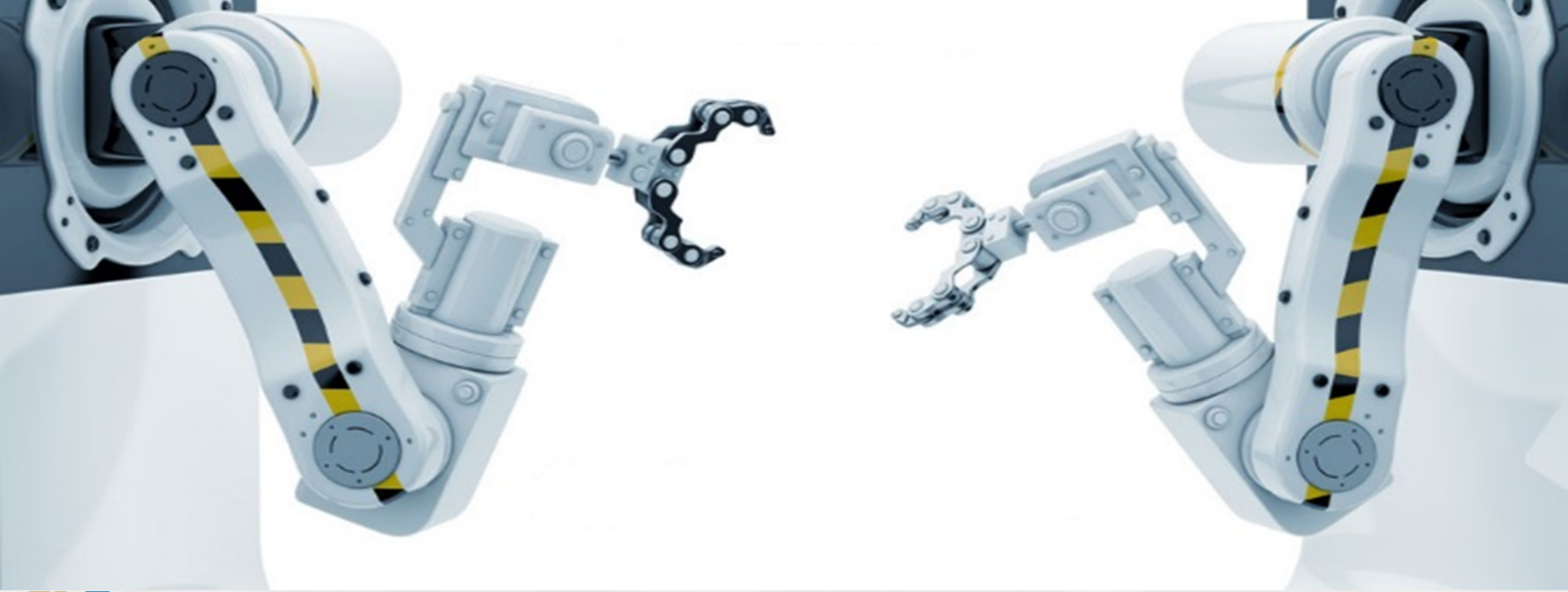
CPS Framework Open Source Workshop

Sept. 19th 2017- NIST/NCCoE

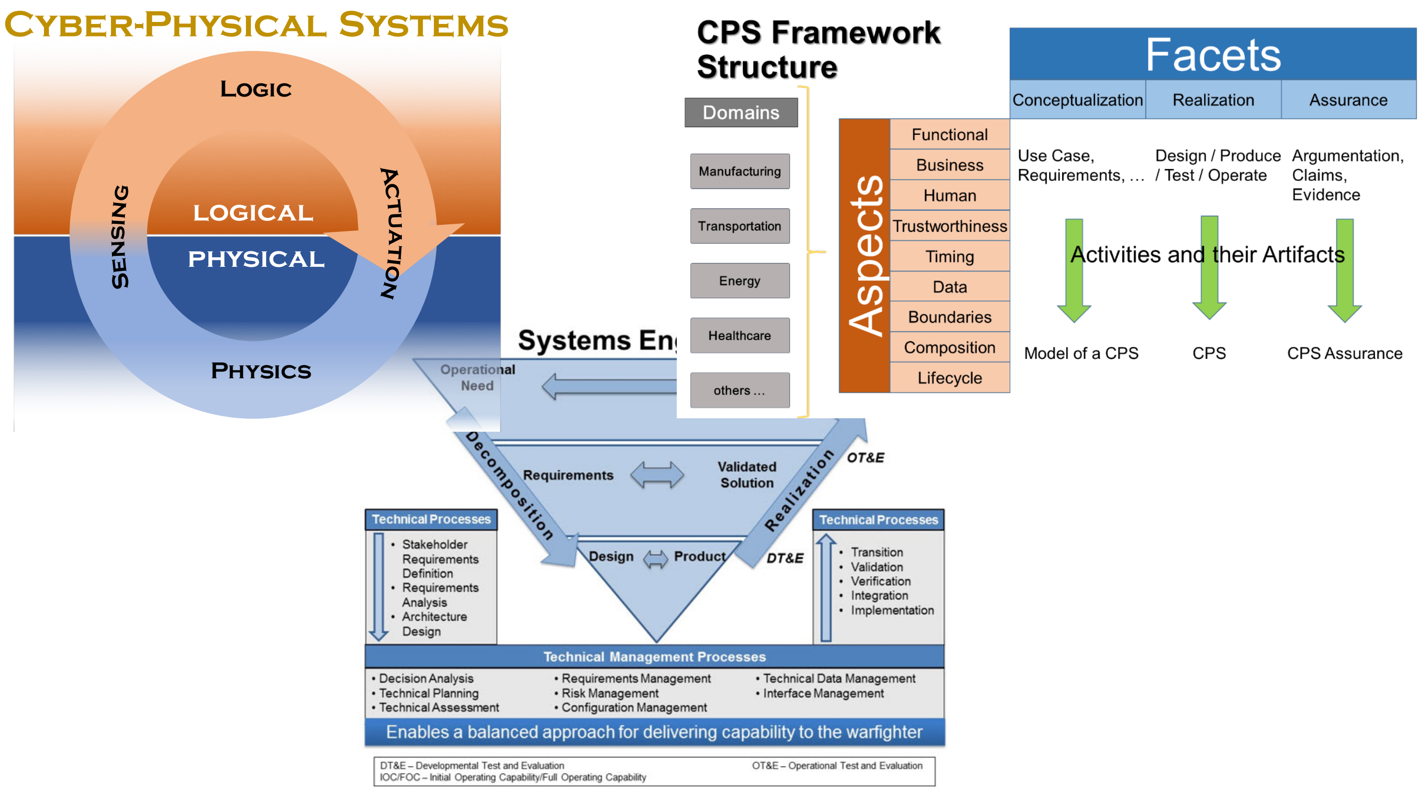


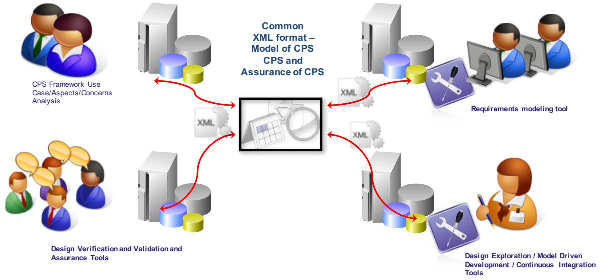
Sessions

1. Registration
2. Welcome (Greer)
3. Goals (Griffor)
4. Keynote (Ross)
5. CPS Framework Overview (Wollman)
6. CPS Framework Applications
    1. Math (Griffor)
    2. Transportation (McShane, Brandao)
    3. IES City (Burns)
    4. Security to Trustworthiness (Vishik)
    5. Ontology (Balduccini)
7. Panel Discussion (Greer)
8. Systems Engineering and CPS Framework (Roth)
9. Modeling (Burns/Song)
10. Community Building (Griffor)

2. Welcome - Greer

NIST and the Smart Grid and Cyber-Physical Systems Program Office – CPS Program



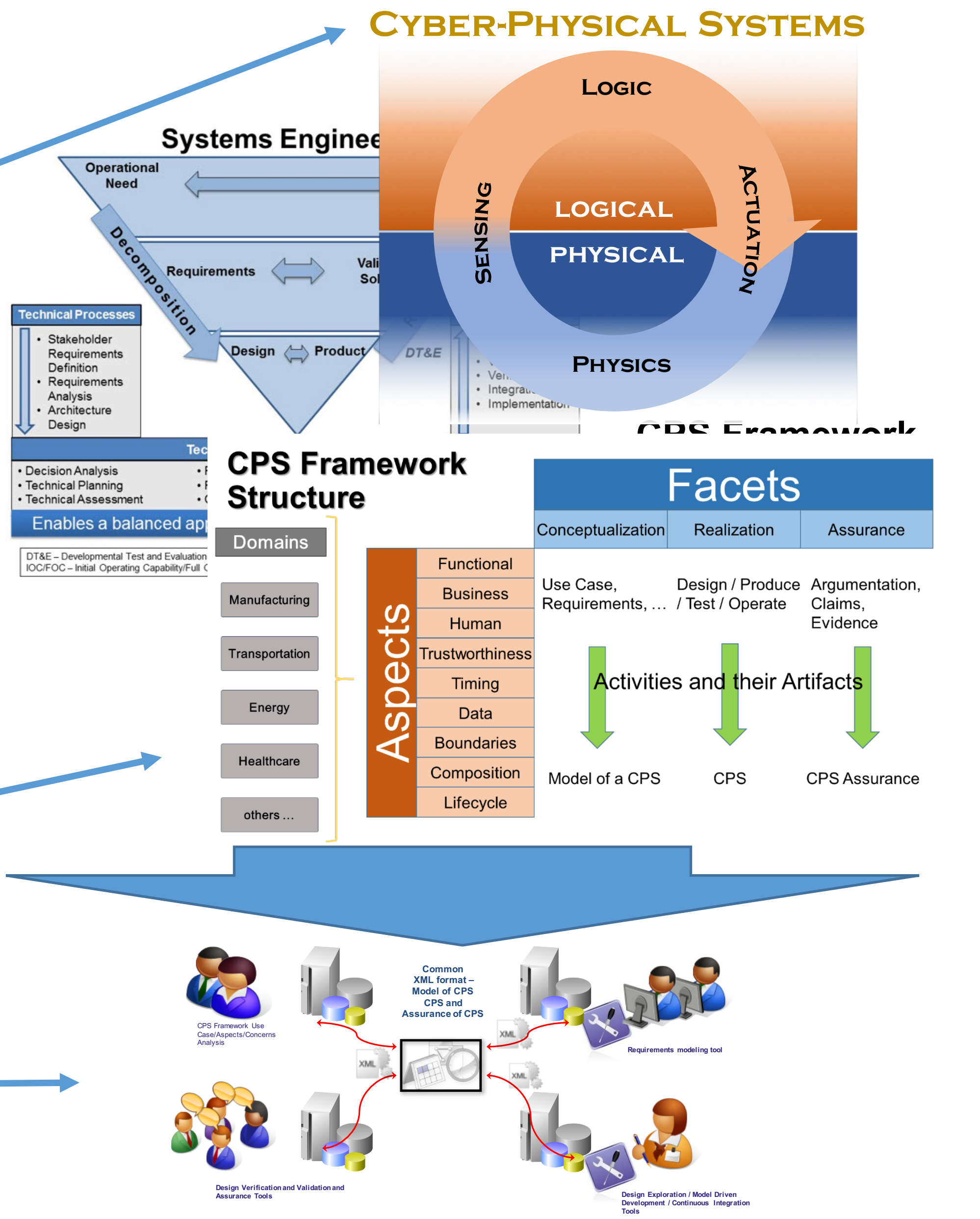


CPS Framework Open Source: Continuous Integration for CPS Development

3. Workshop Goals - Griffor

This workshop aims to address key CPS challenges: how we conceive, design, build, deliver and maintain them.

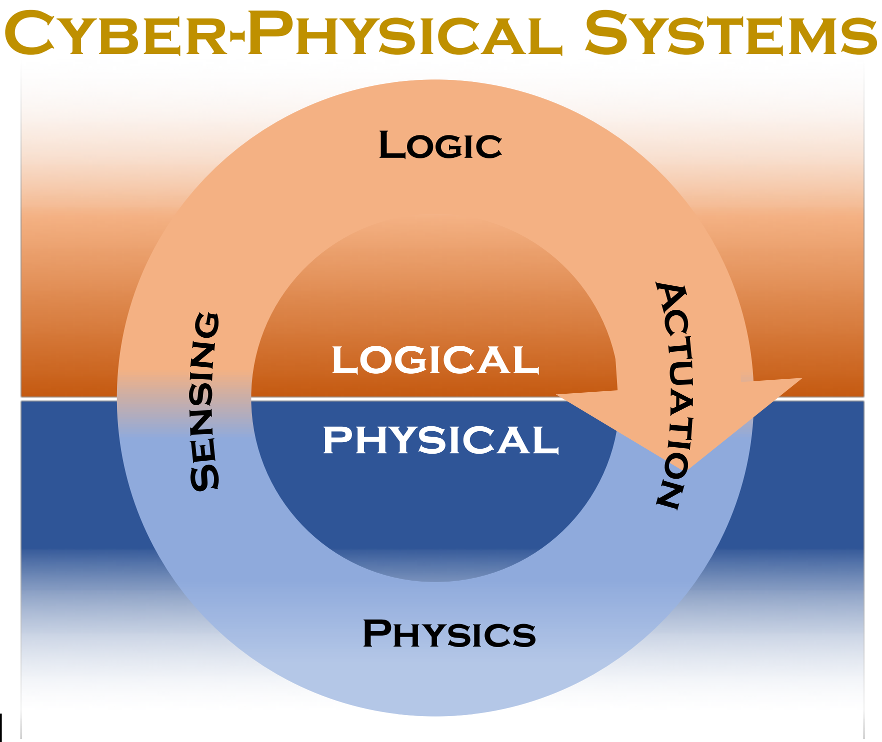
1. What is CPS?
2. How do we design, build and assure CPS throughout their lifecycle?
3. What discipline do we need to address the concerns that drive requirements and engineering?
4. What needs to be the common core tooling?



Dashboard for Continuous Integration of CPS Development

3.1 What is CPS?

Cyber-Physical Systems (CPS) comprise interacting digital, analog, physical, and human components engineered for function through integrated logic and physics.

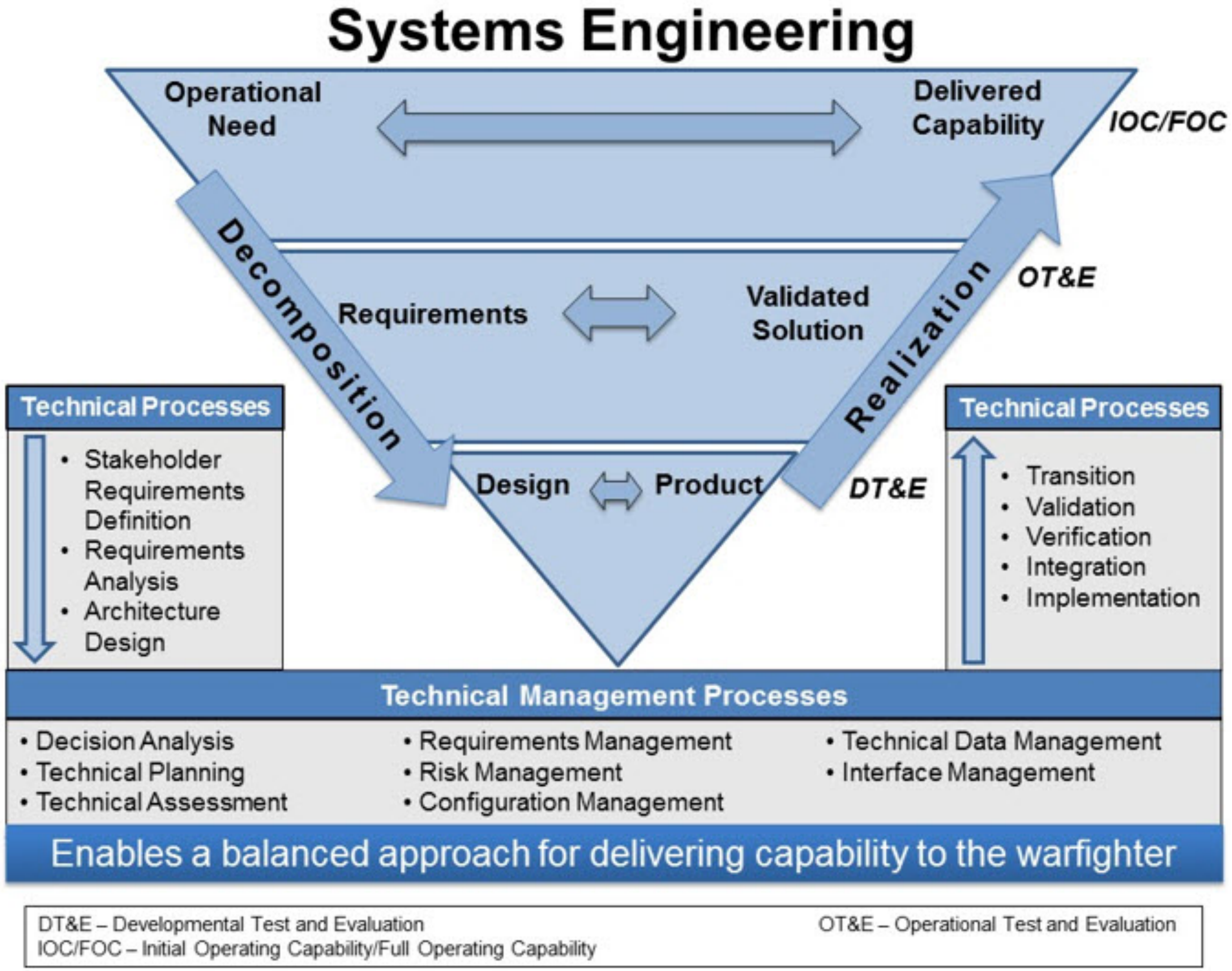


Internet of Things (IoT) emphasizes digital infrastructure for widely connected, interacting, physical ‘things,’ forming systems that integrate logic and physics for function.

NIST Smart Grid and Cyber-Physical Systems Program Office

3.2 How do we design, build and test CPS?

- Develop requirements.
- Specify the system, sub-systems and components.
- Build components.
- Unit test components.
- Assemble and test sub-systems.
- Assemble and test/validate full system.



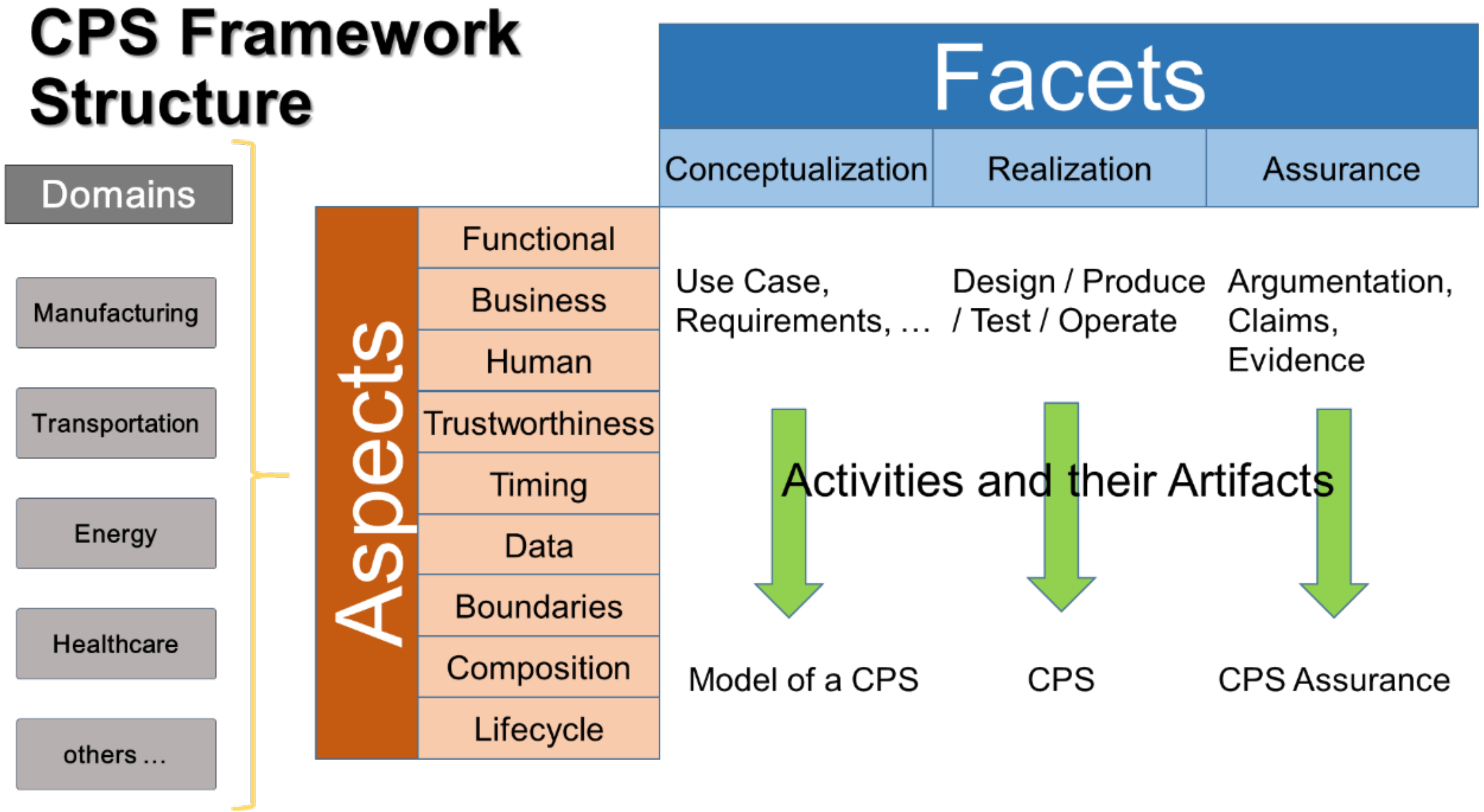
3.3 What discipline do we need to address the concerns?

Concern Structure:

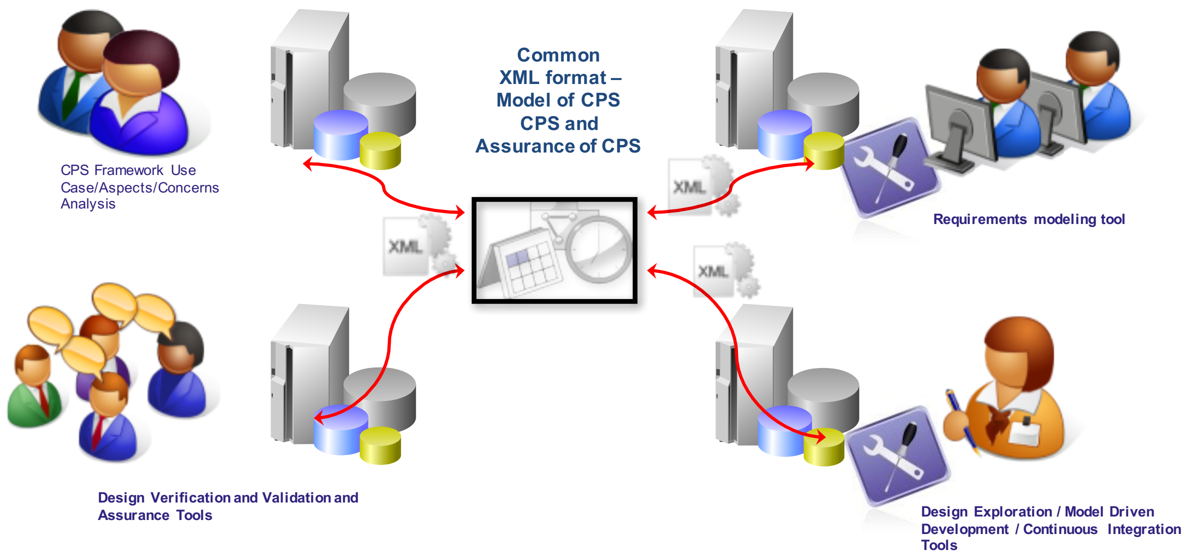
- Develop a full set of concerns.
- Develop the relationships between the concerns.

Systems Engineering Activities:

- Determine requirements needed to address each concern.
- Design, build and test to each set. (composition of concerns).
- Build the Assurance Case



3.4 What needs to be the common core tooling?



Continuous Integration for CPS Development

CPS Framework Open Source provides:

1) **'Type Structure' for:**

- Aspects and concern; and
- Facets, engineering activities and outcomes

2) **That type and sort** compositionally:

- properties/requirements and
- artifacts

3) **Encoded** in a portable, reusable XML format.

3.5 Expanded Concern Risk and Risk Mitigation Surface

	Primary Impact of Failure	
	Digital	Physical
IT System	✓	
CPS	✓	✓

	Mitigation Mechanisms		
	Digital	Analog	Physical
IT System	✓		
CPS	✓	✓	✓

"E.g. Better cybersecurity through physics!"

4. Achieving Trustworthy Systems - Ross

Rethinking Cybersecurity from the Inside Out

An Engineering and Life Cycle-Based Approach for Achieving Trustworthy Secure Systems

Dr. Ron Ross
Computer Security Division
Information Technology Laboratory

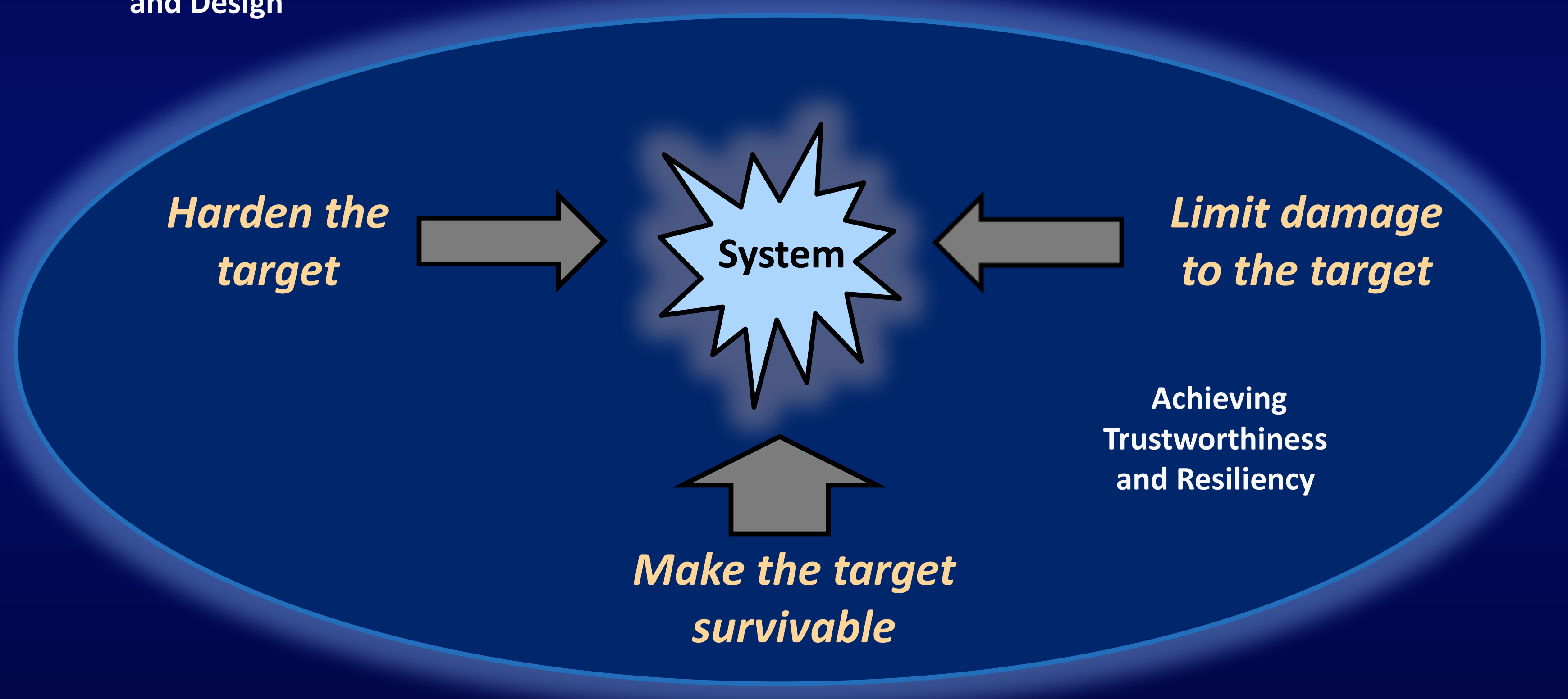
Our appetite for *advanced technology* is rapidly exceeding our ability to protect it.

Complexity.

The n+1 vulnerabilities problem.

Security Architecture and Design

Reducing susceptibility to ***cyber threats*** requires a multidimensional systems engineering approach.



Security.

An emergent property.

Risk assessment.

Assets and consequences.

NIST Special Publication 800-160

Systems Security Engineering

Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

Multidisciplinary integration of security best practices.

Technical Processes

- Business or mission analysis
  - Stakeholder needs and requirements definition
    - System requirements definition
      - Architecture definition
        - Design definition
          - System analysis
            - Implementation
            - Integration
          - Verification
        - Transition
      - Validation
    - Operation
  - Maintenance
- Disposal

ISO/IEC/IEEE 15288:2015

Systems and software engineering — System life cycle processes

Nontechnical Processes

- Project planning
- Project assessment and control
- Decision management
- Risk management
- Configuration management
- Information management
- Measurement
- Quality assurance
- Acquisition and Supply
- Life cycle model management
- Infrastructure management
- Portfolio management
- Human resource management
- Quality management
- Knowledge management

ISO/IEC/IEEE 15288:2015

Systems and software engineering — System life cycle processes

Nontechnical Processes

- Project planning
- Project assessment and control
- Decision management
- Risk management
- Configuration management
- Information management
- Measurement
- Quality assurance
- Acquisition and Supply
- Life cycle model management
- Infrastructure management
- Portfolio management
- Human resource management
- Quality management
- Knowledge management

ISO/IEC/IEEE 15288:2015

Systems and software engineering — System life cycle processes

Appendices

A Wealth of Trusted Systems Development Principles, Concepts, and Best Practices

- References
- Glossary
- Acronyms
- Summary of Security Activities / Tasks
- Roles, Responsibilities, and Skills
- Design Principles for Security
- Engineering and Security Fundamentals

Security should be a by-product of good design and development practices—integrated throughout the system life cycle.

Institutionalize.

The ultimate objective for security.

Operationalize.

Government

Academia

Security is a team sport.

Industry

NIST Systems Security Engineering Project

Race to the Top — Better Security Through Engineering

Ron Ross

100 Bureau Drive Mailstop 7730
Gaithersburg, MD USA 20899-7730

Email
ron.ross@nist.gov

Mobile
301.651.5083

LinkedIn
www.linkedin.com/in/ronross-cybersecurity

Twitter
@ronrossecure

Web
csrc.nist.gov

Comments
sec-cert@nist.gov

5. CPS Framework Review-Wollman

5.1 Frameworks – NIST Convening of Stakeholders

2008 2009 2010 2011 2012 2013 2014 2015 2016

Smart Grid
Dec 2007
EISA SG Legislation

Cloud Computing
2010

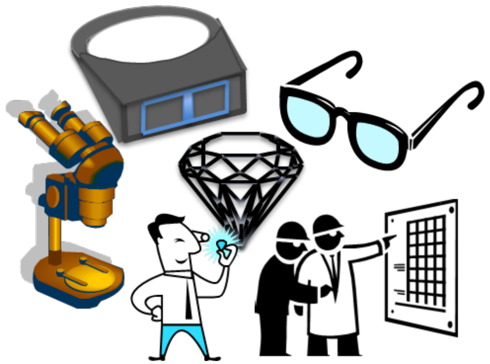
Cybersecurity
Feb 2013
Executive Order

Community Disaster Resilience
June 2013
Climate Action Plan

Big Data
June 2013

Smart America/Global Cities

Cyber-Physical Systems
June 2014



Perspectives, Viewpoints, Views, …

Communities of practice, processes, …

- **Frameworks**: documented conceptual structures that organize and make clear collective wisdom (vision, principles, underlying structure, functions, requirements, …)
  - Frameworks are created with technical expertise and consensus-based process

5.2 Frameworks – NIST Convening of Stakeholders

2008 2009 2010 2011 2012 2013 2014 2015 2016

Smart Grid

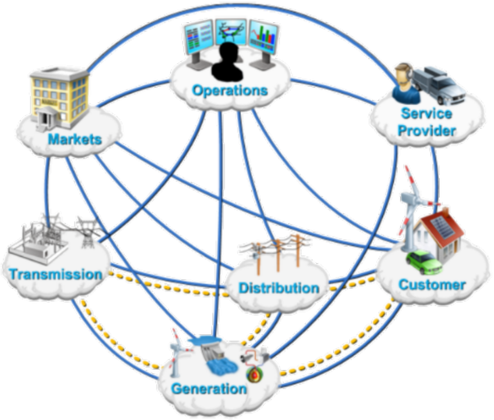
Dec 2007
EISA SG Legislation

NIST Special Publication 1108r3

NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0

Smart Grid and Cyber-Physical Systems Program Office
and Energy and Environment Division,
Engineering Laboratory

Priority Action Plans (PAPs)



Cloud Computing

2010

Cybersecurity

Feb 2013
Executive Order

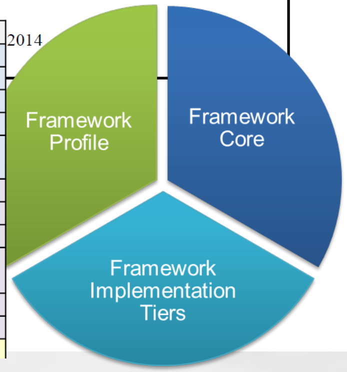
Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

2014

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
	Anomalies and Events	DE.AE



Community Disaster Resilience

June 2013
Climate Action Plan

Big Data

June 2013

NIST Special Publication 1500-4

NIST Big Data Interoperability Framework:
Volume 4, Security and Privacy

Final Version 1

NIST Big Data Public Working Group
Security and Privacy Subgroup

Smart America/Global Cities

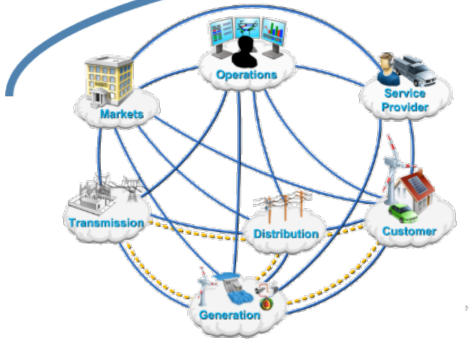
Cyber-Physical Systems

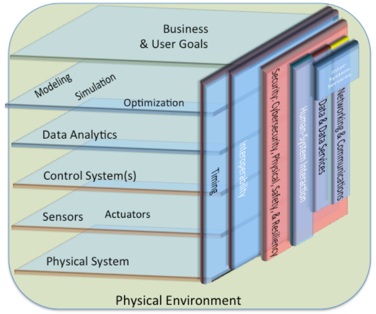
June 2014

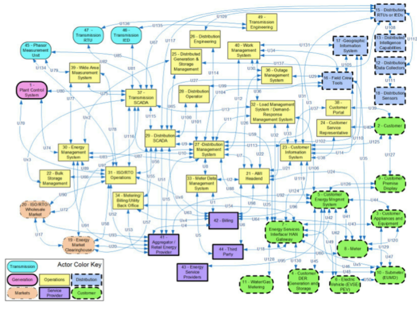
5.3 NIST CPS Public Working Group

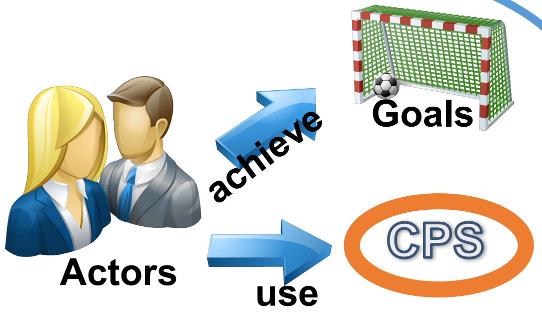
- Goal: create CPS Framework to support CPS research, development and deployment (applicable to CPS and Internet of Things IoT)
- Need: multi-domain perspective baked in
  - Applicable within all CPS domains, supports cross-CPS domain applications

CPS Framework









Smart infrastructure (grid, water, gas, …)

Smart buildings

Smart emergency response

Smart healthcare

Many more!!

Smart manufacturing

Smart transportation

5.4 NIST CPS Public Working Group

NIST CPS PWG leadership: David Wollman and Chris Greer					
Co-Chairs	Reference Arch	Use Cases	Security	Timing	Data Interop
NIST	Abdella Battou, Ed Griffor	Eric Simmon	Vicky Pillitteri, Steve Quinn	Marc Weiss	Marty Burns
Academia	Janos Sztipanovits	John Baras	Bill Sanders	Hugh Melvin	Larry Lannom
Industry	Stephen Mellor, Shi-Wan Lin	Stephen Mellor	Claire Vishik	Sundeep Chandhoke	Peggy Irelan, Eve Schooler

NIST SP 1500-201 and 1500-202

Framework for Cyber-Physical Systems

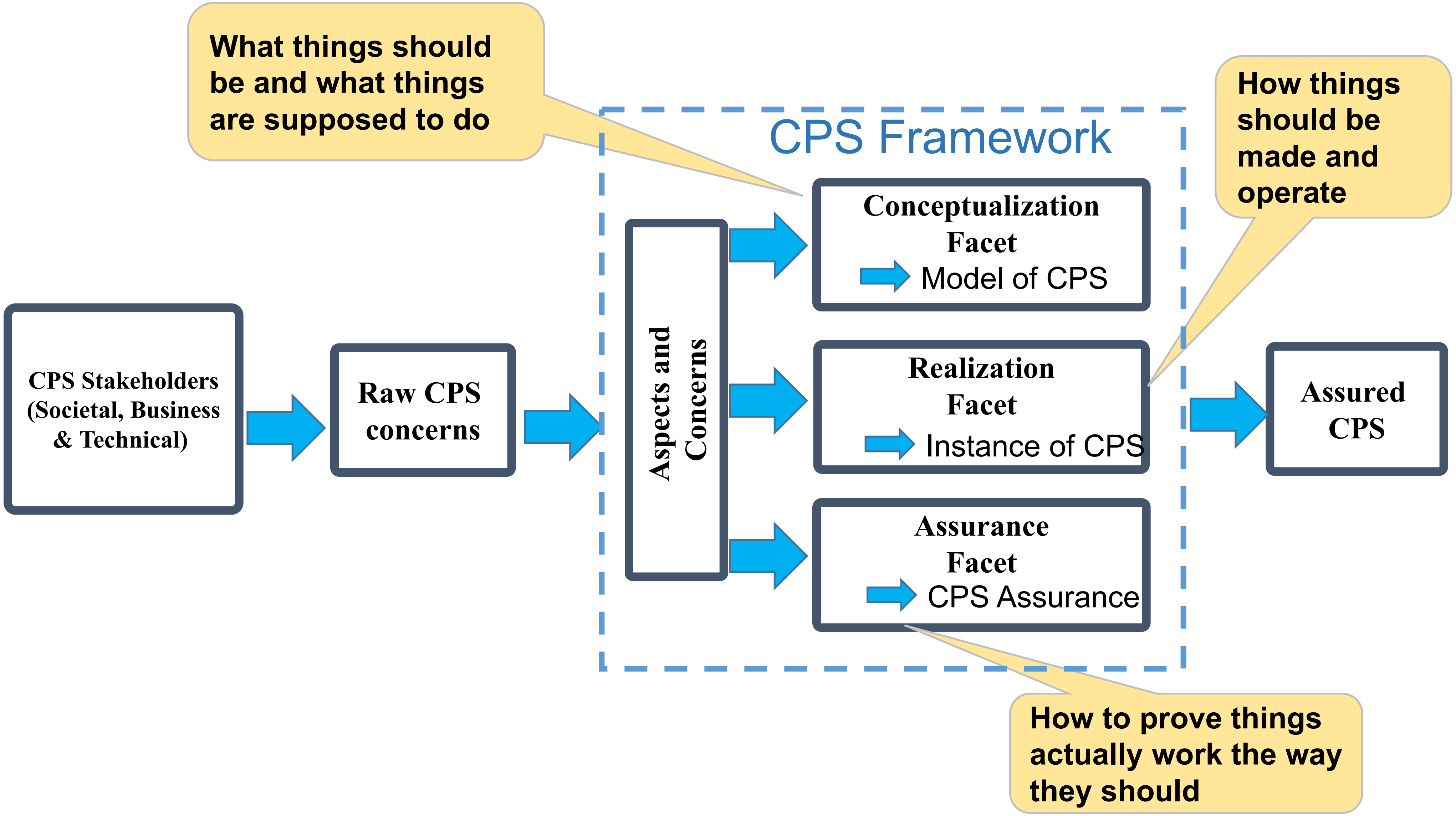
Release 1.0

May 2016

Cyber Physical Systems Public Working Group

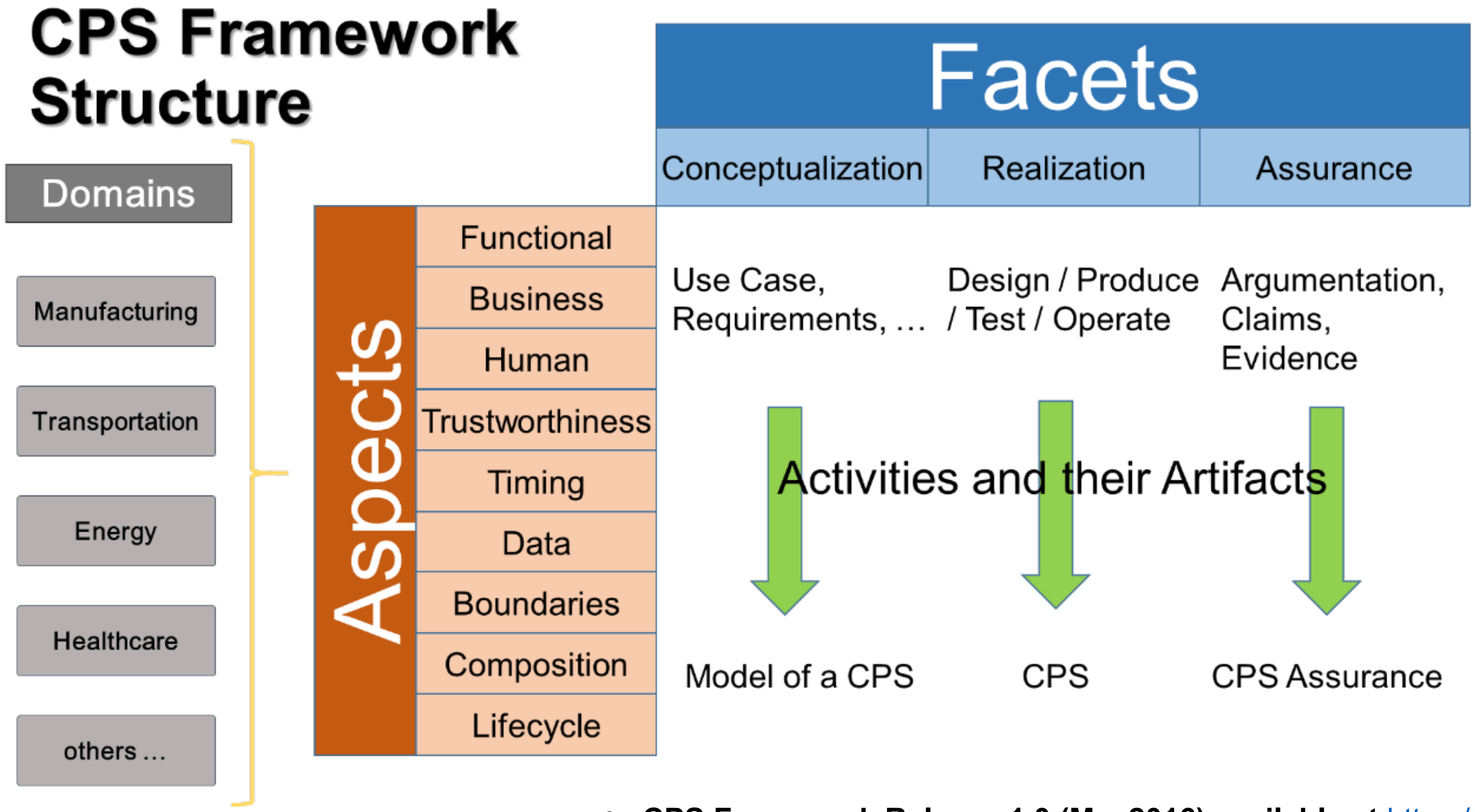
pages.nist.gov/cpspwg

5.5 CPS Framework Development



5.6 NIST CPS PWG – CPS Framework

‘Concern-driven’: holistic, integrated approach to CPS/IoT concerns.



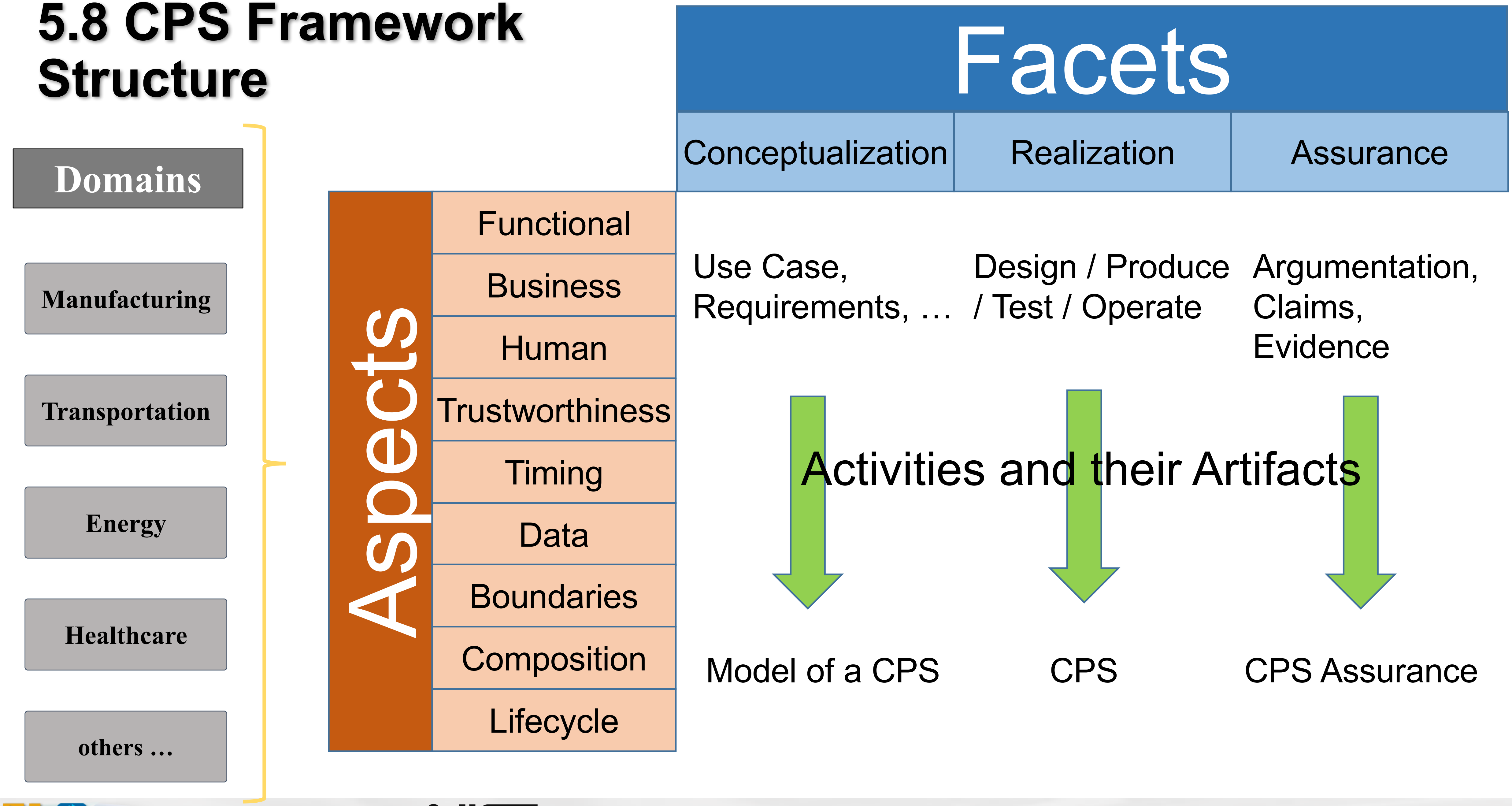
- **CPS Framework Release 1.0 (May2016) available at https://pages.nist.gov/cpspwg/**

5.7 Purpose of the CPS Framework

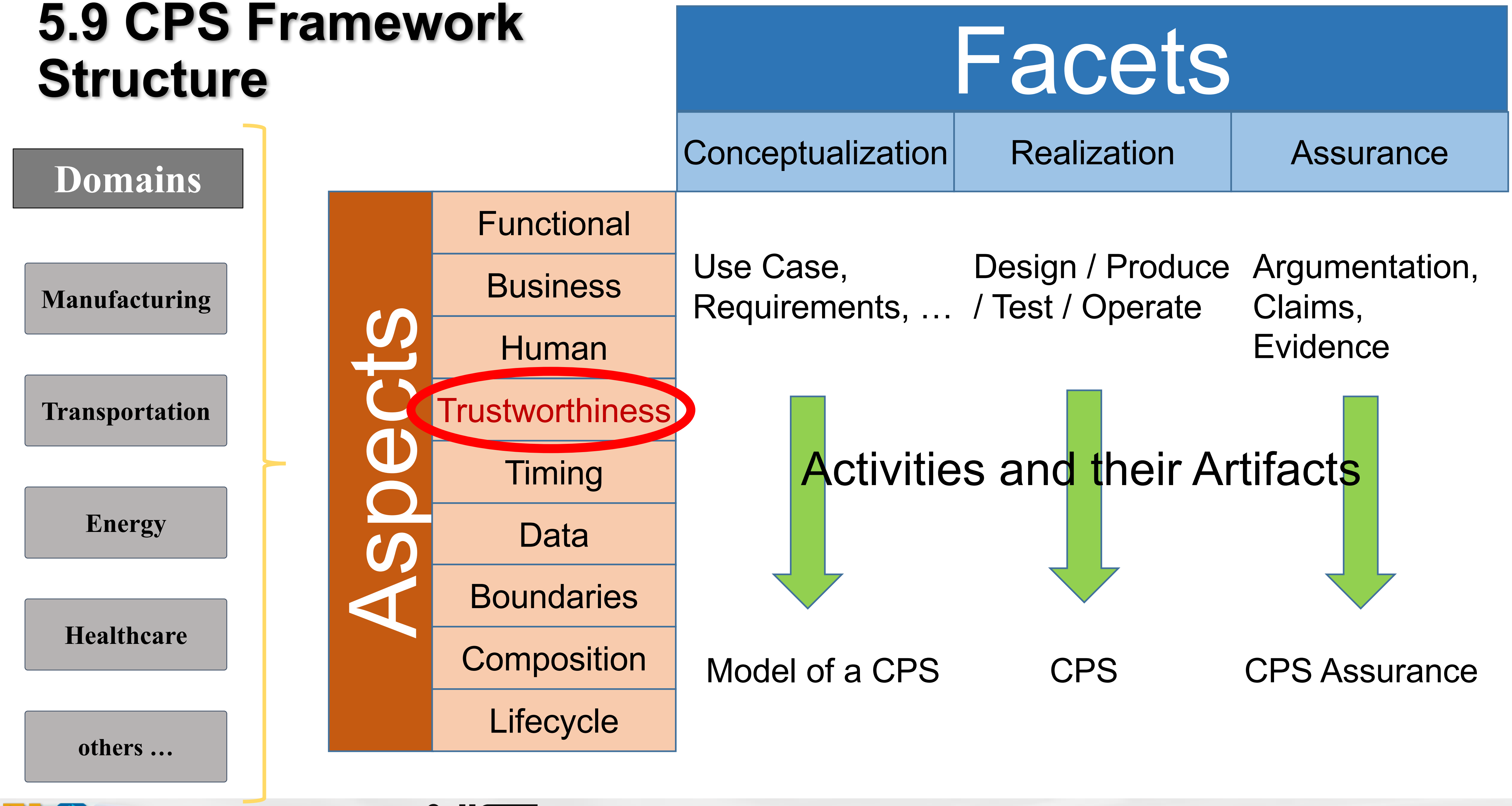
- **Concern-driven structuring of development artifacts:** to facilitate assurance cases (by representing or analyzing a system along these dimensions, points of commonality or interoperability with other systems are revealed)
- **A normal-form for CPS/IoT system** (common way of presenting CPS/IoT that enables comparison of what is done, across the system, for the sake of any individual concern)
- Provides a **method for integrating CPS/IoT across domains** – the future of CPS/IoT is cross-domain integration. While some domains may have robust, integrated approaches to some concerns, there are typically radically different standards across domains.

CPS Framework is NOT A PROCESS!!
It is a *method for integrating concerns into systems engineering processes*!

5.8 CPS Framework Structure



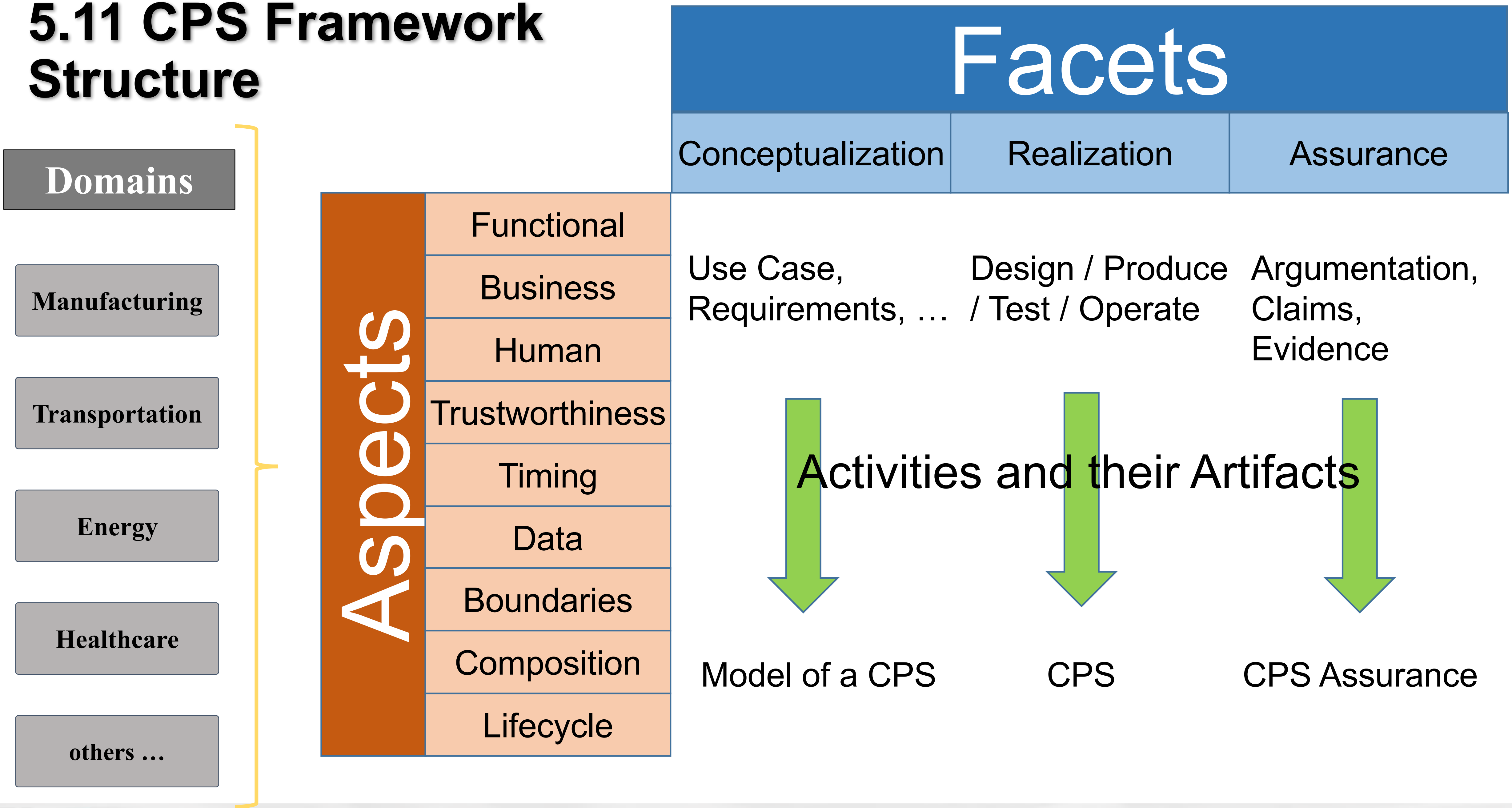
5.9 CPS Framework Structure



5.10 Aspects (groupings/categories of concerns)

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/cybersecurity, 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.

5.11 CPS Framework Structure

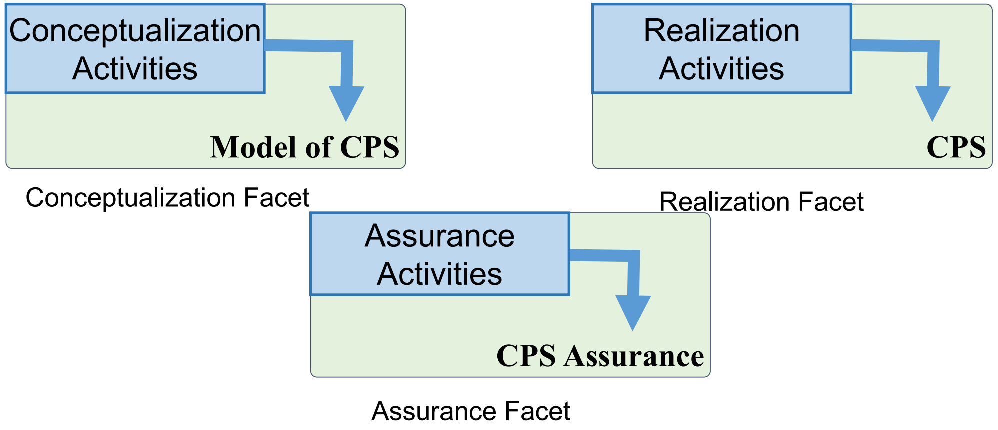


5.12 Activities and Artifacts

In using the framework to analyze and document CPS, a series of *activities* is performed. For example, a typical waterfall-like process will include:

- use case development
- functional decomposition
- requirements analysis
- design
- etc.

An *activity* produces one or more *artifacts.*



For example, the activities and associated artifacts of the *conceptualization facet* commonly include:

Mission and Business Case Development
Artifact: Business use cases

Functional Decomposition
Artifact: Detailed use cases, actors, information exchanges

Requirements Analysis
Artifact: Functional and non-functional requirements

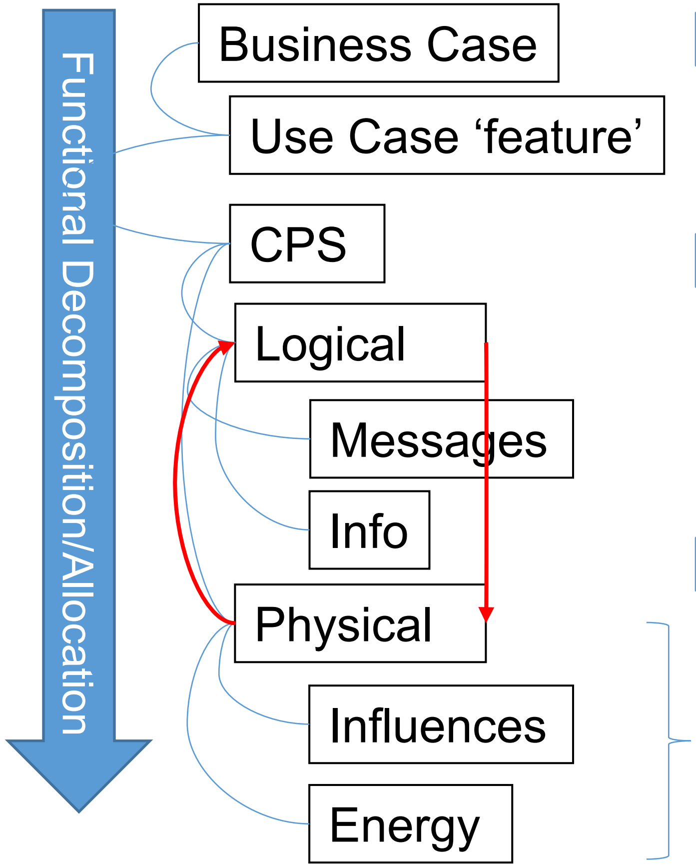
Requirements Allocation
Artifact: HW/SW configuration Items

Interface Requirements Analysis
Artifact: Interface requirements

5.13 Analyzing and Developing CPS: Decomposition

Functional Decomposition (Logical and Physical)

CPS/Function Types



*transductions

Safety "Properties" of a Function: Automatic Emergency Braking (AEB)

- Vehicle provides automated collision safety function
- Vehicle provides/maintains safe stopping
- Braking function reacts as required
- Stopping algorithm provides safe stopping
- Messaging function receives distance to obstacles and speed from propulsion function
- Distance and speed info is understood by braking function
- Friction function provides appropriate friction, depending on the road, tire pressure, etc.

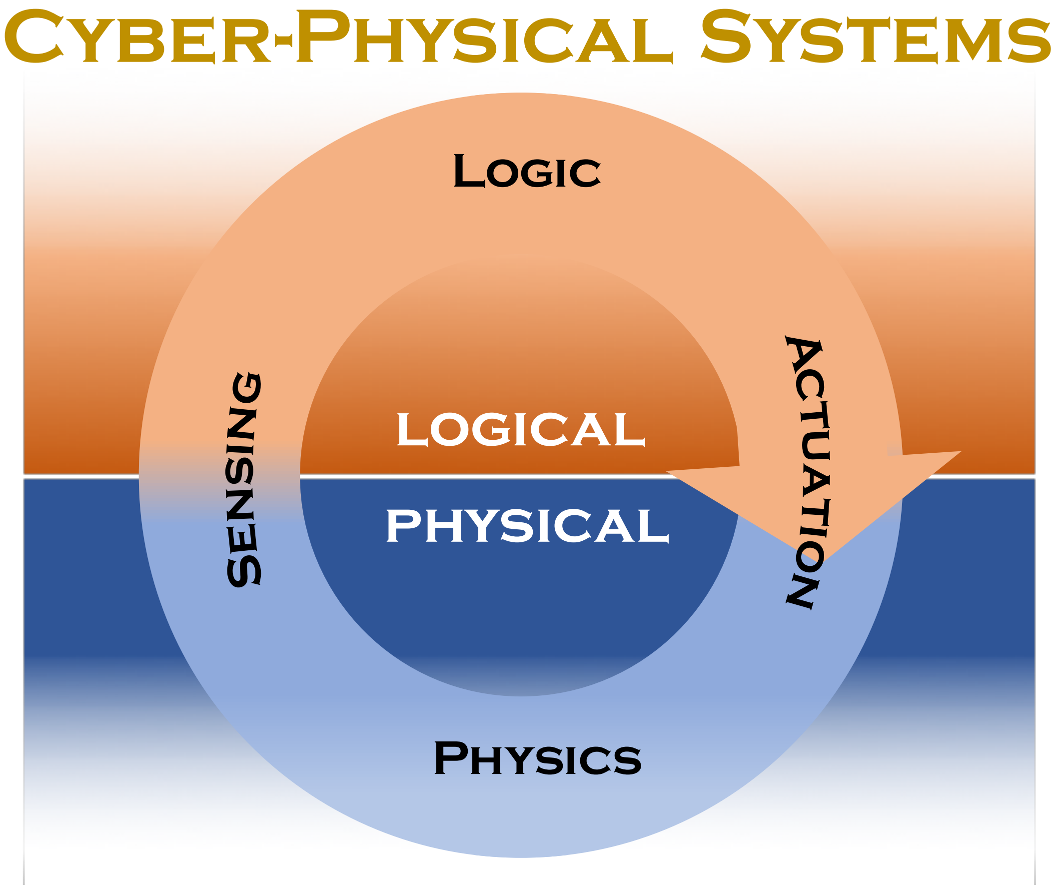
Apply Aspects/Concerns → Generate System Properties

6. Applications - Griffor

1. Mathematics of CPS and the CPS Framework (E. Griffor)
2. Applications to Transportation (D. McShane, F. Brandao/Ricardo LLC)
3. IES City Tables – CPS Framework as Benchmarking Tool (M. Burns)
4. From Security to Trustworthiness (C. Vishik/Intel)
5. Trustworthiness Ontology (M. Balduccini/St. Joseph's University)

6.1.1 Mathematics of CPS

Cyber-Physical Systems (CPS) comprise interacting digital, analog, physical, and human components engineered for function through integrated logic and physics.



Internet of Things (IoT) emphasizes digital infrastructure for widely connected, interacting systems.

NIST Smart Grid and Cyber-Physical Systems Program Office

6.1.2 The Category CyPhy

- The cyber-physical category CyPhy has as objects:
  - **Action/Actuation**
  - **Sense**
  - **Phys_State**
  - **Decision**
- The morphisms of CyPhy are given by:
  - **Mor(Act,Physical_State)** = {phy_act-phys}
  - **Mor(Decision,Act)** = {log_dec-act}
  - **Mor(Sense,Decision)** = {log_sen-dec}
  - **Mor(Sense,Act)** = {phys_sen-act}
  - **Mor(Phys_State,Sense)** = {phy_Phys_State-Sense}.

6.1.3 Symmetric Monoidal Categories

- For purposes here **systems will be viewed as processes and interactions between them** (*process algebra* in the sense of Milnor for example)
- We distinguish two sorts of interactions between processes:
  - **Logical interactions** (exchanges of information)
  - **Physical interactions** (exchanges of energy)
- Math model of physical interactions is **algebraic systems of ODEs**
- Math model of logical interactions are **formalizations of agent-based models** such as *complex adaptive systems* (J. Holland)
- We choose symmetric monoidal categories (SMC) as an example of a **model of systems in category**

6.1.4 CPS as Functors

A cyber-physical system, in the sense of process algebra, can be represented as a **functor from a symmetric monoidal category to the category CyPhy.**

Such a functor represents:

- Processes as instances of **Sensing, Decision, Action or Physical**
- Interactions as **exchanges of information or exchanges of energy**

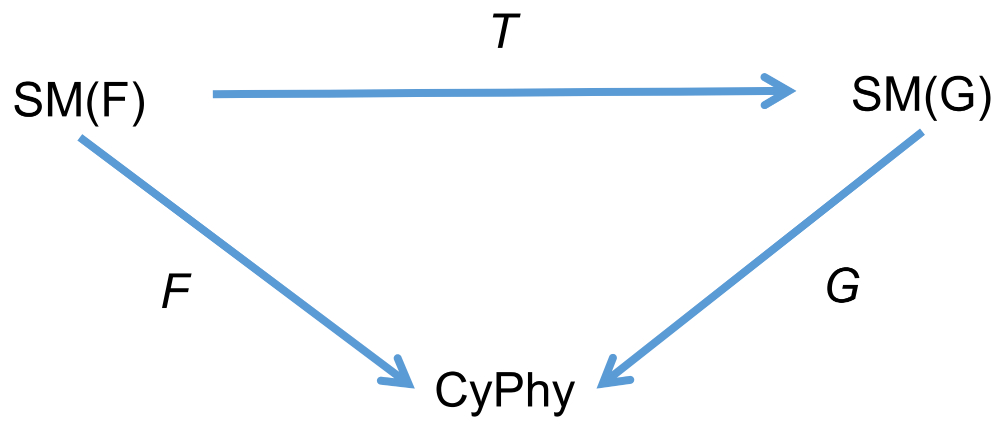
Benefit of this representation can be derived from:

- Structural representation of one CPS 'in another' (isomorphic with a *sub-CPS*)

6.1.5 The category *CPS*

Given two representations of CPS as functors *F* and *G*, let SM(F)/SM(G) denote the symmetric monoidal categories that F and G map into CyPhy

Mor(F,G) is the functors *T* from SM(*F*) to SM(*G*) such that the following diagram commutes:



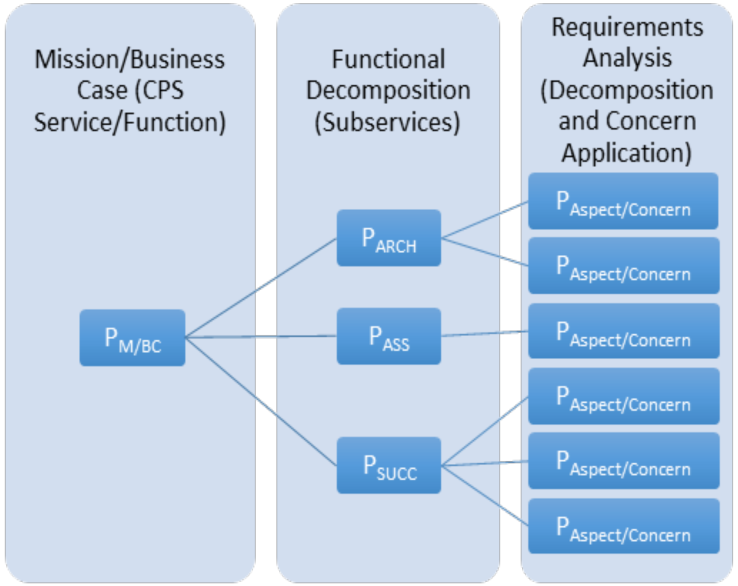
6.1.6 Mathematics of CPS Framework

Property-Tree of a CPS

Legend

$P_{M/BC}$ = Mission/Business Case
P_{ARCH} = Integration Steps
P_{ASS} = Assumptions
P_{SUCC} = Success Criteria
$P_{Aspect/Concern}$ = Aspect/Concern

- Branches capture the 'genealogy' of a property
- Branching gives assurance conditions for the branching node property
- Concerns may give rise to multiple properties in the Functional Decomposition
- 'Edges' should be read 'depends on' (L2R) or 'needed to satisfy' (R2L)



Semantics of CPS Framework

$$P \in \overline{Concern}^{CPS}$$

$$\bar{P}^{CPS} = \{tests\ T\ for\ P\}$$

$$Supp_M(T) = \{measurement\ support\ \mu_1, \dots, \mu_k\ of\ T\}$$

$$\overline{Evidence}^{CPS}(P) = \sum_{T \in \bar{P}^{CPS}} \bar{T}^{CPS}$$

… defines **composition of concerns**

$$\overline{C_1 * C_2}^{CPS} = \overline{C_1}^{CPS} \cup \overline{C_2}^{CPS}$$

Formal Methods for Assurance of a CPS

$$< d, e, a > \in P(CPS) \equiv_{Def}\ design\ element\ d, test\ evidence\ e\ are\ sufficient\ based\ on\ argument\ a\ to\ conclude\ that\ the\ CPS\ satisfies\ P$$

$$\overline{Assurance\ Case}^{CPS} = \sum_{C \in Aspect^{CPS}} \sum_{P \in \bar{C}^{CPS}} \sum_{d \in Design^{CPS}} \sum_{e \in Evidence(P)^{CPS}} \overline{Argumentation}^{CPS}(P)$$

6.2 Applications to Transportation – McShane/Brandao

6.2.1 Delivering Excellence Through Innovation & Technology

An introduction to the Ricardo Group

V1 16G U (July 2016)

6.2.2 100 Years: Delivering excellence through innovation and technology

- **A global, multi-industry, multi-discipline consultancy and niche manufacture of high-performance products**
- **The objective throughout our history has been to maximize efficiency and eliminate waste in everything we do**

6.2.3 Strategy for growth: Global engineering, environmental consulting and niche product manufacture…

Megatrends driving focus for solutions:

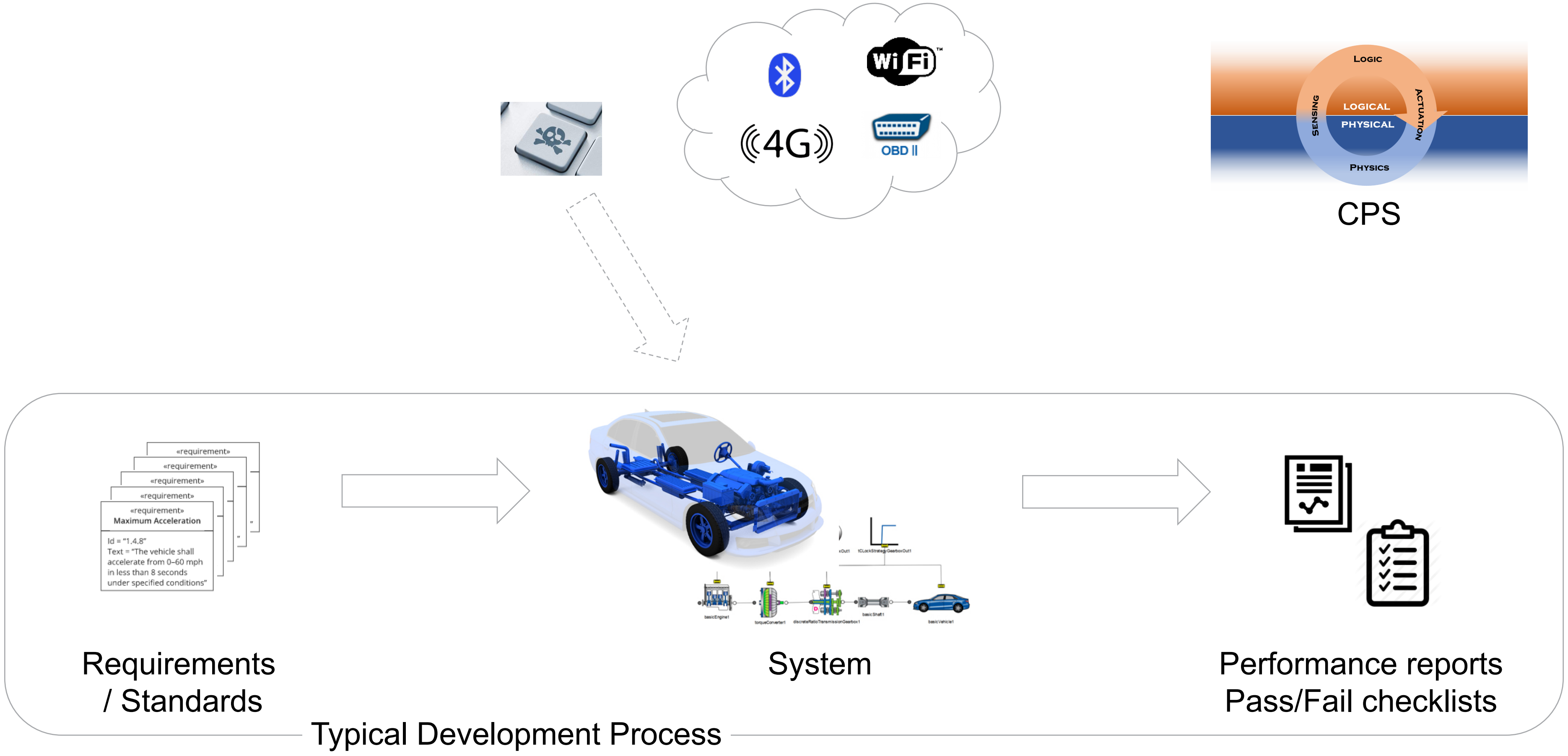
- **Climate change**
  (Emissions and waste)
- **Resource scarcity**
  (Oil/water usage)
- **Urbanization**
  (Transport, energy, efficiency)
- **Energy security**
  (Renewables, bio-fuels)

6.2.4 Products & services that cover global engineering and test, consultancy, independent assurance & niche product manufacture

- Engines
- Vehicle Engineering
- Driveline & Transmissions Systems
- Hybrid & Electrical Systems
- Critical Systems
- Strategic Consulting
- Environmental Consulting
- Energy Consulting
- Niche Manufacturing
- Independent Assurance
- Software
- Test Services

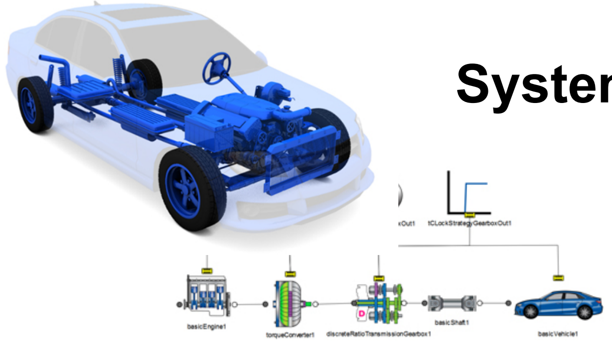
A broad range of capabilities and expertise

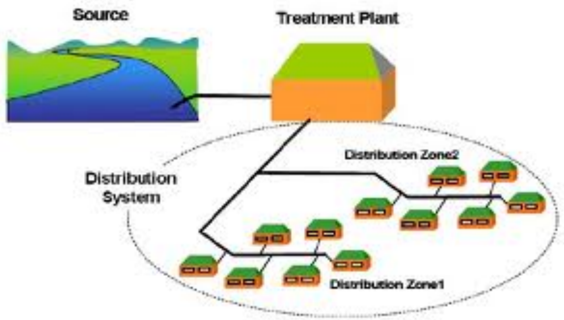
6.2.5 Automotive Use Case Setup

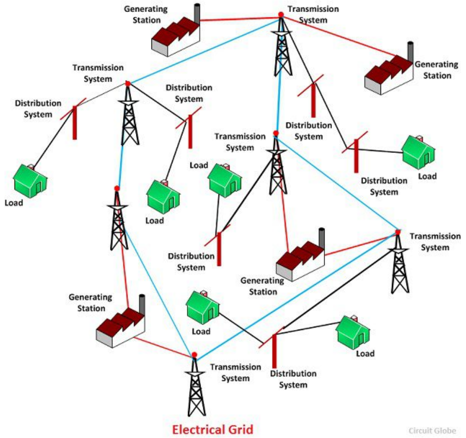


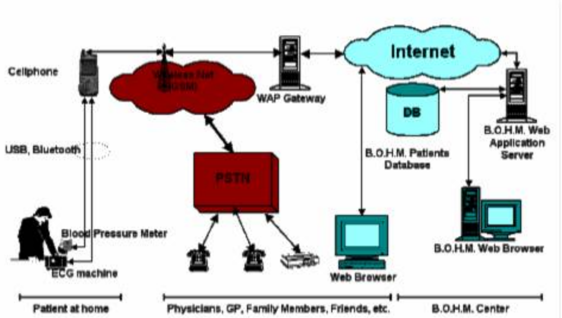
6.2.6 Use Case Setup - System

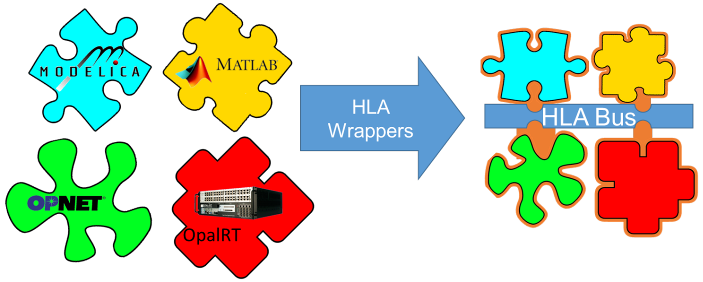
System











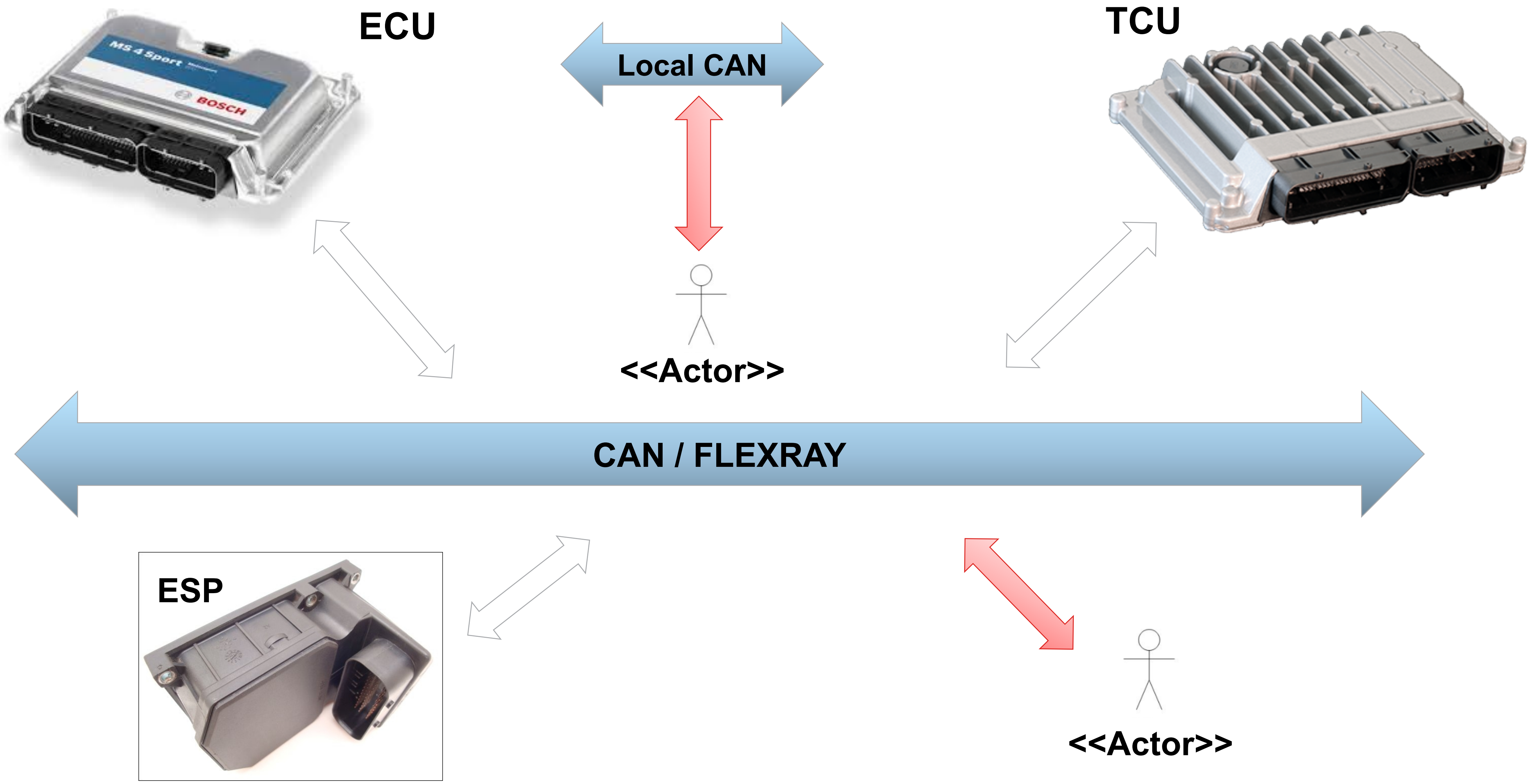
System can be:

- Automotive
- Water Process and Distribution System
- Electrical Grid
- Medical/Health System application
- …

Diverse testbed options/configurations:

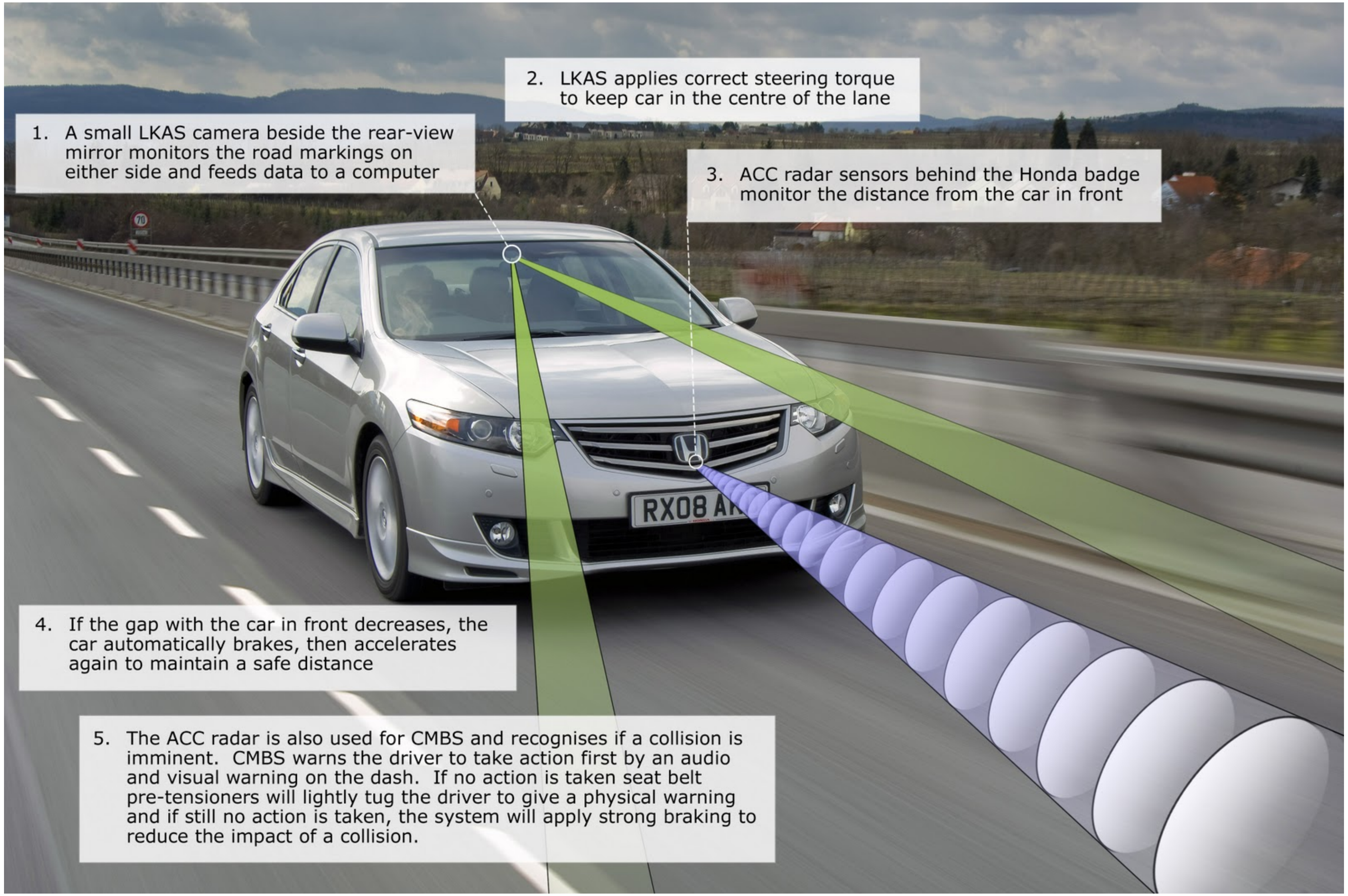
- All virtual prototype using MiL and SiL
- HiL system(s) at different phases of the development process
  - with emulated HW
  - HW as they are made available
- Real-time
- Sub-systems and components may have diverse ownership / suppliers
- IP protections
- On-board and off-board interactions and attacks

6.2.7 Sample of multiple control units' communication

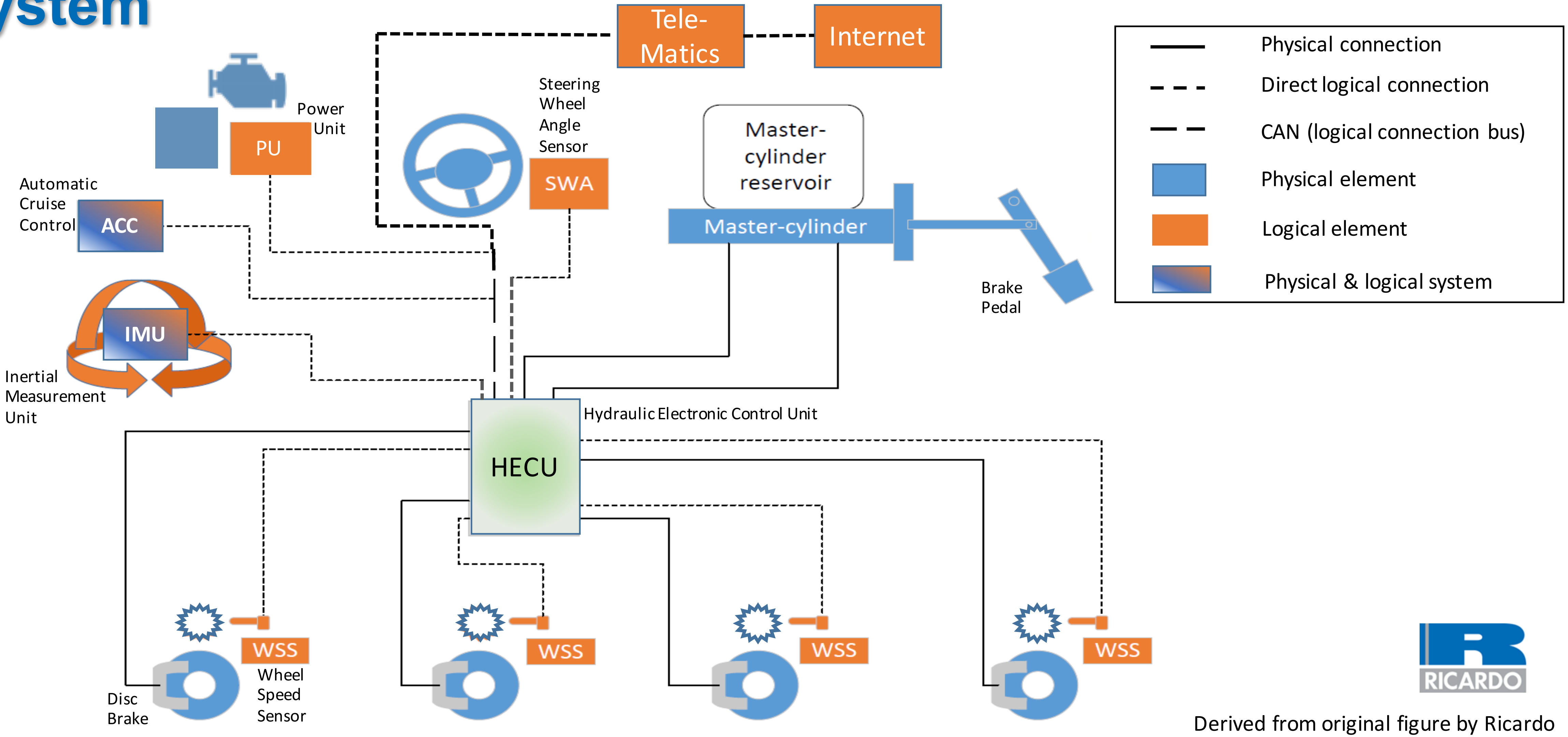


6.2.8 Automatic Emergency Braking - Example

RICARDO



6.2.9 Automotive System Functional Level: Brake System



Derived from original figure by Ricardo
www.ricardo.com

6.2.10 Sub-System Behaviors: Brake System

- **Passive Braking** – Basic functionality
  - Brake pressure applied no feedback (Open loop)

- **ABS** – Avoid locking of wheels
  - Brake pressure applied, feedback based on wheel speed sensors (Closed loop)
  - Basic Stability control – not loosing control of vehicle due to braking, based on wheel speed and other sensors

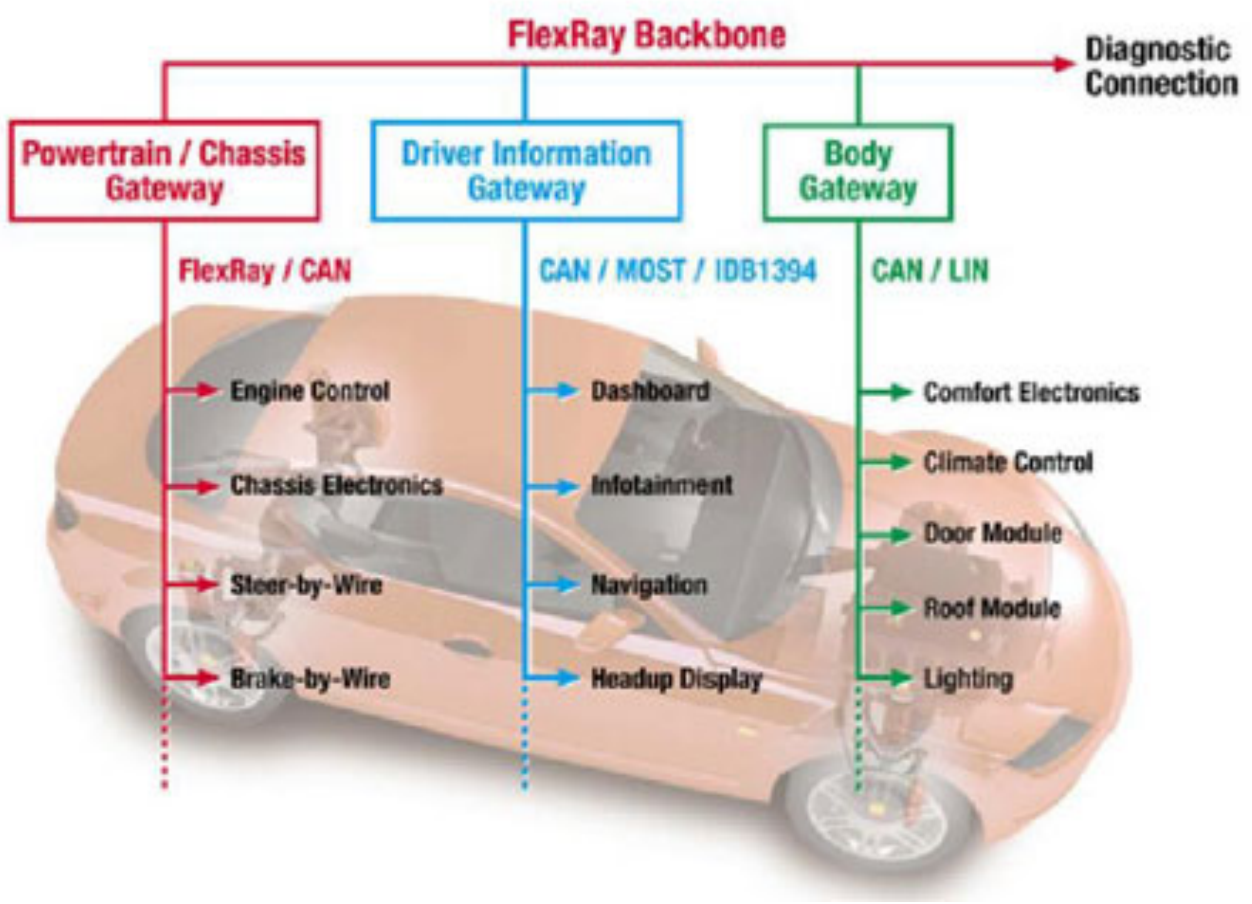
- **Automated – Collision avoidance**
  - Proximity sensors trigger braking event due to;
    - Car brakes by itself (Distracted Driver / reaction time)
    - Driver not braking soon enough or hard enough
  - Keep in the direction of travel, Systems controls steering and brake pressure
    - Similar to LKA

6.2.11 Demo Plan

Concept:

- **Multiple control systems** developed by different suppliers
- **Communication via CAN Bus** using encrypted signals
- **Confidential/proprietary information** passing.
- **Potential to be Hil /Sil** or a combination of both
- **Federated experiments** could be;
  - **Cyber attack** through the infotainment system or on-board component
  - **Braking system Hardware malfunctions** and doesn't send the correct signals

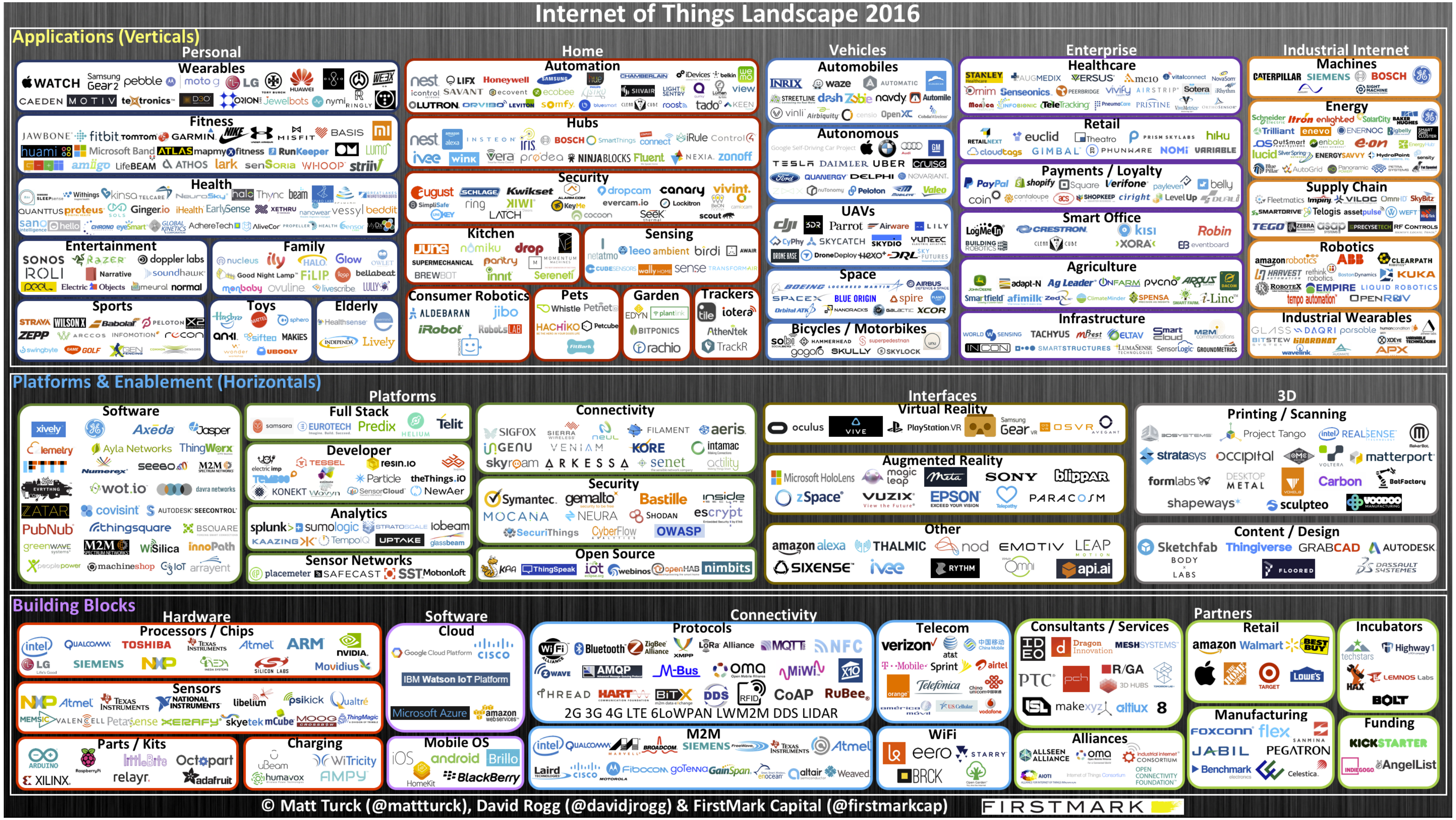
State of the Art Vehicle Control Network



Reference: http://ercim-news.ercim.eu/images/stories/EN87/hanzlik1.jpg

6.3 IES City Tables: CPS Framework as Benchmarking Tool - Burns

6.3.1 The Challenge - Divergent CPS/IoT Technology Landscape

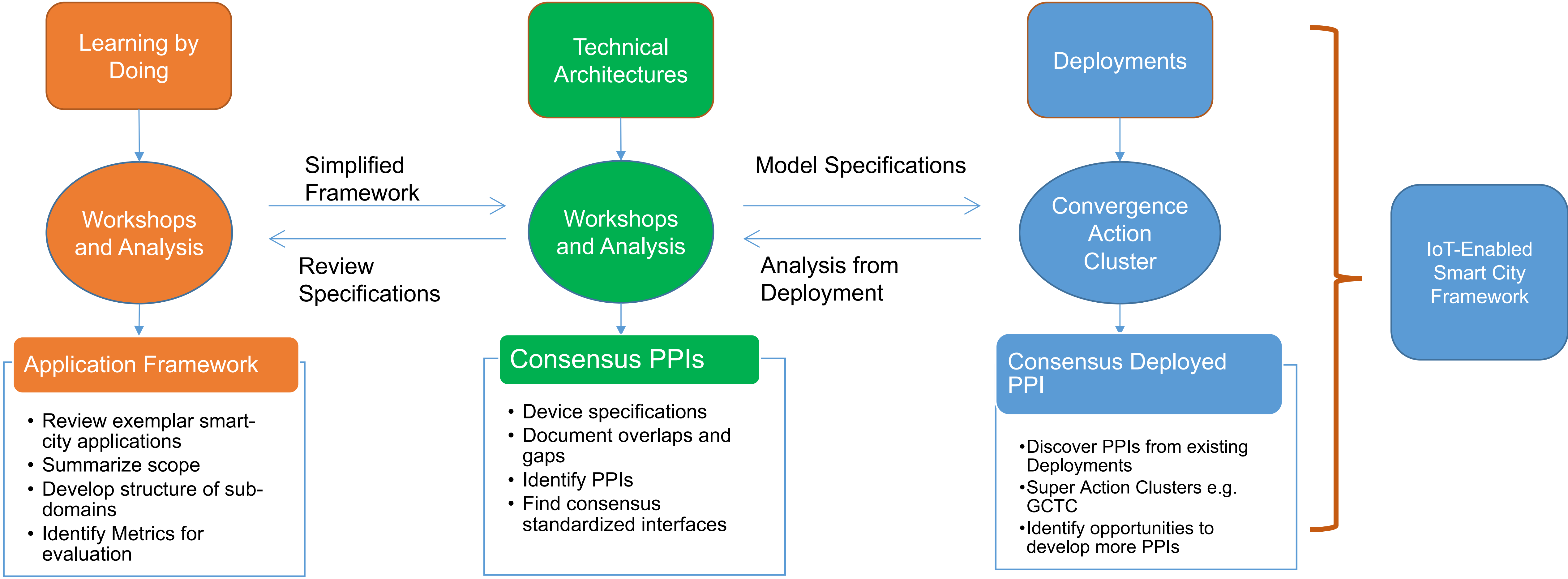


6.3.2 Internet of Things-Enabled Smart (IES) City Framework

- IES-City ("Yes-City") Int'l Working Group NIST and its partners have convened a public working group to distill a common set of smart city architectural features and to identify "Pivotal Points of Interoperability"
  - 3 working groups, collaboration site: https://pages.nist.gov/smartcitiesarchitecture/
  - Completion in fall 2017

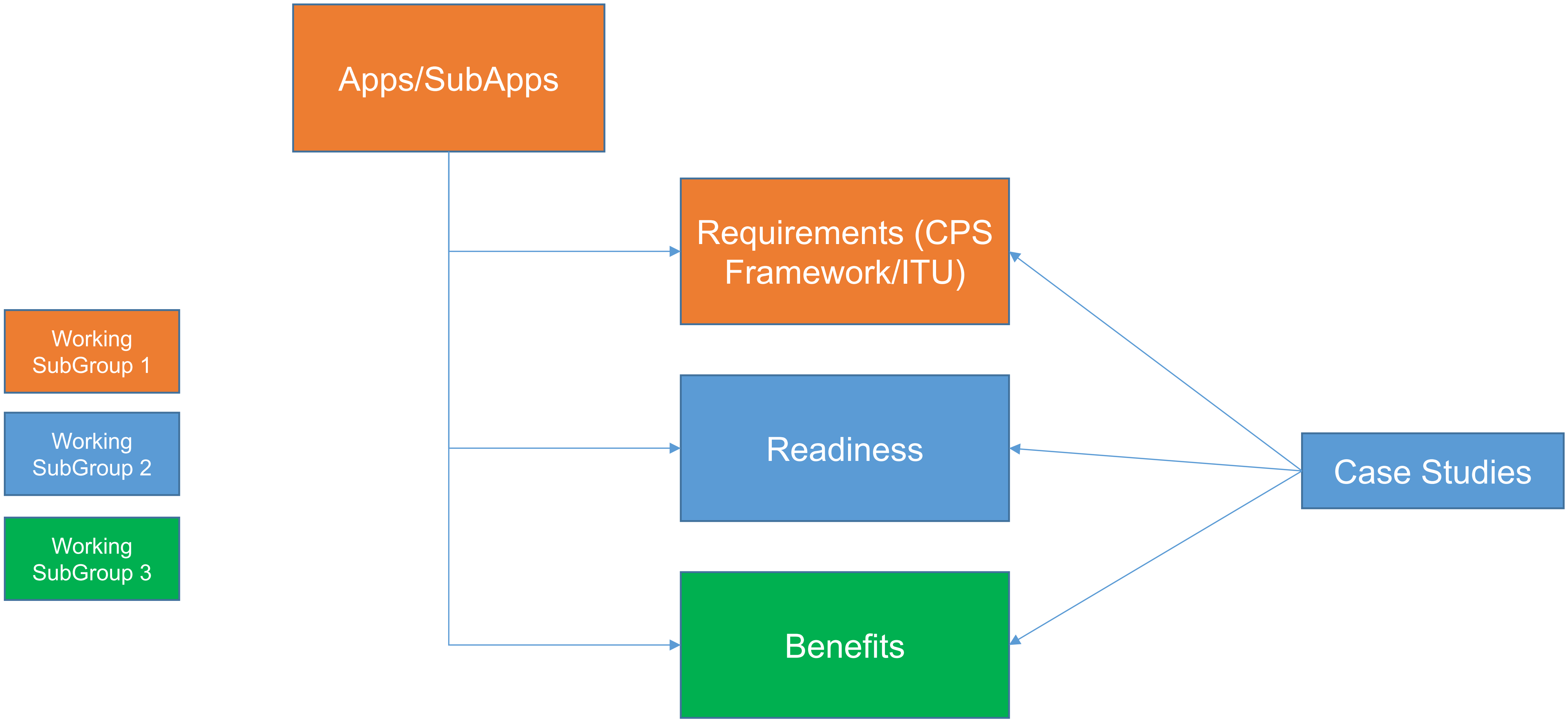
FIWARE MSIP NIST National Institute of Standards and Technology U.S. Department of Commerce ETSI World Class Standards ANSI U.S. Green Building Council USGBC ENEA Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile TIA Advancing Global Communications

6.3.3 NIST Public Working Groups



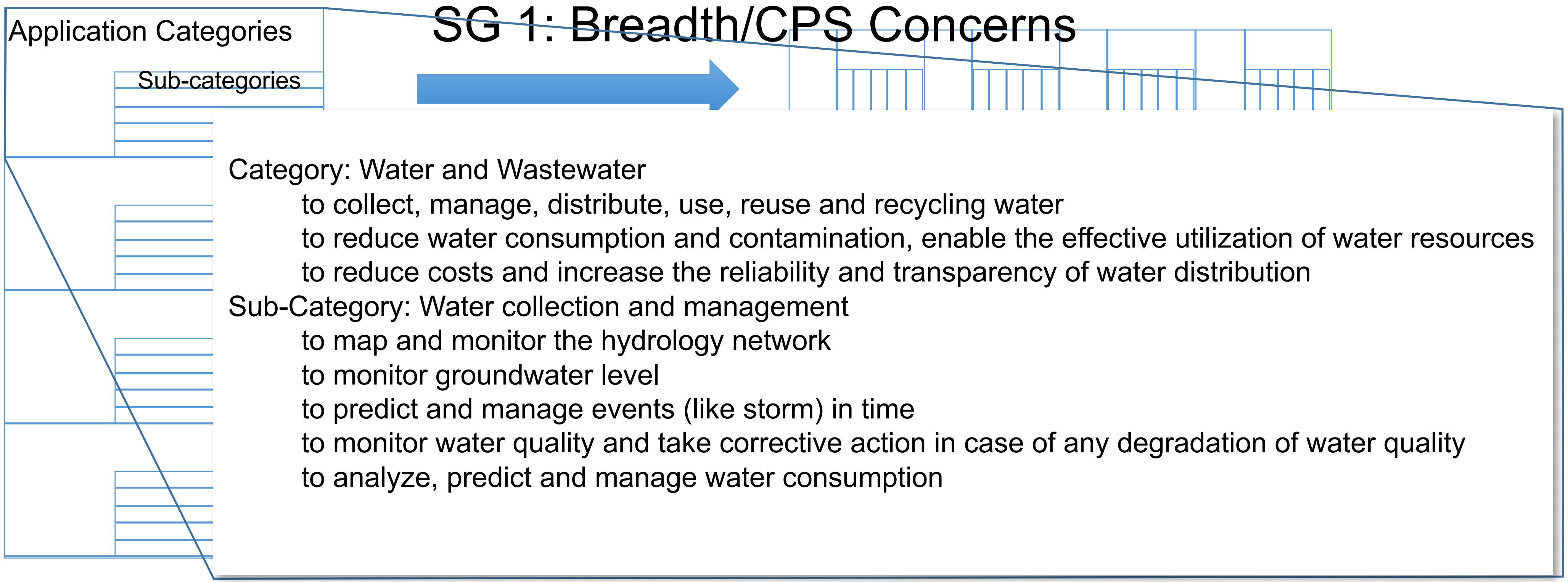
Participants: City CTOs, Experts, Companies, Technical Stakeholders, …

6.3.4 Application Framework Model

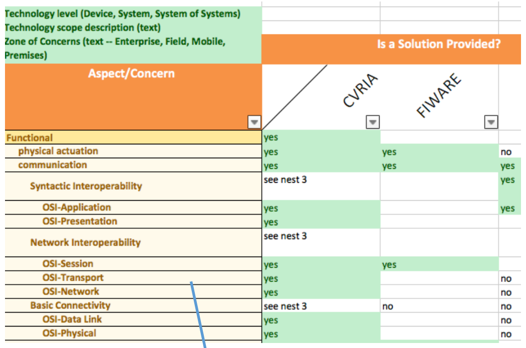


6.3.5 Application Framework Data Analysis

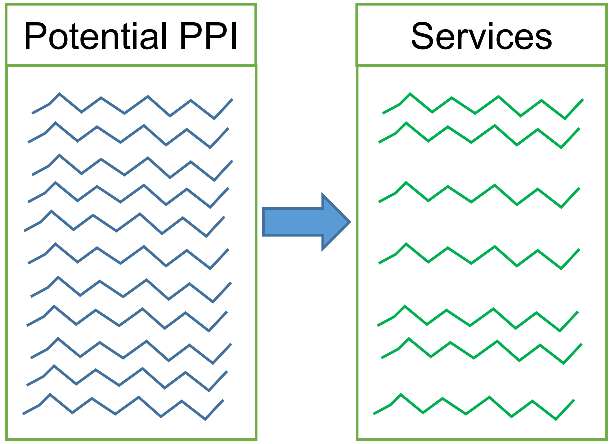
Spreadsheet Database Model of Application Framework



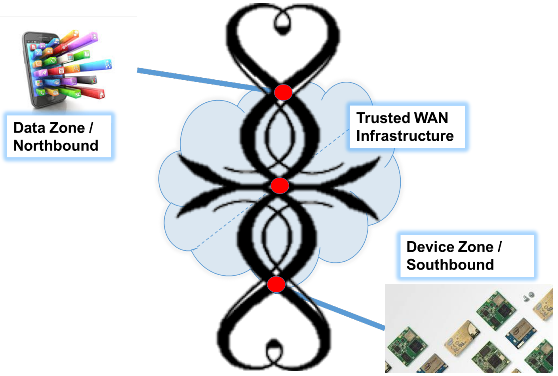
6.3.6 Consensus PPI



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



Zone of Concerns = bundles of services that address a "vector" of concerns



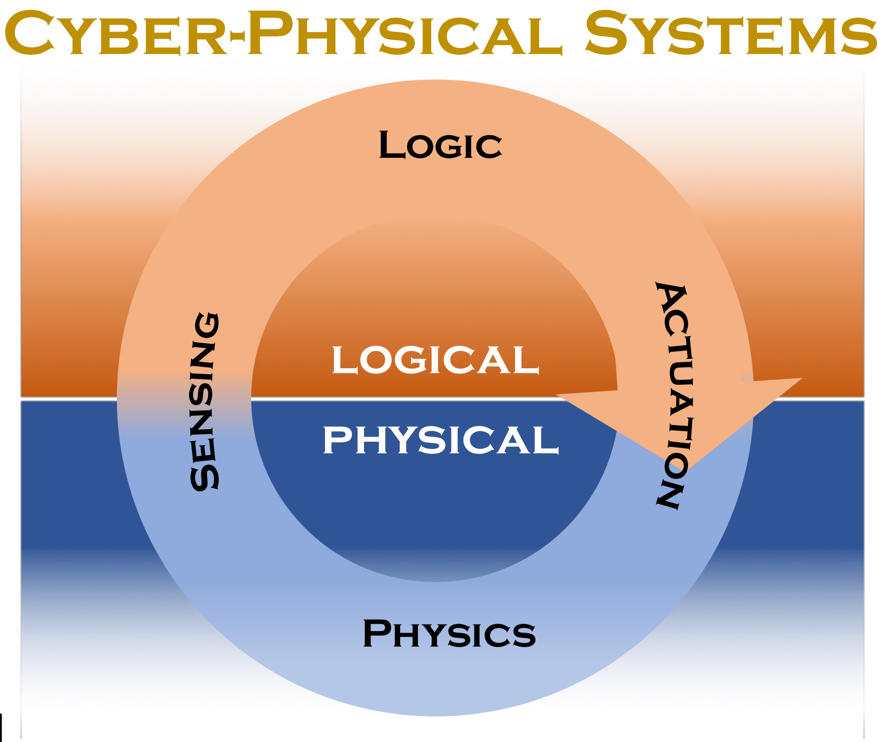
Simplified by Aspects and Concerns

Complex Specifications and Architectures

6.4 From Security to Trustworthiness - Vishik

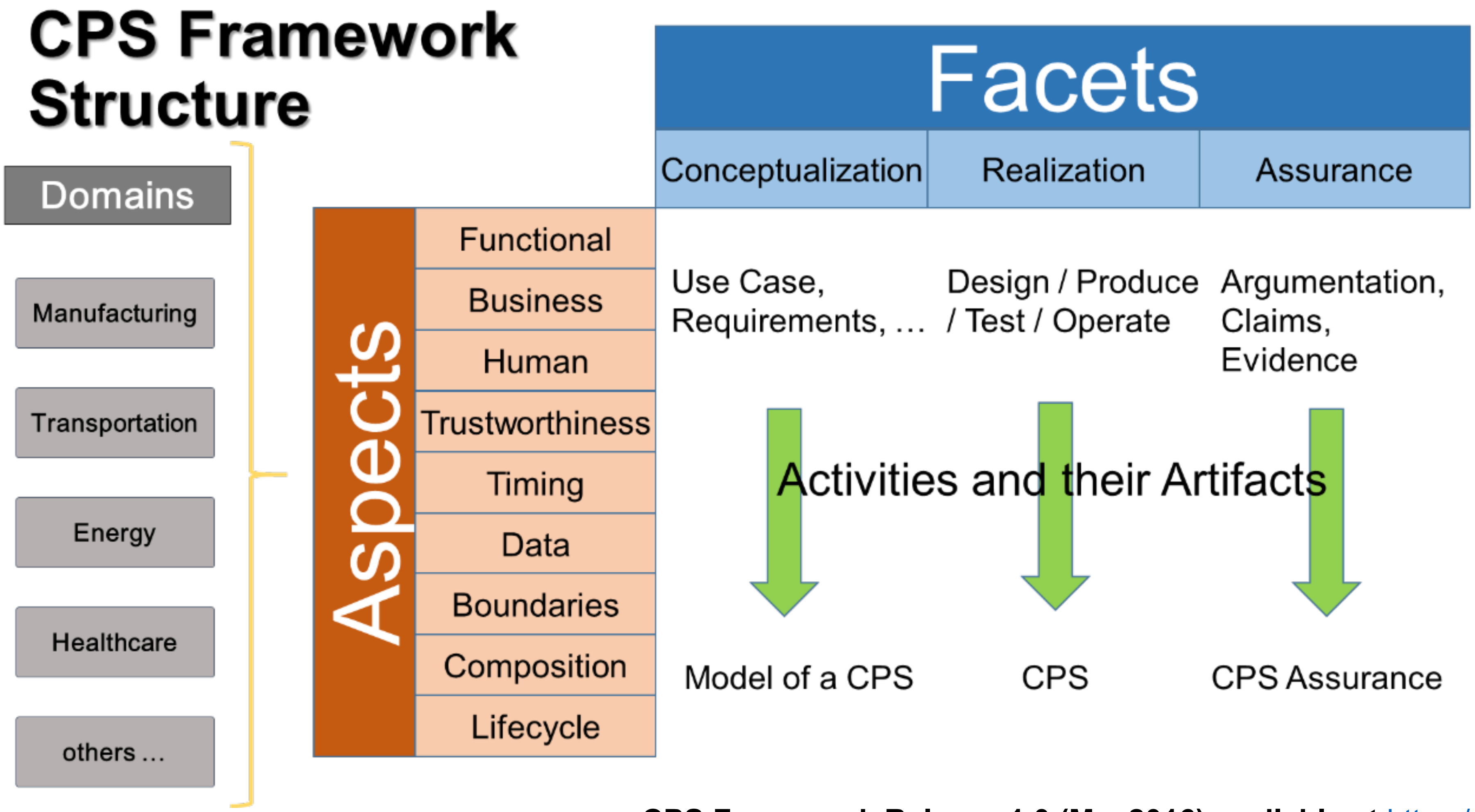
6.4.1 Definition of CPS

Cyber-Physical Systems (CPS) comprise interacting digital, analog, physical, and human components engineered for function through integrated logic and physics.



Internet of Things (IoT) emphasizes digital infrastructure for widely connected, interacting systems.

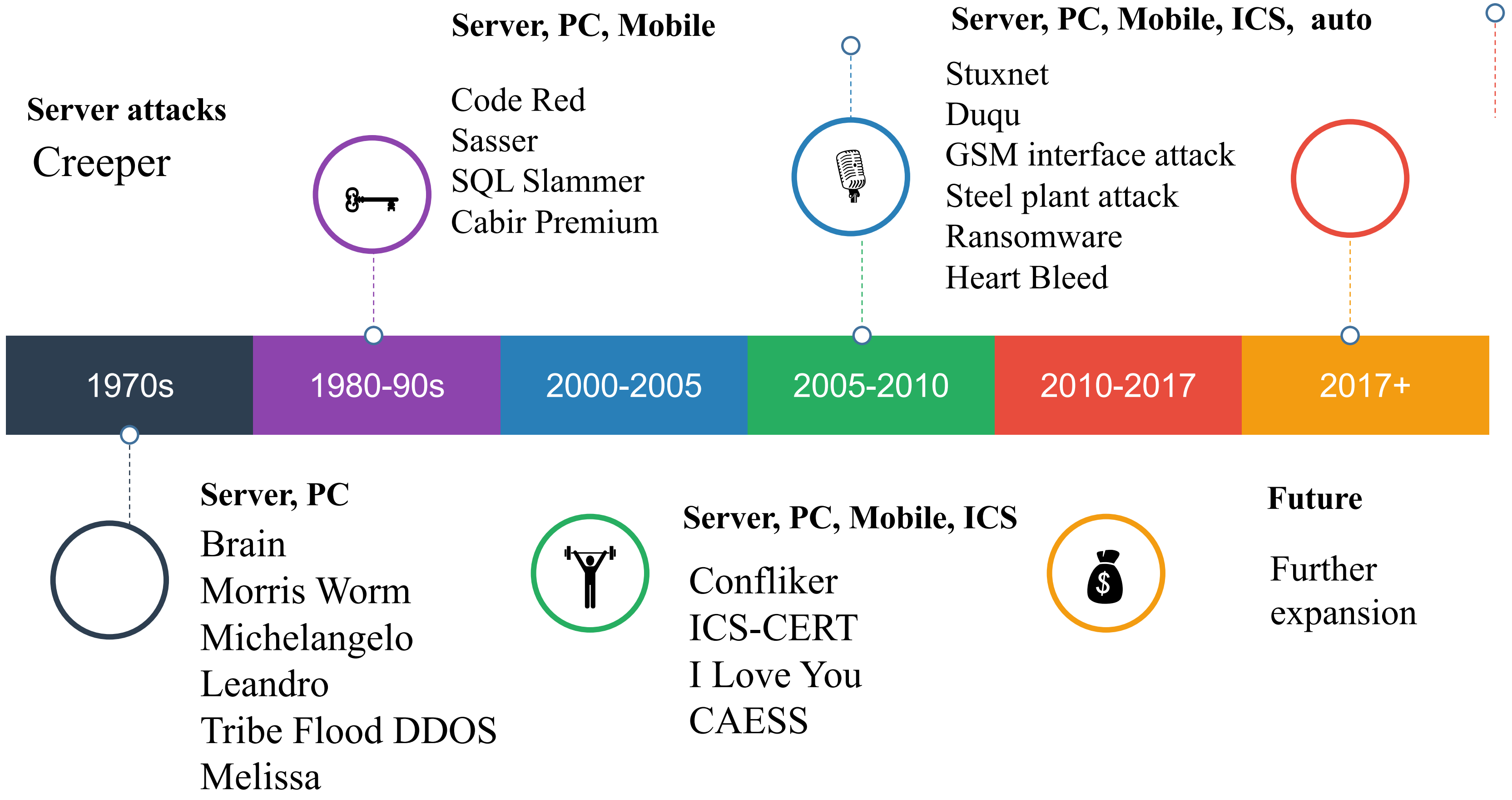
6.4.2 Trustworthiness in the CPS Framework



- **CPS Framework Release 1.0 (May2016) available at** https://pages.nist.gov/cpspwg/

6.4.3 Reach of cyberattacks is expanding

Adequate protection mechanisms have to include privacy, safety, security, and other areas (reliability, resilience) treated in an Integrated fashion



6.4.4 Trustworthiness: integrated concept

From NIST CPS Framework (https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf_

Safety	Ability to ensure the absence of catastrophic consequences on the life, health, property, or data of stakeholders
Security	Internal or external protection from unintended and unauthorized access, change, damage, destruction, or use of systems
Privacy	Risks to individuals arising from the processing of their personal information
Reliability	Ability to deliver stable and predictable performance in expected conditions
Resilience	Ability of withstand instability, unexpected conditions, and gracefully return to predictable, but possibly degraded, performance.

Definition: Demonstrable likelihood that the system performs according to designed behavior under a typical set of conditions as evidenced by its characteristics, such as safety, security, privacy, reliability and resilience.

6.4.5 Integrated trustworthiness: sample categories of use cases

Modeling	Use the integrated approach to model current and future systems and complex environments
Design and development	Anticipate connections, features, and constraints in designing CPS
Analysis and assessment	Assess existing systems to understand their potential vulnerabilities and to optimize deployment

6.4.5 Integrated trustworthiness: some challenges

Misalignment of metrics	Even for probabilistic models, the values for failure rates for, e.g., security and safety are very different
Mutually exclusive requirements	Requirements for adjacent areas are misaligned. E.g., transparency requirements are fundamentally different for security and privacy
No mechanism for composition	No reliable tools to model a component in context, e.g., autonomous vehicle in a Smart City

6.4.6 Next steps: from TW positioning to ontology & reasoning

Current state	CPS framework positions trustworthiness within CPS and allows the technologists to decompose this concept
Ontology and reasoning	Future work needs to create a trustworthiness ontology matching the current CPS framework and reasoning algorithms to analyze trustworthiness
Trust language	Trust language will need to be developed as a tool for trustworthiness calculus (building on existing 'reasoning languages' such as OCL, OWL, etc.)

6.4.7 Useful concept: trust evidence

Ability to rely on a broader list of characteristics (evidence) to assess trustworthiness. Some examples below.

Trust posture	Nuanced rather than black & white approach to trust
Identification	Provable device identification, proof of ownership, provable transaction identification
Measurement	Verified proof of domain integrity and software integrity, integrity measurement, time stamp
Evaluation	Evidence of self certification & evaluation, conformance to standards, data quality
Configuration	Proof of the integrity of configurations; up-to-date maintenance record

Definition: trust evidence is an agreed upon system of parameters that could help define trustworthiness in a complex environment

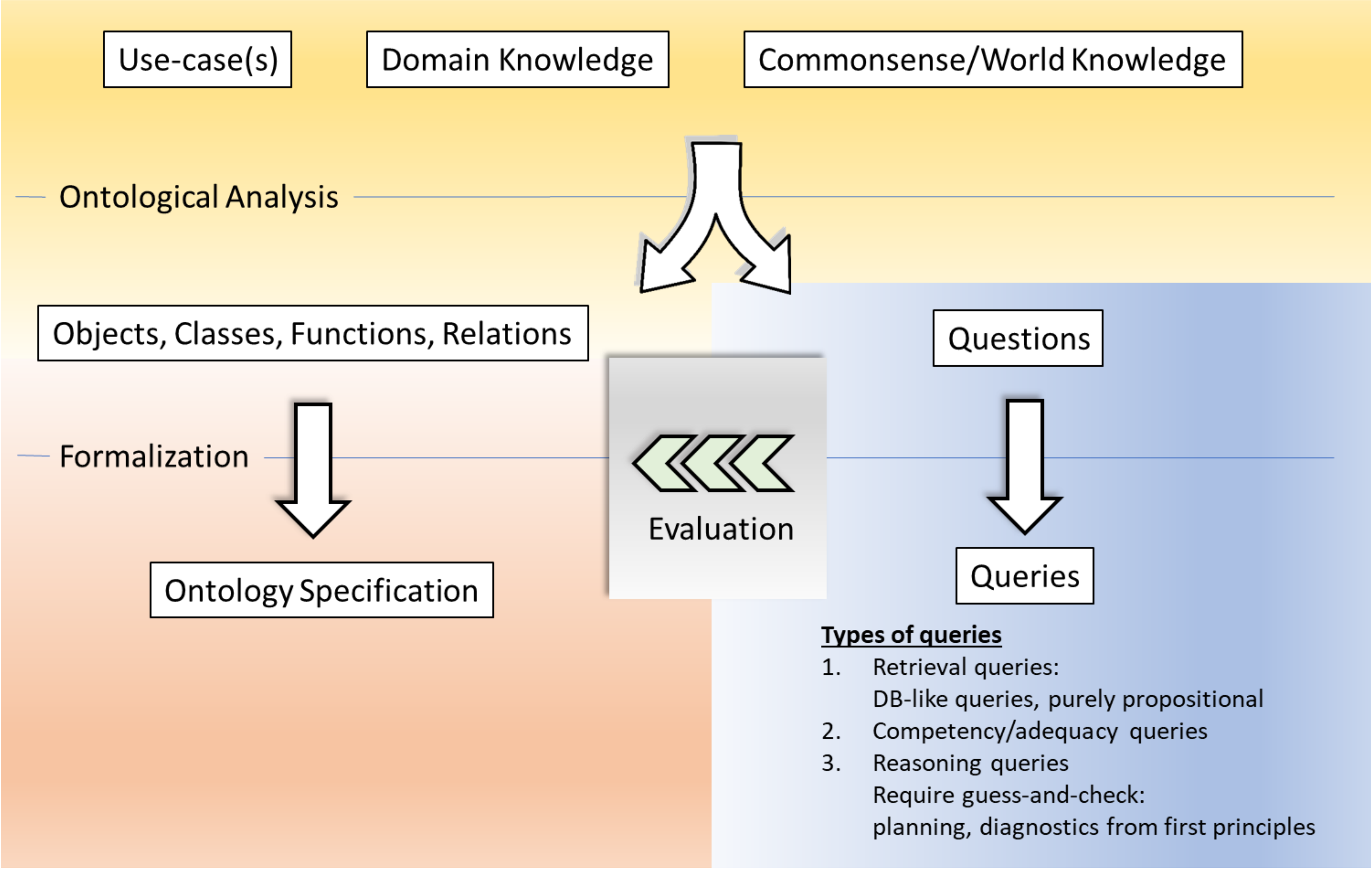
6.4.8 Relevant area: human/technology connection

- **Intent semantics** — The intent of the user or developer while designing and using a system
- **Usability** — Ease, with which a system can be used, learned, and integrated into an environment or process
- **Transparency** — Ease, with which a system can be understood for functions that a user or other systems need to know

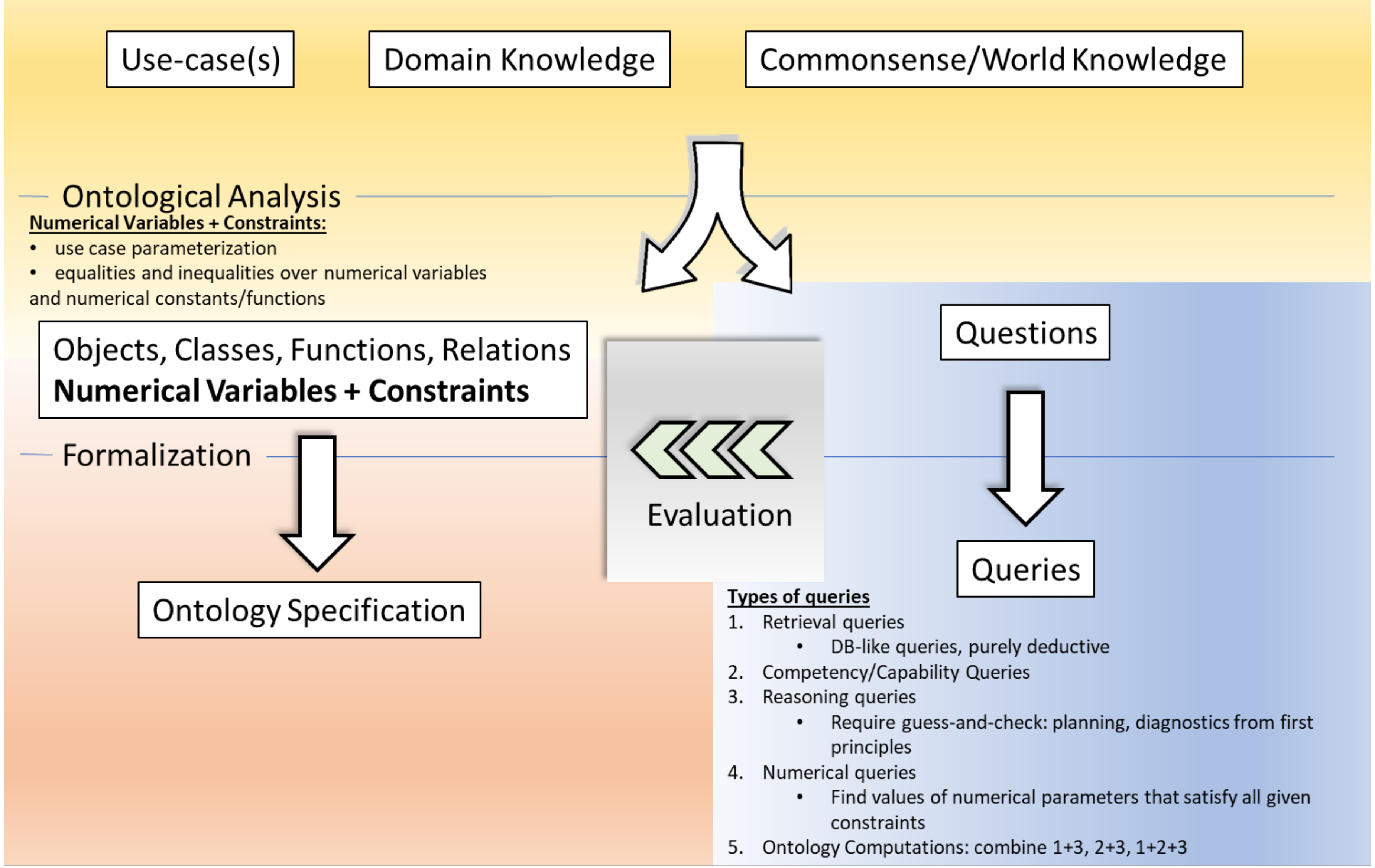
Although the majority of interactions are machine to machine, the human aspect is very important!

6.5 Trustworthiness Modeling - M. Balduccini

6.5.1 Modeling Methodology: Conceptual Ontology



6.5.2 Modeling Methodology: Parametrization, Ontology Calculus



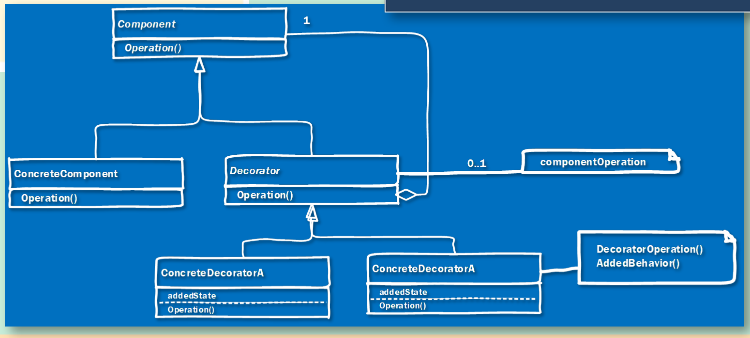
6.5.3 Modeling Tools

UML

Unified Modeling Language (UML) is a general-purpose, developmental, modeling language in the field of software engineering, that is intended to provide a standard way to visualize the design of a system. (Wikipedia)

Focus: systems, system design, code generation

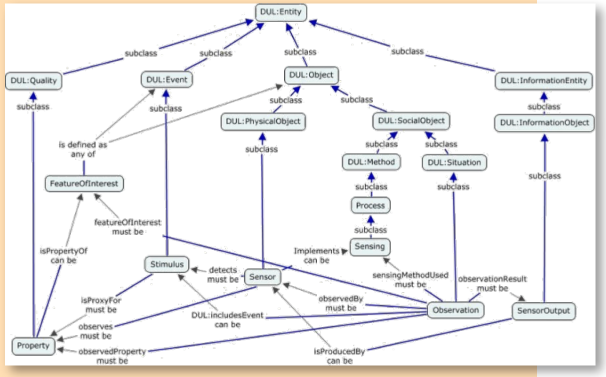
```
public class Footer2 extends TicketDecorator {
  public Footer2 (Component myComponent) {
    super (myComponent);
  }
  public void prtTicket() {
    super.callTrailer();
    //place printing footer 2 code here
  }
}

public class Factory {
  public Component getComponent () {
    Component myComponent;
    myComponent = new SalesTicket();
    myComponent = new Footer1(myComponent);
    myComponent = new Header1(myComponent);
    return myComponent;
  }
}
```



Knowledge Representation (KR) Languages, OWL

The W3C Web Ontology Language (OWL) is a Semantic Web language designed to represent rich and complex knowledge about things, groups of things, and relations between things. OWL is a computational logic-based language such that knowledge expressed in OWL can be exploited by computer programs, e.g., to verify the consistency of that knowledge or to make implicit knowledge explicit (W3C)

Focus: "world" knowledge, commonsense, automated reasoning



Which Sensor can detect Stimulus x?

6.5.4 Modeling Use-Case

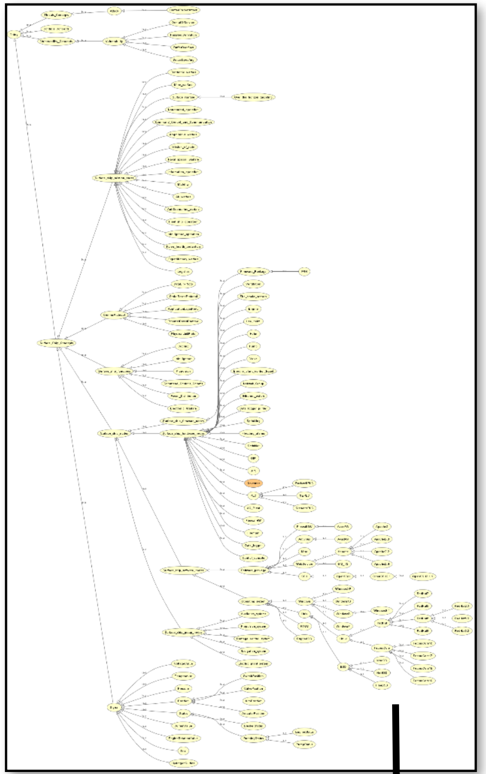
Device model

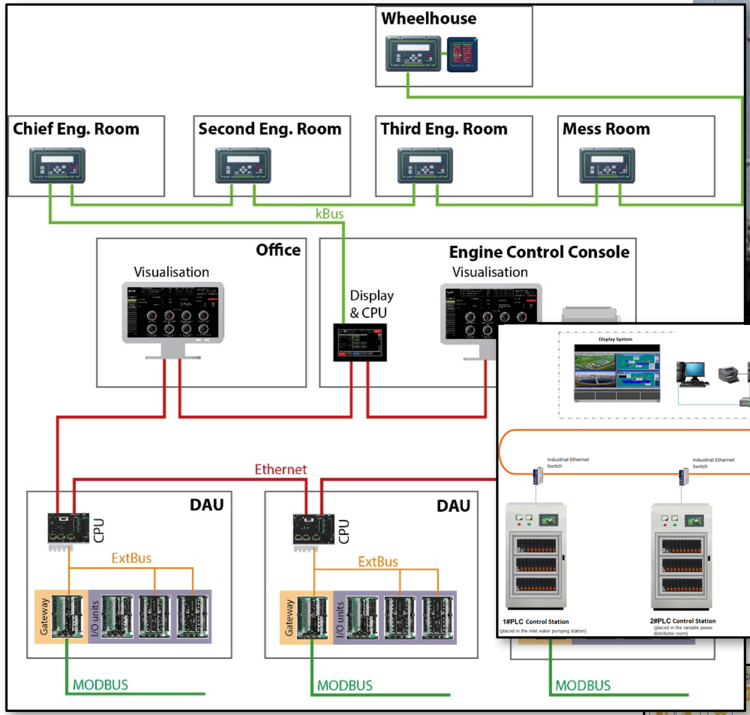
- Police body cameras
  - Body cameras, location sensors, alarm sirens

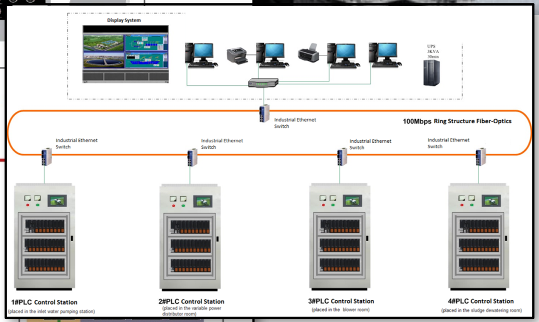
Trustworthiness elements

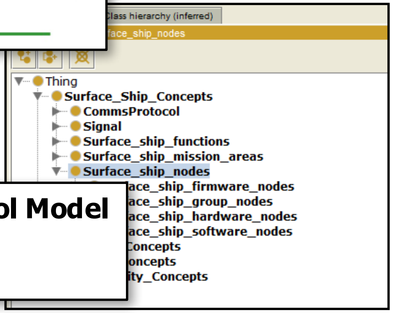
- Security
  - Physical Security: broken, stolen
  - Cyber Security: CIA of data streams
    - Important if used in court
    - Potential approach: timestamp
- Privacy
  - Is face recognition in use?
  - Who has access to the information?
- Reliability: will the camera work 24/7?
  - Data reliability:
    - Multiple cameras, multiple streams
    - Stored on a server
    - Who has access? Who can access all streams?
- Resilience
  - What if a camera does not work?
  - Can the stream from a nearby camera be used as a substitute?
    - "Stitch camera feeds from home security systems"

6.5.5 Earlier Work: Cone-of-Impact Vulnerability Assessment









MCS Architecture Model
- Hierarchy of systems
- Physical/network links

Vulnerability Model
- Vulnerabilities
- Affected systems

Threat Model
- Target
- Consequences

Mitigation/Control Model
- Mitigation type
- Effect

7. Panel Discussion - Greer

- **Discussion Topic**: “Why do we need holistic concern-driven engineering? “
- **Moderator**: Dr. Chris Greer
- What kinds of questions keep CPS leaders “up at night”?
- How should a CPS engineering process address questions like: Where are we in the process, how do we stand? What’s the degree of completion? What’s the test coverage?
- How do current practices reveal and resolve competing/interacting concerns in complex CPS?
- What has to change in education and training to succeed in engineering CPS? To drive a holistic concern-driven culture into the skills-based engineering curriculum of today?

8. Systems Engineering and the CPS Framework - Roth

8.1 Our goals for the CPS Framework

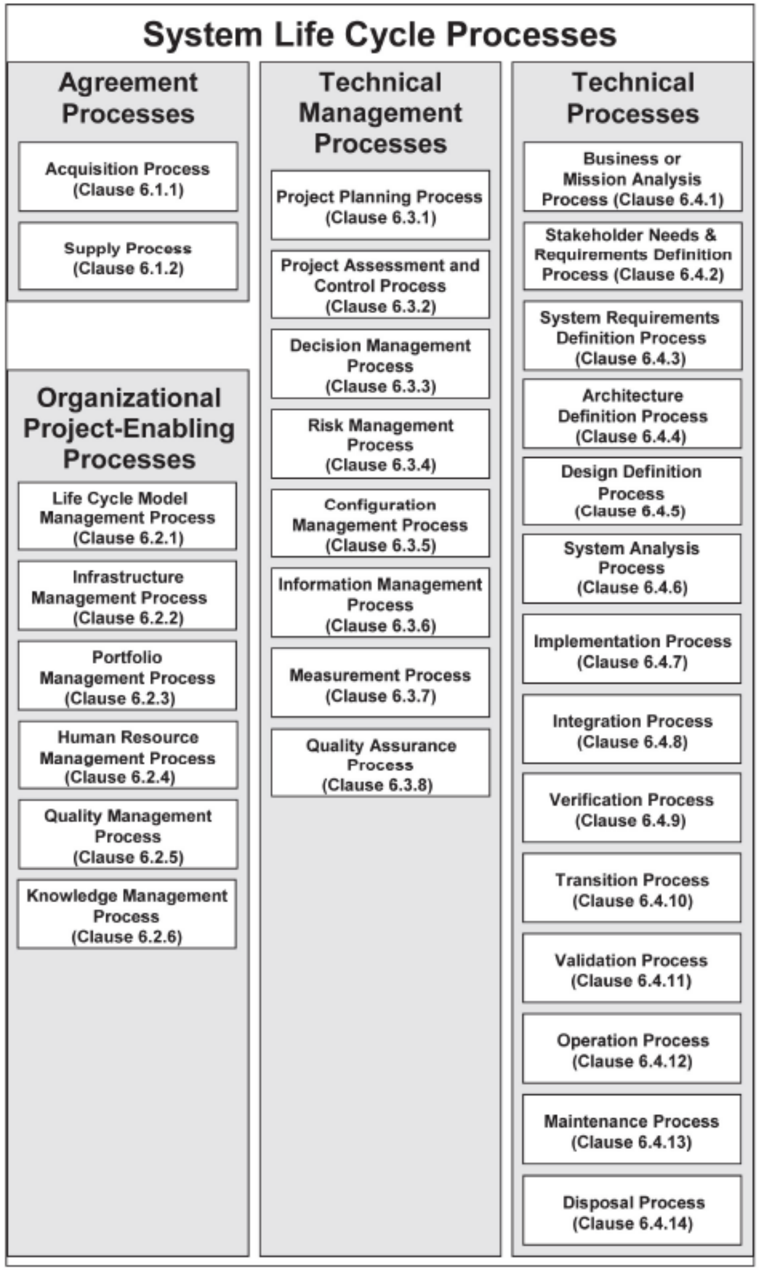
- Our goal is **not to replace** systems engineering processes!
- We believe that **existing approaches do not explicitly consider the breadth of concerns** required for CPS
- Our goal is to **enhance** existing systems engineering processes with a methodology **to apply a rich set of concerns** that are traceable throughout the CPS life cycle

ISO/IEC/IEEE 15288

A Systems Engineering Process Standard

8.2 What is 15288?

- An international standard that describes *"a common framework of process descriptions for describing the life cycle of systems created by humans"*
- Defines a **set of processes** that span the system life cycle separated into 4 categories (see right)
- Each **process description** has:
  1. a statement of **purpose**
  2. a set of **outcomes**
  3. a list of **activities** and their tasks



Source: ISO/IEC/IEEE 15288

8.3 15288 is designed to be adaptive

- It **does not prescribe a development methodology** for the implementation of process descriptions in a project

- It recommends to **use only the sub-set of relevant processes** for a given system of interest

- It **defines a tailoring method** to modify existing life cycle processes or create new processes

NIST SP 800-160

Special Publication on Systems Security Engineering

8.4 How can we build a secure system?

- **15288 provides no guidance** on what must be considered at each stage of the system life cycle to build a secure system

- **Modern systems are too complex** for concerns such as security to be separated from the system life cycle processes

- Trustworthiness is achieved by **holistic consideration of security concerns during system engineering processes**

8.5 What is 800-160?

- **Tailors 15288** process descriptions (purpose, outcomes, and activities) **to incorporate trustworthiness concerns**

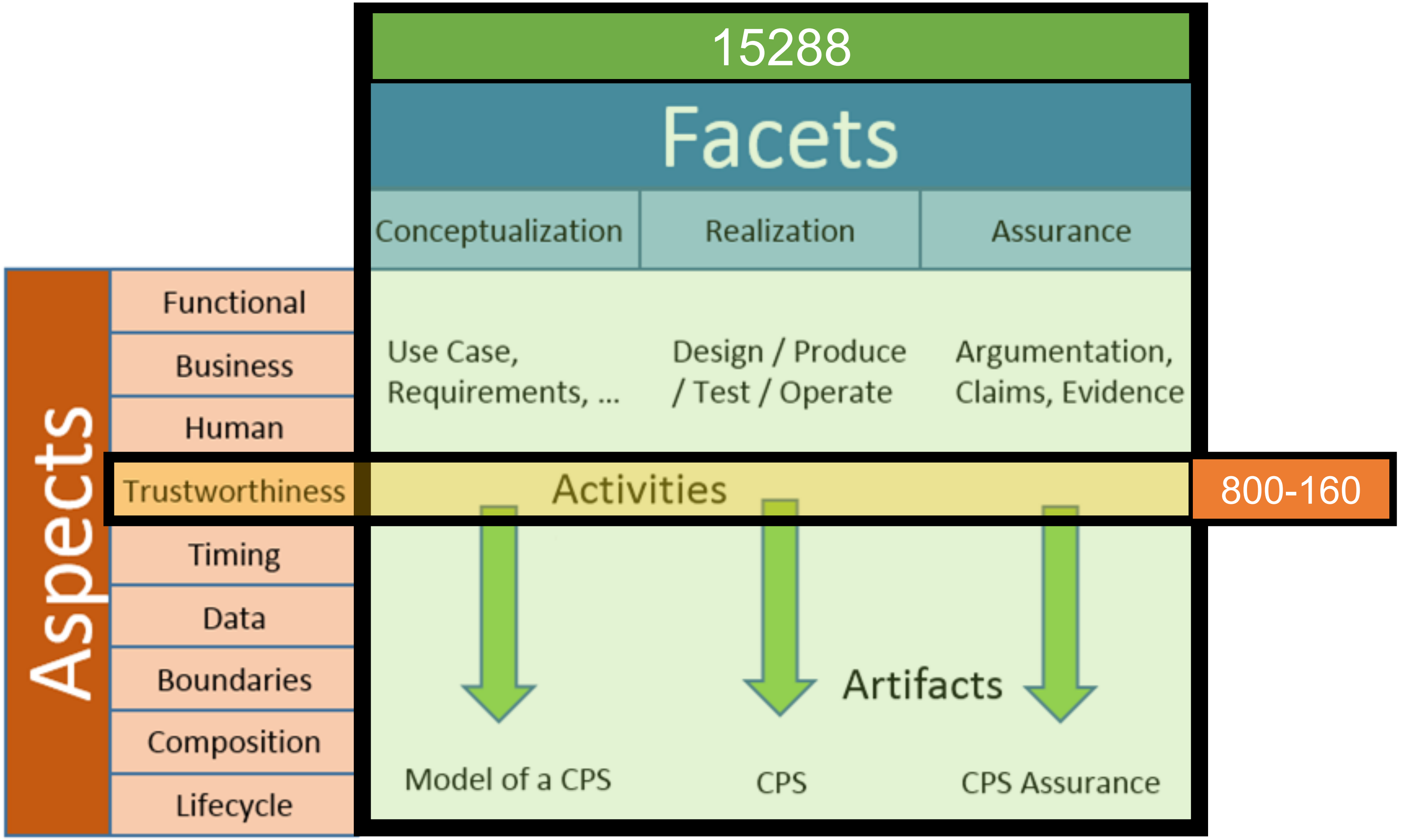
ID	PROCESS	ID	PROCESS
AQ	Acquisition	MS	Measurement
AR	Architecture Definition	OP	Operation
BA	Business or Mission Analysis	PA	Project Assessment and Control
CM	Configuration Management	PL	Project Planning
DE	Design Definition	PM	Portfolio Management
DM	Decision Management	QA	Quality Assurance
DS	Disposal	QM	Quality Management
HR	Human Resource Management	RM	Risk Management
IF	Infrastructure Management	SA	System Analysis
IM	Information Management	SN	Stakeholder Needs and Requirements Definition
IN	Integration	SP	Supply
IP	Implementation	SR	System Requirements Definition
KM	Knowledge Management	TR	Transition
LM	Life Cycle Model Management	VA	Validation
MA	Maintenance	VE	Verification

Source: NIST SP 800-160

CPS Framework

A Holistic Concern-Driven Approach

8.6 How does the CPS Framework fit?



NIST CPS PWG Framework Release 1.0

8.7 The need for a holistic approach

- All CPS aspects/concerns intrinsically depend on each other and we need a holistic approach for such **cross-cutting concerns**

- Examples:
  - **Cyber security mechanisms can be defeated by physical attacks**
  - **The most secure system is one that does nothing**
  - **The dichotomy between being fast and secure**

CPS Framework Open Source

The Road to a Development Process Tool

8.8 Our current state

- We **need** a **holistic, concern-driven methodology** for the development of CPS
- We **have** multiple **system engineering processes** that provide an outline for how to develop a CPS
- We **have** an **ontology of cross-cutting concerns** extracted from domain experts in CPS

8.9 Our plan moving forward

- CPS Framework satisfies our need at a conceptual level
- There is still a gap on **how to implement** the framework:
  - How to annotate the artifacts (process outcomes) with concerns?
  - How to manage and exchange the artifacts that are produced?
  - How to trace concerns across artifacts throughout the life cycle?
- We are working towards a **tool and data exchange format** to manage artifacts produced by 15288 / 800-160 / …

9. Modeling for a ‘CPS Framework Tool’ (Burns/Song)

1. Moving the CPS Framework Forward
2. Use Case Methodology
3. Model Realization
4. Modeling the CPS Framework and Use Case
5. Tools Demonstration

9.1 Moving the CPS Framework Forward

- We wanted to move adoption of the CPS Framework concepts into common practice in engineering CPS
- We believe that the CPS Framework enhances and extends existing system engineering processes and does not alter or replace them
- We hoped to quantify the discussion of CPS so that it can be studied from multiple disciplines

- So we developed a useable model of the CPS Framework

9.1.1 CPS Framework Model Requirements

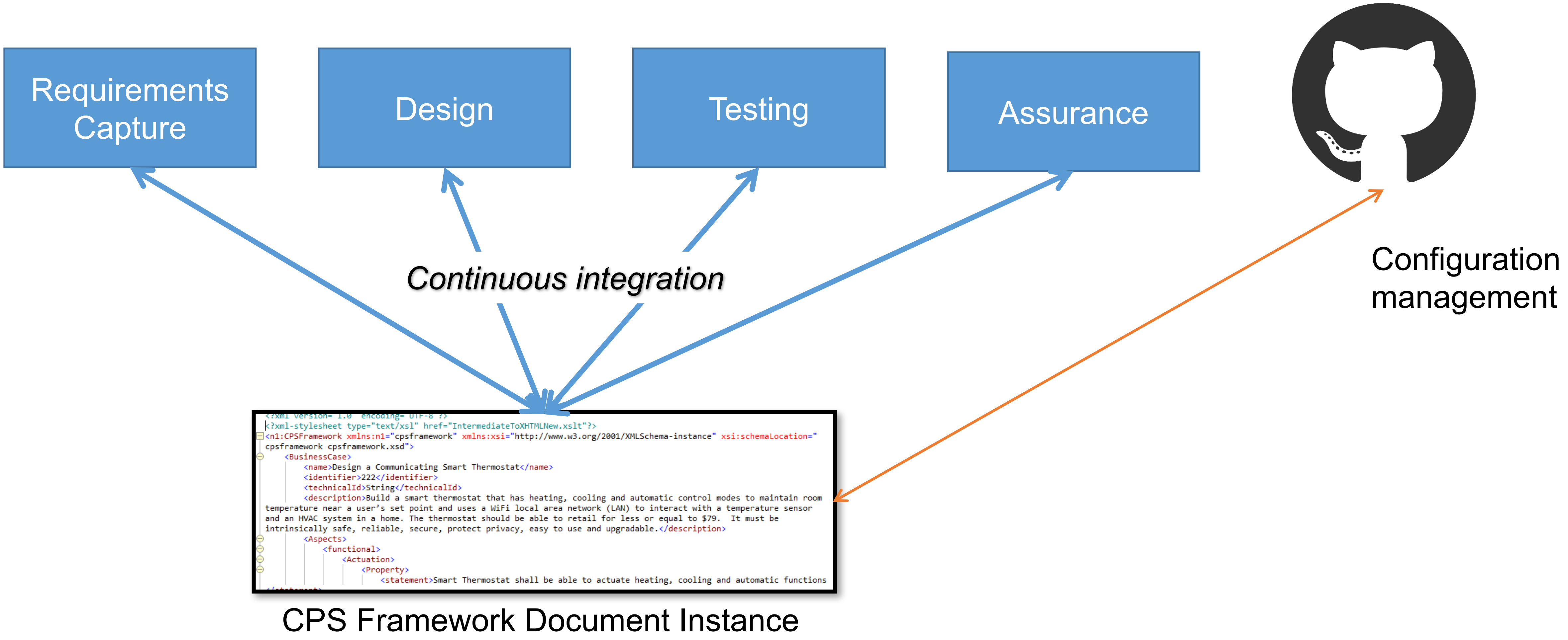
- Capture Concern-Driven Analysis
- Supports traceability of requirements, designs that realize them, tests that verify them, and argumentation that validates them
- Allows for maturity and versioning of parts
- Allows for reuse
  - composition of existing and new parts
- Supports referencing external artifacts and specifications
  - External documents and specifications
  - Standards and certification test references
  - Development process tool artifacts
- Supports reasoning over data set in single XML Document

9.1.2 Tech Transfer Concept

- We built this model so it can accessorize existing tool suites for system engineering process execution
- The result is a simple XML data file that can be an import or export to any tool
- The data structure of the XML document object is composable so that various tools can add/edit detail at any time
- The UML model and XMLSchema is provided as an open source tool set (more on this later) at:
  - https://github.com/usnistgov/cpsframework
- We encourage interested parties to evolve this with us to suit your collective needs

9.1.3 Evolution of CPS Design Instance

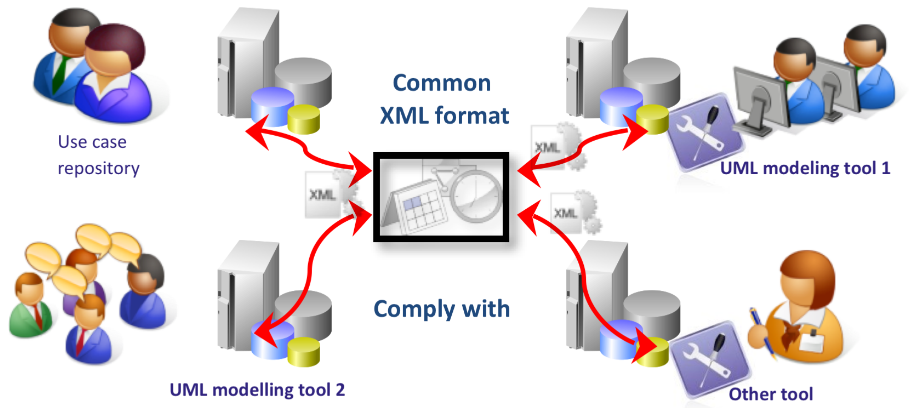
Tools for conceptualization, realization, and assurance of CPS



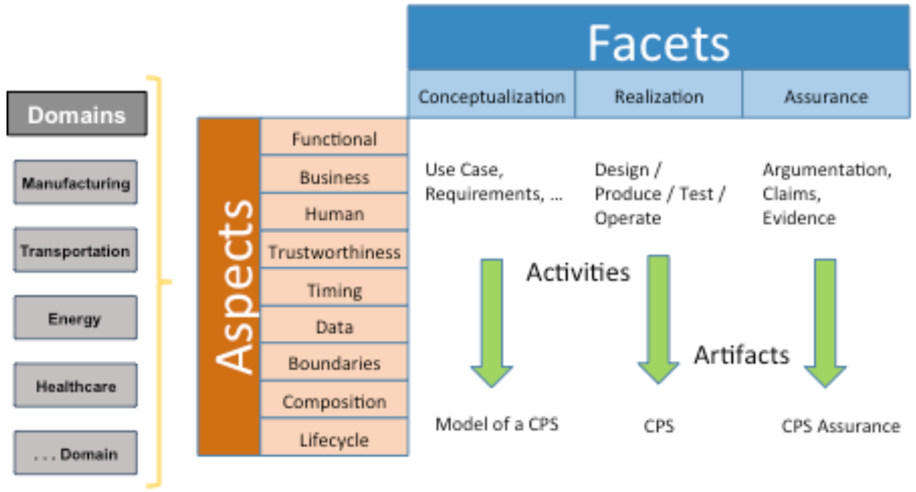
And now the details ….

9.1.4 A Union of Technologies

IEC 62559 Use Case Methodology



NIST CPS Framework Methodology



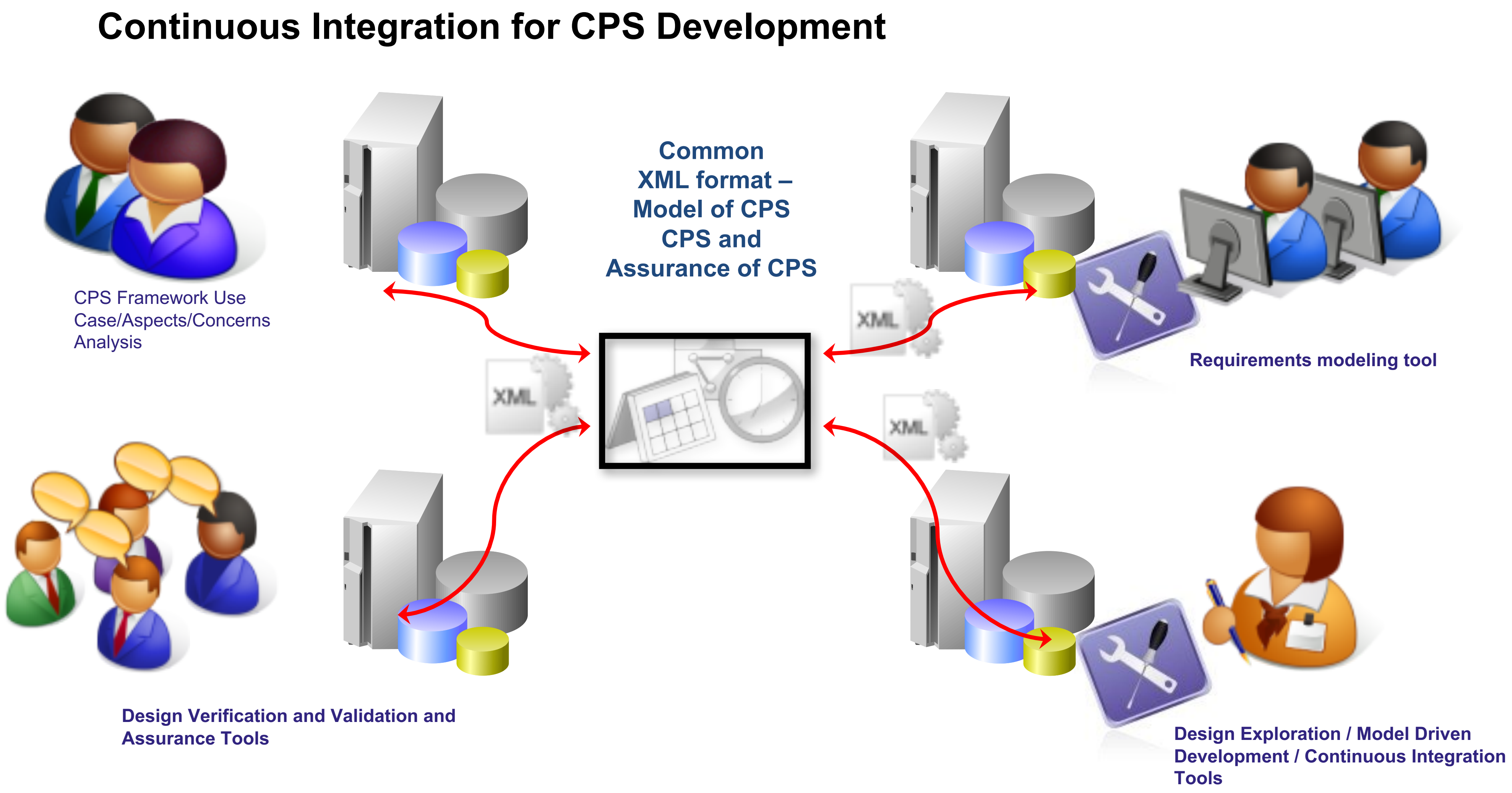
Standardized XML Schema

Conceptualization
- Business Case
- Use Case
- Requirements

Realization
- Design
- Traceability to Requirements

Assurance
- Algorithmically Prove Design Meets Requirements

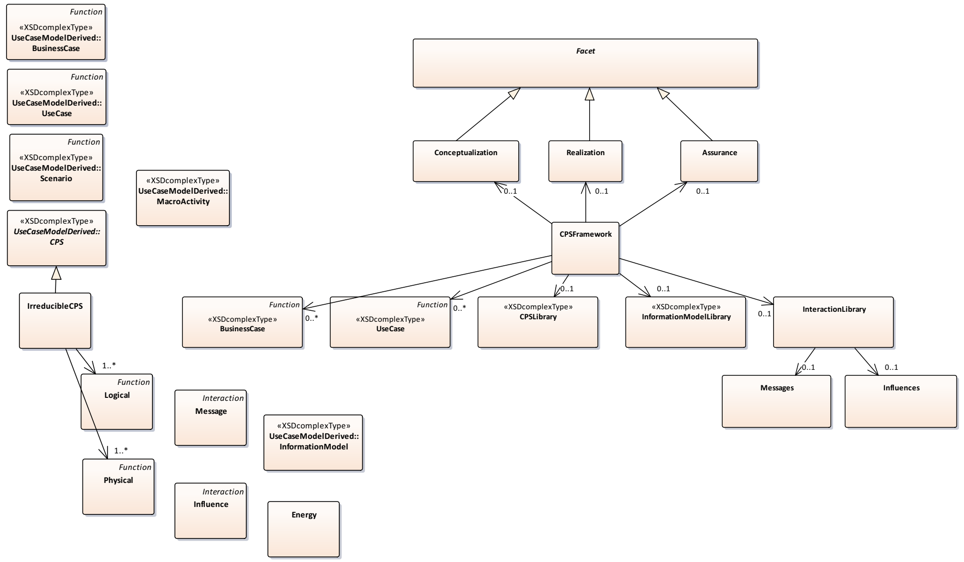
9.1.5 Framework Open Source Project



https://github.com/usnistgov/cpsframework

9.1.6 Methodology

1. Capture the CPS Framework in UML
   - Class hierarchy of facets, aspects, concerns, …
   - Functional decomposition based on an IEC Use Case standard



2. Generate an XMLSchema of the model
   - Which governs an XML instance document of a CPS Framework

```
<xs:element name="CPSFramework" type="CPSFramework"/>
<xs:complexType name="CPSFramework">
    <xs:sequence>
        <xs:element name="BusinessCase" type="BusinessCase" minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="UseCase" type="UseCase" minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="Conceptualization" type="Conceptualization" minOccurs="0" maxOccurs="1"/>
        <xs:element name="CPSLibrary" type="CPSLibrary" minOccurs="0" maxOccurs="1"/>
        <xs:element name="Realization" type="Realization" minOccurs="0" maxOccurs="1"/>
        <xs:element name="Assurance" type="Assurance" minOccurs="0" maxOccurs="1"/>
        <xs:element name="InformationModelLibrary" type="InformationModelLibrary" minOccurs="0" maxOccurs="1"/>
        <xs:element name="InteractionLibrary" type="InteractionLibrary" minOccurs="0" maxOccurs="1"/>
        <xs:element name="Maturity" type="Maturity" minOccurs="0" maxOccurs="1"/>
    </xs:sequence>
</xs:complexType>
```

3. Produce a test example CPS
   - A smart communicating thermostat

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="IntermediateToXHTMLNew.xslt"?>
<n1:CPSFramework xmlns:n1="cpsframework" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="
cpsframework cpsframework.xsd">
    <BusinessCase>
        <name>Design a Communicating Smart Thermostat</name>
        <identifier>222</identifier>
        <technicalId>String</techn
        <description>Build a smart
temperature near a user's set poin
and an HVAC system in a home. The
intrinsically safe, reliable, secu
        <Aspects>
            <functional>
                <Actuation>
                    <Property>
                        <statement
```

1.3 Scope and Objectives of Use Case

Scope and Objectives of Use Case	
Related business case	Design a Communicating Smart Thermostat
Scope	Build a smart thermostat that has heating, cooling and automati user□□□s set point and uses a WiFi local area network (LAN) to i in a home. The thermostat should be able to retail for less or equ protect privacy, easy to use and upgradable.
Objective	

9.2 Use Case Methodology - Song

9.2 IEC 62599 Standard-based Smart Thermostat Use Case

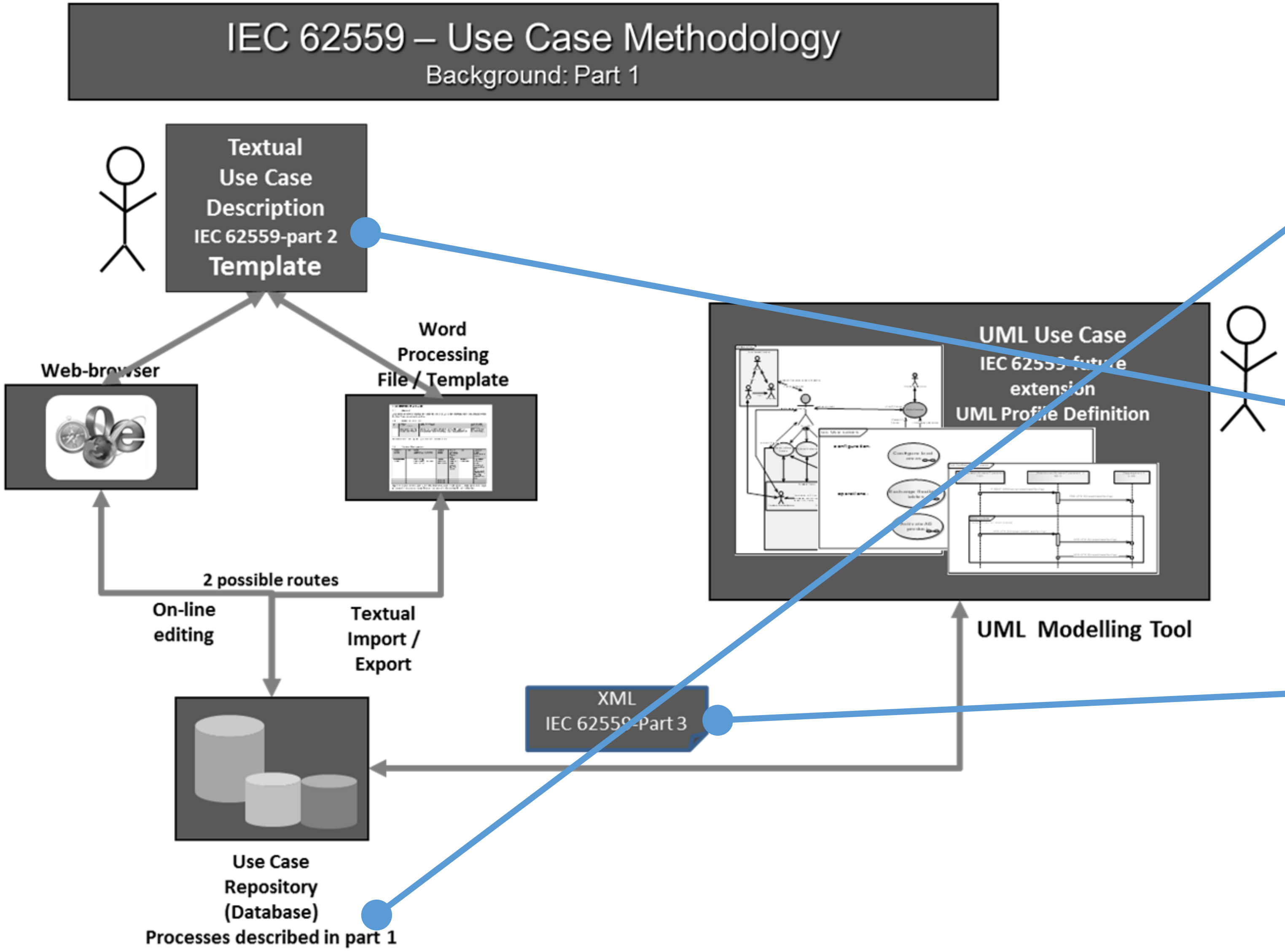
1) What Is A Use Case?
2) IEC 62599 Standard - Use Case Methodology
3) IEC 62599-2 Standard - Template Format for Use Case
4) IEC 62599-2 Standard-based Smart Thermostat Use Case
5) Benefits of Standard-based Use Case

9.2.1 What Is A Use Case?

- A use case is an abstraction of a function of a system.
- A use case is a specification of a set of actions performed by a system. (ISO/IEC 19505-2:2012)
- Use cases are used to capture functional requirements of a system.

For example:
Smart thermostat has heating, cooling and automatic control modes (**three actions**) to control HVAC system to maintain room temperature near a user's set point

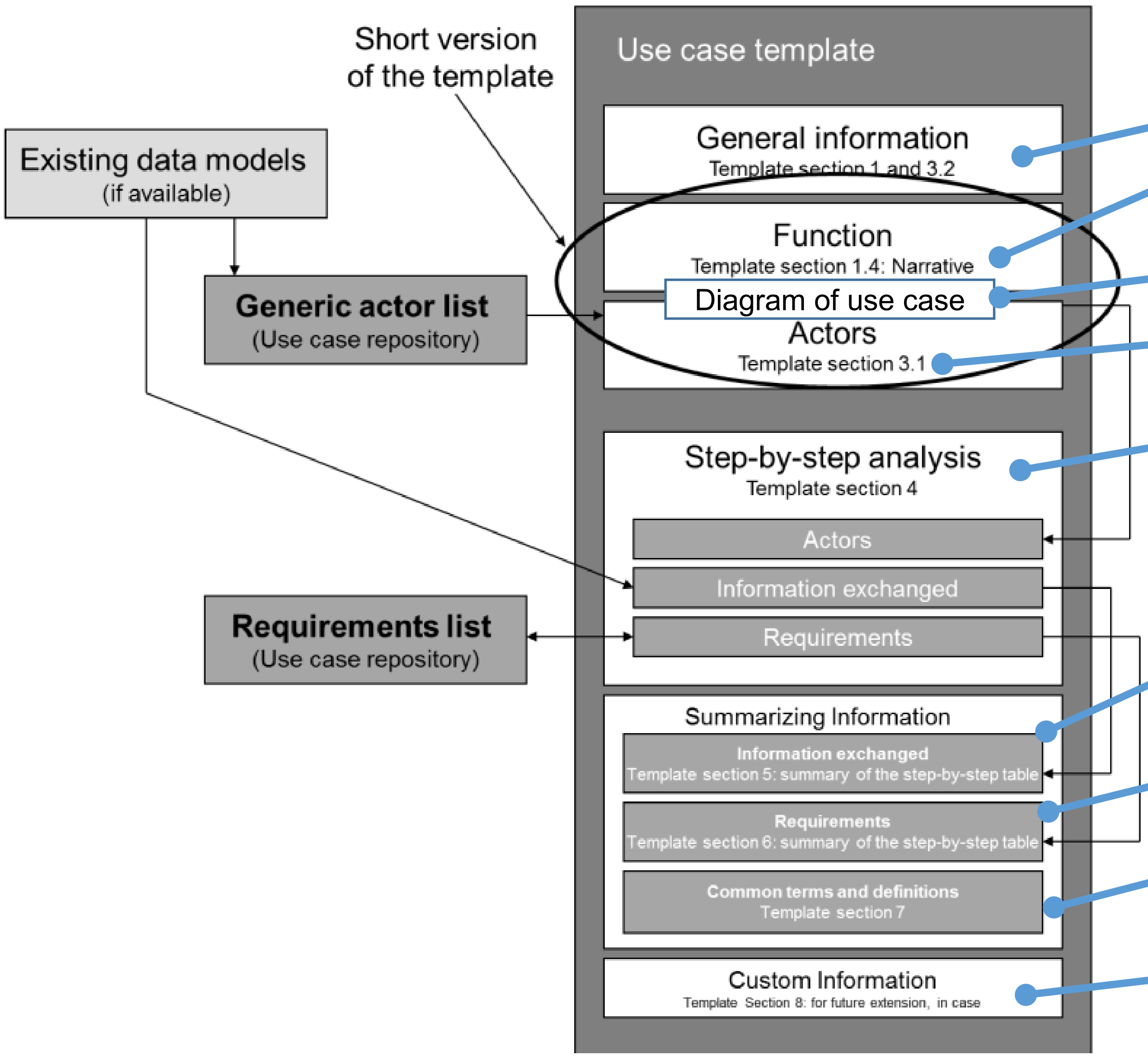
9.2.2 IEC 62559 - Use Case Methodology



IEC 62559 - Use Case Methodology:

- **Part 1** – **Concept and processes** **in standardization**
- **Part 2** – **Definition of a template format** for use cases, actor list and requirements list
- **Part 3** – **UML Model and XML Serialization** of use case template artifacts

9.2.3 IEC 62559-2 - Template Format for Use Case



1. **Description of the use case**
2. **Diagrams of use case**
3. **Technical details**
4. **Step by step analysis of use case**
5. **Information exchanged**
6. Requirements (optional)
7. **Common terms and definitions**
8. Custom information (optional)

9.2.4 IEC 62559-2 Standard-based Smart Thermostat Use Case

A Business Case for Smart Thermostat

- Build a smart thermostat (ST) that has heating, cooling and automatic control modes to maintain room temperature near a user's set point and uses a WiFi local area network (LAN) to interact with a temperature sensor and an HVAC system in a home.

- The thermostat should be able to retail for less or equal to $79. It must be intrinsically safe, reliable, secure, protect privacy, easy to use and upgradable.

9.2.4.1 IEC 62559-2 Standard-based Smart Thermostat Use Case (Cont'd)

1. Description of use case

1.1 Name of Use Case

Use case identification		
ID	Domain(s)	Name of Use Case
1.1.1	User	Maintain room temperature near a user's set point

1.2 Version Management

Version management				
Version No.	Date	Name Author(s)	Changes	Approval Status
0.7	2016-04-06	Eugene/Cuong	Initial	Initial
0.8	2017-08-31	Eugene/Ed	Remove sensor gateway, change control message	

1.3 Scope and Objectives of Use Case

Scope and objectives of use case	
Scope	A smart thermostat to remotely control the HVAC system through a local area network (LAN) in the home
Objective(s)	Provide the functional requirements for a smart thermostat to control the HVAC system based on user inputs or set points.
Related business case(s)	See it before

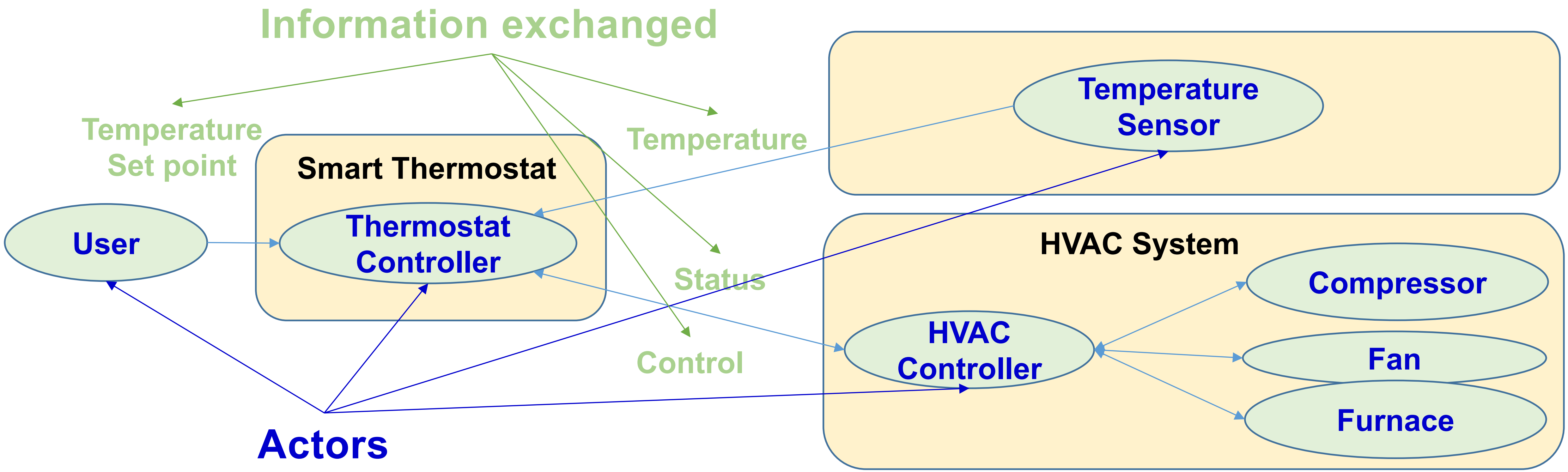
9.2.4.2 IEC 62559-2 Standard-based Smart Thermostat Use Case (Cont'd)

1.4 Narrative of Use Case

Narrative of use case
Short description
This use case **describes the operations of a smart thermostat (ST) to control an HVAC system**. It has three operational modes – **heating, cooling, and automatic control**.
Complete description
This use case describes the operations of a ST to control an HVAC system. It has three operational modes – heating, cooling, and automatic control. **User** can set the temperature set point for ST locally. **Thermostat controller** in ST can pull the room temperature from the **temperature sensor**, compare it to the set point and then remotely control **heating and cooling systems of an HVAC system** via an **HVAC controller** through a WLAN to maintain room temperature near the desired set point. The ST communicates over the network and is globally reachable from the WLAN. This allows remote client applications to read the status of the ST and manipulate its set points.

9.2.4.3 IEC 62559-2 Standard-based Smart Thermostat Use Case (Cont'd)

2. Diagram of Smart Thermostat Use Case



9.2.4.4 IEC 62559 Standard-based Smart Thermostat Use Case (Cont'd)

3.1 Actors: People, Systems, Applications, Databases, the Power System, and Other Stakeholders

Actors

Actors			
Grouping (Community)		Group description	
Home Energy System		The components of a home energy management system	
Actor name	**Actor type**	**Actor description**	**Further information**
Thermostat Controller	**Controller**	**A controller in smart thermostat can send and receive messages, as well as control the HVAC system**	
HVAC Controller	Controller	A controller in the HVAC can send and receive messages from the thermostat, as well as trigger the HVAC operations	
Temperature Sensor	Sensor	Thermostat reads data from temperature sensor	
User	Person	The owner of the thermostat. A User would provide the inputs or set points for the operation of the thermostat	

9.2.4.5 IEC 62559-2 Standard-based Smart Thermostat Use Case (Cont'd)

4 Step by Step Analysis of Use Case

4.1 Overview of scenarios

Scenario Conditions						
No.	**Scenario name**	**Scenario description**	**Primary actor**	**Triggering event**	**Pre-condition**	**Post-condition**
4.1	Heating Mode	This is the heat mode setting on the ST	Thermostat Controller	Temperature difference	Temperature is **lower than or equal** to temperature set point	The HVAC is running until the temperature is **higher than** the set point
4.2	Cooling Mode	This is the cool setting on the ST	Thermostat Controller	Temperature difference	Temperature is **higher than or equal** to temperature set point	The HVAC is running until the temperature is **lower than** the set point
4.3	Automatic Control Mode	This is the automatic mode setting on the ST	Thermostat Controller	Temperature difference	Temperature is **lower than or equal** to temperature set point Temperature is **higher than or equal** to temperature set point	The HVAC is running until the temperature is **higher than or equal** to the set point The HVAC is running until the temperature is **lower than or equal** to the set point

9.2.4.6 IEC 62559-2 Standard-based Smart Thermostat Use Case (Cont'd)

4.2.1 Steps – Scenarios

Scenario								
Scenario Name :	**Heating Mode (The commands and statuses reference to both furnace and fan)**							
Step No.	**Event**	**Name of process/ activity**	**Description of process/ activity**	**Service**	**Information producer (actor)**	**Information receiver (actor)**	**Information exchanged (IDs)**	**Requirements R-ID**
1	Set Temperature Set Point				User	Thermostat Controller	Temperature SetPoint	
2	Temperature Change	Temperature update	Temperature sensor reports the new temperature	**REPORT**	Temperature Sensor	Thermostat Controller	Temperature	
3	HVAC Operation	HVAC switch on	If the temperature **is** **lower than or equal to the set point,** then the thermostat controller sends a command to **turn on the heating system** of HVAC system [0 1 1]	**CHANGE**	Thermostat Controller	HVAC Controller	Control	
4	Status Update	HVAC Status On	The HVAC controller reports that the status of HVAC system	**REPORT**	HVAC Controller	Thermostat Controller	Status	
5	Temperature Change	Temperature update	The HVAC controller reports the new temperature	**REPORT**	Temperature Sensor	Thermostat Controller	Temperature	
6	HVAC Operation	HVAC switch Off	If the temperature is **higher than the set point,** then the thermostat controller sends a command to **turn off the heating system** of HVAC system [0 0 0]	**CHANGE**	Thermostat Controller	HVAC Controller	Control	
7	Status Update	HVAC Status Off	The HVAC controller reports that the HVAC system is on	**REPORT**	HVAC Controller	Thermostat Controller	Status	

9.2.4.7 IEC 62559-2 Standard-based Smart Thermostat Use Case (Cont'd)

5 Information Exchanged

Information exchanged ID	Name of information	Description of information exchanged	Requirements IDs
Temperature	Temperature	Float temperature value	
TemperatureSetPoint	Temperature	Float temperature value	
Control	**Control**	**Control:** **1 = On, 0 = Off** **Example:** Cool: 0, Fun: 0, Heat: 0	
Status	Status of HVAC	Contains the current status of the HVAC: 0 = Off, 1 = On Example: Cool: 1, Fun: 1, Heat: 0	

9.2.4.8 IEC 62559-2 Standard-based Smart Thermostat Use Case (Cont’d)

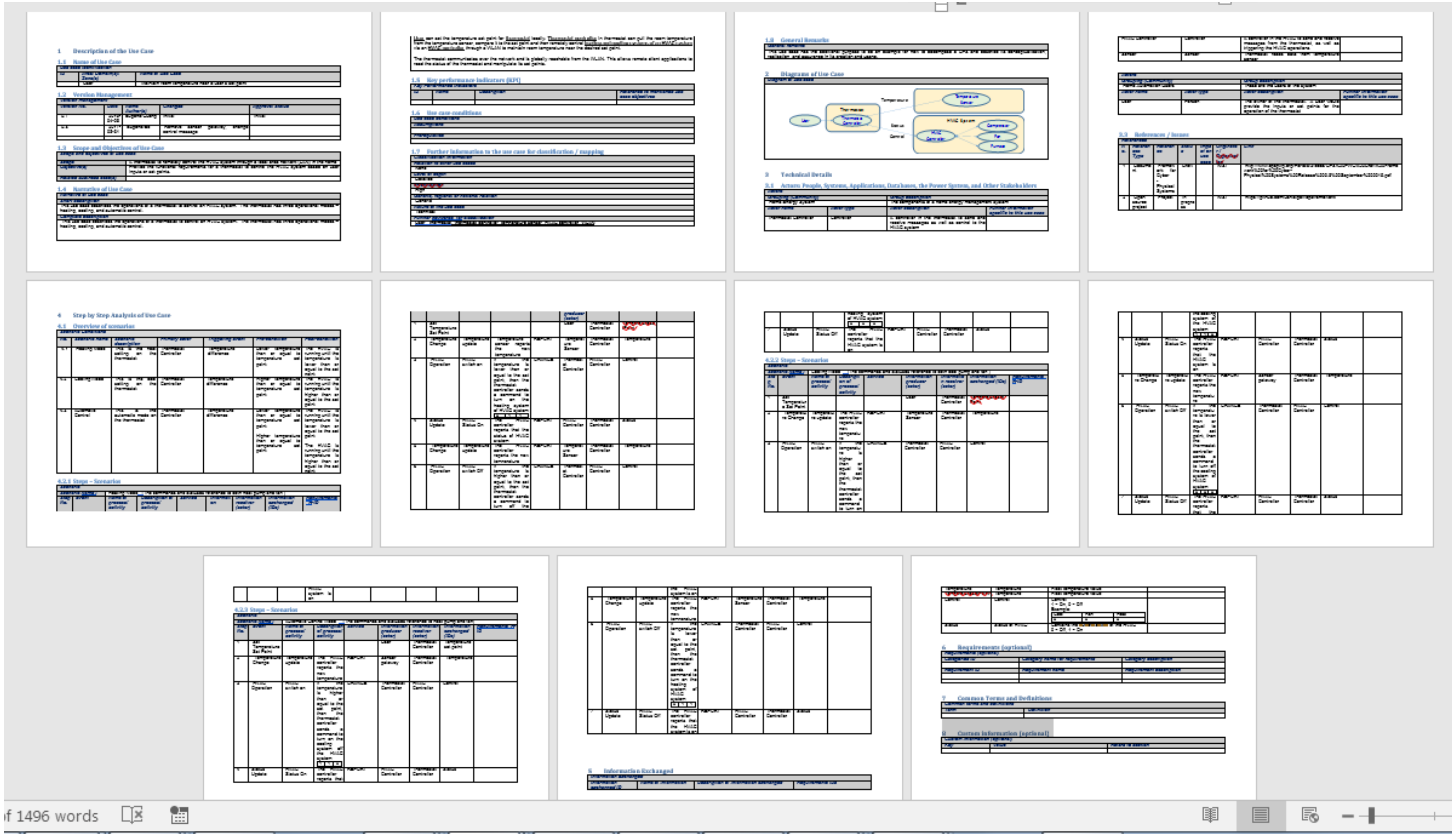
Smart Thermostat Use Case (IEC 62599-2) (Microsoft Word file)

↓

Software Tool (Conversion)

↓

Smart Thermostat Use Case (IEC 62599-3) (XML Data file)

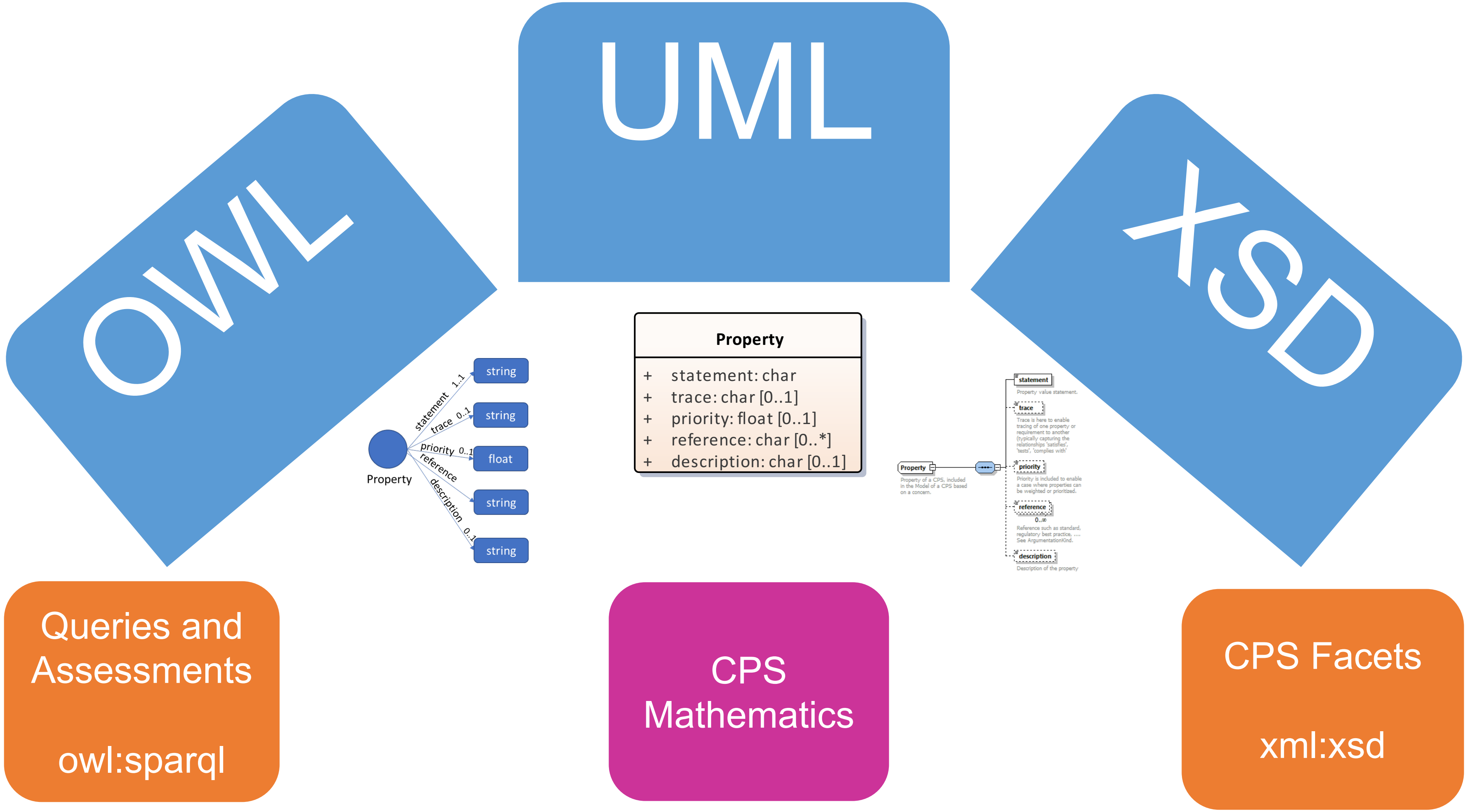


9.2.5 Benefits of a Standard-based Use Case Methodology

- provide a standardized format and common understanding of use cases (including functionalities, actors and interactions) of CPS systems
- help to easily understand functions and requirements of CPS systems.
- help to easily exchange or share of use cases among CPS system development processes

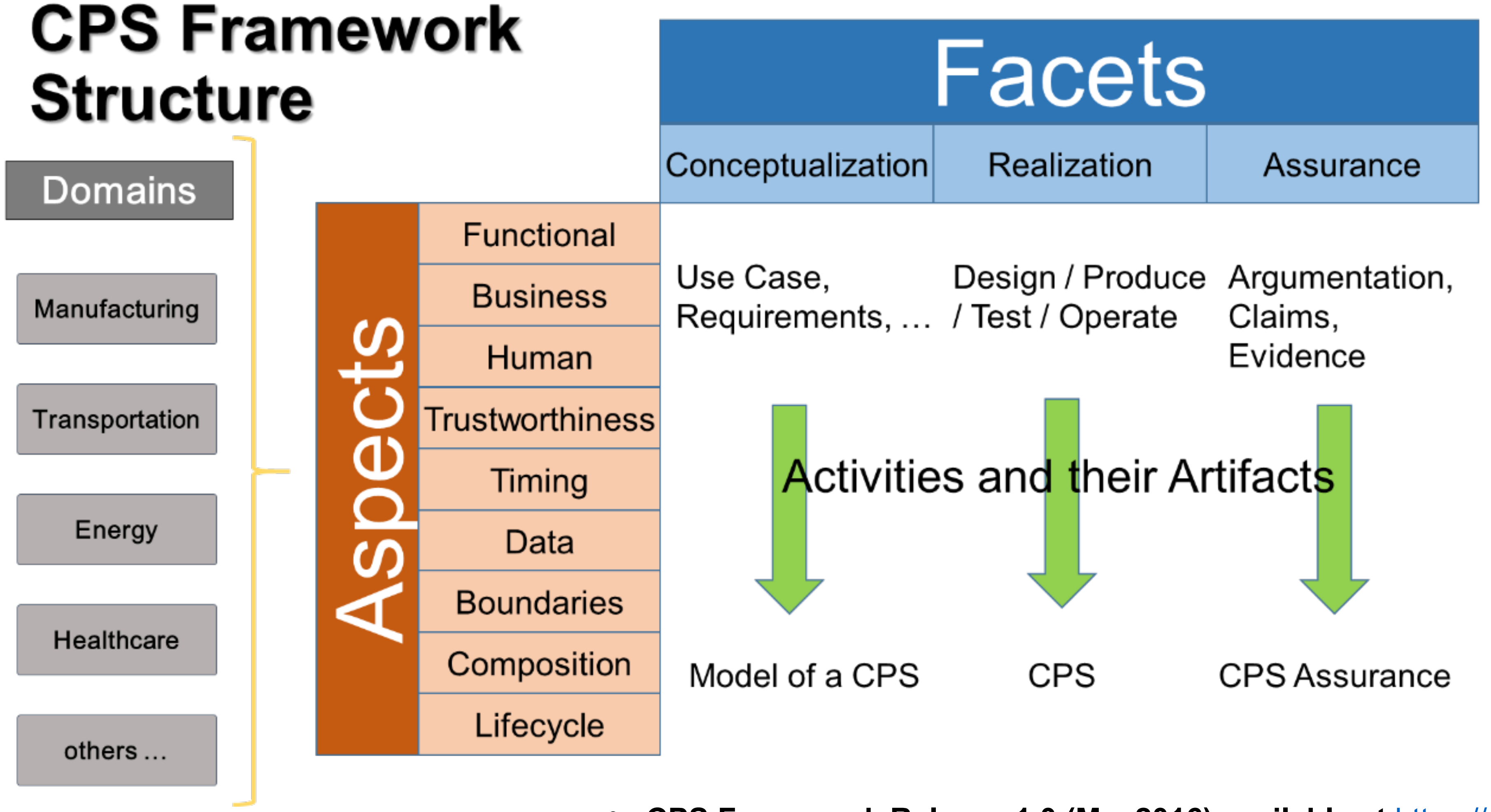
9.3 Model Realization - Burns

9.3.1 CPS Framework Modeling Tools



9.3.2 NIST CPS Framework

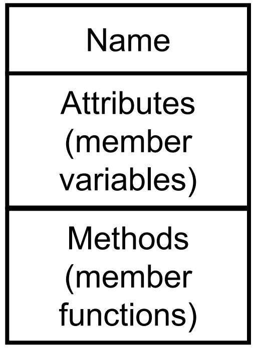
‘Concern-driven’: holistic, integrated approach to CPS/IoT concerns.



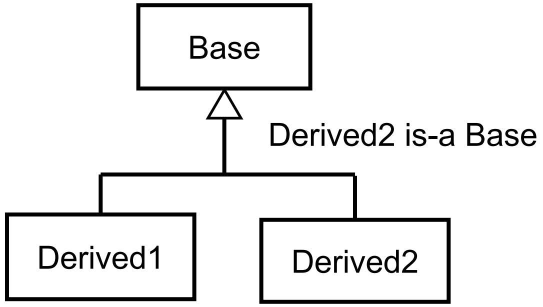
- **CPS Framework Release 1.0 (May2016) available at https://pages.nist.gov/cpspwg/**

9.3.3 Crash course in UML

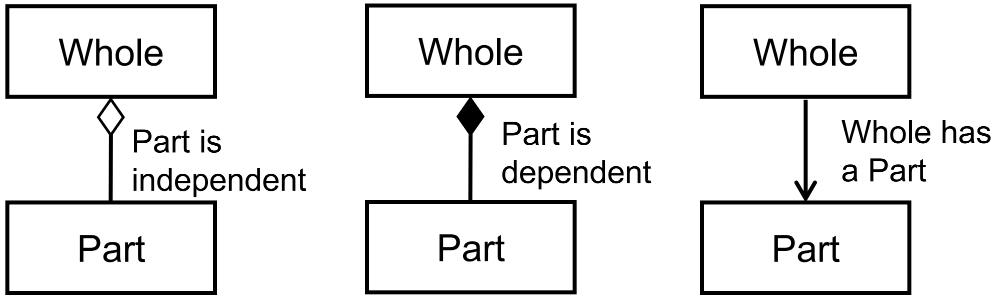
Class



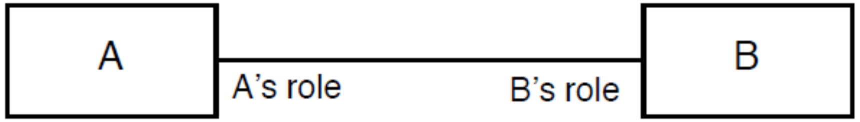
Inheritance (is-a) relationship



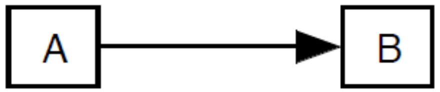
Aggregation and Composition (has-a) relationship

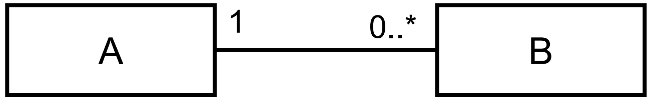


Association (uses, interacts-with) relationship



Navigability - can reach B starting from A





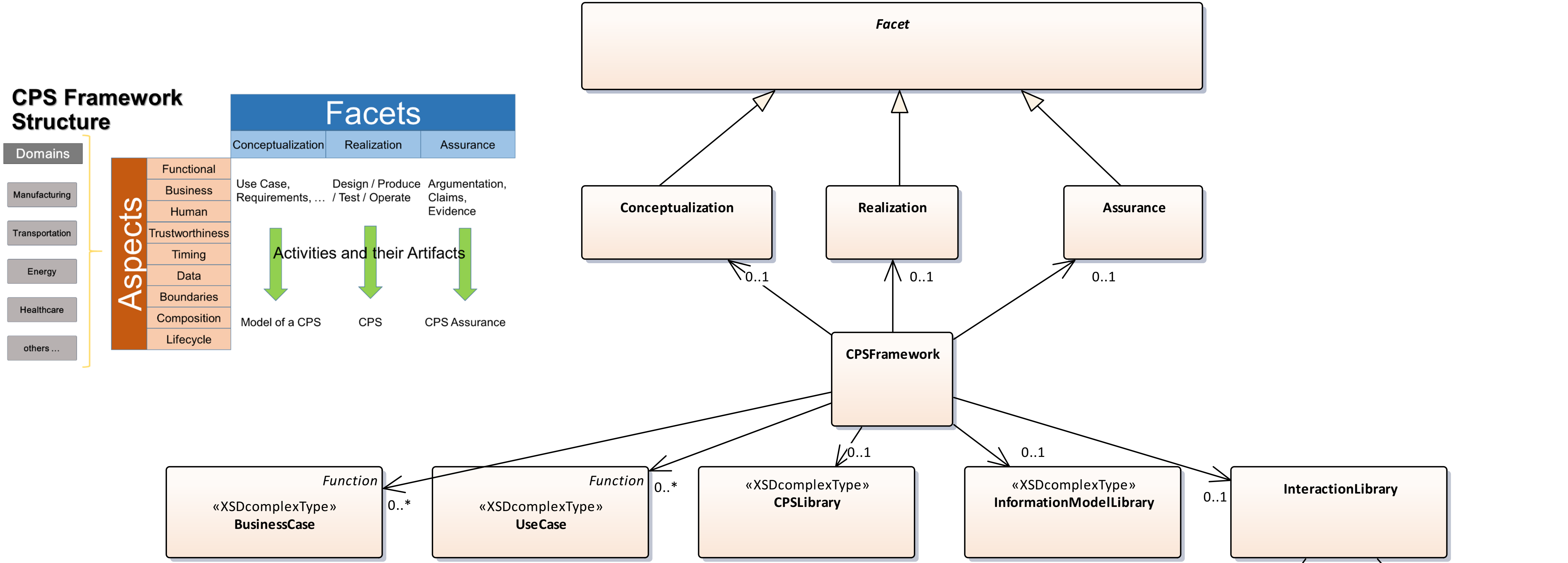
B is associated with one A
A is associated with 0 or more B

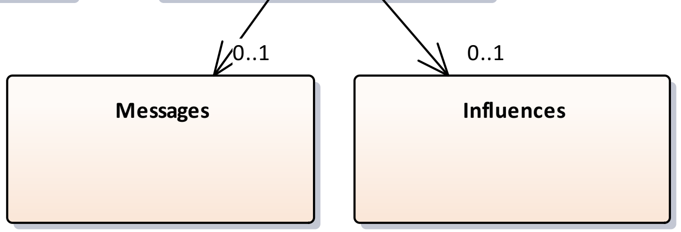
Multiplicity in Aggregation, Composition, or Association

* - any number 0..1 - zero or one
1 - exactly 1
1..* - 1 or more
n - exactly *n*
n .. *m* - *n* through *m*

9.4 Modeling the CPS Framework and Use Case

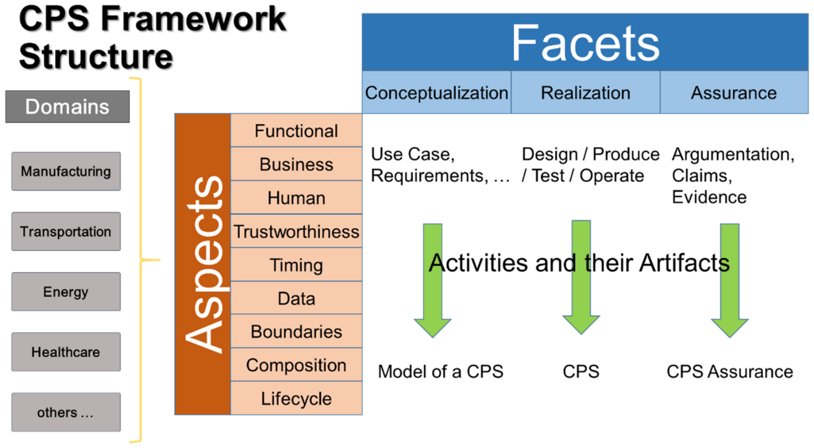
9.4.1 CPS Framework Object Model in UML



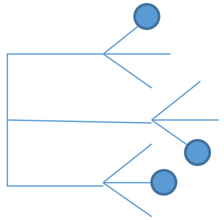


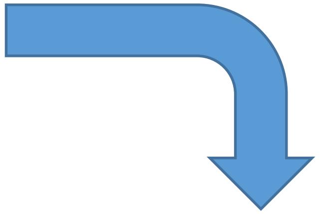
See Aspects on subsequent slide

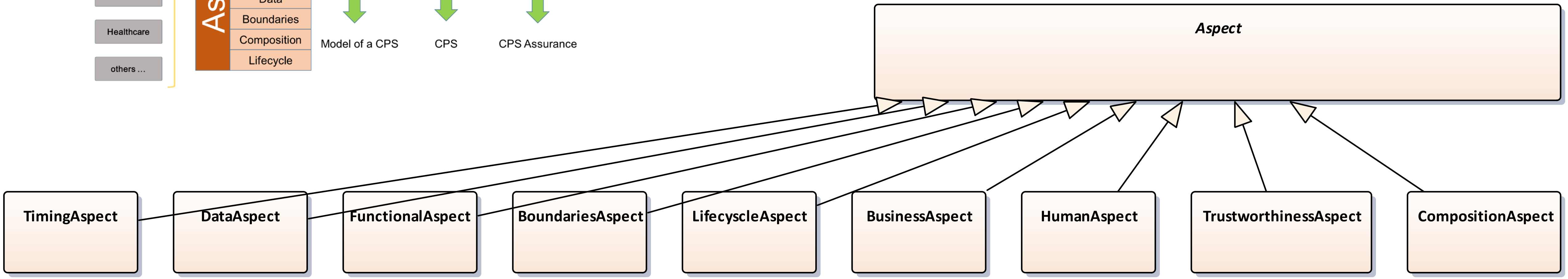
9.4.2 CPS Framework Aspects



From functional decomposition

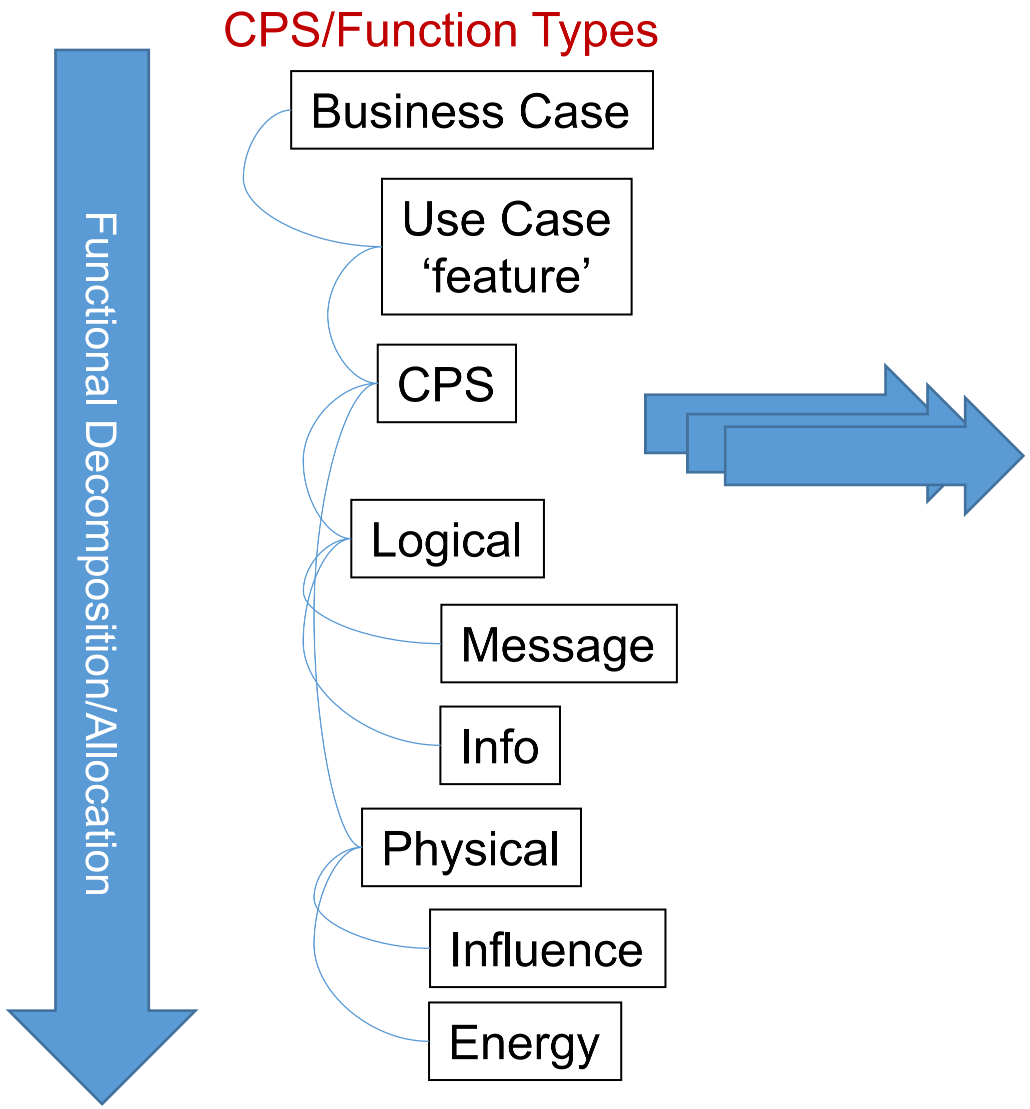


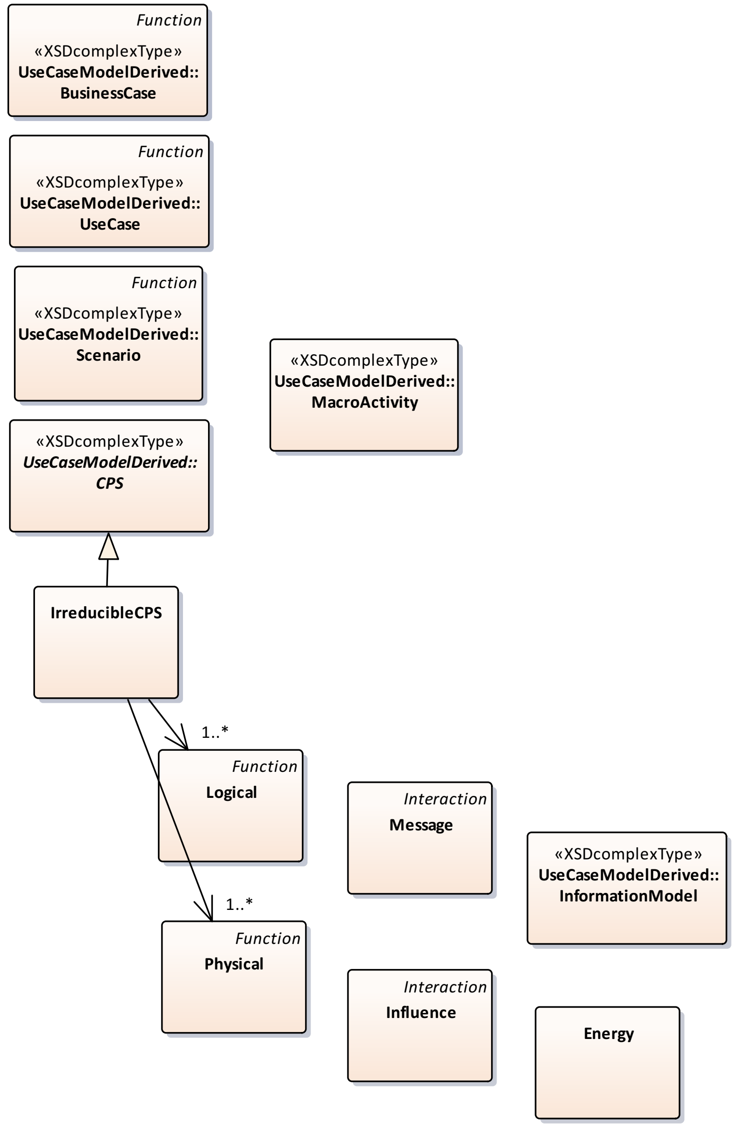




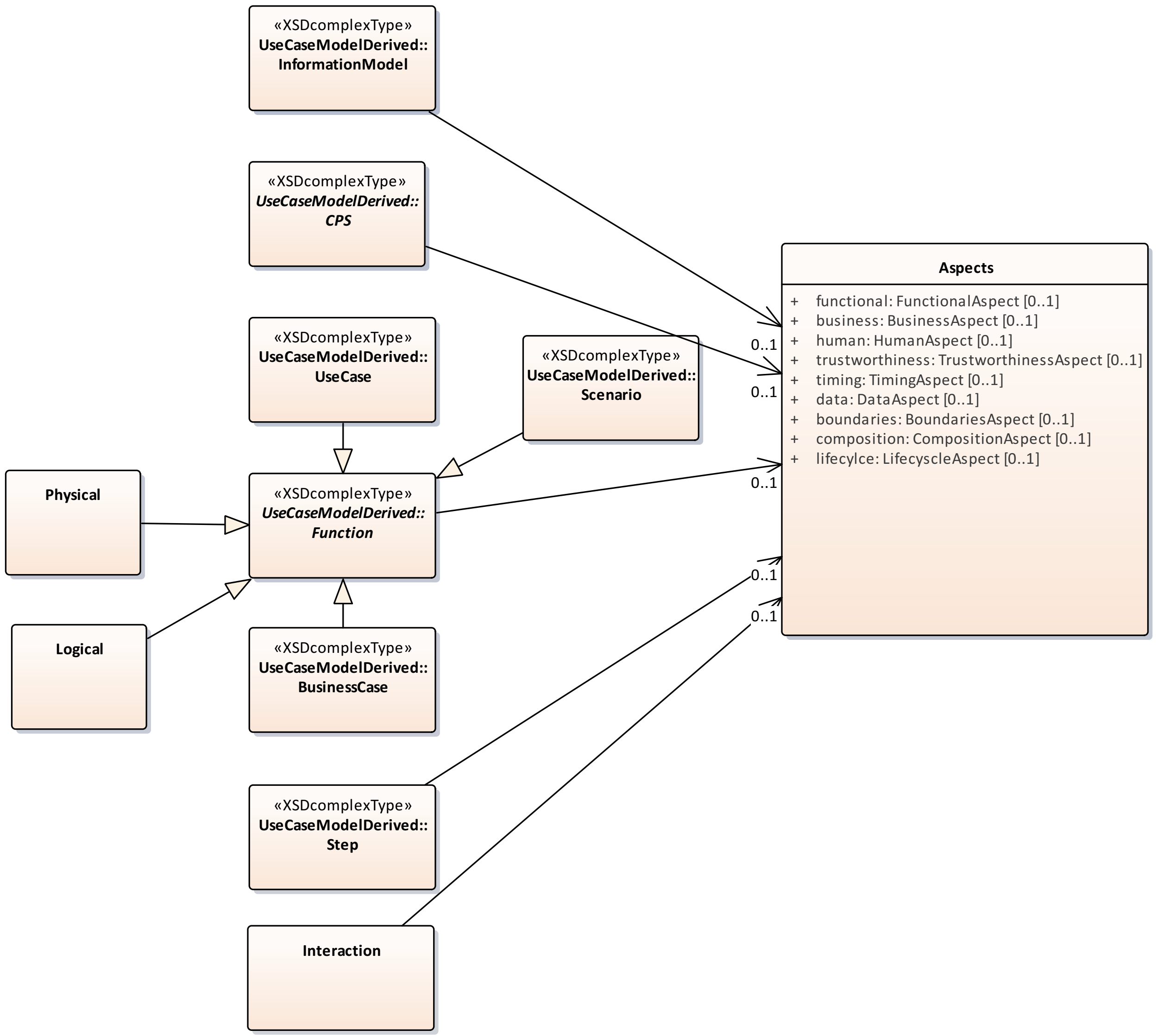
**Each Aspect has a hierarchically arranged set of concerns

9.4.3 Functional Decomposition



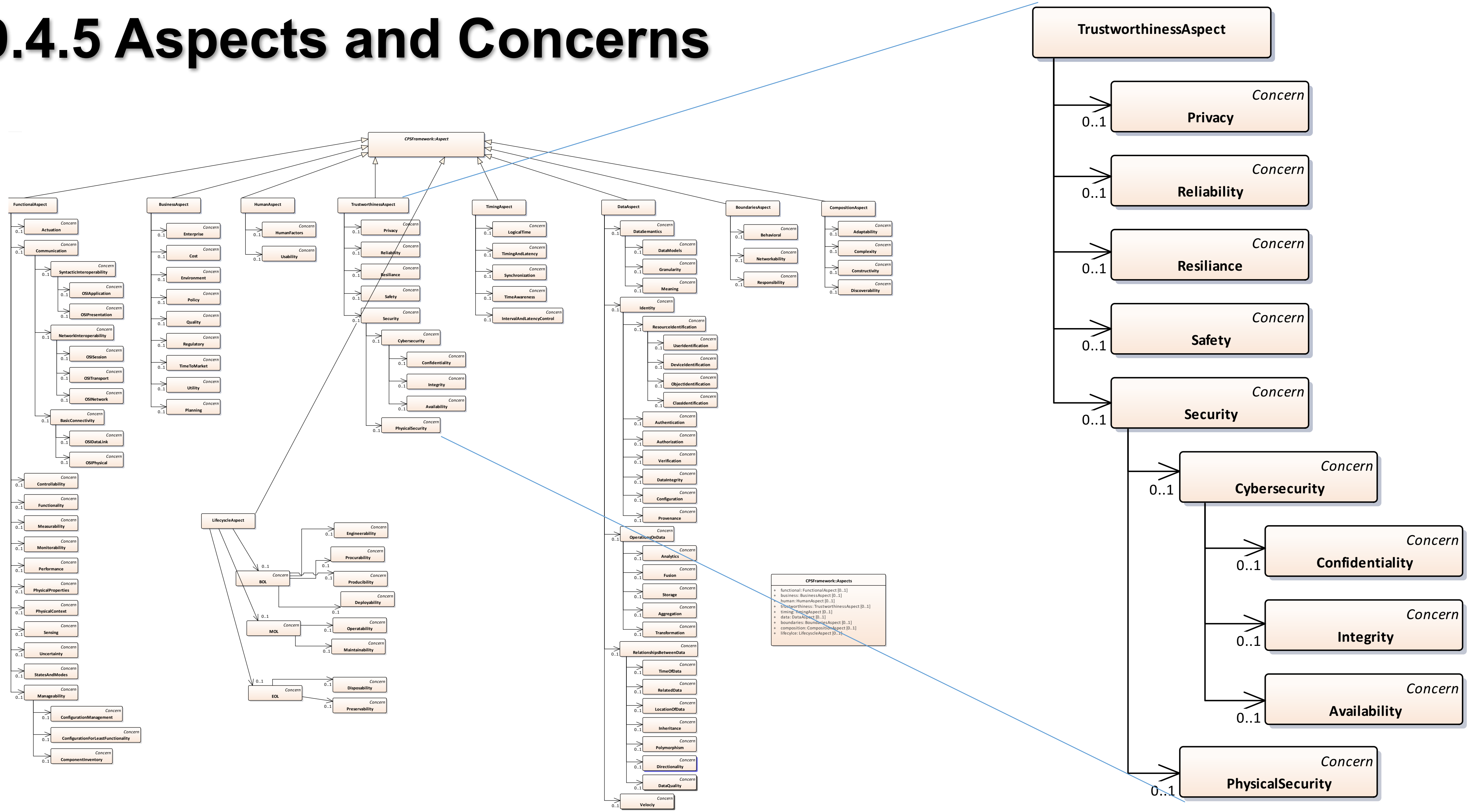


9.4.4 Allocation of Aspects to Model Elements



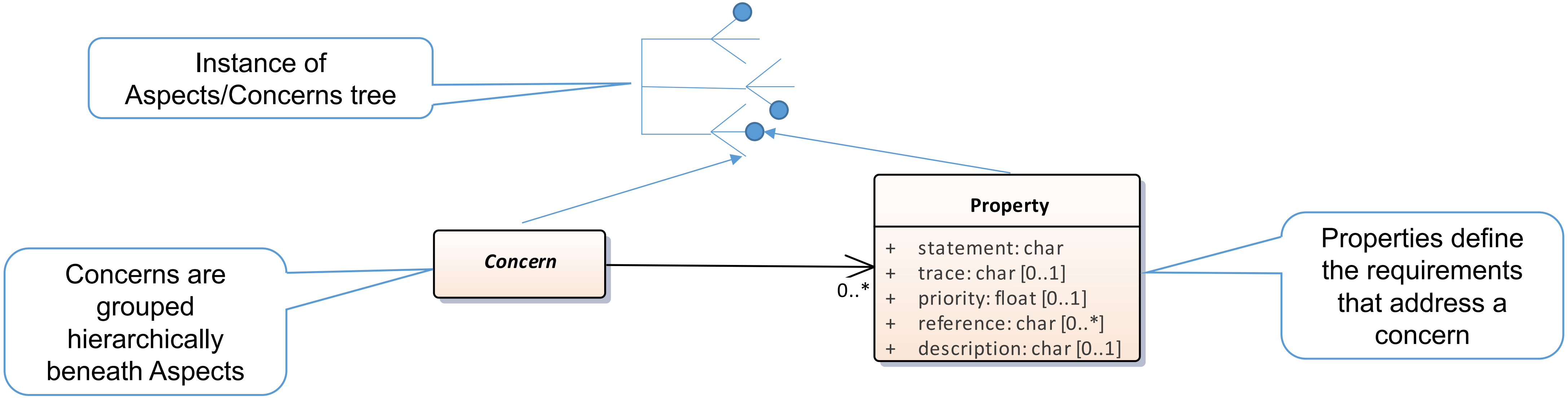
Note how each major component of functional decomposition can have apportionment of Aspects and Concerns

9.4.5 Aspects and Concerns



9.4.6 Concerns and Properties

Properties, like requirements, are assertions intended to address a concern and evaluate to true or false to facilitate testing and verification

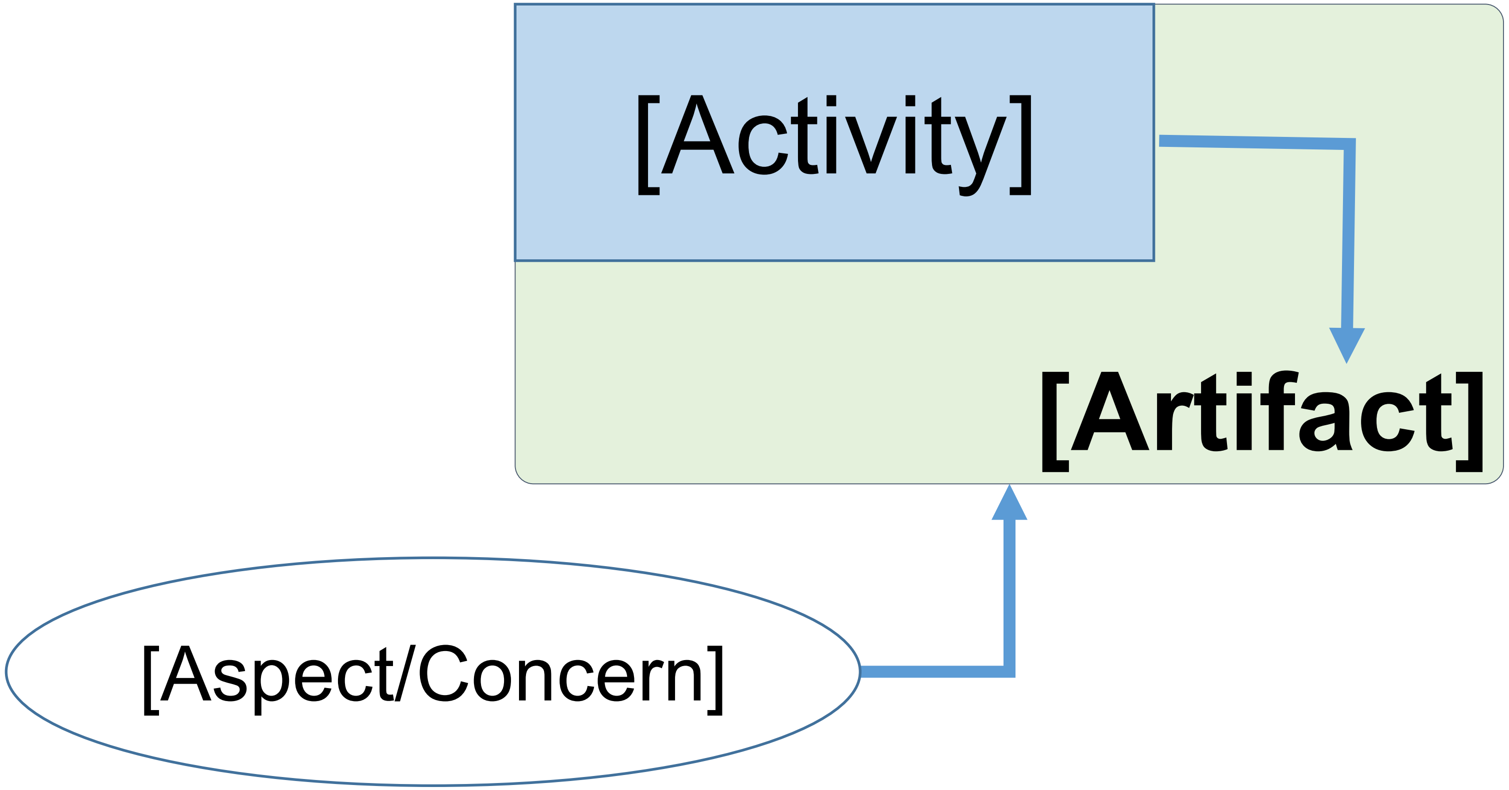


Property is defined as containing:

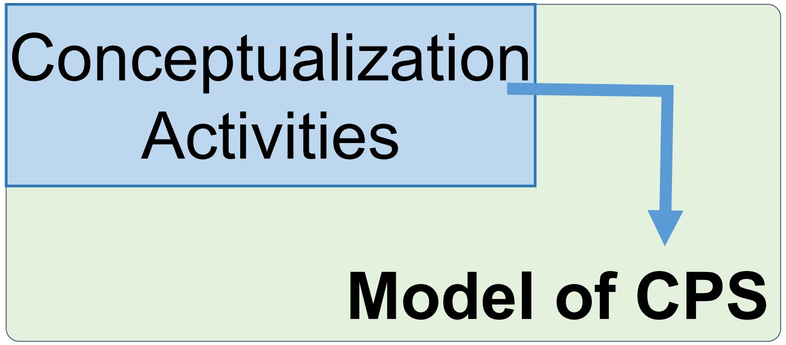
- statement: a requirements-like assertion that is either true or false
- trace: a reference to another Property elsewhere in the graph
- priority: a priority to be used to referee competing properties
- reference: a reference such as a standard, regulatory or best practice
- description: a more elaborate description of the statement

9.4.7 Model of a Facet: a collection of process activities

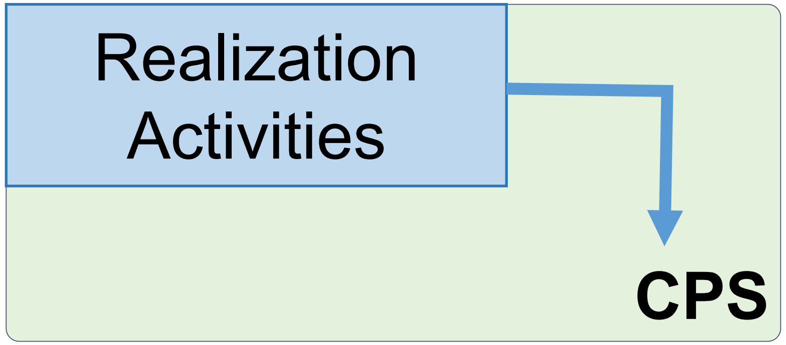
CPS are conceived and build in order to address certain needs while addressing any concerns the stakeholders may have. There will be activities, or sets of activities, with well-defined outcomes or deliverables that are designed to fulfill those needs and, at the same time, address stakeholder concerns.



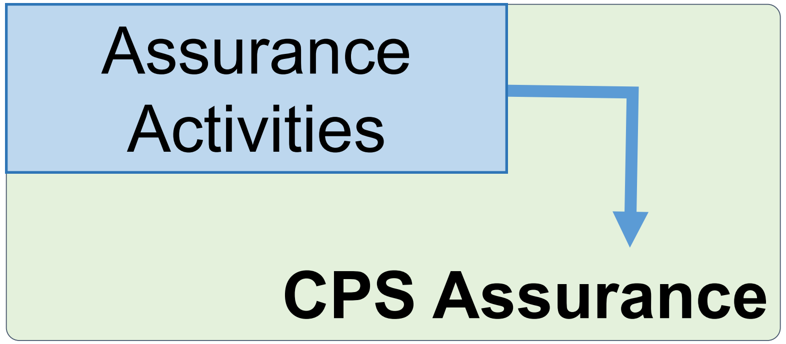
9.4.8 Process Element Depiction of CPS Framework Facets



Conceptualization Facet

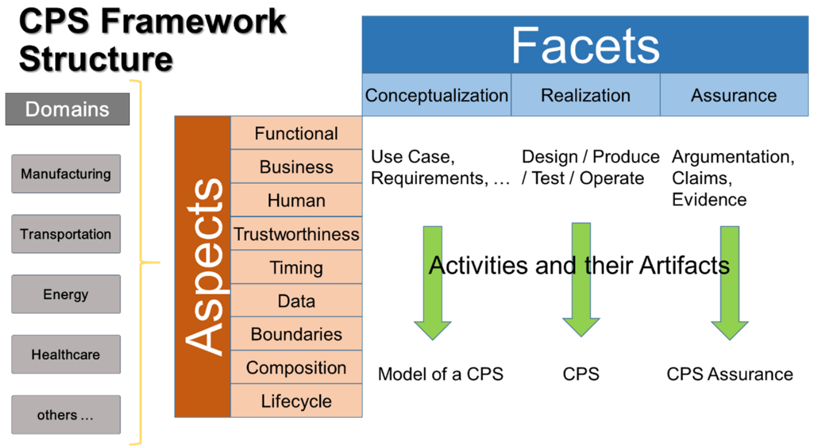


Realization Facet

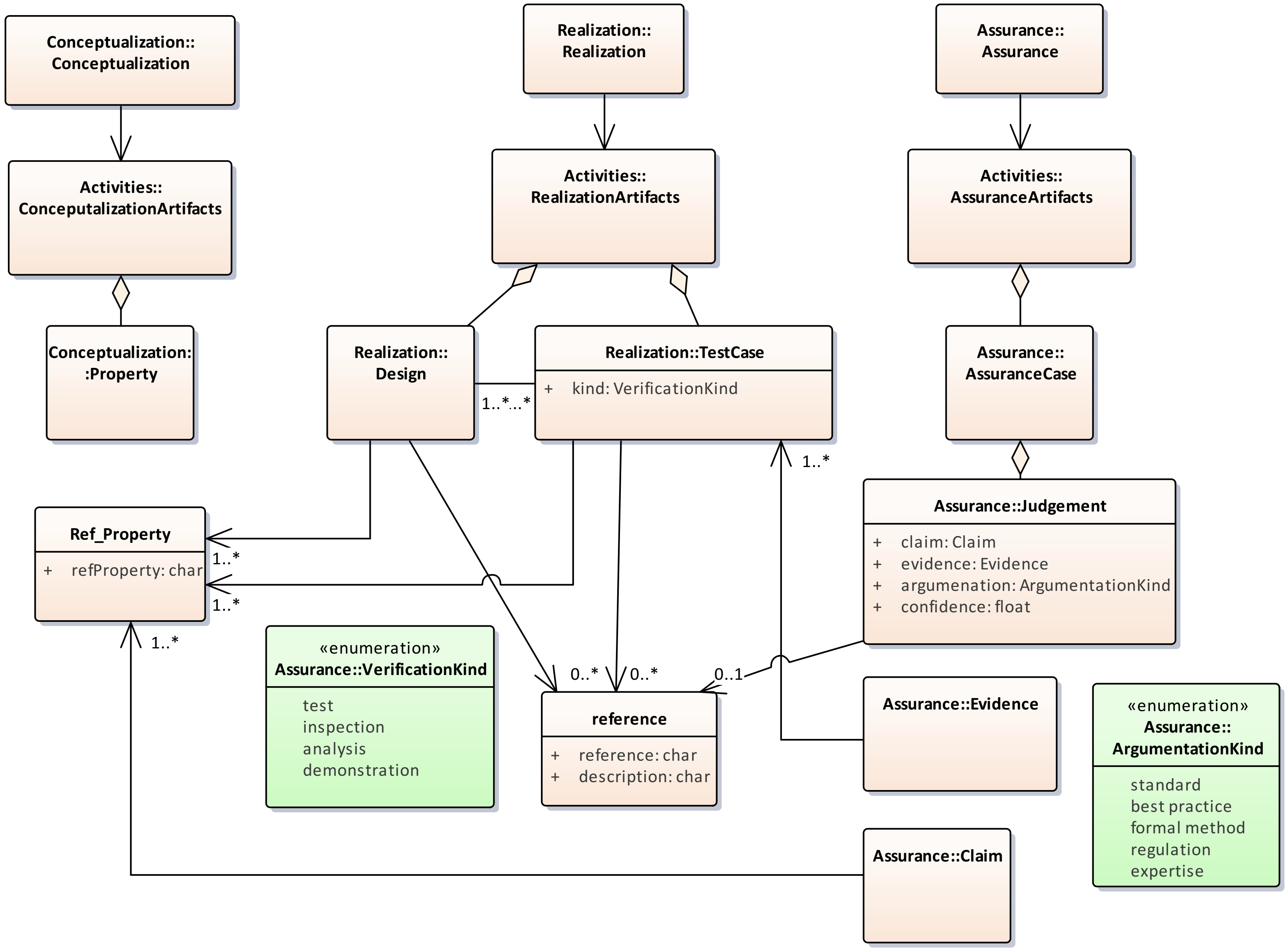


Assurance Facet

9.4.9 Facets

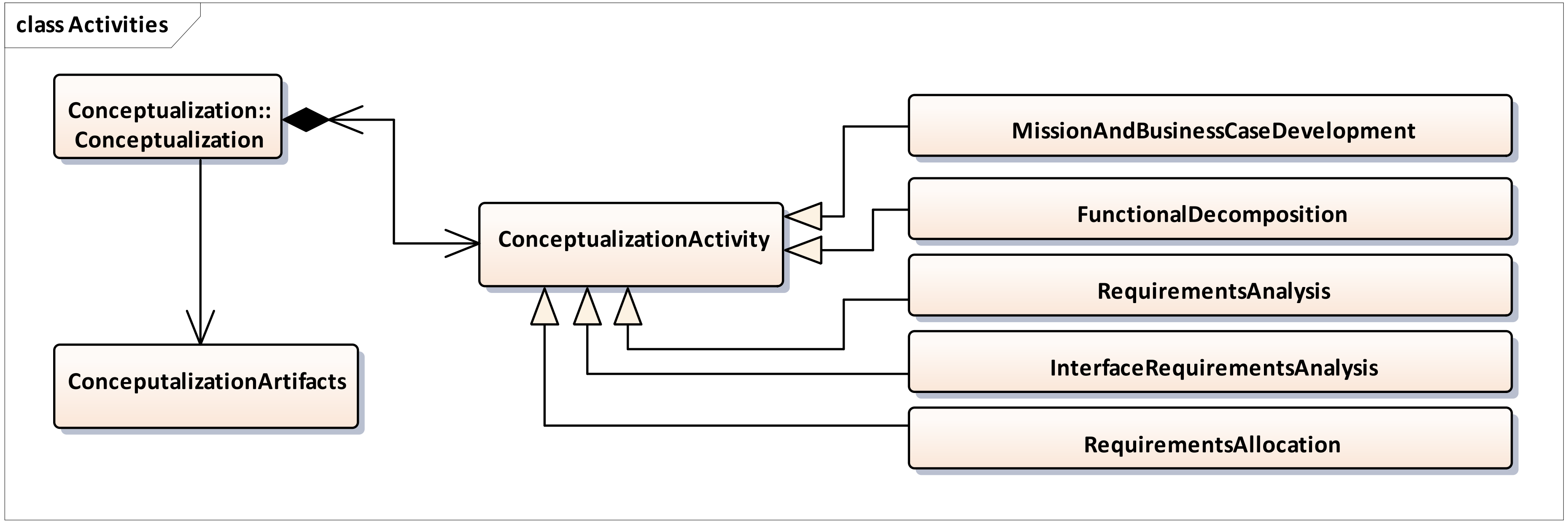


CPS Framework Structure
Facets
Conceptualization
Realization
Assurance
Domains
Manufacturing
Transportation
Energy
Healthcare
others ...
Aspects
Functional
Business
Human
Trustworthiness
Timing
Data
Boundaries
Composition
Lifecycle
Use Case, Requirements, …
Design / Produce / Test / Operate
Argumentation, Claims, Evidence
Activities and their Artifacts
Model of a CPS
CPS
CPS Assurance

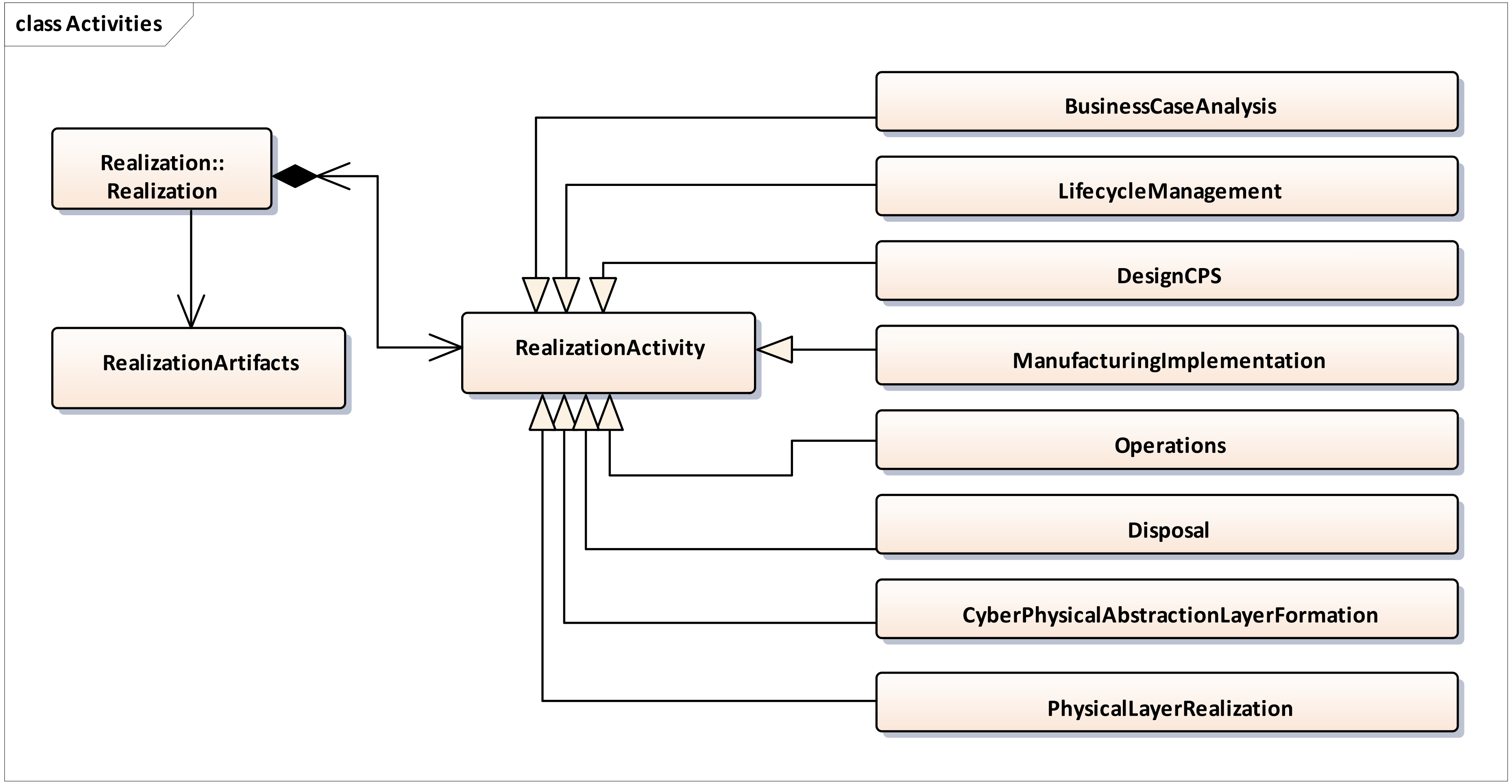


Conceptualization:: Conceptualization
Activities:: ConceptualizationArtifacts
Conceptualization: :Property
Realization:: Realization
Activities:: RealizationArtifacts
Realization:: Design
Realization::TestCase
+ kind: VerificationKind
1..*...*
Assurance:: Assurance
Activities:: AssuranceArtifacts
Assurance:: AssuranceCase
Assurance::Judgement
+ claim: Claim
+ evidence: Evidence
+ argumenation: ArgumentationKind
+ confidence: float
1..*
Ref_Property
+ refProperty: char
1..*
1..*
1..*
«enumeration» Assurance::VerificationKind
test
inspection
analysis
demonstration
0..*
0..*
0..1
reference
+ reference: char
+ description: char
Assurance::Evidence
«enumeration» Assurance:: ArgumentationKind
standard
best practice
formal method
regulation
expertise
Assurance::Claim

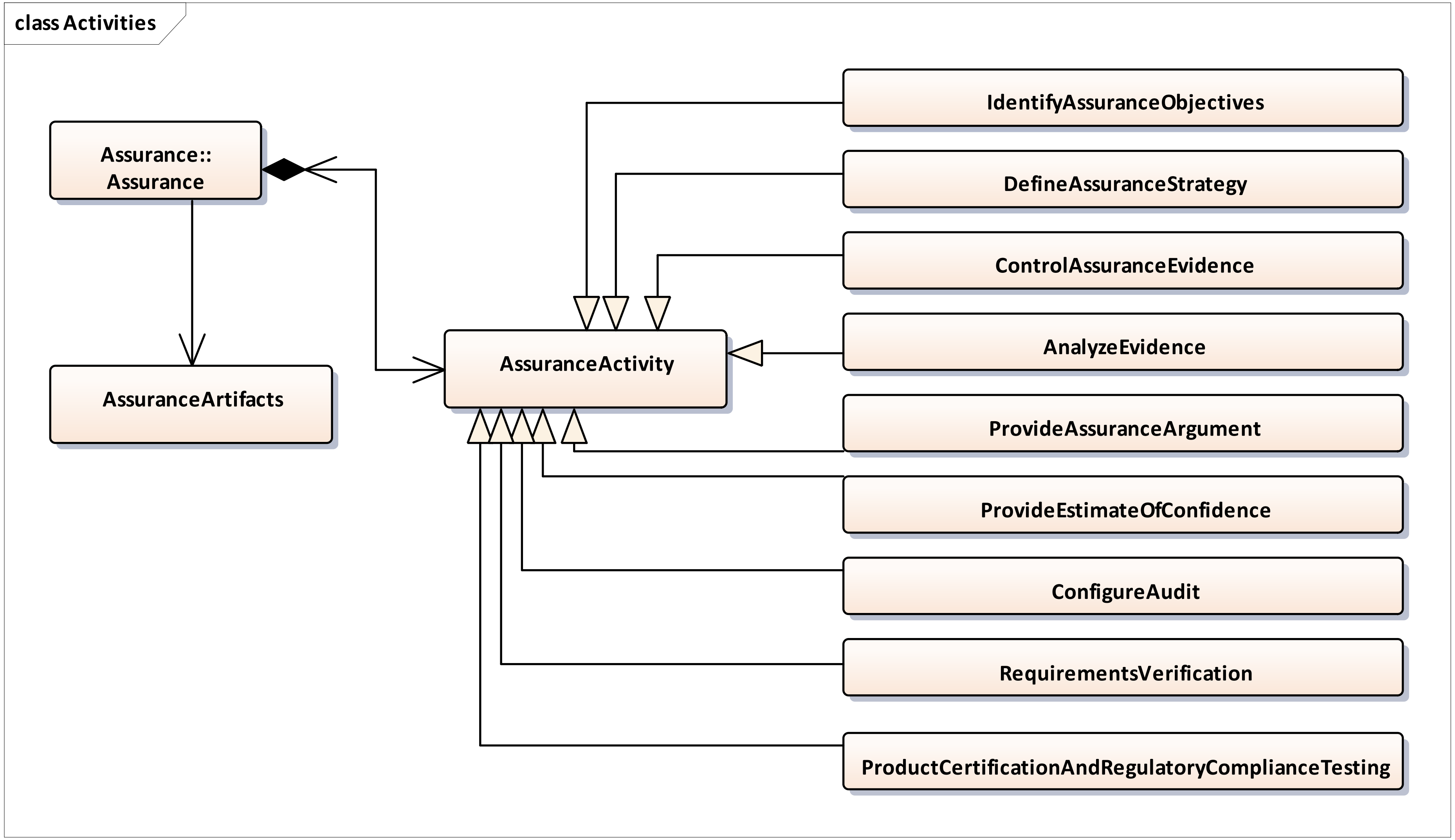
9.4.10 Activities: Conceptualization Facet



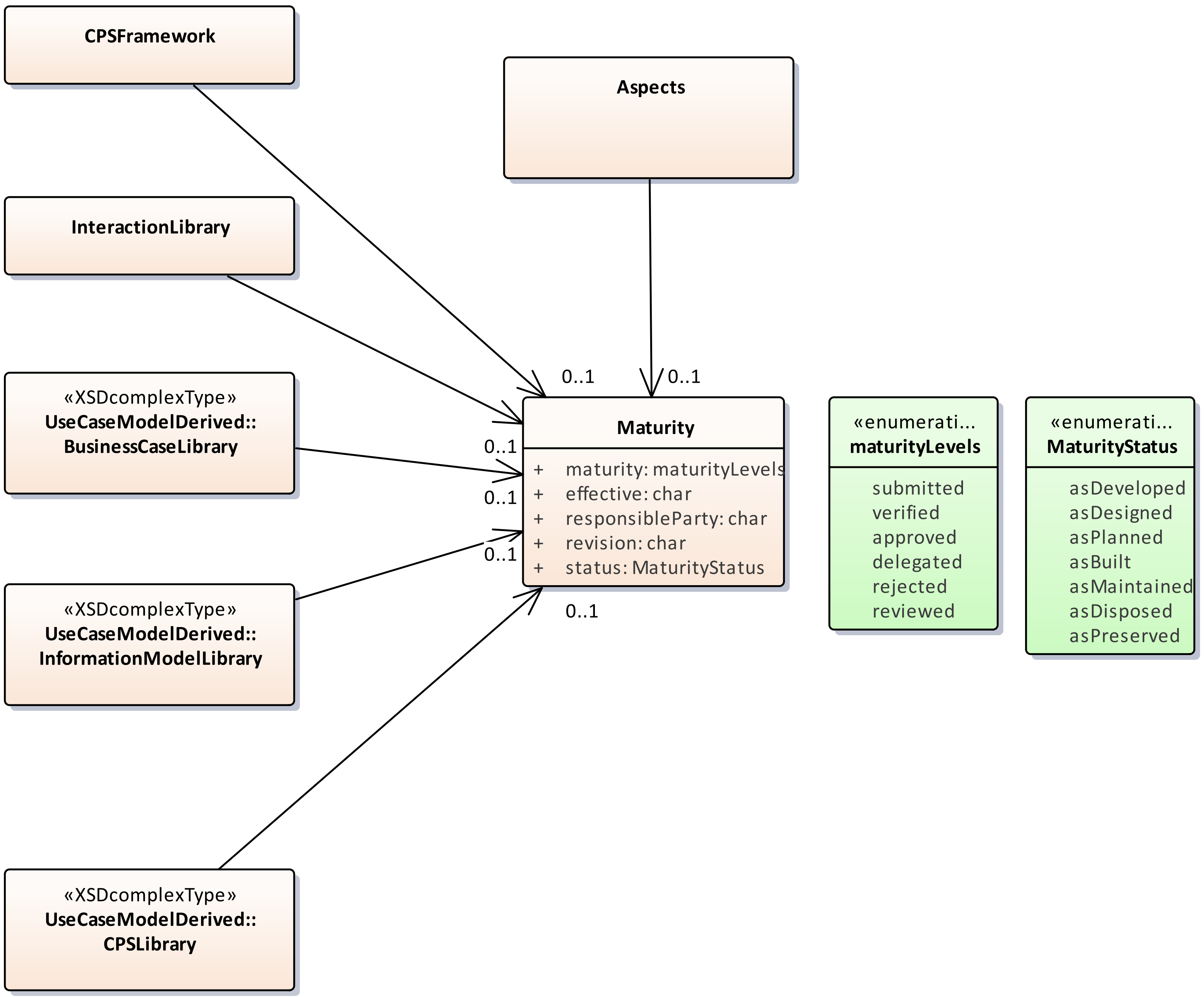
9.4.11 Activities: Realization Facet



9.4.12 Activities: Assurance Facet

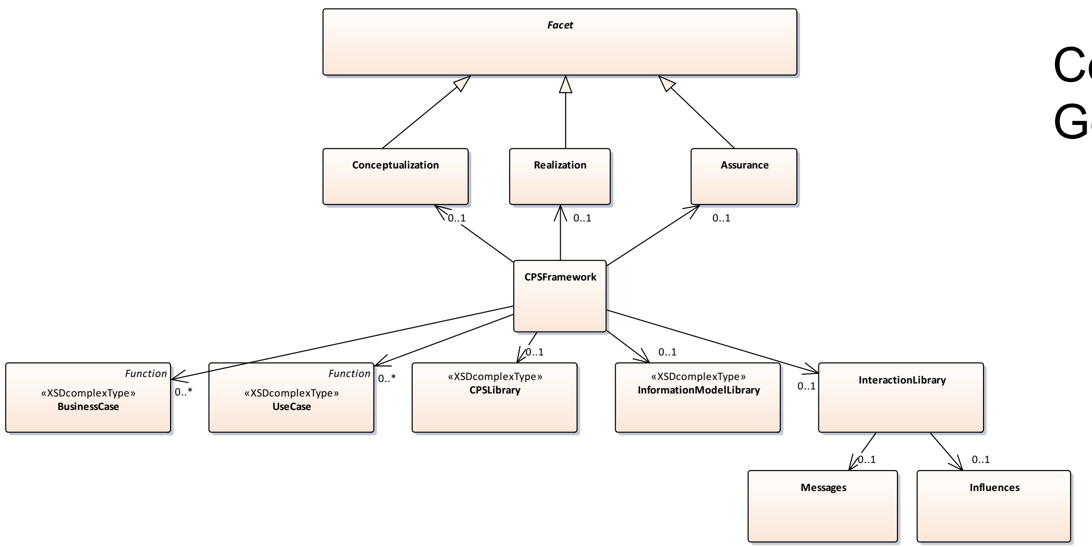


9.4.13 Maturity and Versioning



9.4.14 Turn the crank to generate the schema

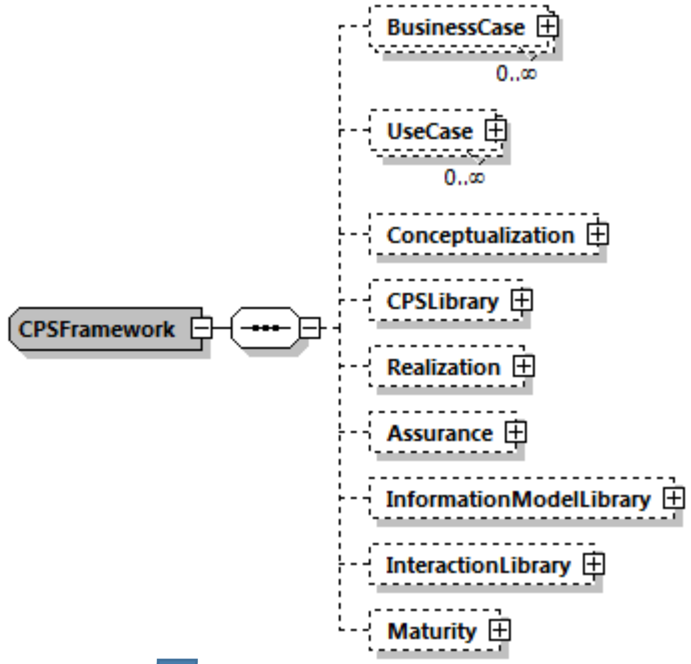
Model in UML



Sparx Systems Enterprise Architect V13.5

Code Engineering /
Generate XML Schema

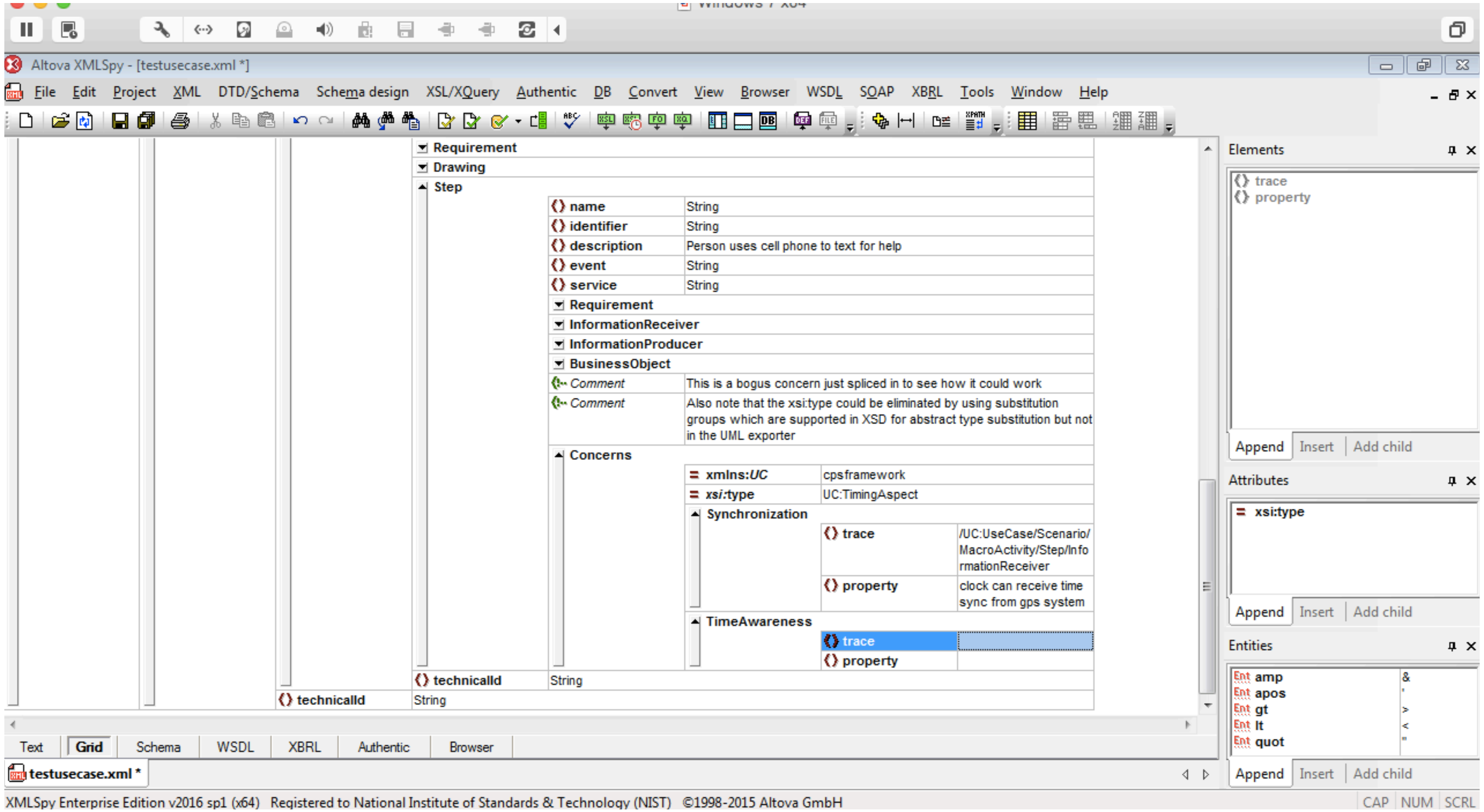
Model in XMLSchema



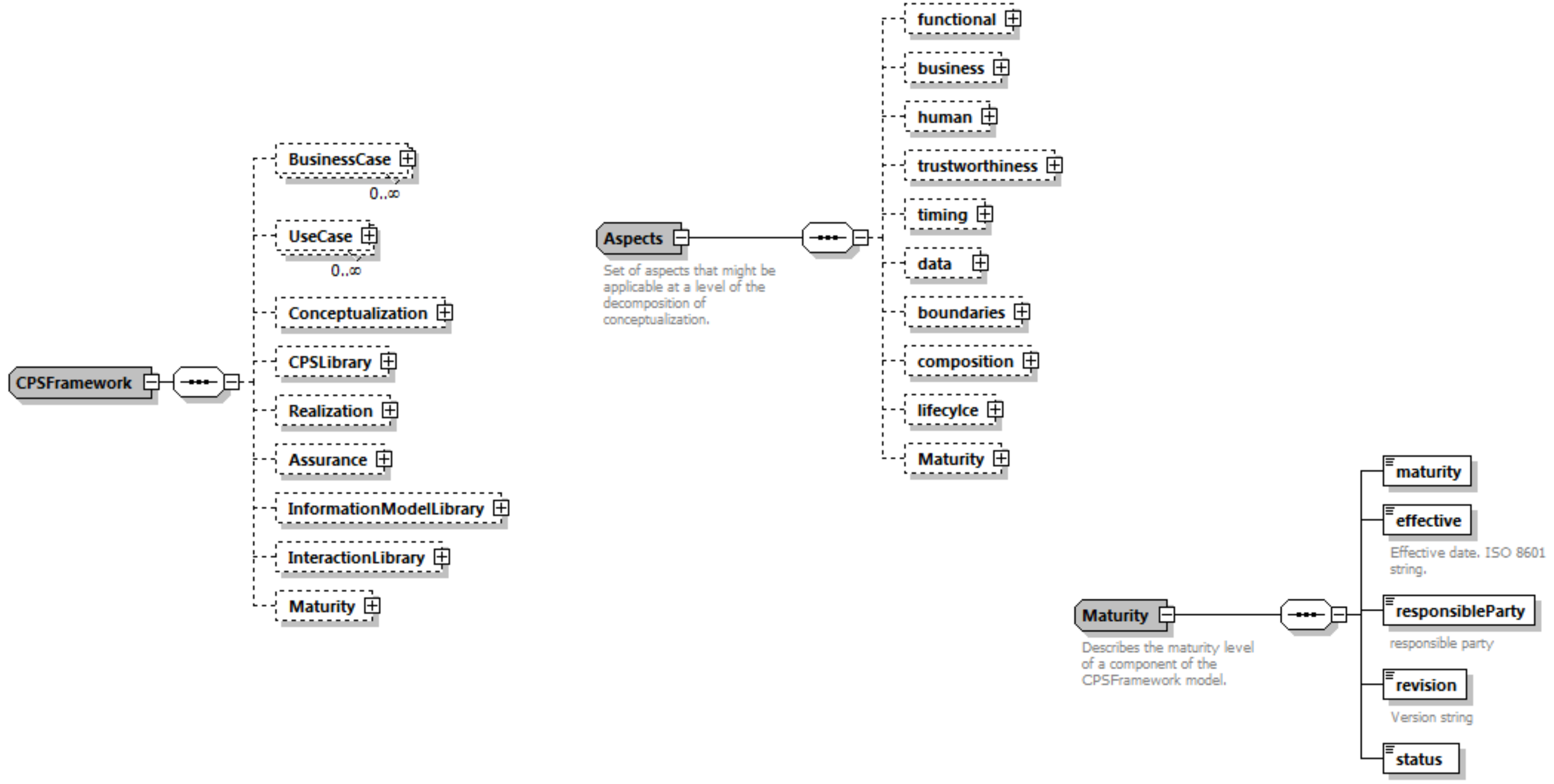
Altova XMLSpy 2017

Revise to optimize
schema

9.4.15 XML Editor of a Use Case



9.4.16 CPS Framework in XML Schema



9.4.17 CPS Framework Instance: Thermostat Design

- **xml-stylesheet** type="text/xsl" href="IntermediateToXHTMLNew.xslt"
- ***n1*:CPSFramework**
  - **xmlns:*n1*** cpsframework
  - **xmlns:*xsi*** http://www.w3.org/2001/XMLSchema-instance
  - ***xsi*:schemaLocation** cpsframework cpsframework.xsd
  - **BusinessCase**
    - **name** Design a Communicating Smart Thermostat
    - **identifier** 222
    - **technicalId** String
    - **description** Build a smart thermostat that has heating, cooling and automatic control modes to maintain room temperature near a user's set point and uses a WiFi local area network (LAN) to interact with a temperature s should be able to retail for less or equal to $79. It must be intrinsically safe, reliable, secure, protect privacy, easy to use and upgradable.
    - **Aspects**
      - **functional**
        - **Actuation**
          - **Property**
            - **statement** Smart Thermostat shall be able to actuate heating, cooling and automatic function
        - **Communication**
          - **Property**
            - **statement** Smart Thermostat shall communicate with sensor and HVAC using WiFi
      - **trustworthiness**
        - **Security**
          - **Cybersecurity**
            - **Property**
              - **statement** Smart Thermostat shall
        - **Privacy**
          - **Property**
            - **statement** Smart Thermostat shall protect privacy
        - **Reliability**
          - **Property**
            - **statement** Smart Thermostat shall be reliable (no unacceptable variation in function)
        - **Safety**
          - **Property**
            - **statement** Smart Thermostat shall be safe. (no unacceptable risk)
    - **Domain** (2)

	name	technicalId
1	Home Automation	String
2	Energy	String

  - **UseCase**
    - **name** Maintain room temperature near a user's set point
    - **identifier** CPS-T-1
    - **technicalId** CPS-T-1 UUID
    - **nature** Technical
    - **classification** Generic
    - **keywords** User, thermostat, thermostat controller, temperature sensor, HVAC controller, WLAN
    - **levelOfDepth** Detailed

9.5 Tools Demonstration

1) UML Model Review
2) XSD Export and Review
3) XML Model Browse
    1) XSLT (text view vs browser view)
    2) Xpath (//*/Aspects/trustworthiness/*/Property/..)

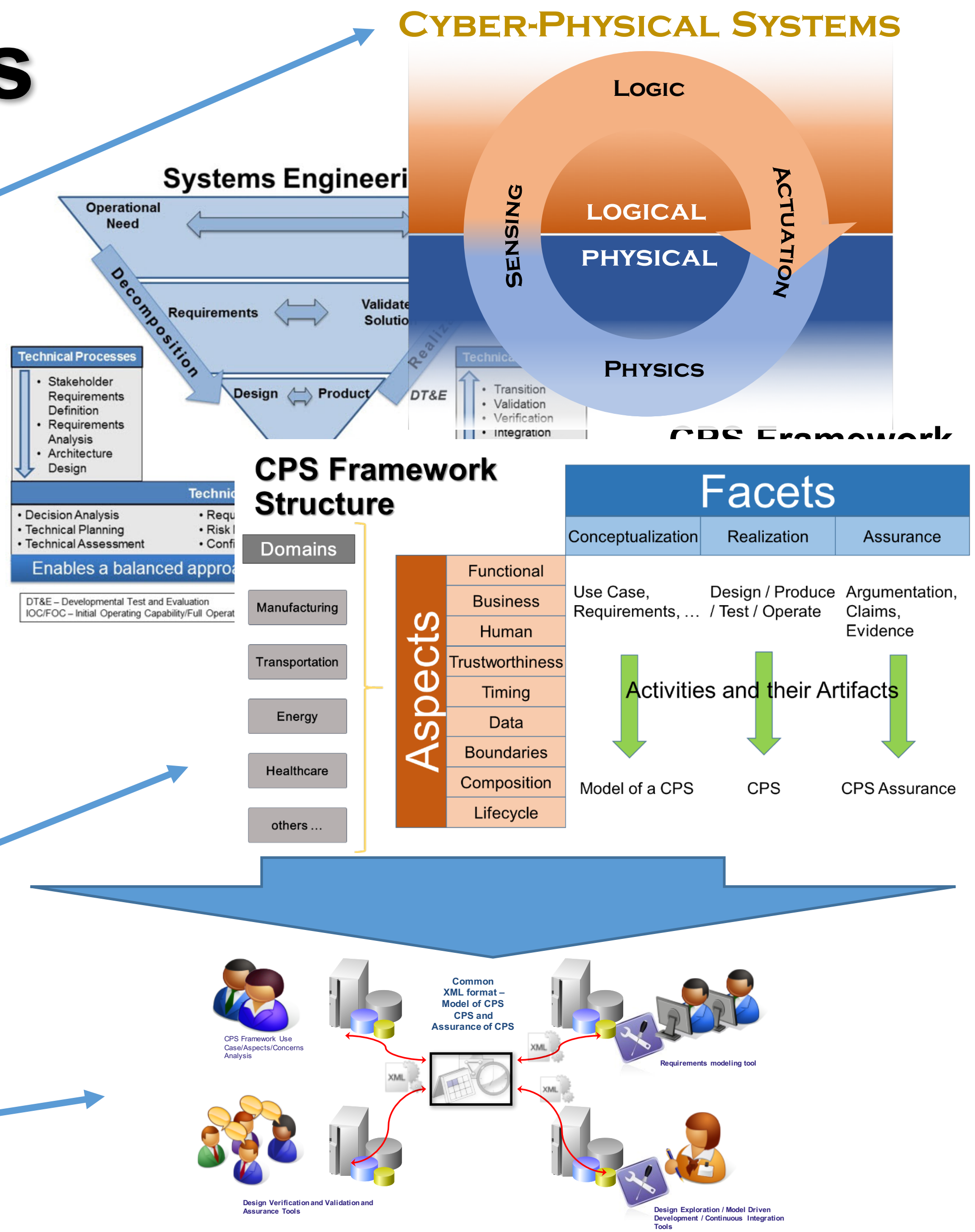
10. Building Community around CPS Framework Open Source - Griffor

- What are the hoped-for outcomes
- Collaboration Tools – GitHub Environment
- Embedding this technology in your CPS Engineering Tool
- Open Discussion on Next Steps

10.1 Revisiting Workshop Goals

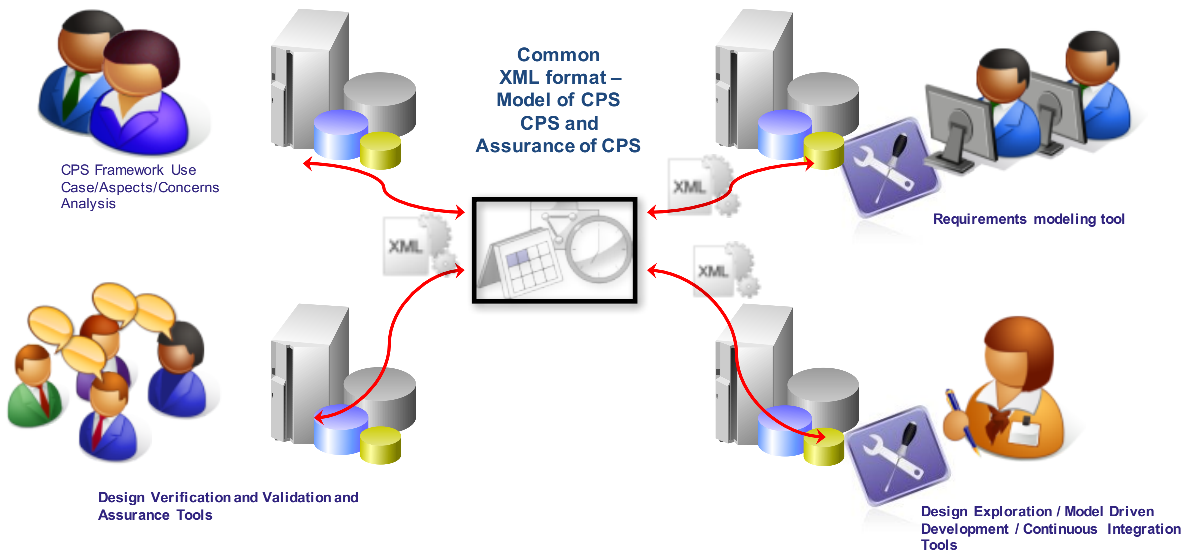
This workshop addresses key CPS challenges: what are the methods and tools needed to conceive, design, build, deliver and maintain Cyber-Physical Systems.

1. What is CPS?
2. How do we design, build and assure CPS throughout their lifecycle?
3. What discipline do we need to address the concerns that drive requirements and engineering?
4. What needs to be the common core tooling?



Continuous Integration for CPS Development

10.2 Concept common core tooling: CPS Framework Open Source



Continuous Integration for CPS Development

1) 'Type Structure' for:

- Aspects and concern; and
- Facets, engineering activities and outcomes

2) That type and sort compositionally:

- Properties/requirements and
- Artifacts

3) Encoded in a portable, reusable XML format.

Program Speakers and Panelists

NIST Participants

- E. Griffor (EL)
- Ron Ross (ITL)
- D. Wollman (EL)
- M. Burns (EL)
- C. Greer (EL)
- T. Roth (EL)
- E. Song (EL)

External Participants

- D. McShane (Ricardo LLC)
- F. Brandao (Ricardo LLC)
- C. Vishik (Intel)
- M. Balduccini (St. Joseph University)
- A. Rajhans (Mathworks)
- H. Neema (Vanderbilt University)
- S.-W. Lin (Thingswise)
- J. Weimer (UPenn-PRECISE)