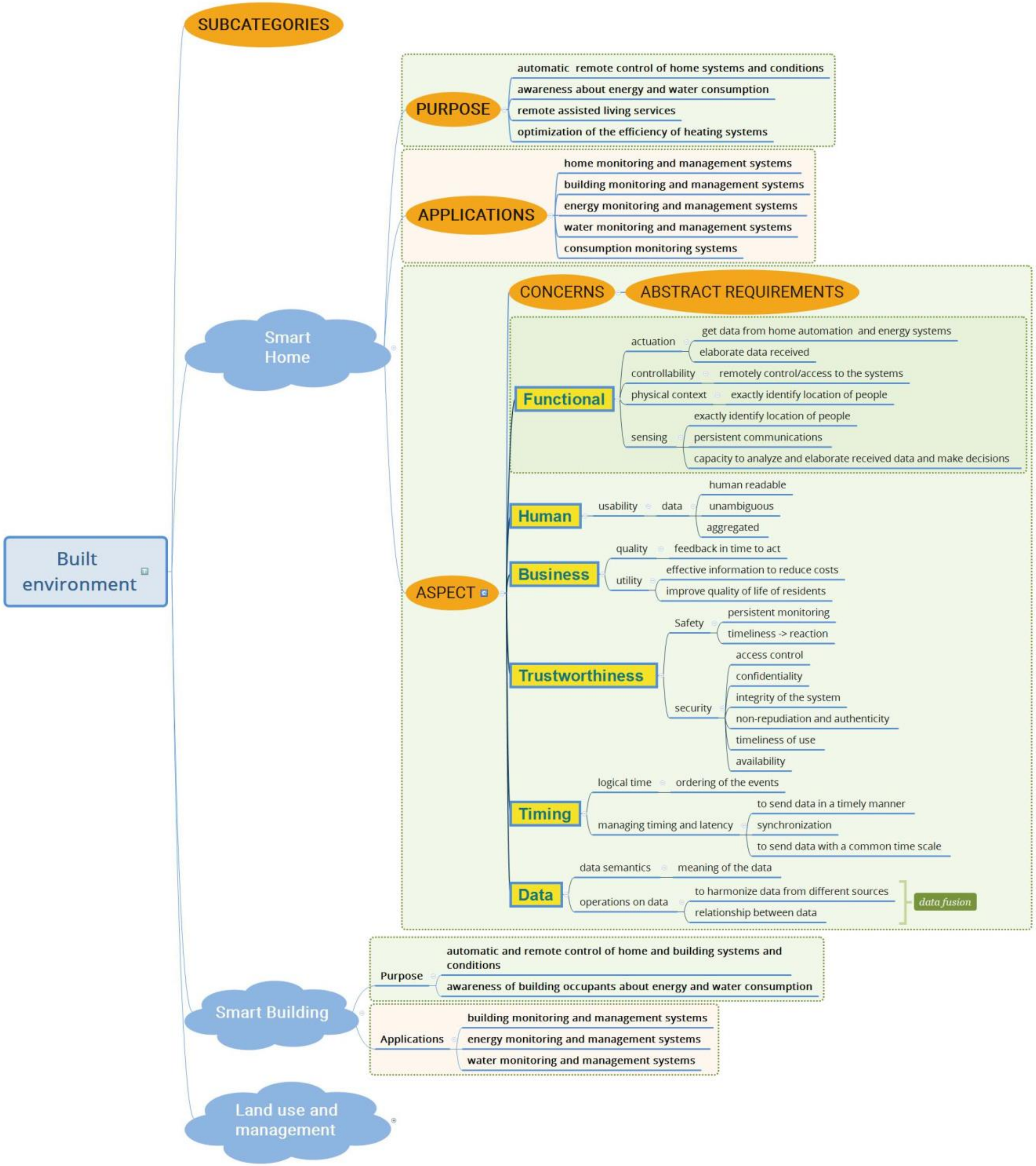
: IES-City Framework

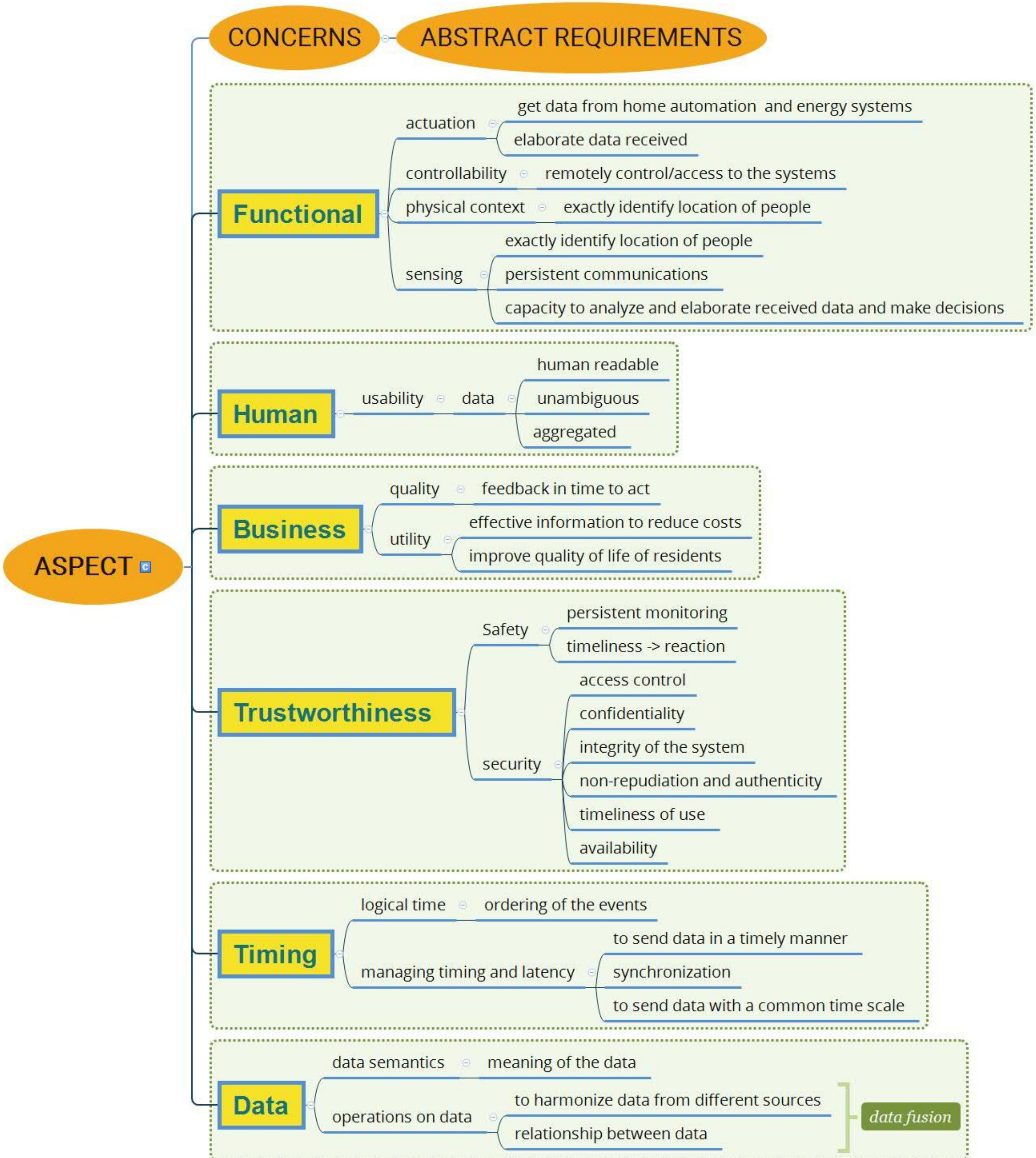


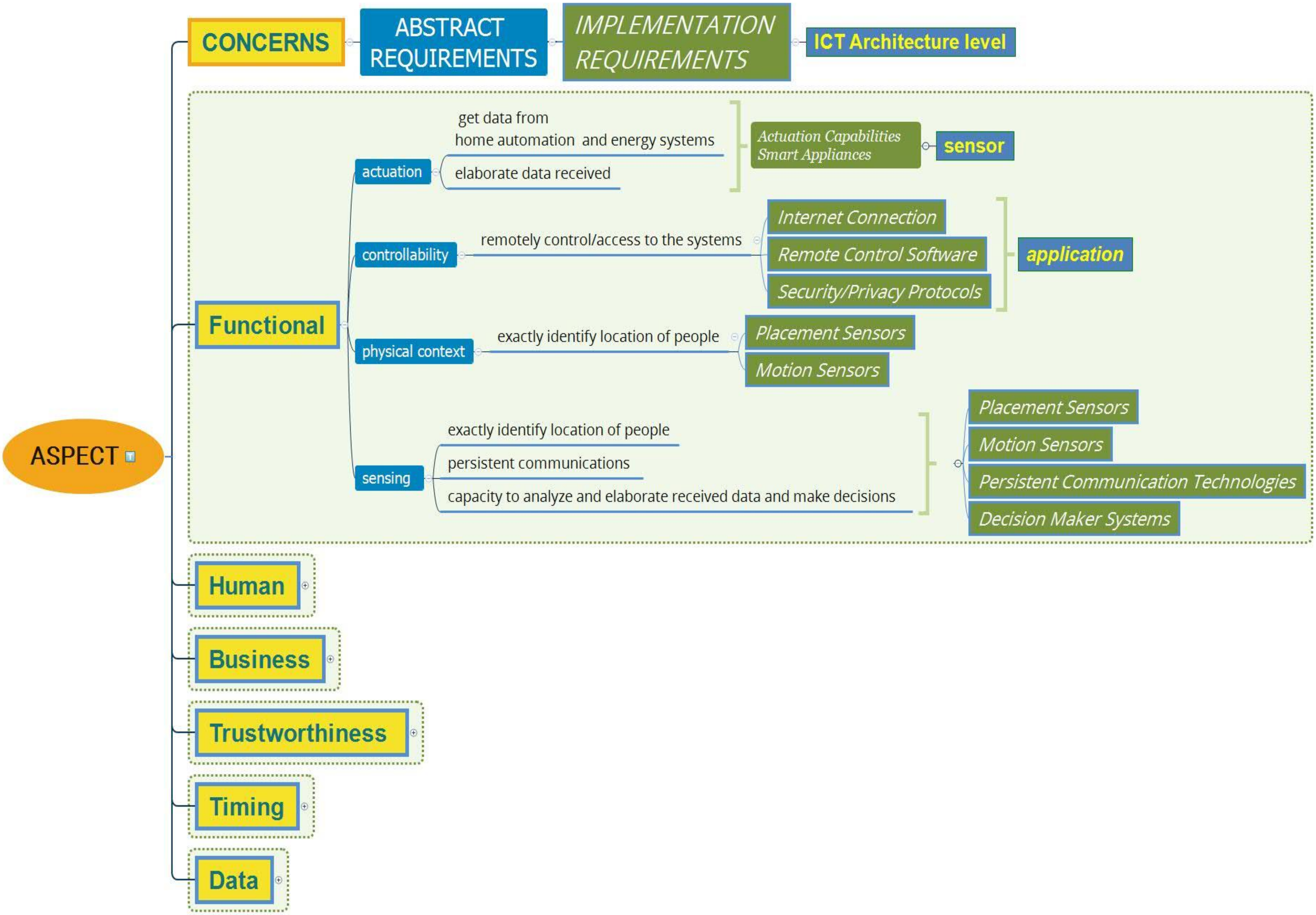

CITIZEN CENTRIC
BREADTH
ICT Level
REQUIREMENTS
Geodomain
Subcategory
Categories / Subcategories


ICT Level
BREADTH
List of requirements
Sub-Category
List of requirements
List of requirements
Geodomains
Category


DOMAIN
CATEGORIES
SUBCATEGORIES
Information world
Cyber-physical system
Human environment
Physical environment
CPS Framework
Smart City Framework
Built environment
Water and wastewater
Waste
Energy
Transportation
Education
Health
Socio-economic development
Public safety, policing and emergency response
Smart Home
Smart Building
Land use and management


SUBCATEGORIES
Built environment
Smart Home
PURPOSE
automatic remote control of home systems and conditions
awareness about energy and water consumption
remote assisted living services
optimization of the efficiency of heating systems
APPLICATIONS
home monitoring and management systems
building monitoring and management systems
energy monitoring and management systems
water monitoring and management systems
consumption monitoring systems
ASPECT
CONCERNS
ABSTRACT REQUIREMENTS
Functional
actuation
get data from home automation and energy systems
elaborate data received
controllability
remotely control/access to the systems
physical context
exactly identify location of people
sensing
exactly identify location of people
persistent communications
capacity to analyze and elaborate received data and make decisions
Human
usability
data
human readable
unambiguous
aggregated
Business
quality
feedback in time to act
utility
effective information to reduce costs
improve quality of life of residents
Trustworthiness
Safety
persistent monitoring
timeliness -> reaction
security
access control
confidentiality
integrity of the system
non-repudiation and authenticity
timeliness of use
availability
Timing
logical time
ordering of the events
managing timing and latency
to send data in a timely manner
synchronization
to send data with a common time scale
Data
data semantics
meaning of the data
operations on data
to harmonize data from different sources
relationship between data
data fusion
Smart Building
Purpose
automatic and remote control of home and building systems and conditions
awareness of building occupants about energy and water consumption
Applications
building monitoring and management systems
energy monitoring and management systems
water monitoring and management systems
Land use and management


CONCERNS
ABSTRACT REQUIREMENTS
ASPECT
Functional
actuation
get data from home automation and energy systems
elaborate data received
controllability
remotely control/access to the systems
physical context
exactly identify location of people
sensing
exactly identify location of people
persistent communications
capacity to analyze and elaborate received data and make decisions
Human
usability
data
human readable
unambiguous
aggregated
Business
quality
feedback in time to act
utility
effective information to reduce costs
improve quality of life of residents
Trustworthiness
Safety
persistent monitoring
timeliness -> reaction
security
access control
confidentiality
integrity of the system
non-repudiation and authenticity
timeliness of use
availability
Timing
logical time
ordering of the events
managing timing and latency
to send data in a timely manner
synchronization
to send data with a common time scale
Data
data semantics
meaning of the data
operations on data
to harmonize data from different sources
relationship between data
data fusion


CONCERNS
ABSTRACT REQUIREMENTS
IMPLEMENTATION REQUIREMENTS
ICT Architecture level
ASPECT
Functional
actuation
get data from home automation and energy systems
elaborate data received
Actuation Capabilities
Smart Appliances
sensor
controllability
remotely control/access to the systems
Internet Connection
Remote Control Software
Security/Privacy Protocols
application
physical context
exactly identify location of people
Placement Sensors
Motion Sensors
sensing
exactly identify location of people
persistent communications
capacity to analyze and elaborate received data and make decisions
Placement Sensors
Motion Sensors
Persistent Communication Technologies
Decision Maker Systems
Human
Business
Trustworthiness
Timing
Data