

Cyber-Physical Systems Framework

NASA Goddard Colloquium
12 October 2016

Dr. Edward Griffor, Associate Director
Cyber-Physical Systems



engineering laboratory



National Institute of Standards and Technology • U.S. Department of Commerce

Outline

- CPS Framework – Aspects and Facets
- Interactions Across Aspects and Facets
- Expanded Mitigation Surface
- SAE Collaborative Agreement – Trustworthy Autonomous Vehicles

CPS Framework Structure

Facets

- Domains
- Manufacturing
- Transportation
- Energy
- Healthcare
- others ...

Aspects	Functional
	Business
	Human
	Trustworthiness
	Timing
	Data
	Boundaries
	Composition
Lifecycle	

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 arguments)



Model of a CPS CPS CPS Assurance



Outline

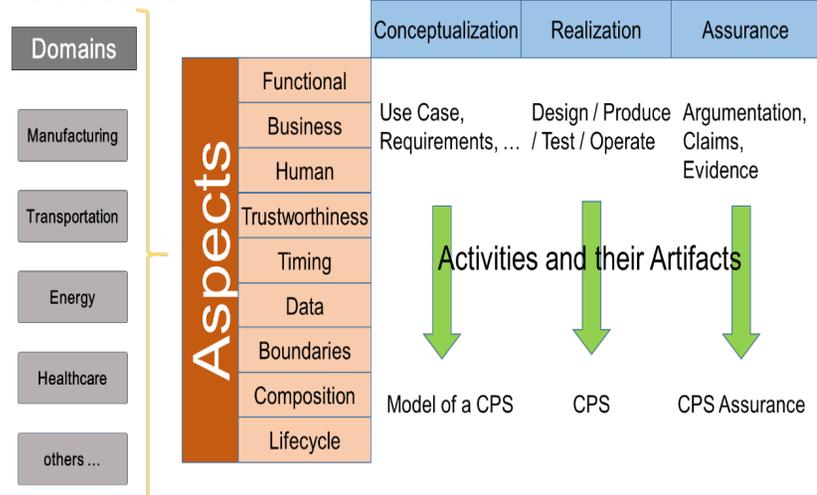
- CPS Framework – Aspects and Facets
- **Interactions Across Aspects and Facets**
- Expanded Mitigation Surface
- SAE Collaborative Agreement – Trustworthy Autonomous Vehicles

CPS Public Working Group

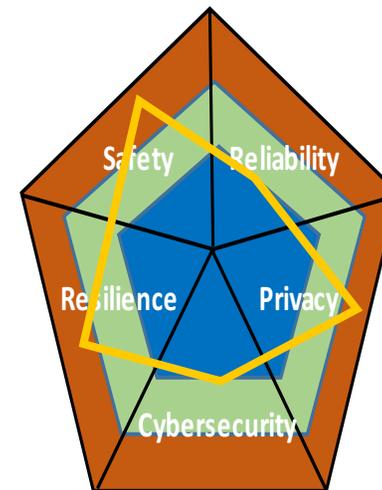
- Provides technical, concern-driven foundation for CPS/IoT: CPS Framework
- NIST leadership w/industry, academia, government; CPS experts in 5 working groups have contributed to draft CPS Framework, now revised based on public review comments and released in May 2016.
- EL, ITL, PML collaborative effort (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



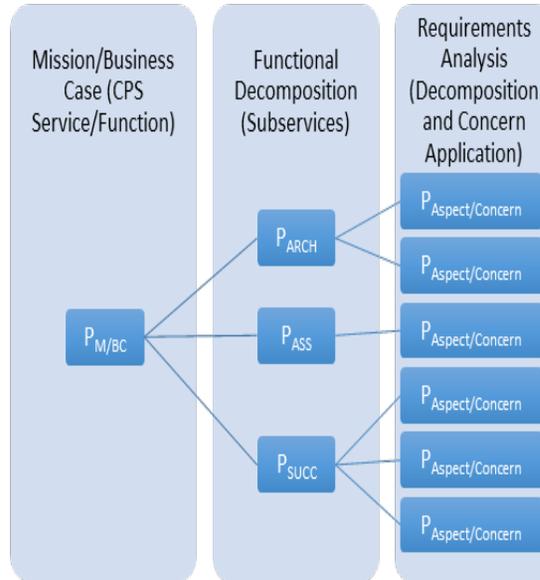
CPS Framework Mathematics

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)



semantics of CPS Framework

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

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

$$\text{Supp}_M(T) = \{\text{measurement support } \mu_1, \dots, \mu_k \text{ of } T\}$$

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

... defines **composition of concern**:

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

formal methods for assurance

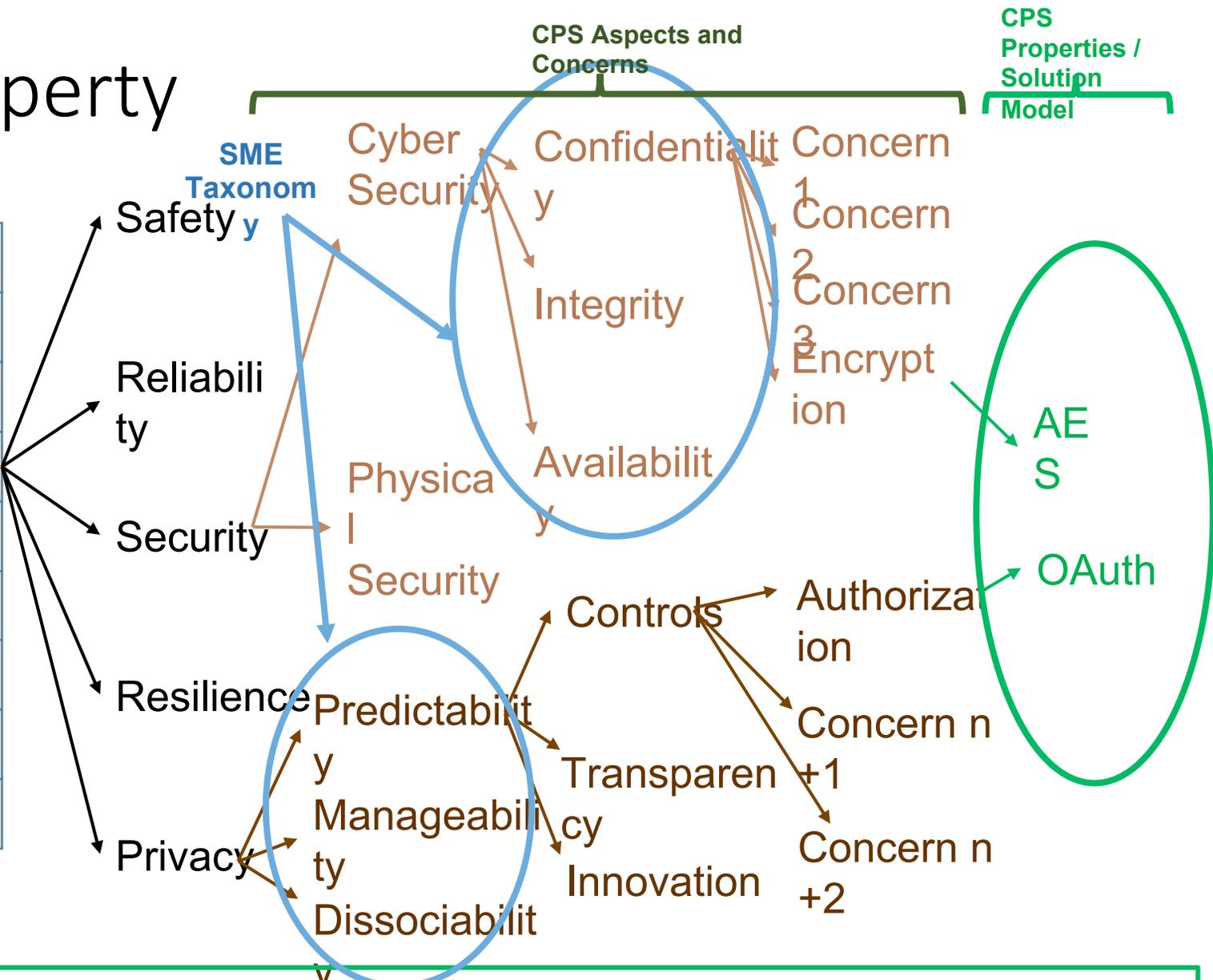
of a CPS
 $\langle a, e, a \rangle \in P(CPS) \equiv_{Def}$ design element d , test evidence e are

sufficient based on argument a to conclude that the CPS satisfies P

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

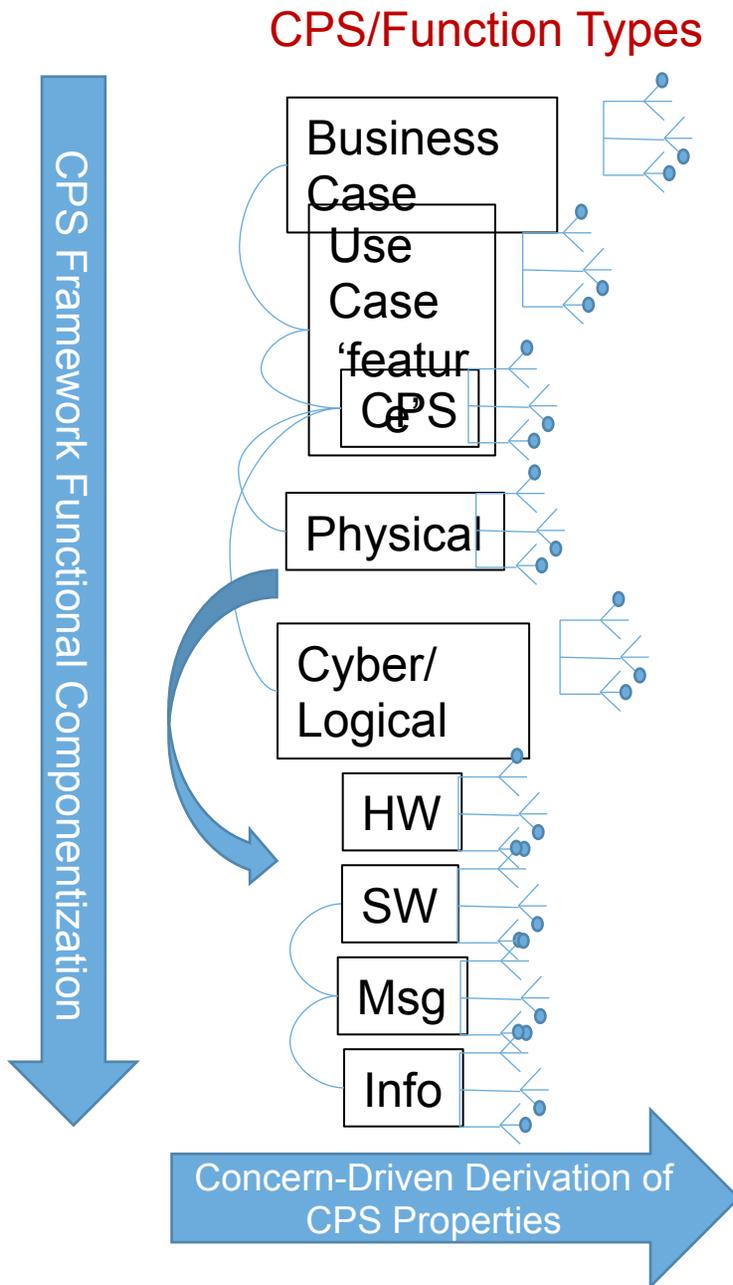
CPS Property Tree

Aspects	Functional
	Business
	Human
	Trustworthiness
	Timing
	Data
	Boundaries
	Composition
	Lifecycle



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



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

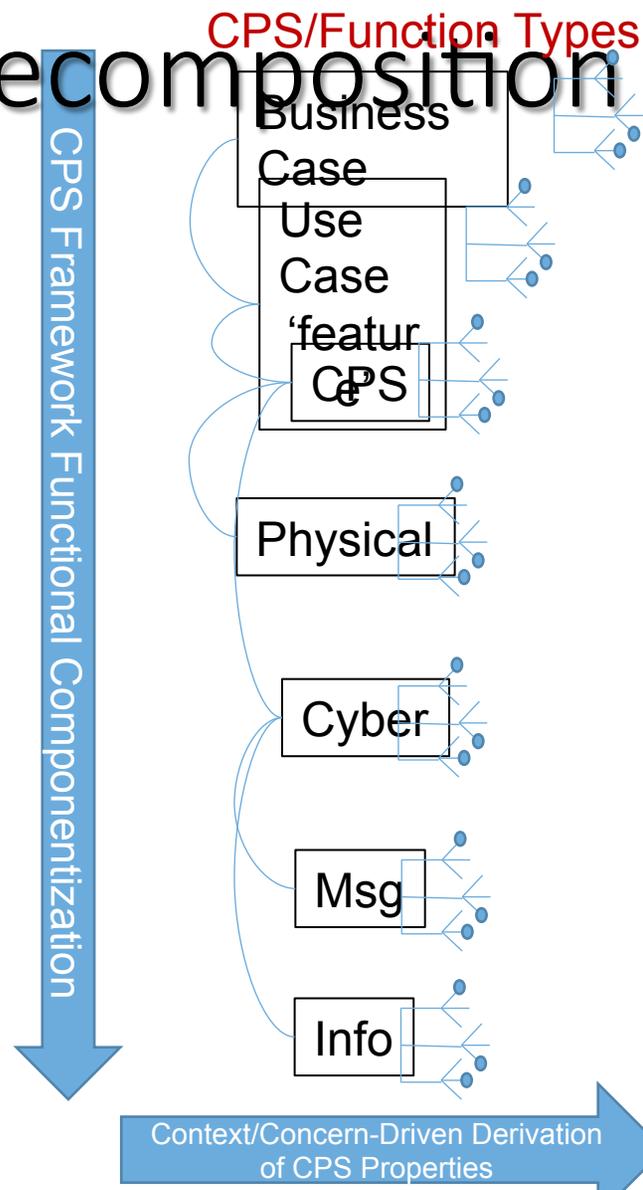
Example: Trustworthiness

0	Trustworthiness	Concerns about trustworthiness of CPS including cybersecurity, privacy, safety, reliability, and resilience.
1	privacy	Concerns related to the ability of the CPS to prevent entities (people, machines) from gaining access to data stored in, created by, or transmitted through the manipulation of physical environments. Privacy is a condition that results from maintenance of a collection of methods to support the mitigation of risks to individuals arising from the processing of their personal information.
1	reliability	Concerns related to the ability of the CPS to deliver stable and predictable performance in expected conditions.
1	resilience	Concerns related to the ability of the CPS to withstand instability, unexpected conditions, and gracefully return to predictable, but possibly degraded, performance.
1	safety	Concerns related to the ability of the CPS to ensure the absence of catastrophic consequences on the life, health, property, or data of CPS users in their environment.
1	security	Concerns related to the ability of the CPS to ensure that all of its processes, mechanisms, physical and data, and services are afforded integrity, confidentiality, and availability. Confidentiality: Integrity: Availability:
2	cybersecurity	Concerns about cybersecurity.
3	confidentiality	Preserving authorized restrictions on access and disclosure.
3	integrity	Guarding against improper modification or destruction of system, and includes ensuring non-repudiation and authenticity.
3	availability	Ensuring timely and reliable access to and use of a system.
2	physicalsecurity	Concerns about physical security.

Concern
'cascade' for
Trustworthiness:

- Level 0 is an 'aspect'
- Level 1 are the primary sub-concerns
- Level 2 are decompositions of Level 1 concerns

Framework Functional Decomposition



CPS/Function Types

Properties of System Functions
(Automatic Emergency Braking)

AEB – vehicle provides automated collision safety

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 b function

Context/Concern-Driven Derivation of CPS Properties

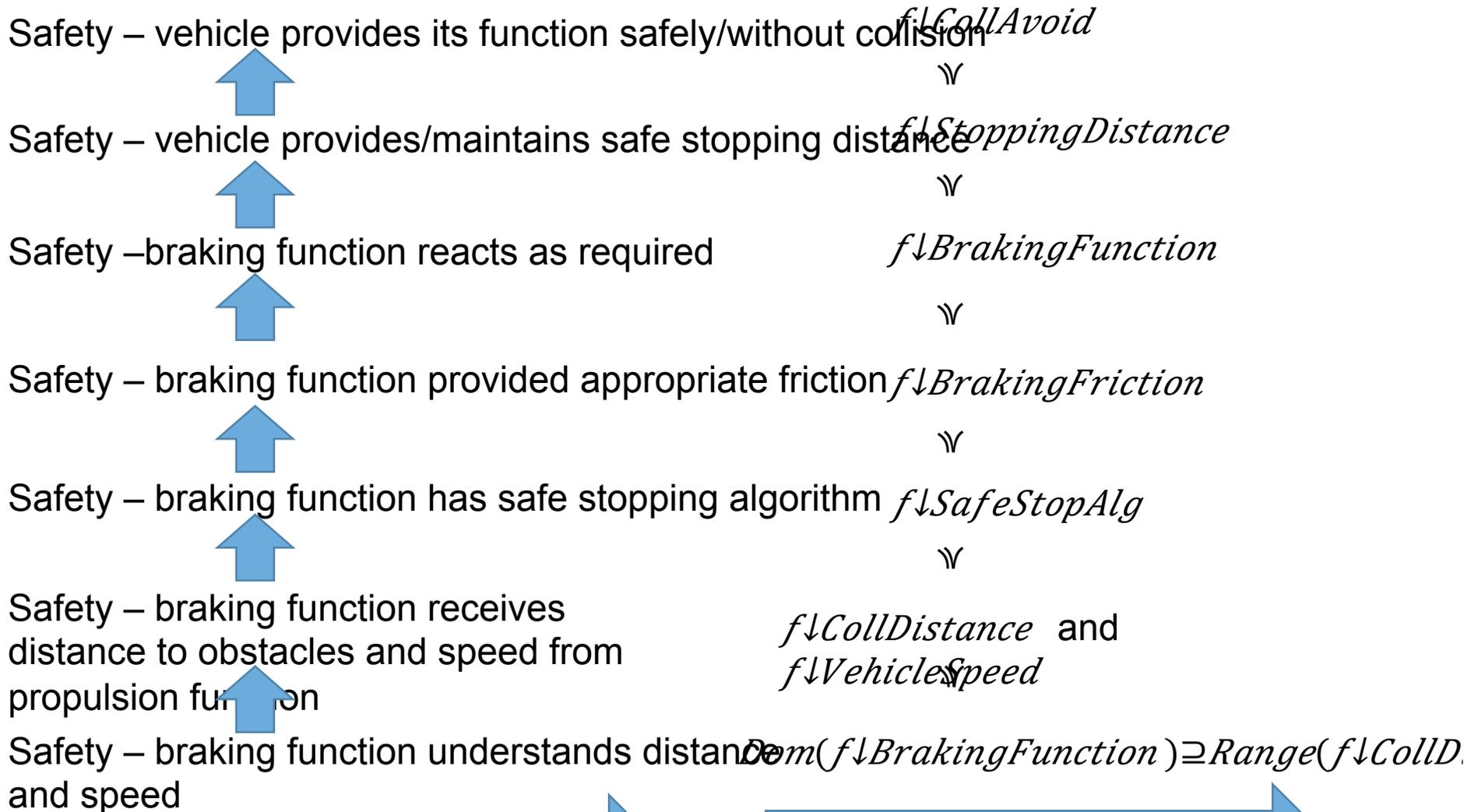
Functions as Sets of Properties



Hierarchy of Functions of a CPS

Properties of System Functions (AEB)

Function Hierarchy



Dependencies

Function Hierarchy

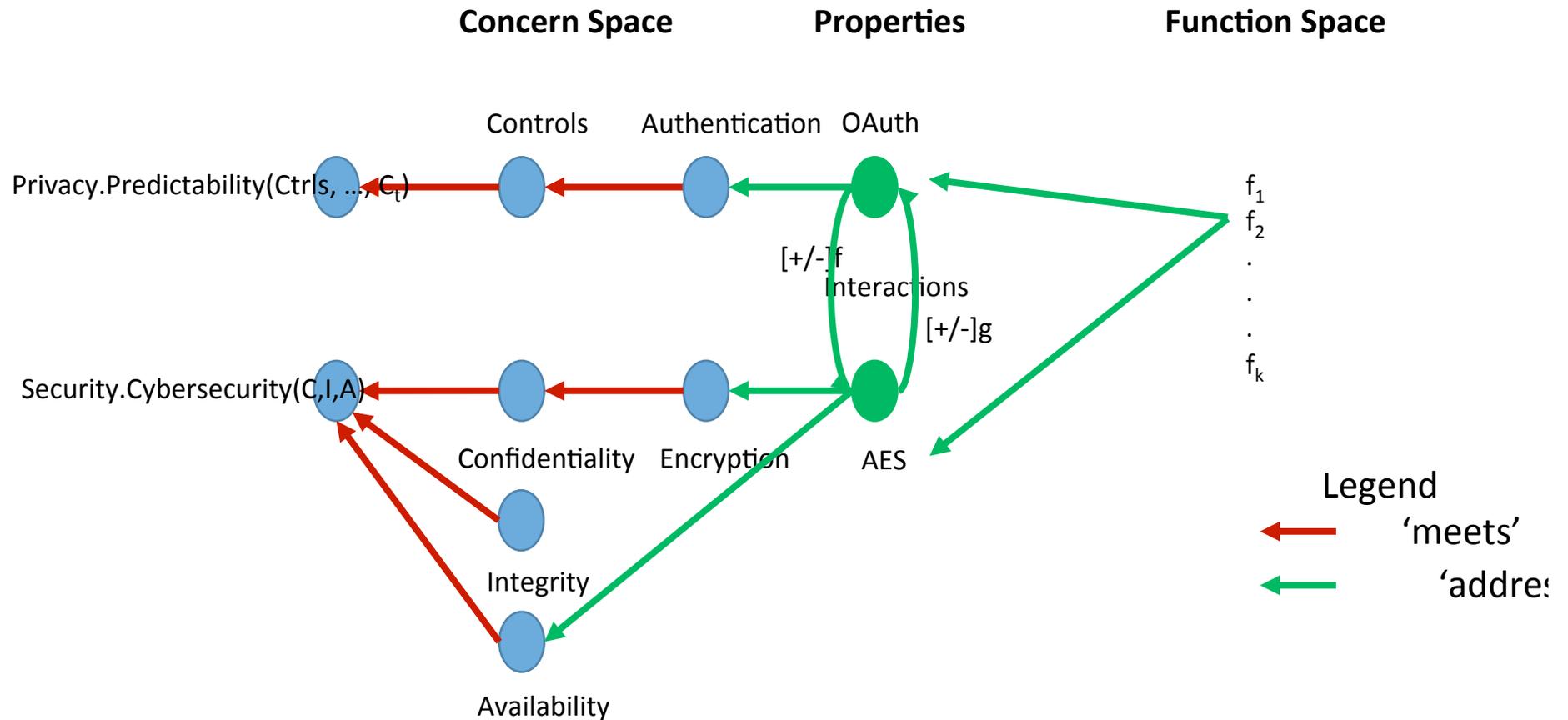


engineering laboratory



National Institute of Standards and Technology • U.S. Department of Commerce

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)

Outline

- CPS Framework – Aspects and Facets
- Interactions Across Aspects and Facets
- **Expanded Mitigation Surface**
- SAE Collaborative Agreement – Trustworthy Autonomous Vehicles

IT vs IoT/CPS Threats

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

Better Cybersecurity Through Physics

GPS is vulnerable to spoofing attacks. Here's how we can defend these important navigation signals

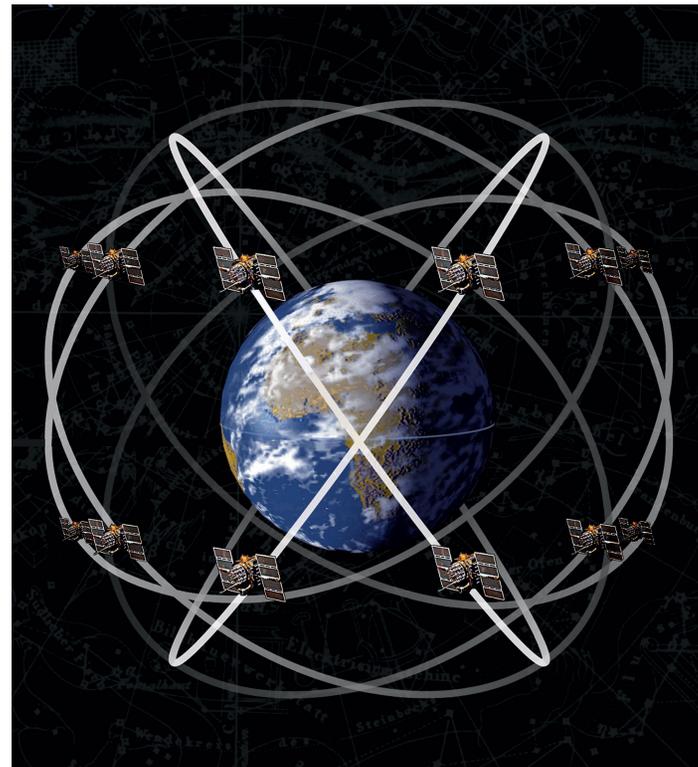
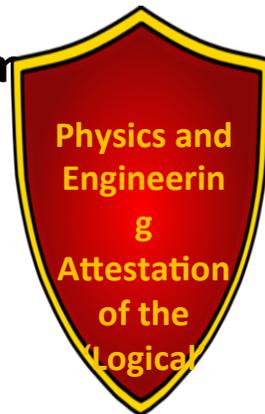
By Mark L. Psiaki and Todd E. Humphreys

Posted 29 Jul 2016 | 19:00 GMT

Cornell/Virginia Tech

UT Austin

IEEE Spectrum
29 Jul 2016



Outline

- CPS Framework – Aspects and Facets
- Interactions Across Aspects and Facets
- Expanded Mitigation Surface
- SAE Collaborative Agreement – Trustworthy Autonomous Vehicles



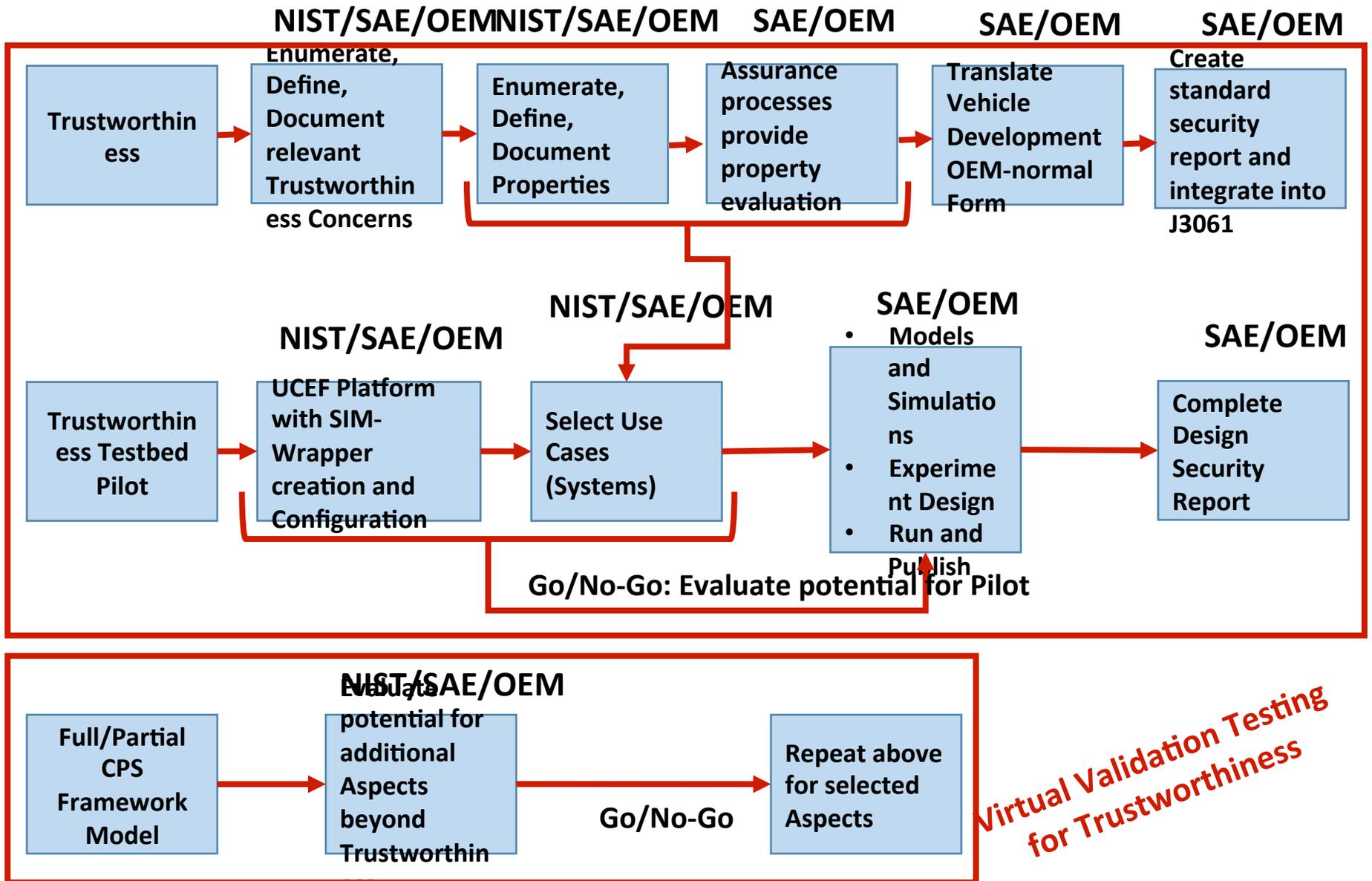
SAE-NIST Collaboration Meeting
 Week of Sep 25, 2016- date TBD
 755 W. Big Beaver Rd., Suite 1600
 Troy, MI
 Room TBD

Contacts: Tim Weisenberger, SAE International: tim.weisenberger@sae.org, tel. 248.840.2106
 Mary Doyle, SAE International: mary.doyle@sae.org, tel. 248-273-2467
 Ed Griffor, NIST: edward.griffor@nist.gov, tel. 301-973-4743

Item	Required	Lead	
1. Welcome and Introductions.		SAE Staff	10:10-11:00
2. Agenda changes/additions, Anti-trust, Patent Disclosure, Transparency, and IP statements are reviewed.		SAE Staff	10:10-11:00
3. Administration of the collaboration a. Goals for the collaboration (for each side) b. Structure of the group- working group, cooperative research project, dedicated resources, etc. c. Stakeholder voices needed d. End product(s)- SAE standard document, s/w package, Test/Certification Process doc, Federated test bed s/w tool, etc.		SAE Staff	10:10-11:00
4. Scoping The Work- covers items 5-12		Ed Griffor, NIST, Lisa Boran, Ford	10:10-11:00
5. Trustworthiness Development Process a. Model for the development process- Ed presentation b. Review current automotive cybersecurity activities and their positioning in the vehicle development process- Lisa lead		Ed Griffor, NIST, Lisa Boran, Ford	10:10-11:00
6. Break			11:00-11:15
7. Automotive Trustworthiness Concerns a. Background material from the CPS Framework's trustworthiness aspect- Ed presentation b. DISCUSSION: Enumerate, define and document the automotive trustworthiness concerns, including any potential obstacles to the proposed platform useful to all the stakeholder organizations c. Working Lunch		Ed Griffor, NIST	11:15-12:00
9. Automotive Trustworthiness Requirements a. DISCUSSION: Rough in the high-level, functional objectives for the chosen trustworthiness concerns and their metrics		Lisa Boran- Ford	12:00-12:15
10. Trustworthiness Testbed Requirements and Use Cases a. Intro to the NIST federated testbed- Ed presentation b. DISCUSSION: i. Joint approach to security testbed components ii. Potential obstacles to a security co-simulation platform useful to all the stakeholder organizations		Ed Griffor, NIST	12:15-1:00
11. Working with J3061 as a baseline- How does this new work fit? E.g.- Add-on above work as a Proto-Security Case- enumeration data and data structure for potential J3061 Annex		Lisa Boran- Ford	1:15-1:30
12. Work Breakdown/Approach		SAE Staff	1:45-2:00

Trustworthiness Development/Testing/Reporting Form

- Plan and RASIC



Virtual Validation Testing for Trustworthiness

Outline

- CPS Framework – Aspects and Facets
- Interactions Across Aspects and Facets
- Expanded Mitigation Surface
- SAE Collaborative Agreement – Trustworthy Autonomous Vehicles

For additional information

- Program Web Site:

[**www.nist.gov/cps**](http://www.nist.gov/cps)

- CPS Public Working Group

[**www.nist.gov/cps/
cpspwg.cfm**](http://www.nist.gov/cps/cpspwg.cfm)

- CPS Framework Release 1.0

[**https://pages.nist.gov/
cpspwg**](https://pages.nist.gov/cpspwg)

- Contact:

[**edward.griffor@nist.gov**](mailto:edward.griffor@nist.gov)

Takeaways:

- Industry Example: The SAE Cybersecurity Committee, in its released J3061, has provided processes for identifying automotive system threats and for engineering mitigation of those threats into automobiles that:
 - is a Recommended Practice (just as with J2980 recommended practice on functional safety)
 - performs a TARA or Threat and Risk Analysis (in place of the ISO 26262/J2980 HARA)
 - ‘includes’ discussions of Privacy and Reliability (need to assess the sufficiency of these discussions)
 - leaves process open to 3 approaches to integration with the Functional Safety process of ISO 26262/J2980 (tight-coupling, loose-coupling or ‘systems engineering’ approach per J. Miller and B. Czerny)
 - addresses onboard or onboard vehicle cybersecurity
- Value that NIST CPS Framework’s trustworthiness aspect adds:
 - complements all three approaches to integrating cybersecurity with functional safety
 - broadly consensed-upon dimensions of trustworthiness, including security

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 **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:

$\langle f \text{ a function, concern context } \Gamma, \text{ property } P \rangle$, 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

- requires the **property P of the function f**

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

- $\langle f = \text{message exchange,}$
 $\Gamma = \textit{Trustworthiness.Security.Cybersecurity.Confidentiality.Encryption, } P = \text{AES}(\cdot) \rangle$
- $\langle f = \text{message exchange, } \Gamma \uparrow$
 $= \textit{Trustworthiness.Privacy.Predictability.Controls.Authorization, } P' = \text{OAuth}(\cdot) \rangle$

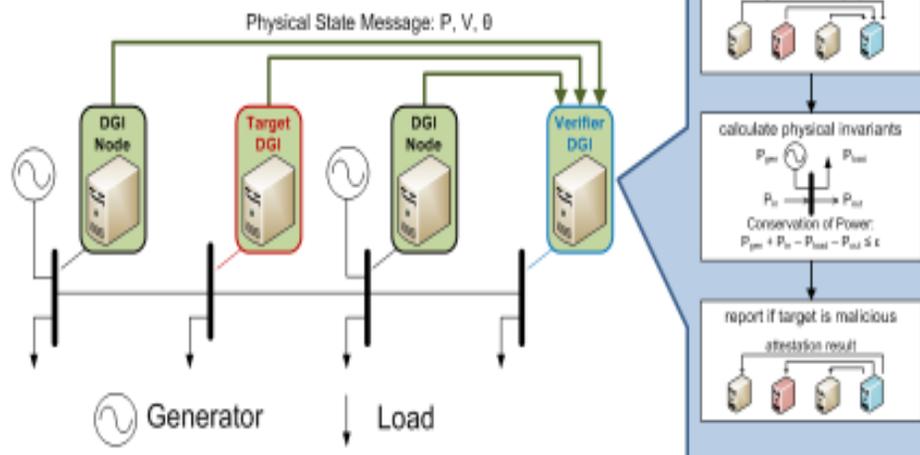
Physical Attestation in the Smart Grid for Distributed State Verification

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

DOI 10.1109/TDSC.2016.25770

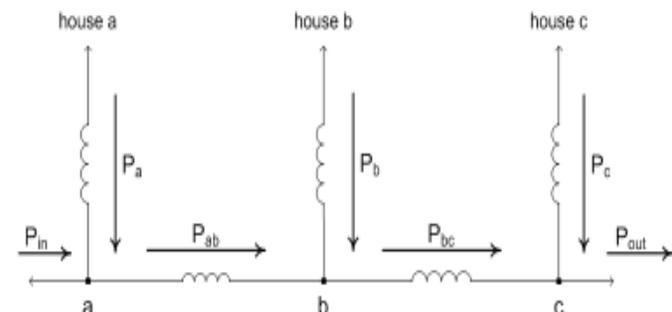
Physical Attestation

- 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.