Implications of the IoT:

The CPS Framework and Key Open Questions

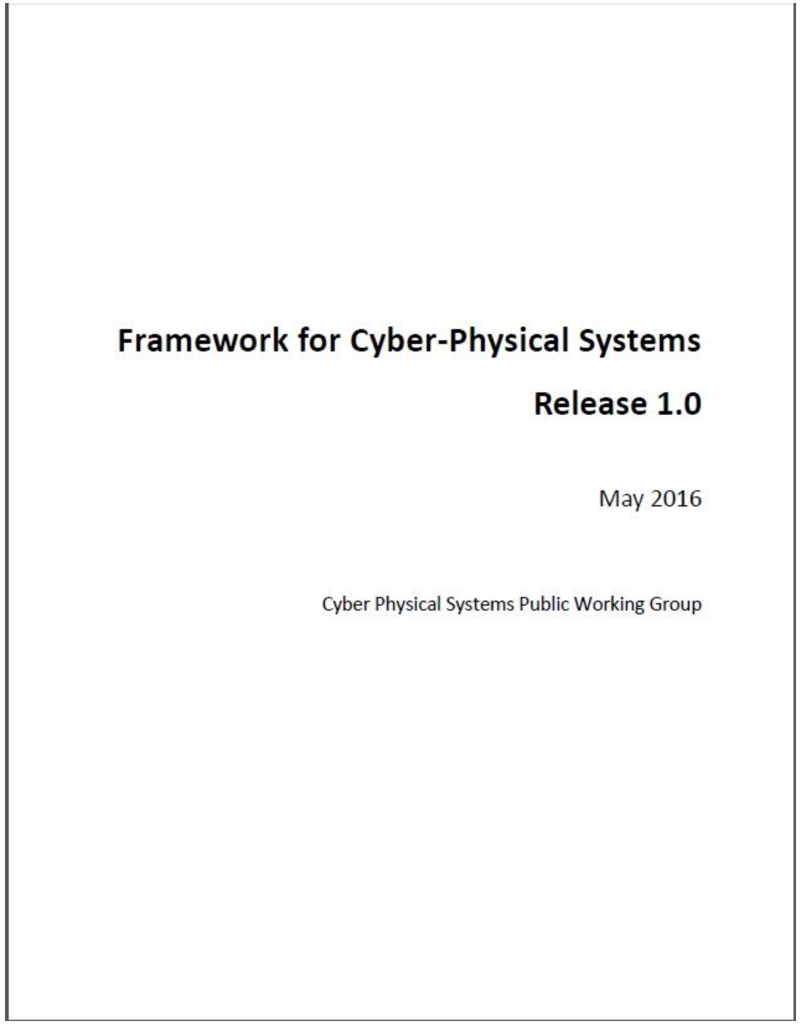
Larry John, PhD
Principal Analyst
ANSER
larry.john@anser.org
703-416-3199

Contents

- Intro to the NIST CPS Framework
  - Motivation
  - Development Process
- Applying the Framework
- Open Questions affecting Standards, Policy and Ethics

Introduction to the NIST CPS Framework

- *Cyber-physical systems*: "… smart systems that include engineered interacting networks of physical and computational components."
  - Enable innovative applications and impact multiple economic sectors
- NIST CPS PWG: Open public forum comprising a broad range of CPS and other experts to help define and shape key characteristics of CPS
  - Gain **shared understanding** of foundational concepts and unique dimensions
  - Exchange ideas and integrate research for **CPS with new functionalities**
  - Develop a comprehensive **standards and metrics** base for CPS
- NIST CPS Framework development goals:
  - Derive **a unifying framework** that covers the range of unique dimensions
  - Populate a significant portion of the CPS Framework with detail
- CPS PWG Subgroups:
  - Reference Architecture
  - Security and Privacy
  - Use Cases
  - Data Interoperability
  - Timing



Framework for Cyber-Physical Systems

Release 1.0

May 2016

Cyber Physical Systems Public Working Group

Why Build the Framework?

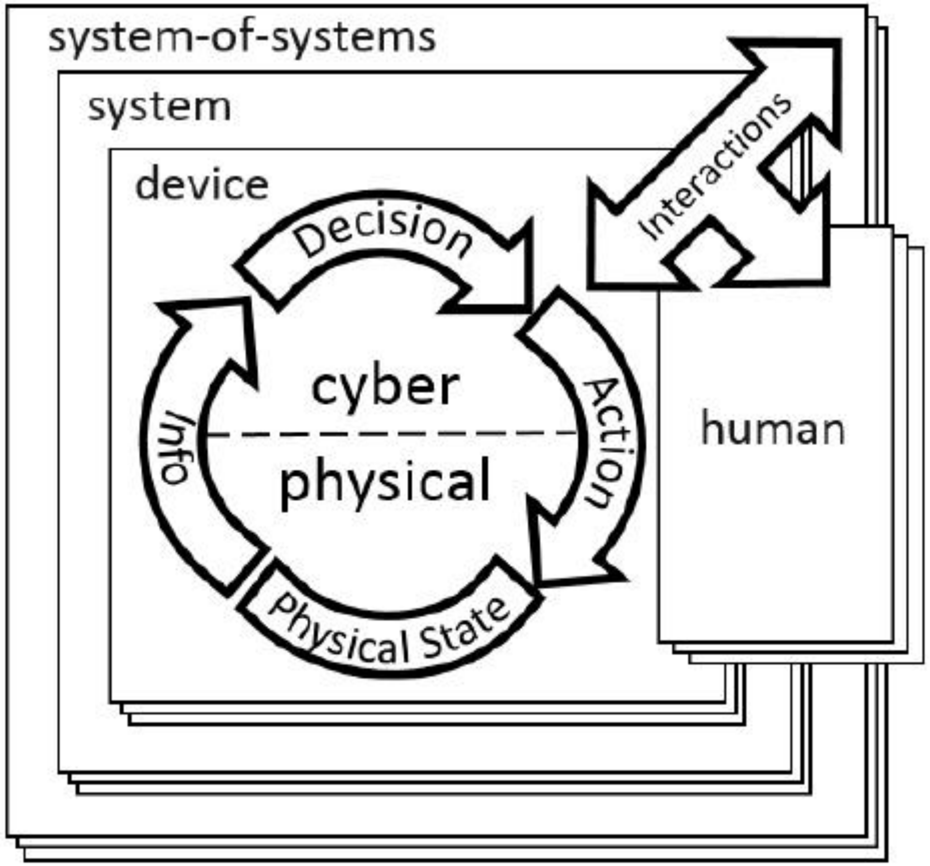
- CPS (especially the IoT) are becoming more **pervasive**
  - Trillions of devices—**growing demand** for connection and interoperability
  - High percentage with little or no **security**
- **CPS can affect the physical world**—damage, destroy, injure and kill
  - Implanted medical devices, manufacturing equipment, power generation and transmission, transportation systems, …
- **Attacks** leveraging or targeting connected devices
  - Stuxnet, Mirai and follow-ons
  - Ransomware vs. hospitals, factories, school districts, transportation …
- Humans must be able to **predict and control** what CPS can do
  - A true system of systems engineering problem that spans the lifecycle: conceivers, designers, developers, owners, users, customers, maintainers, …

Quick Example: IT vs IoT/CPS Threats

	Primary Impact of Failure		Mitigation Mechanisms		
	Digital	Physical	Digital	Analog	Physical
IT System	✓		✓		
IoT/CPS	✓	✓	✓	✓	✓

Traditional IT-based thinking is necessary but insufficient for CPS
We must think more broadly

CPS Conceptual Model

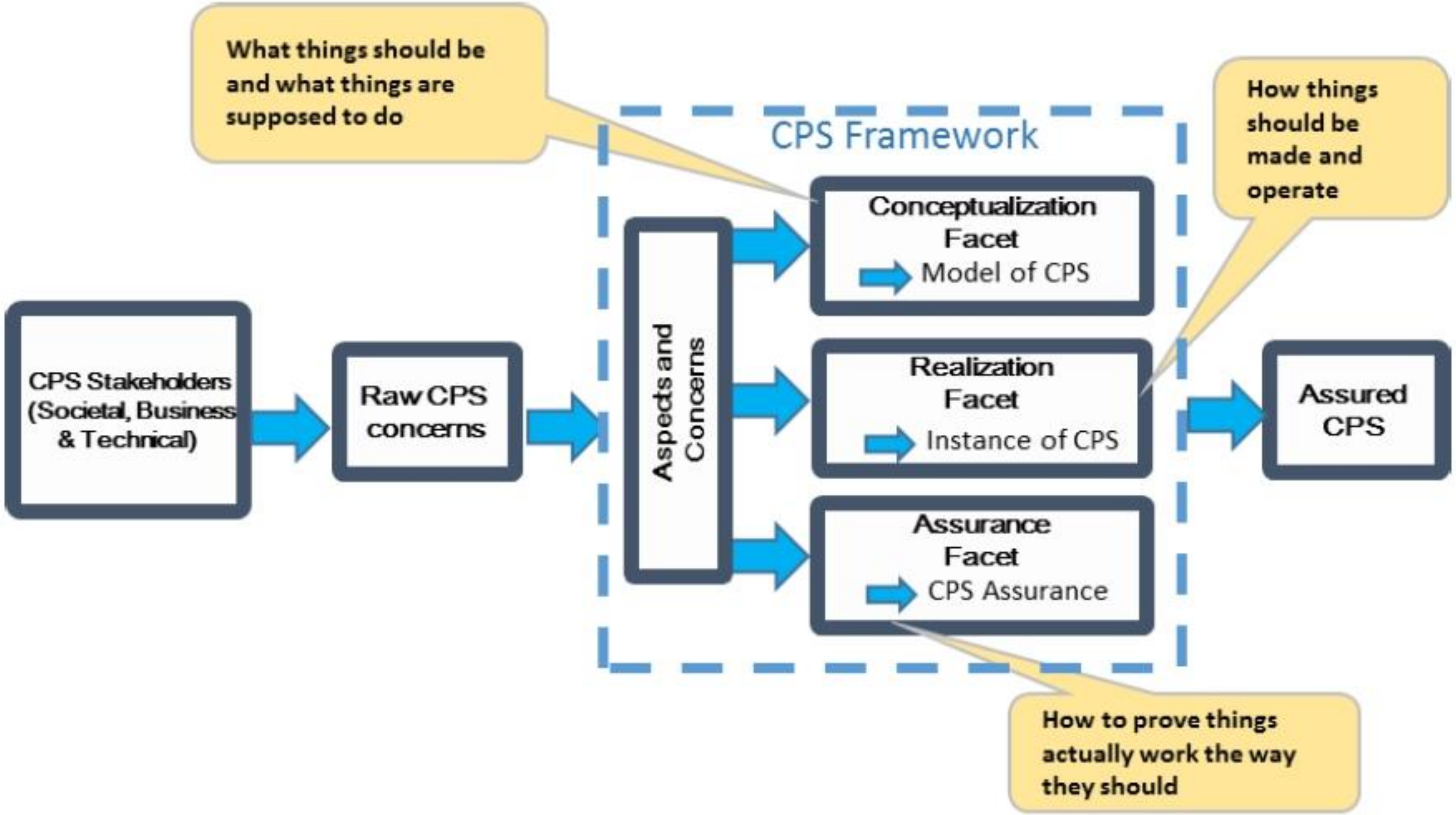


CPS:

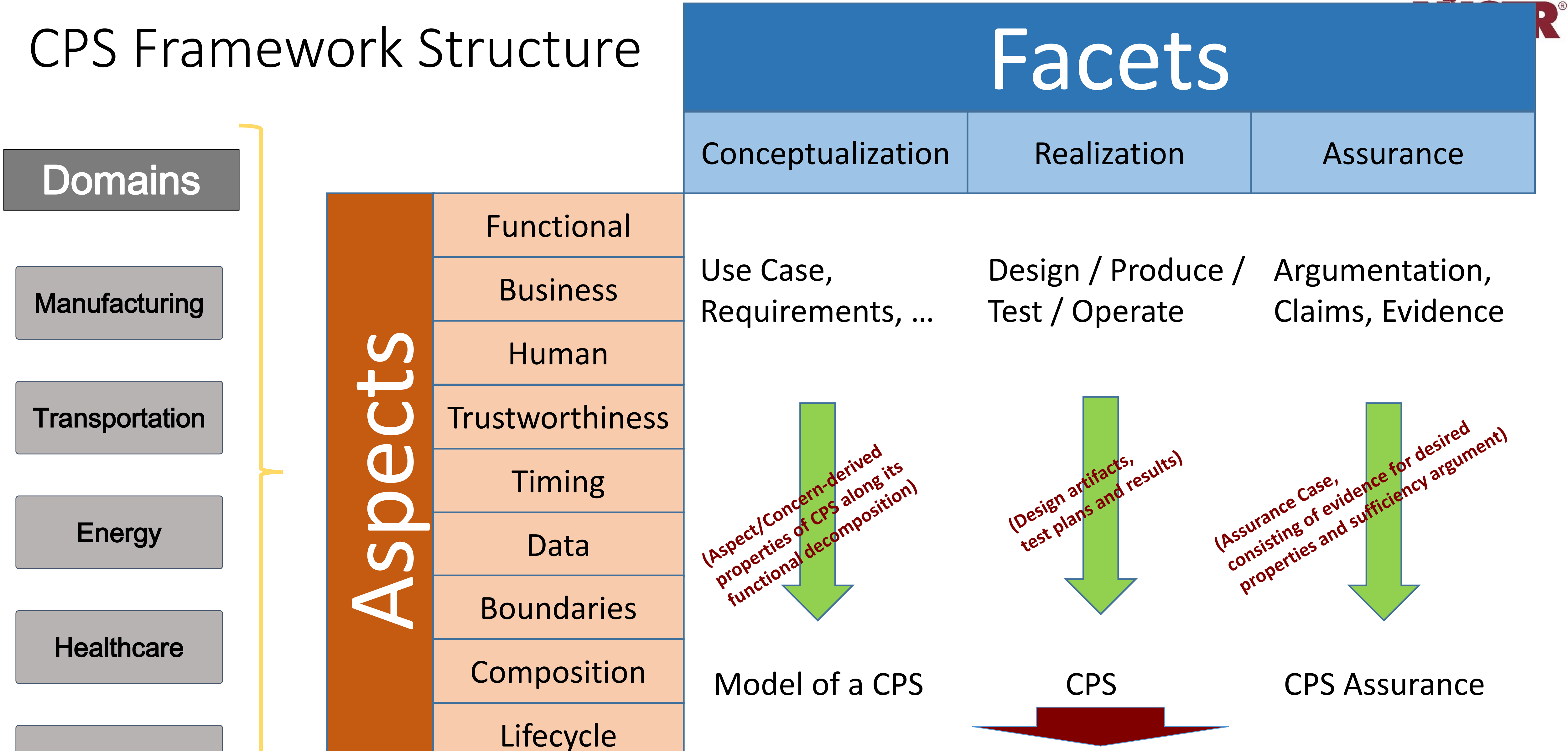
- Can **range** from simple devices to vast systems of systems
- **Interact** with other systems and humans at multiple levels: physical, logical and logical-physical
- Contain:
  - **information flows** (show state of the physical world)
  - **decision flows** (cause impacts on physical world)
- Can enable collaboration **at any scale**

CPS Framework Development Process

- Identify CPS **domains** and domain-specific **concerns**
- Identify **cross-cutting concerns**
- Analyze cross-cutting concerns to **group concerns into aspects**
- Address aspects via activities that produce artifacts in three **facets**:
  - Conceptualization
  - Realization
  - Assurance


What things should be and what things are supposed to do
How things should be made and operate
CPS Framework
CPS Stakeholders (Societal, Business & Technical)
Raw CPS concerns
Aspects and Concerns
Conceptualization Facet
Model of CPS
Realization Facet
Instance of CPS
Assurance Facet
CPS Assurance
Assured CPS
How to prove things actually work the way they should

CPS Framework Structure



Domains

- Manufacturing
- Transportation
- Energy
- Healthcare
- others …

Aspects

- Functional
- Business
- Human
- Trustworthiness
- Timing
- Data
- Boundaries
- Composition
- Lifecycle

Facets

Conceptualization	Realization	Assurance
Use Case, Requirements, …	Design / Produce / Test / Operate	Argumentation, Claims, Evidence
(Aspect/Concern-derived properties of CPS along its functional decomposition)	(Design artifacts, test plans and results)	(Assurance Case, consisting of evidence for desired properties and sufficiency argument)
Model of a CPS	CPS	CPS Assurance

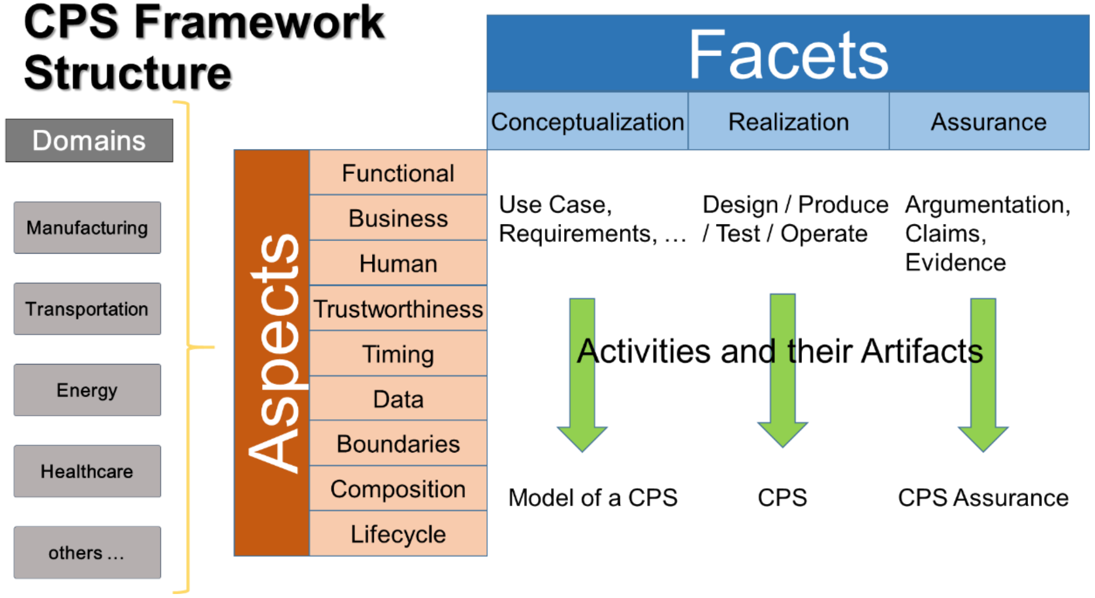
"The CPS property of the design artifacts according to an accepted, consensus mode of argumentation."

CPS Public Working Group

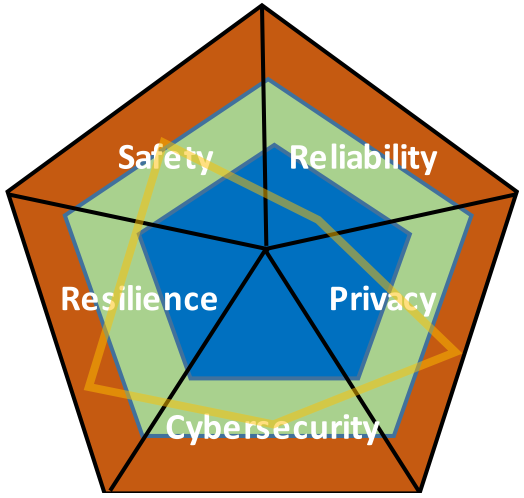
- Provides technical, concern-driven foundation for CPS/IoT: CPS Framework
- NIST leadership w/industry, academia, government
  - CPS experts in 5 working groups contributed to draft CPS Framework
  - Working Group revised draft based on public review comments
  - Version 1.0 released in May 2016
- EL, ITL, PML collaborative effort (Overall leads: Griffor, Wollman – plus Burns, Battou, Simmon, Quinn/Pillitteri, Weiss)
- Collaboration site: https://pages.nist.gov/cpspwg/

'Concern-driven': holistic, integrated approach to CPS concerns.

CPS Framework Structure



Concerns as Dimensions of CPS Measurement



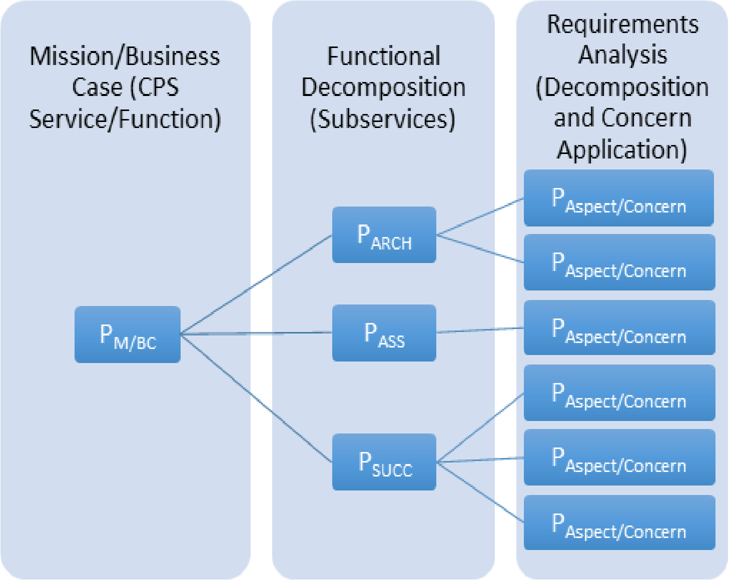
CPS Framework Mathematics

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)



Mission/Business Case (CPS Service/Function)

Functional Decomposition (Subservices)

Requirements Analysis (Decomposition and Concern Application)

$P_{M/BC}$

P_{ARCH}

P_{ASS}

P_{SUCC}

$P_{Aspect/Concern}$

$P_{Aspect/Concern}$

$P_{Aspect/Concern}$

$P_{Aspect/Concern}$

$P_{Aspect/Concern}$

$P_{Aspect/Concern}$

semantics of CPS Framework

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

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

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

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

… defines **composition of concerns**

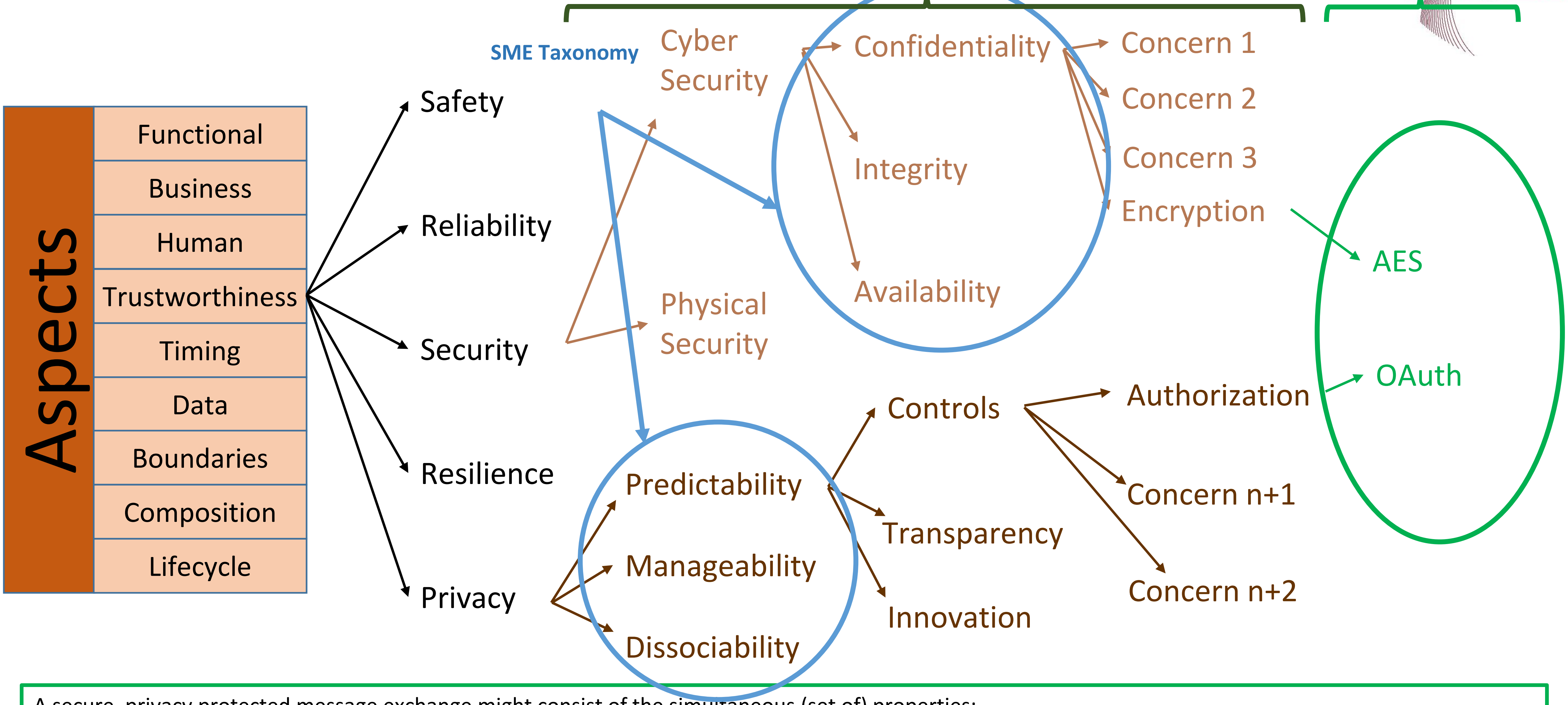
$$\boxed{\overline{C_1 * C_2}^{CPS} = \overline{C_1}^{CPS} \cup \overline{C_2}^{CPS}}$$

formal methods for assurance of a CPS

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

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

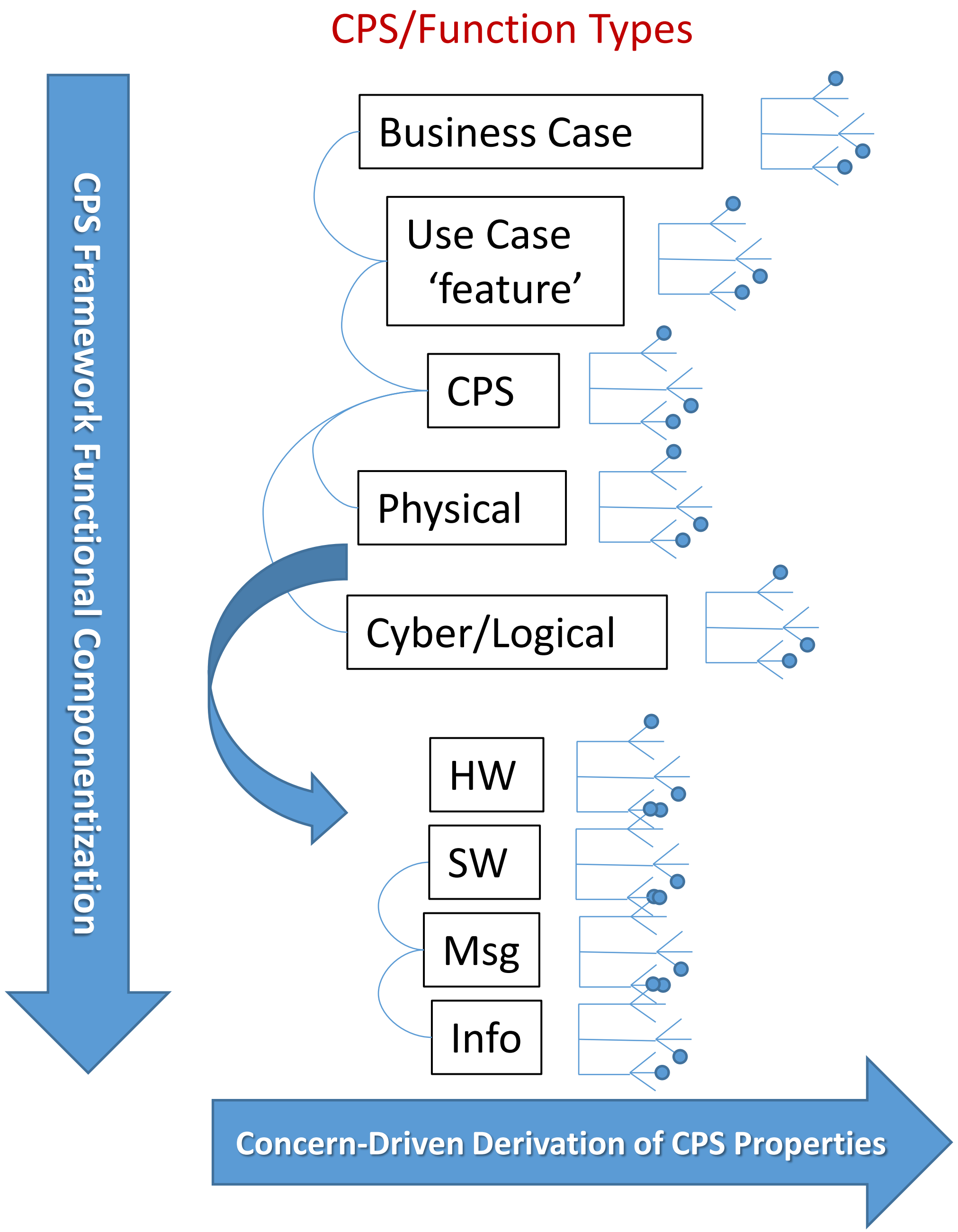
CPS Aspect/Concern/Property Tree



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}

Decomposing a CPS in the CPS Framework


CPS/Function Types
Business Case
Use Case ‘feature’
CPS
Physical
Cyber/Logical
HW
SW
Msg
Info
CPS Framework Functional Componentization
Concern-Driven Derivation of CPS Properties

Function Types correspond to:

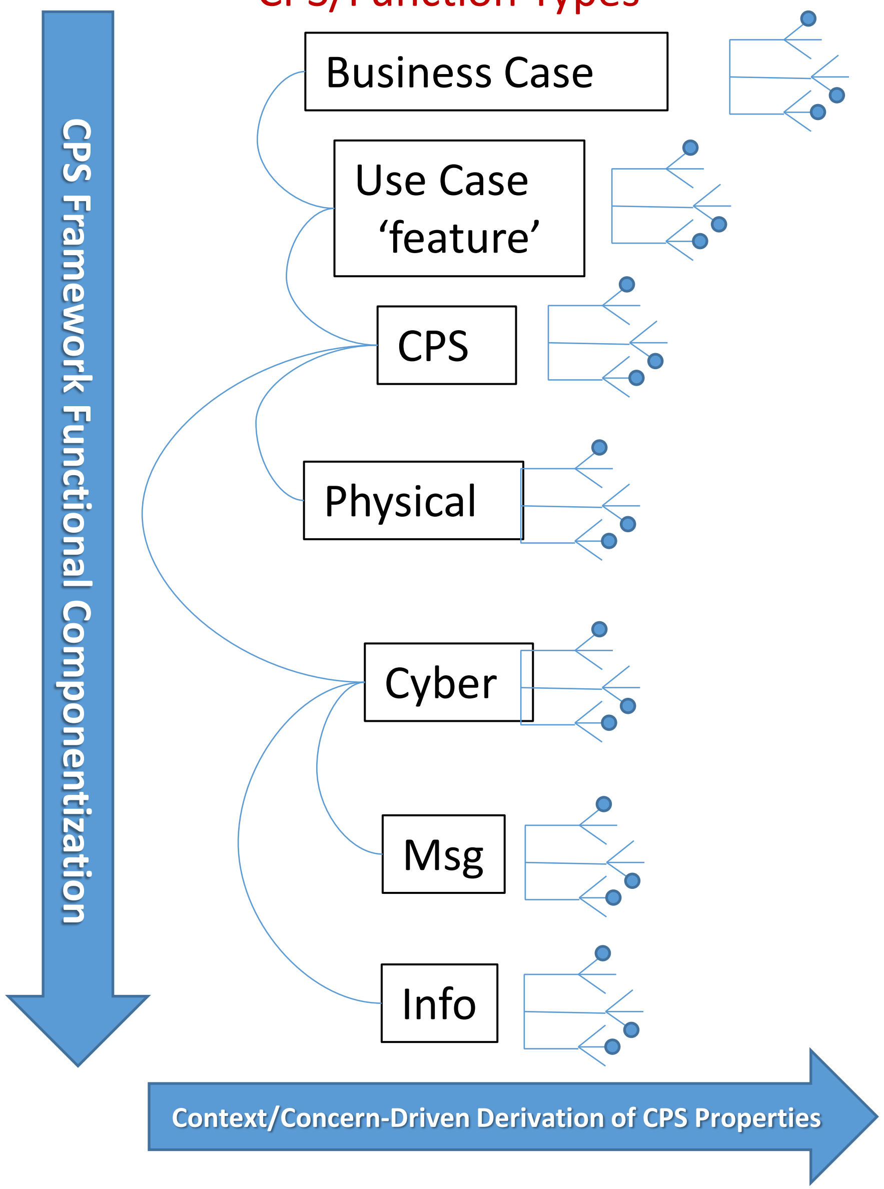
- input/output characteristics
- methods/tools used to develop and reason about the functions

Including:

- Business Case (content and constraints)
- Use Case (feature/function)
- CPS (cyber-physical subsystems)
- Physical functions
- Cyber/logical functions
- Allocation to SW/HW
- Message and Signal

Framework Functional Decomposition

CPS/Function Types



Business Case

Use Case
'feature'

CPS

Physical

Cyber

Msg

Info

CPS Framework Functional Componentization

Context/Concern-Driven Derivation of CPS Properties

Properties of System Functions
(Automatic Emergency Braking)

AEB – vehicle provides automated collision safety function

AEB – vehicle provides/maintains safe stopping

AEB –braking function reacts as required

AEB – friction function provides appropriate friction

AEB – stopping algorithm provided safe stopping

AEB – messaging function receives distance to obstacles and speed from propulsion function

AEB – distance and speed info is understood by braking function

Functions as Sets of Properties

Hierarchy of Functions of a CPS

Properties of System Functions (AEB)

Safety – vehicle provides its function safely/without collision

Safety – vehicle provides/maintains safe stopping distance

Safety –braking function reacts as required

Safety – braking function provided appropriate friction

Safety – braking function has safe stopping algorithm

Safety – braking function receives distance to obstacles and speed from propulsion function

Safety – braking function understands distance and speed

Dependencies

Function Hierarchy

$$f_{CollAvoid}$$

$$\curlyvee$$

$$f_{StoppingDistance}$$

$$\curlyvee$$

$$f_{BrakingFunction}$$

$$\curlyvee$$

$$f_{BrakingFriction}$$

$$\curlyvee$$

$$f_{SafeStopAlg}$$

$$\curlyvee$$

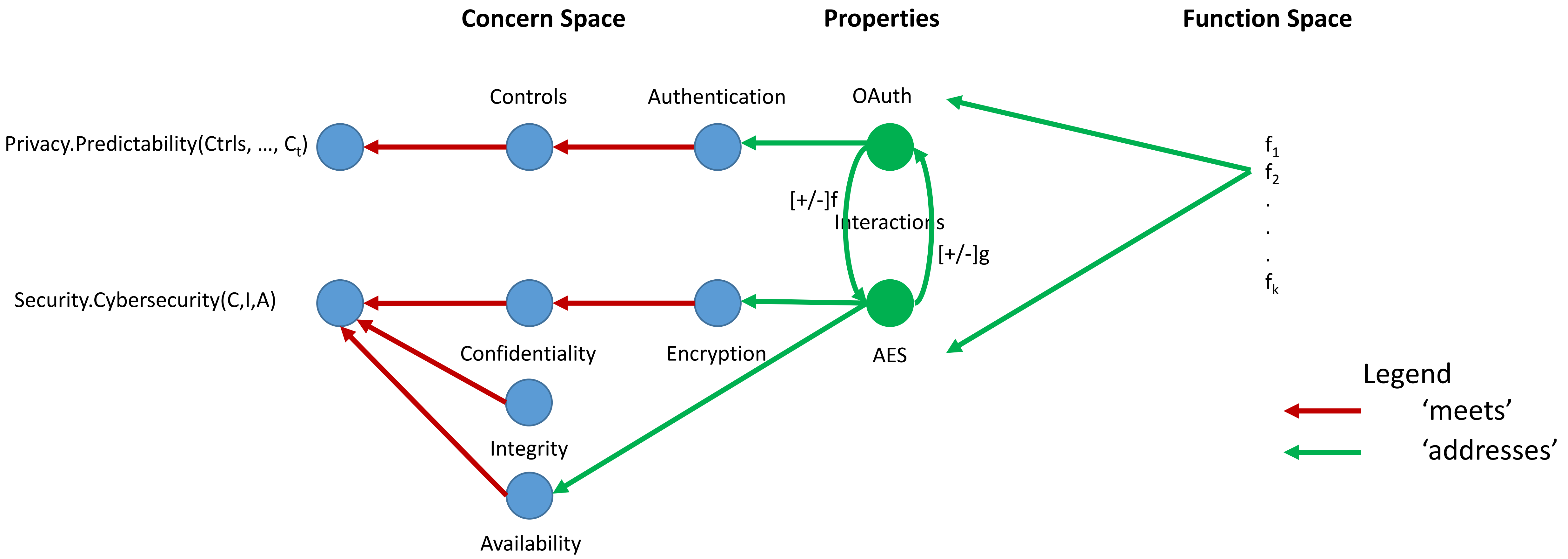
$$f_{CollDistance} \text{ and } f_{VehicleSpeed}$$

$$\curlyvee$$

$$Dom(f_{BrakingFunction}) \supseteq Range(f_{CollDistance}) \cup Range(f_{VehicleSpeed})$$

Function Hierarchy

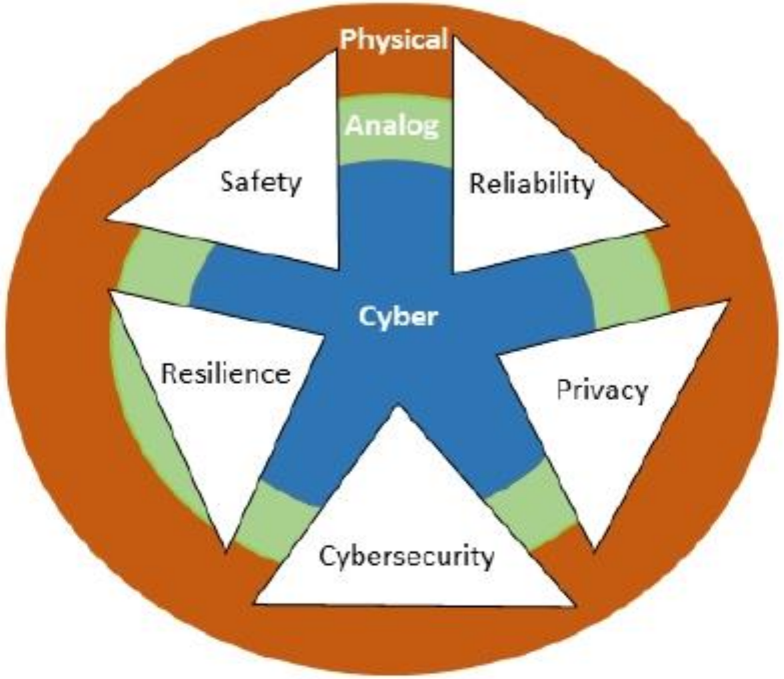
CPS Framework: The Interaction Calculus

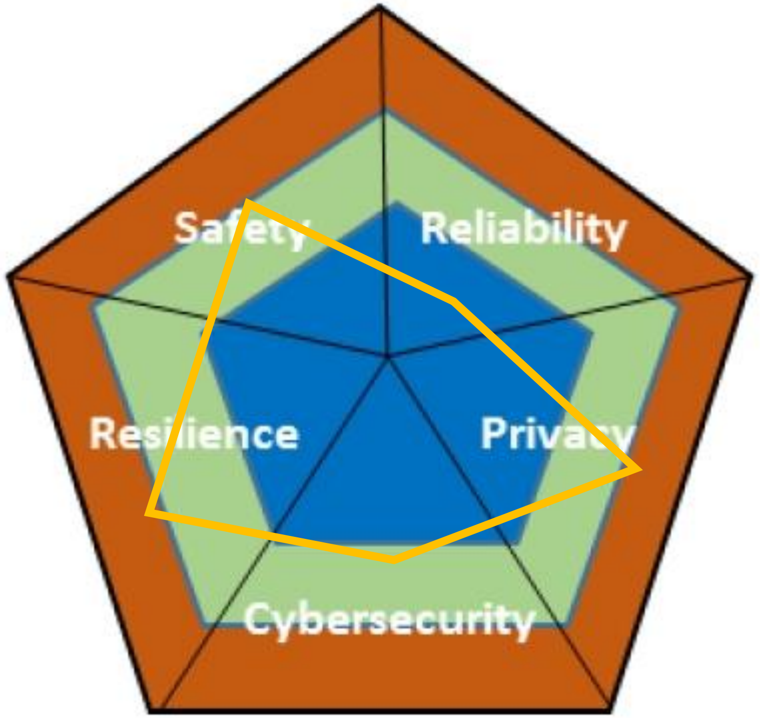


Example Impact of one concern on another:

- Calculated using pathways through the up- or down-regulation relationships between the Properties of the CPS
- These correspond to generalized derivatives (an incremental change in one results in a negative or positive impact on the other)
- Impact is the 'generalized integral' over all pathways

Envisioning Risk in CPS--Trustworthiness





Silo-based risk management won't work for unmanaged composition of CPS.
Integrating trustworthiness domains gives a better picture of risks and enables better mitigation

Four (of many) Open Questions

How do we …

- **Create useful standards** for sets of CPS that can be used to meet many different requirements serving many different needs—some of which we can’t yet predict?
- Design and craft an effective **system of governance** for systems of infinitely composable CPS? What would be its scope? How would we implement it?
- Describe the **ethical responsibilities** of the people in different CPS system lifecycle roles? How do they learn about and discharge them?
- **Establish and enforce liability** for the effects of a CPS in one domain that can be connected to many other sets of CPS in other domains and nations?

Discussion

Larry.John@anser.org

703-416-3199