CPS Foundational Challenges

2June2017

Dr. E. R. Griffor
Associate Director

US National Institute of Standards and Technology

National Institute of Standards and Technology

About NIST

- Part of the U.S. Department of Commerce

- NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.
  - 3,000 employees
  - 2,700 guest researchers
  - 1,300 field staff in partner organizations
  - Two main locations:
    Gaithersburg, MD
    Boulder, CO

Priority Research Areas

CPS Challenges and NIST Research Activities

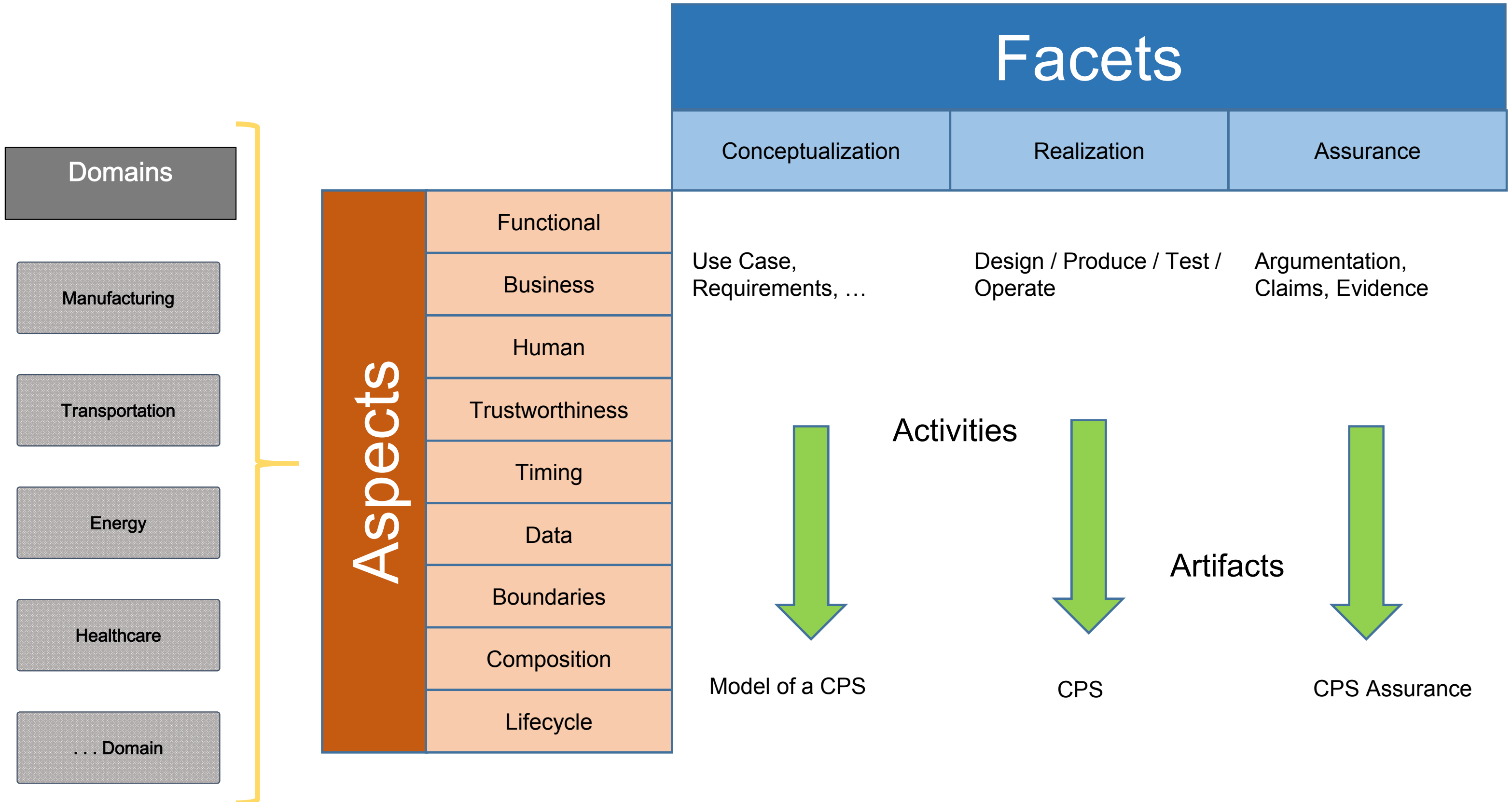
Current

- Analyzing and Developing CPS
- CPS Framework Open Source Project
- Relation between CPS and IoT
- Simulating and Testing CPS
- Assuring CPS: Formal Methods

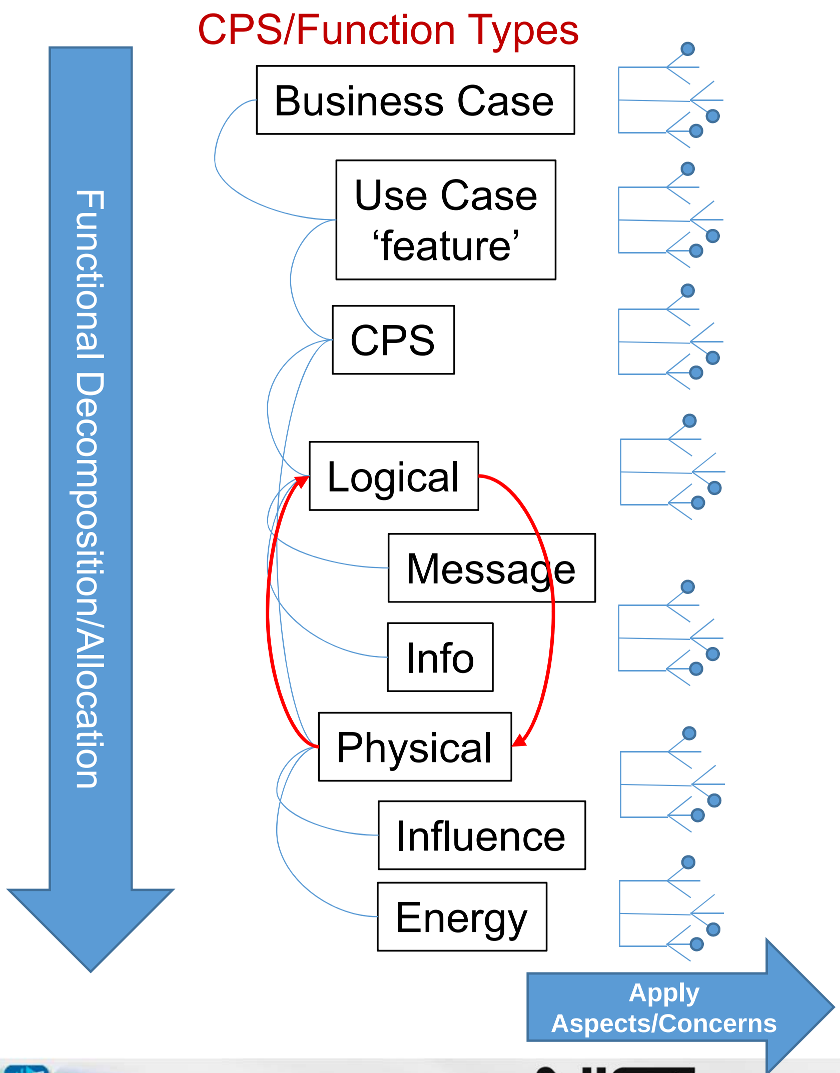
Future

- Mathematical Models of CPS
- Trustworthiness

Analyzing and Developing CPS: CPS Framework



Analyzing and Developing CPS: Decomposition



Safety "Properties" of a decomposed Function: AEB

AEB – vehicle provides automated collision safety function

AEB – vehicle provides/maintains safe stopping

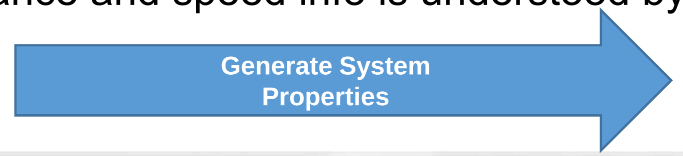
AEB –braking function reacts as required

AEB – friction function provides appropriate friction

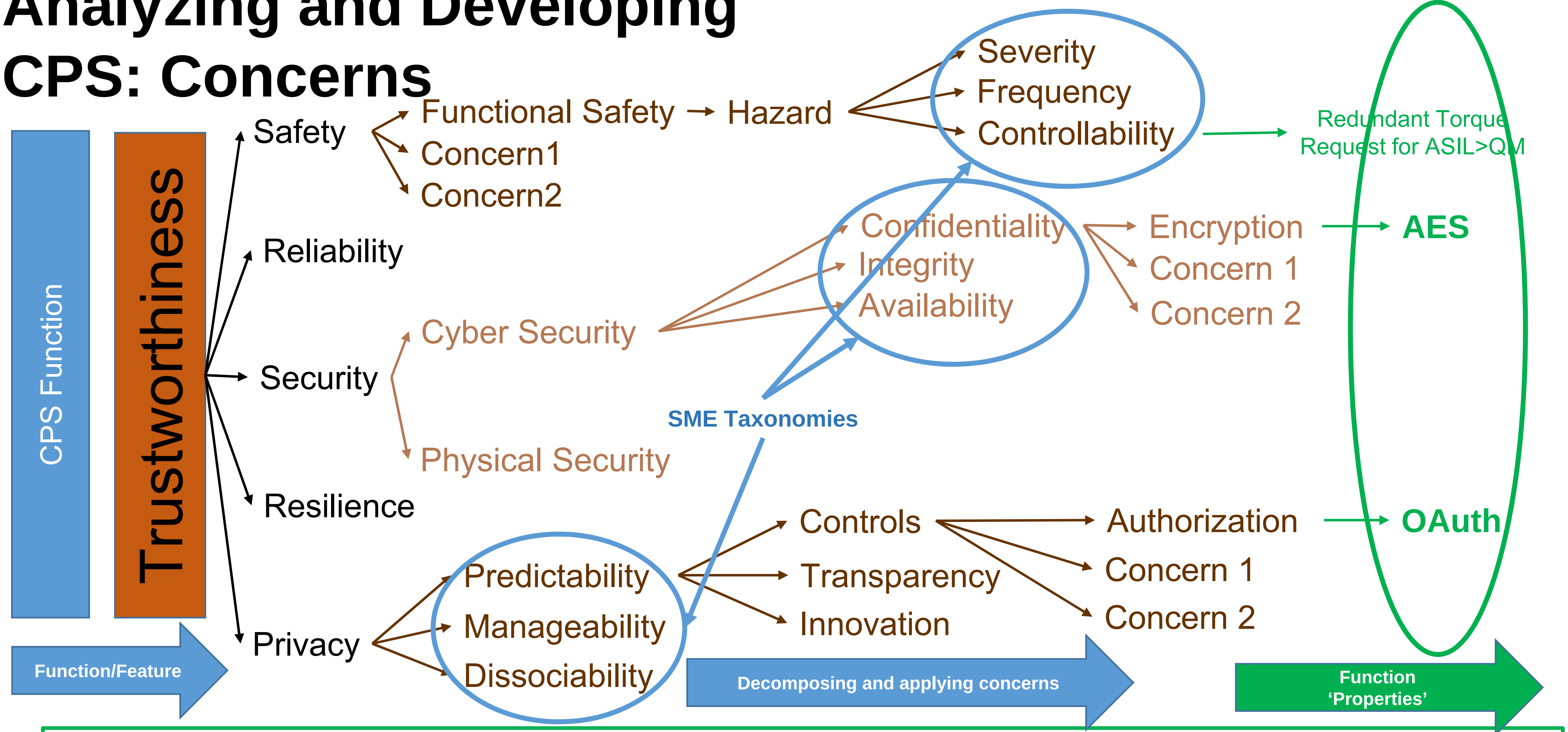
AEB – stopping algorithm provided safe stopping

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

AEB – distance and speed info is understood by braking function



Analyzing and Developing CPS: Concerns



A secure, privacy protected CAN BUS Message may consist of these properties:
{Trustworthiness.Security.Cybersecurity.Confidentiality.Encryption.AES, Trustworthiness.Privacy.Predictability.Controls.Authorization.OAuth}

CPS Framework Open Source Project: Tools

Enterprise Architect: UML Editor

XMLSpy: XML/XMLSchema Editor

ALTOVA® XMLSpy® 2016

TortoiseGit: Windows GitTool

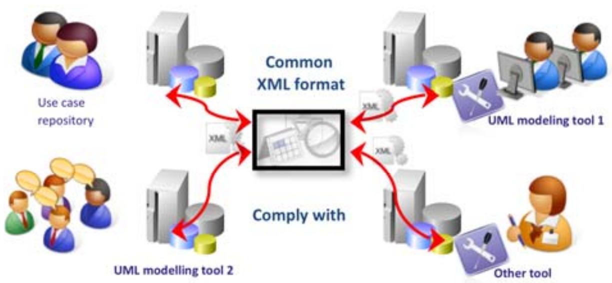
GIT

Notepadd++: Programmers Editor

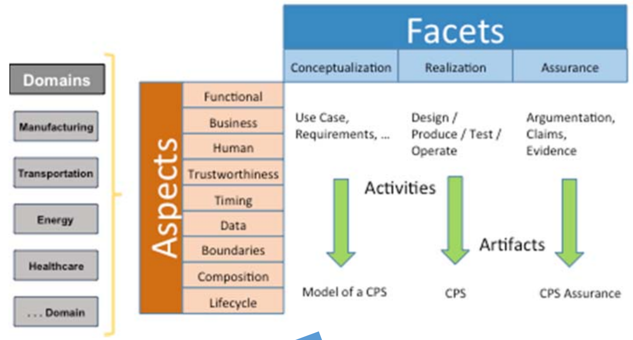
Notepad++

CPS Framework Open Source Project: Union of Technologies

IEC 62559 Methodology



NIST CPS Framework Methodology

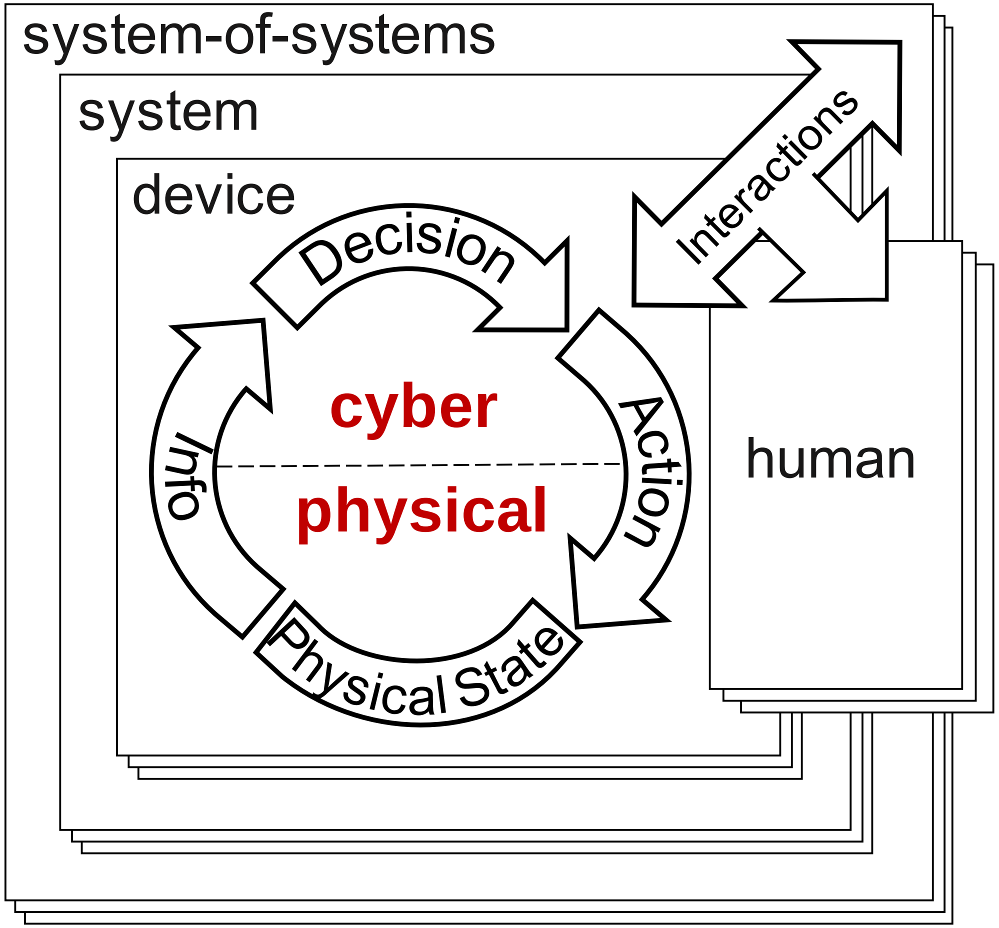


Standardized XML Schema

Conceptualization	Realization	Assurance
• Business Case • Use Case • Requirements	• Design • Traceability to Requirements	• Algorithmically Prove Design Meets Requirements

Relation between CPS and IoT

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



- Examples include a smart gird, a self-driving car, a smart manufacturing plant, an intelligent transportation system, a smart city, and Internet of Things (IoT) instances connecting new devices for new data streams and new applications.
- Common notions of IoT have emphasized networked sensors providing data streams to applications.
- CPS concepts complete these IoT notions, providing the means for conceptualizing, realizing and assuring all aspects of the composed systems of which sensors and data streams are components.

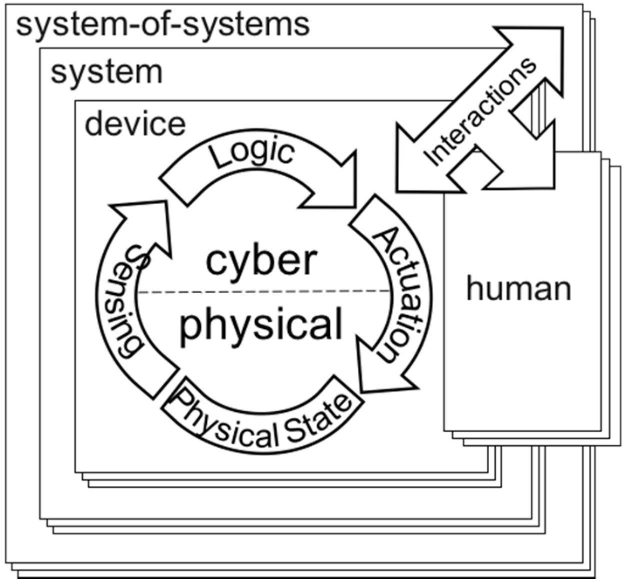
The Framework for Cyber-Physical Systems was released by the NIST CPSPWG on May 26, 2016

Relation between CPS and IoT

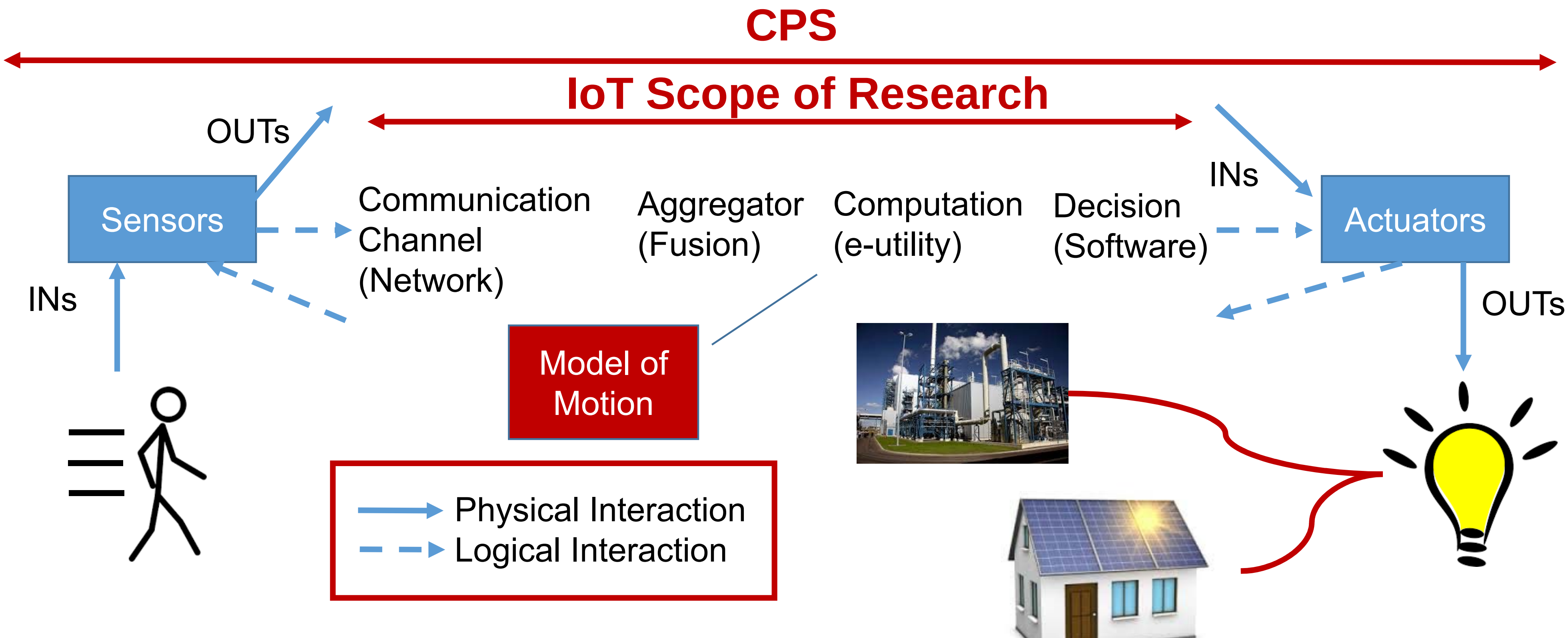
Cyber-Physical Systems (CPS) comprise interacting digital, analog, physical, and human components engineered for function through integrated physics and logic.

Examples of a CPS that are not instances of IoT

- Segway Scooter
- Smart Spoon enabling Parkinson's patients to feed themselves (see https://www.liftware.com/)
- Autonomous vehicle operating without wired or wireless connections outside the vehicle, e.g.
  - o a Mars rover operating between messages from Earth
  - o the original vehicles in the first DARPA Challenge
  - o cruise missile/smart bomb in flight to target
- Generally, any CPS that is fully contained with no outside network connections



Relation between CPS and IoT



Framework Schema: **Phys-Log-Log-Log-Log-Phys**
Testbed: **Experiment, Measurement and Assurance**
Challenges: **Interoperability, Composition and Composition Types, Trustworthiness, etc.**

Relation between CPS and IoT: IT- vs CPS-Based Risk Mitigation

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

"Better cybersecurity through physics!"

Simulating and Testing CPS

- ***CPS Testbed*** (Architecture and instance of HW and SW Tools)
  - UCEF
  - Control Room + Visualization
  - Open Source Project 16May2017 at NIST
- ***CPS Testbed Science***
  - Testbed composition and its semantics (wrappers)
- ***Testing the concerns*** of the CPS Framework in the testbed
  - Setup and Testing as in the case of requirements driven by the Timing concerns

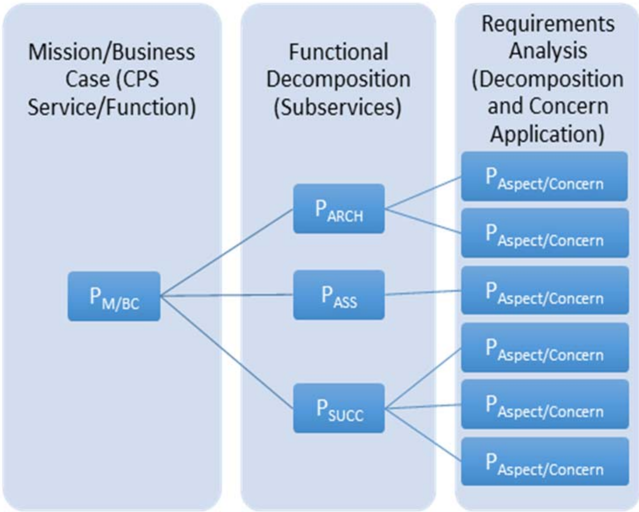
Assuring CPS: Formal Methods

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

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

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

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

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

… defines **composition of concerns**

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

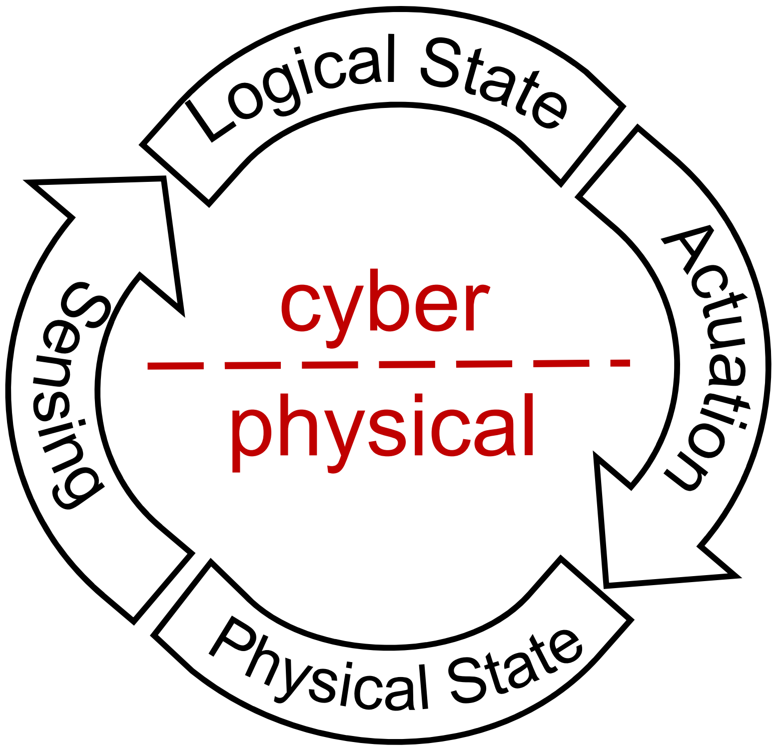
formal methods for assurance of a CPS

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

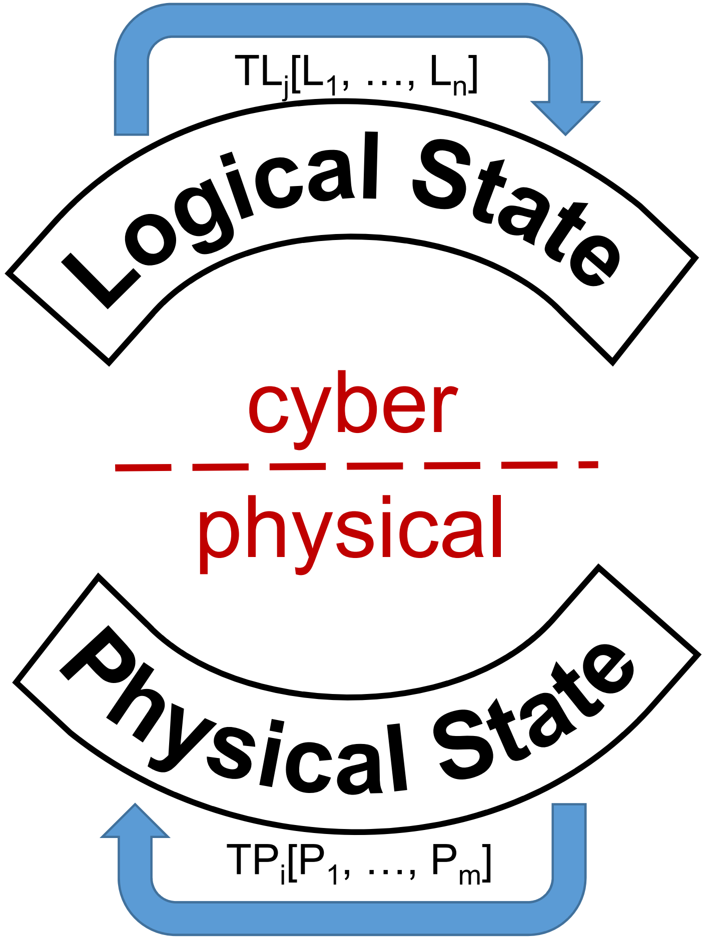
$$\overline{Assurance\ Case}^{CPS} = \sum_{C \in \overline{Aspect}^{CPS}} \sum_{P \in \bar{C}^{CPS}} \sum_{d \in \overline{Design}^{CPS}} \sum_{e \in \overline{Evidence(P)}^{CPS}} \overline{Argumentation}^{CPS}(P)$$

Mathematical Models of CPS

- We need a way of describing general interactions on or between CPS, logical or physical.
- The study of these interactions will result in a unified cyber-physical science.
- To accomplish this requires our ability to 'transfer' key properties of these two realms from one to the other and back.



Mathematical Models of CPS: Operators



- *Logical State of a CPS* is a vector of *logical state parameters* $<L_1, \ldots, L_n>$
- the logical state is acted upon by algorithms $TL_1, \ldots, TL_k$ (each can be viewed as an operator on $<L_1, \ldots, L_n>$, resulting in $<L'_1, \ldots, L'_n>$;
- *Physical state of a CPS* is a vector of *physical state parameters* $<P_1, \ldots, P_m>$;
- a physical state vector is a solution to an algebraic system of differential equations (each equation describing a *waveform* for a choice of free variables)

Mathematical Models of CPS: Interactions

- a logical interaction or *message* in a CPS is an exchange of data or information between its components
- a physical interaction or *influence* in a CPS is an exchange of energy (in some form) between its components; derivatives of one parameter, w.r.t. one or more other physical state parameters, represent these dependencies
- the *algorithms of a CPS* are instances of distributed computation, i.e., multiple components may be performing parts of the computation and their outputs are shared through messaging.
- the derivatives of a physical state parameter, w.r.t. one or more other physical state parameters, are the relations that represent these dependencies

Mathematical Models of CPS: Interaction Calculus

Because the interactions of a CPS are of three basic types, calculations with them are best formalized as a kind of ‘inner product’ (much as vectors in vector algebra where the inner product of two vectors is a third vector orthogonal to both)

- We let alpha $<\Psi|\beta>$ denote the *interaction frame* of the calculus, where Ψ denotes an interaction and β denotes a state in the logical or physical state space of the CPS.
- Ordinary concatenation of interaction frames will be used to denote composition of interactions of the CPS.
- Composition of logical (or physical) interactions are represented by ordinary concatenation: $\Phi<\Psi|\alpha> = <\Phi\Psi|\alpha>$ only if both Φ and Ψ are both logical (or physical)

Mathematical Models of CPS: Formalizing Cyber2Physical and Physical2Cyber Interactions

- A value for the jth logical state parameter and is an element of the payload of a logical interaction of a CPS.
- If the jth logical state parameter is dedicated to the control of a physical state variable representing the kth differential equation in the description of the physical system (P_k is active)

Mathematical Models of CPS: 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}.

Mathematical Models of CPS: 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 theory**

Mathematical Models of CPS: 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**

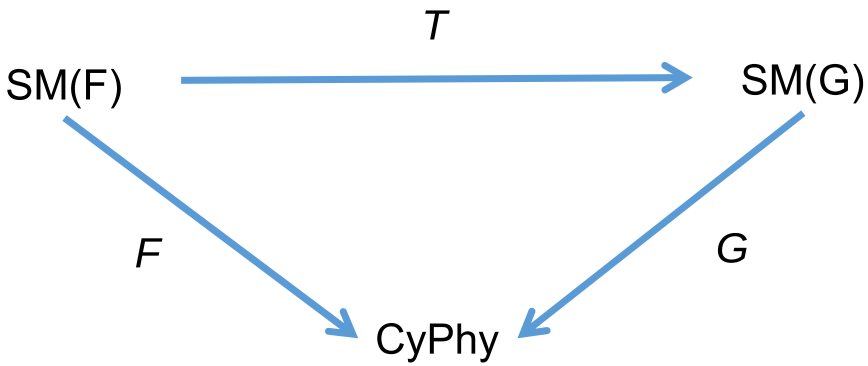
Benefit of this representation can be derived from:

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

Mathematical Models of CPS: 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:



Trustworthiness ‘Deep Dive’ FY18

- ***Trustworthiness Aspect of the CPS Framework***
  - ’Ontology’ of Trustworthiness (object and relations between them)
  - Composition and Interaction between CPS Concerns
- ***Logical and Physical ‘Security***
  - Using physics to enhance cybersecurity
- ***Dependencies between concerns*** (holistic approach to the specifics of individual concerns)
  - Tradeoffs
  - Quantifying tradeoffs between concerns