NIST Cyber-Physical Systems Program

Chris Greer
Senior Executive for Cyber-Physical Systems

Outline

- CPS Framework – Aspects and Facets
- Framework and Formal Logic
- Trustworthiness and Cybersecurity

CPS Framework - NIST CPS Public Working Group

Co-Chairs	Reference Arch	Use Cases	Security	Timing	Data Interop
NIST	Abdella Battou	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, Ed Griffor (now at NIST)	Stephen Mellor	Claire Vishik	Sundeep Chandhoke	Peggy Irelan, Eve Schooler

Co-Leads: Ed Griffor, Dave Wollman

pages.nist.gov/cpspwg

Framework Ver. 1.0 Published May 2016

Framework for Cyber-Physical Systems

Release 1.0

May 2016

Cyber Physical Systems Public Working Group

CPS Framework Structure

Domains

- **Manufacturing**
- **Transportation**
- **Energy**
- **Healthcare**
- **others …**

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

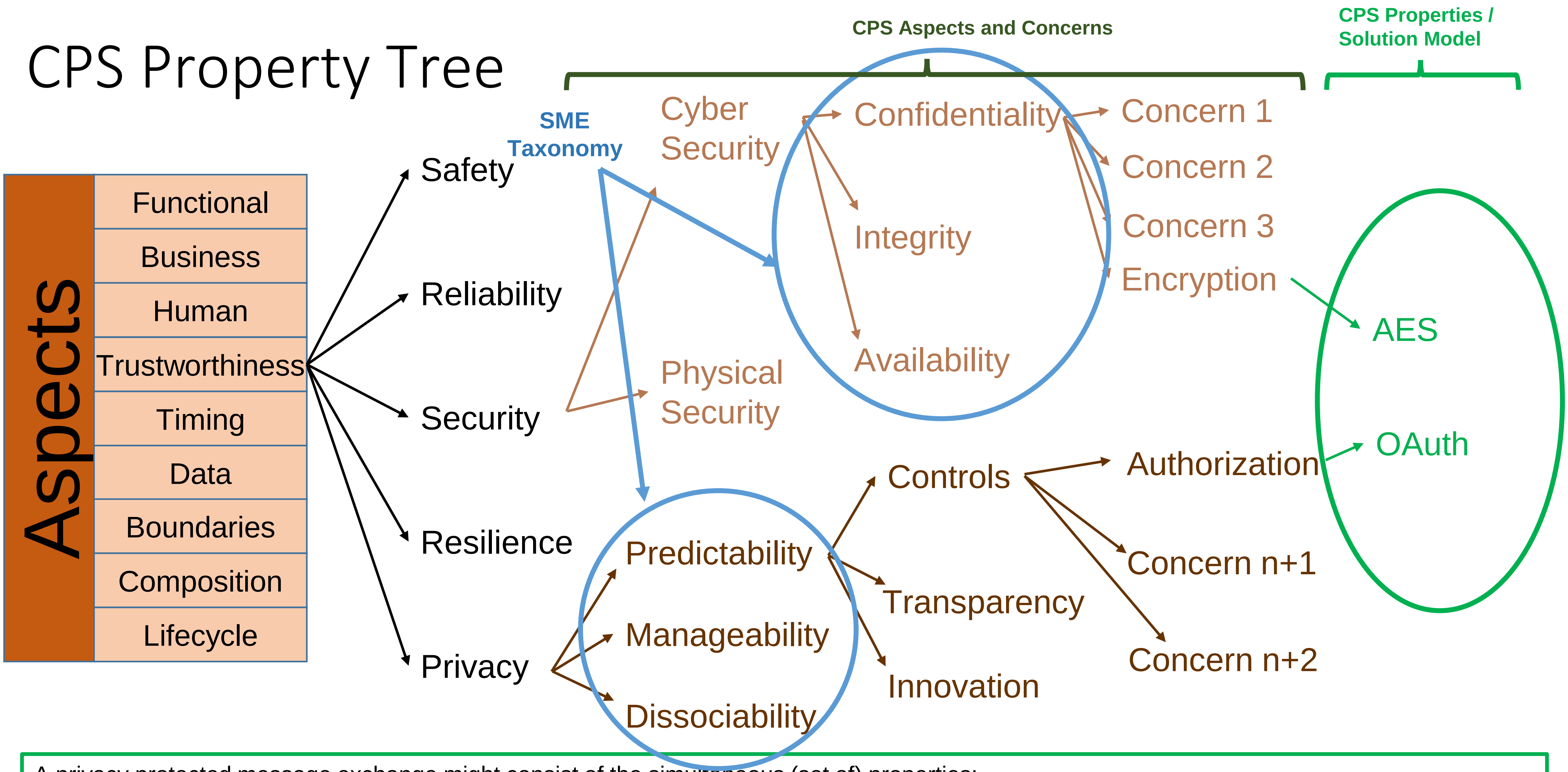
Aspects

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

Outline

- CPS Framework – Aspects and Facets
- Framework and Formal Logic
- Trustworthiness and Cybersecurity

CPS Property Tree



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

Interactions between Concerns

- The conceptualization facet provides **functional decomposition**
- The **tree of concerns** provides:
  - the **decomposition of concerns** (such as Security, decomposed into Physical Security and Cybersecurity)
  - Is a **schema for applying concerns** to a CPS

Concerns and their Interaction Calculus

Derivation of a property P for a CPS function in a context of concerns:

<f a function, concern context Γ, property P>, denoted by $\Gamma \vdash P(f)$

Consisting of:

- **CPS function** f from the Business and Use Case of a CPS
- Γ a '**path**' through the Concern Tree, **rooted** in the Aspects and **providing context for** the function f
- requires the **property P of the function f**

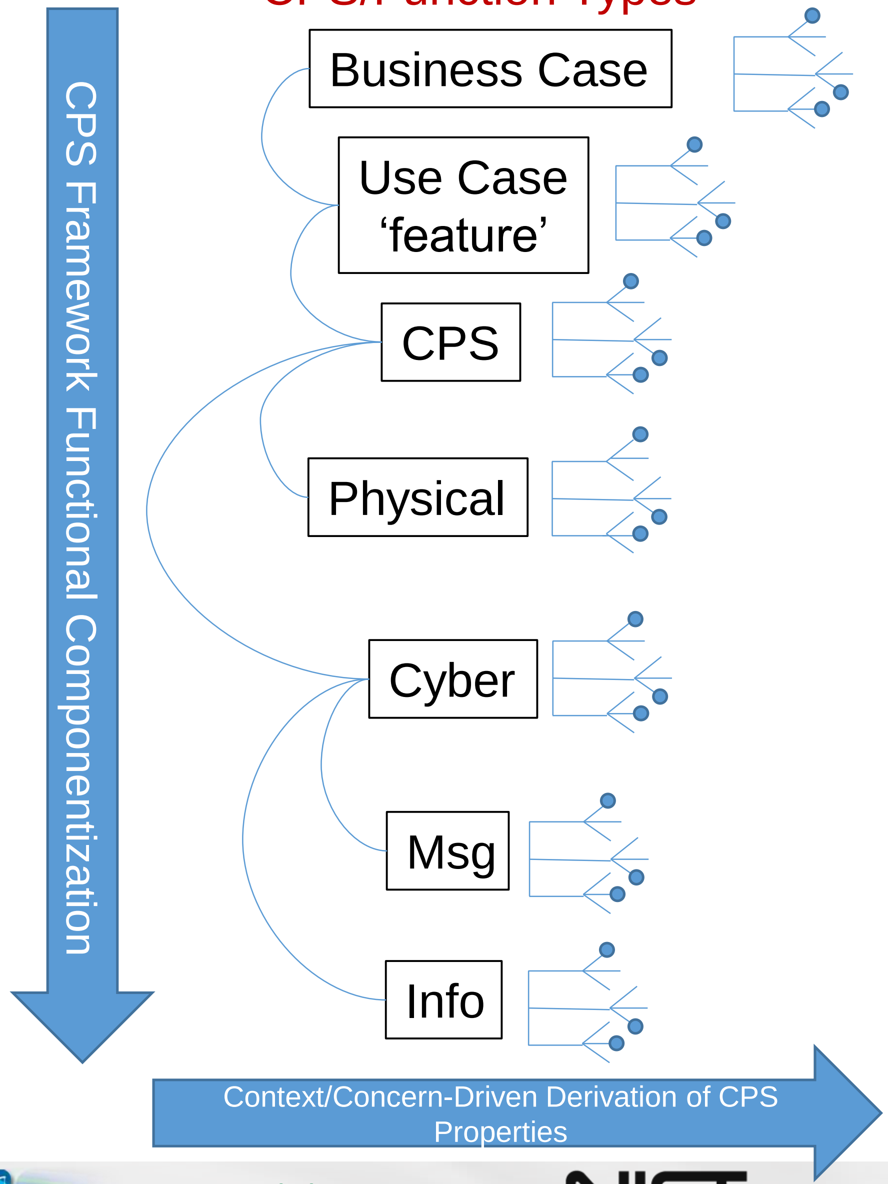
Example: A **secure**, **privacy-protected** message exchange might consist of the simultaneous (set of) properties:

- <f = message exchange, Γ = **Trustworthiness.Security.Cybersecurity.Confidentiality.Encryption**, P=**AES**(.)>
- <f = message exchange, Γ' = **Trustworthiness.Privacy.Predictability.Controls.Authorization**, P'=**OAuth**(.)>

Define the function denoted by f to be [f] = {g| g has properties Trustworthiness.Security.Cybersecurity.Confidentiality.Encryption.AES, Trustworthiness.Privacy.Predictability.Controls.Authorization.OAuth}

Framework Functional Decomposition

CPS/Function Types



Properties of System Functions (Example)

Safety – vehicle provides its function safely/without collision

Safety – vehicle provides/maintains safe stopping distance

Safety –braking function reacts as required

Safety – friction function provides appropriate friction

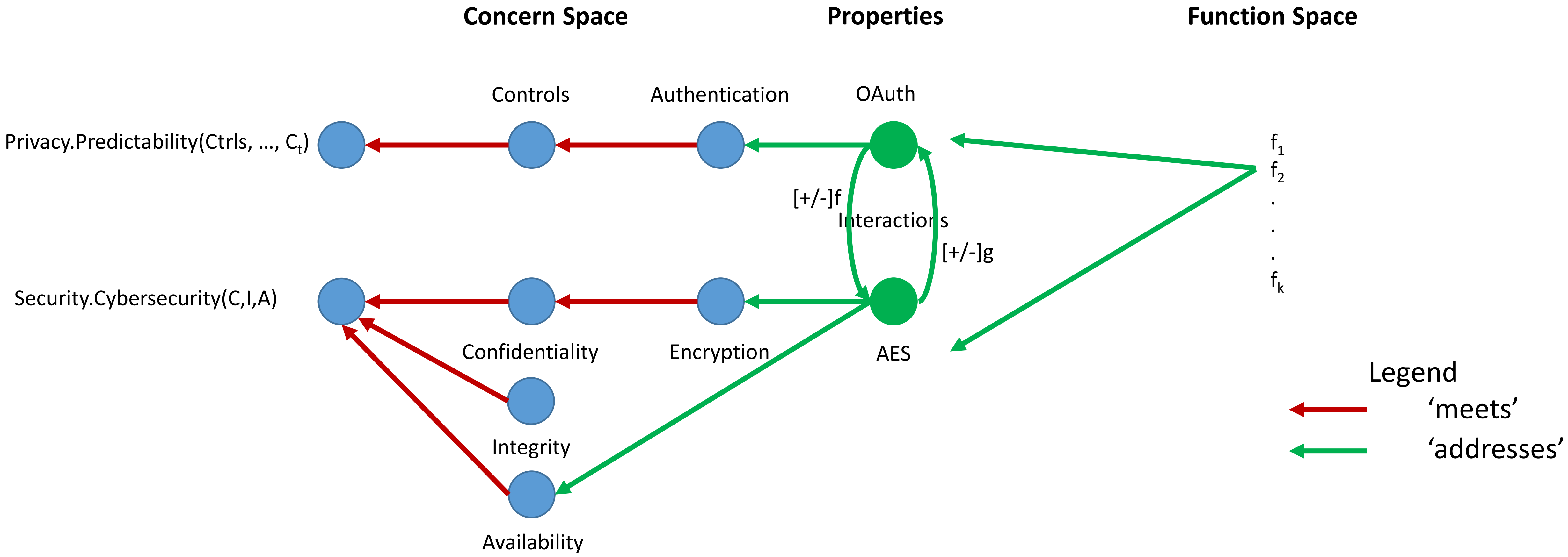
Safety – stopping algorithm function has safe stopping

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

Safety – distance and speed info is understood by braking function

Functions as Sets of Properties

CPS Framework: The Interaction Calculus



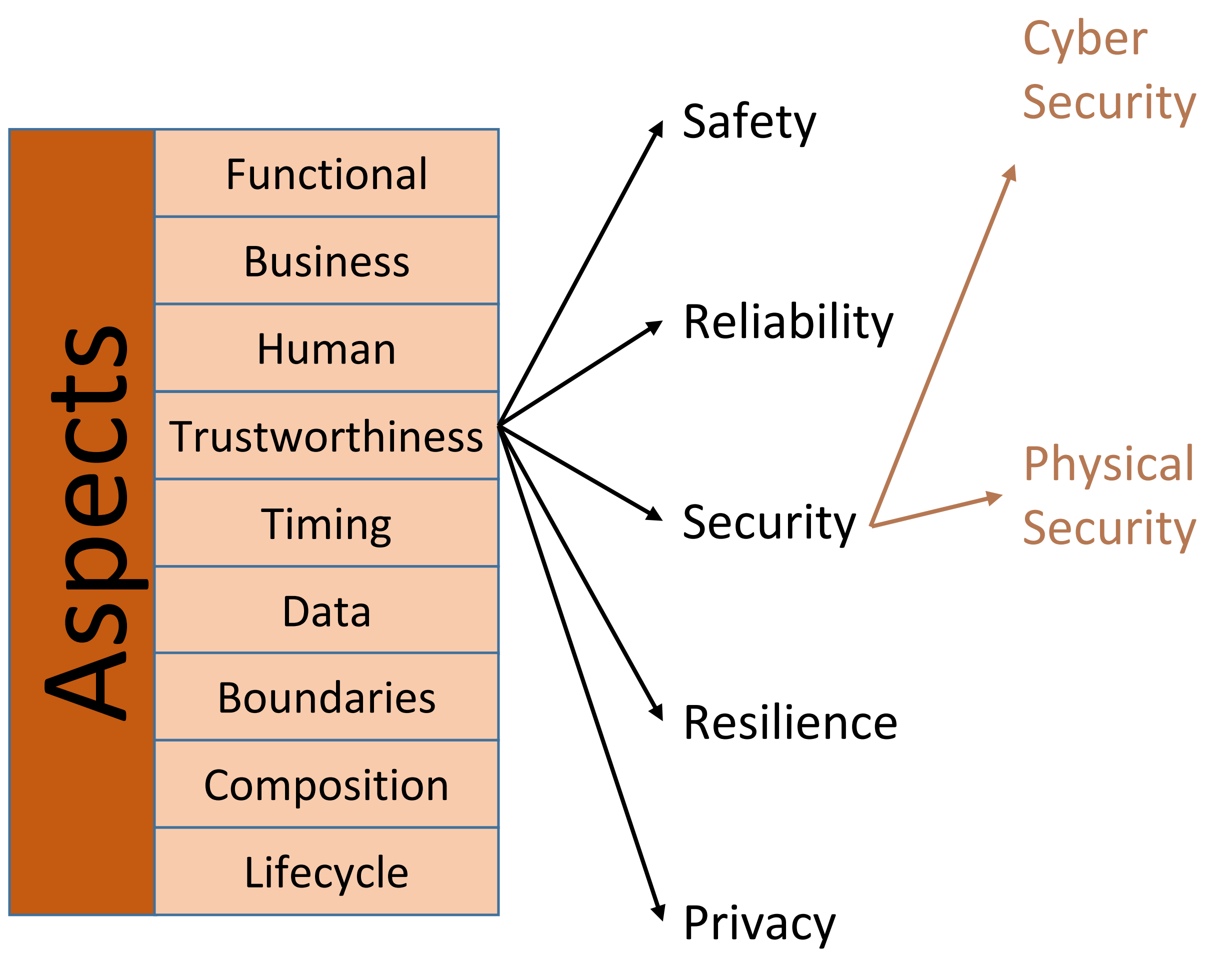
Example Impact of one concern on another:

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

Outline

- CPS Framework – Aspects and Facets
- Framework and Formal Logic
- Trustworthiness and Cybersecurity

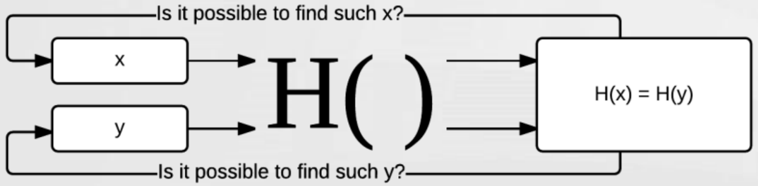
Trustworthiness and Cybersecurity



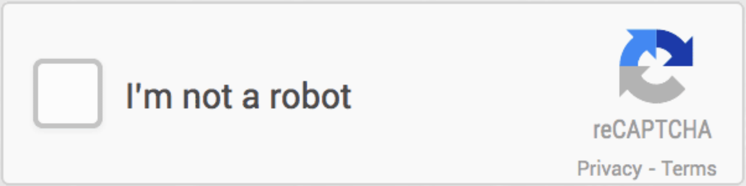
Trustworthiness <Safety.Reliability.Security.Resilience.Privacy>

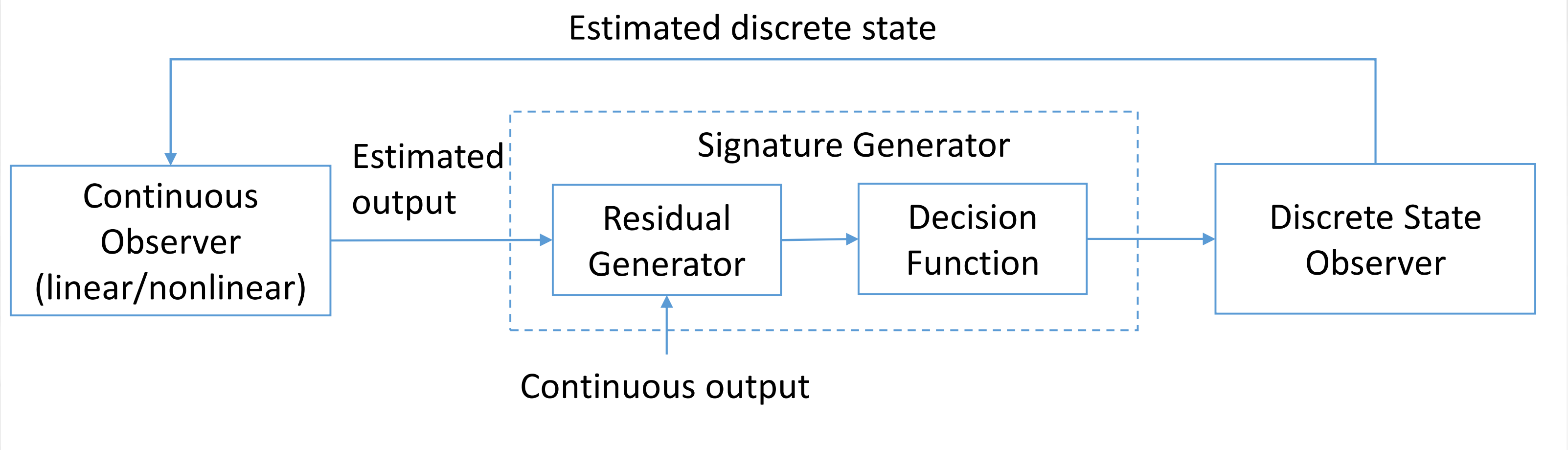
Using physical dynamics to detect intrusions

The null space of H is analogous to collision resistance criteria for hash functions used to secure passwords.



Consider the recent trend towards using noCaptcha reCaptchas to identify bot/ brute force attacks on the hashing algorithm.





- Knowledge about dynamic state variables
- Higher fidelity models of transients
- Probabilistic dependencies between state variables
- Electrical correlation + Environmental correlation

We are at a unique position in being able to do this with advent of sensing and measurement investments made to the power system to capture dynamic or transient states.

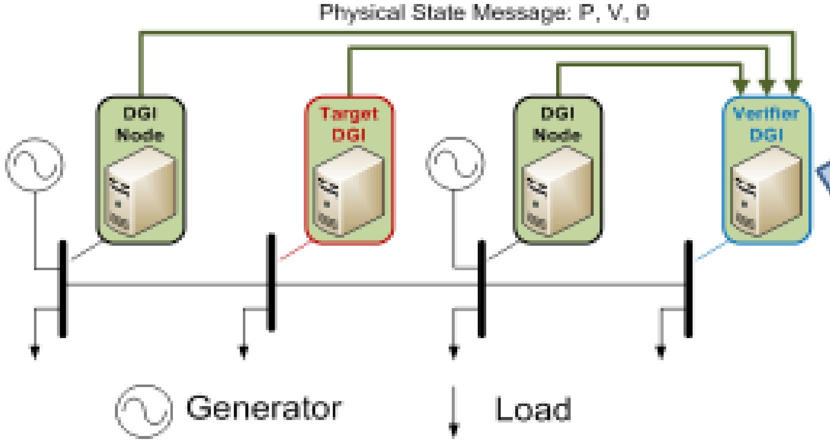
Physical Attestation in the Smart Grid for Distributed State Verification

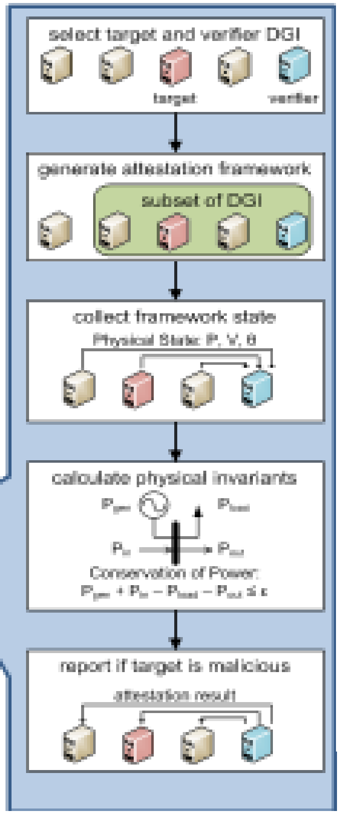
Thomas Roth, *Member, IEEE,* Bruce McMillin, *Senior Member, IEEE,*

DOI 10.1109/TDSC.2016.2577021

Physical Attestation

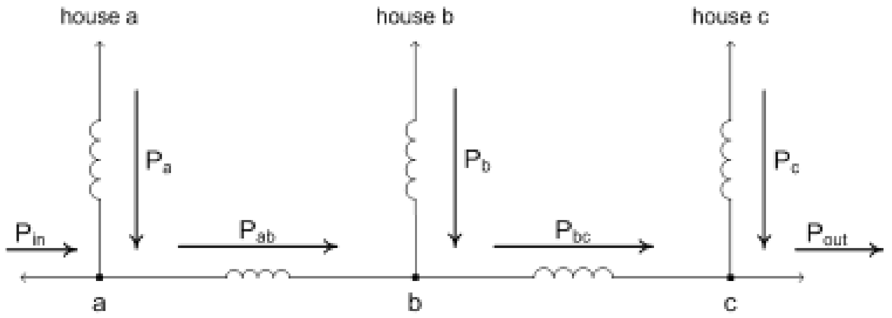
- A distributed security mechanism that utilizes physical invariant violations to detect malicious peers.
- Programmed into the distributed grid intelligence (DGI) at smart inverters.





Physical Invariants

- The physical system must satisfy a set of physical laws which are system invariants that hold throughout system execution.
- Conservation of Power at b: $\{I_b : P_{ab} + P_b - P_{bc} = 0\}$



- If I_b is violated, then at least 1 of $\{P_{ab}, P_b, P_{bc}\}$ must be falsified.

Outline

- CPS Framework – Aspects and Facets
- Framework and Formal Logic
- Trustworthiness and Cybersecurity

For additional information

- Program Web Site:
  www.nist.gov/cps
- CPS Public Working Group
  www.nist.gov/cps/cpspwg.cfm
- CPS Framework Release 1.0
  https://pages.nist.gov/cpspwg
- Contact:
  edward.griffor@nist.gov