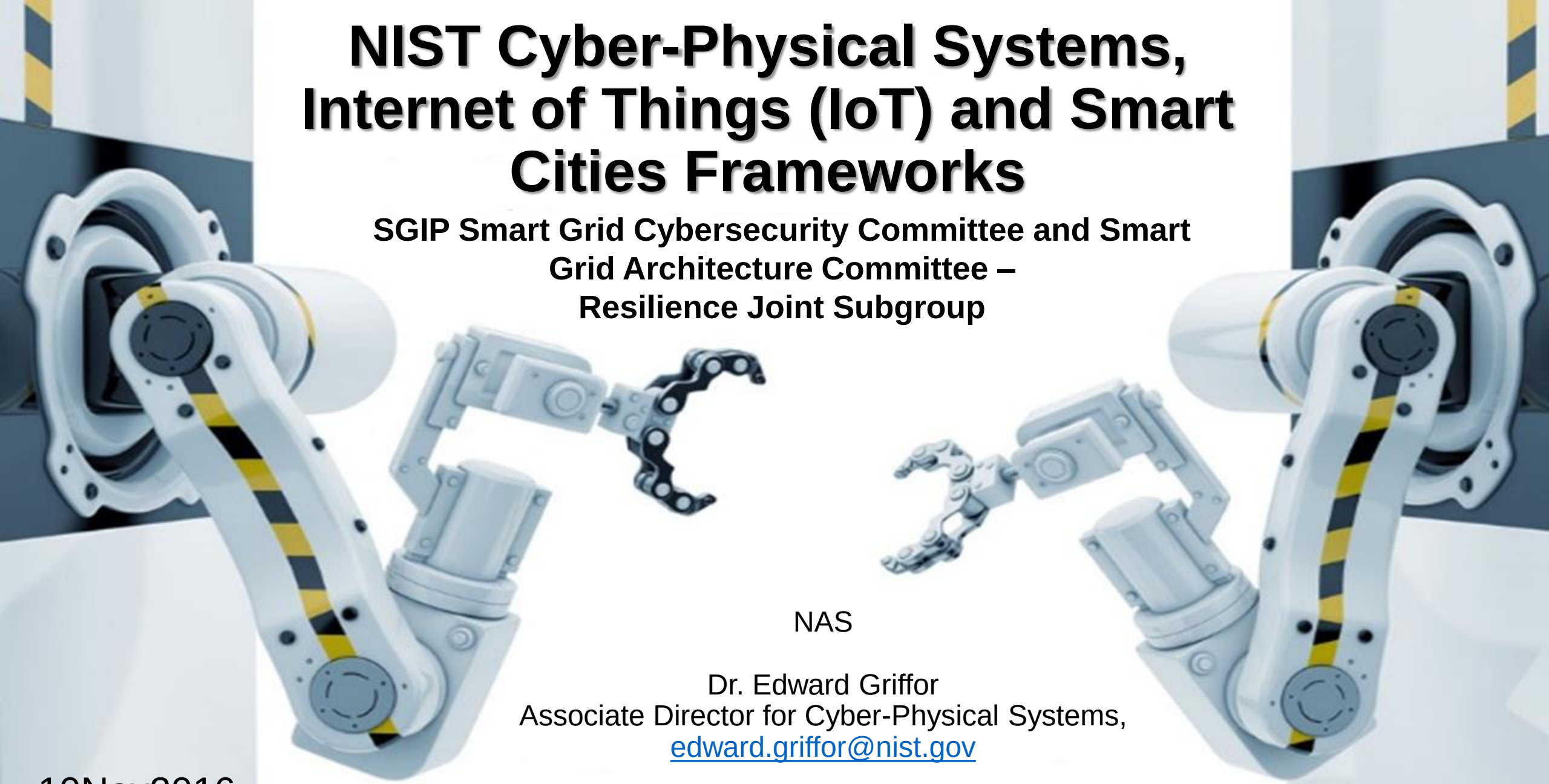
NIST Cyber-Physical Systems, Internet of Things (IoT) and Smart Cities Frameworks

SGIP Smart Grid Cybersecurity Committee and Smart Grid Architecture Committee – Resilience Joint Subgroup



NAS

Dr. Edward Griffor
Associate Director for Cyber-Physical Systems,
edward.griffor@nist.gov

10Nov2016

What the CPS Framework brings to grid?

- The grid has made significant investments in **safety**, **reliability and resilience** just as have other critical infrastructures
- The **smart grid** is an electricity supply network that uses communications technology to detect and react to changes in usage in order to reliably and resiliently meet demand
- Efficient reaction to grid change (failure and changing demand) involves **distributed, communicating, multi-modal generation**
- A **trusted source of electrical energy** is a 'must' for growing a modern economy
- Ubiquitous communications in the grid bring with them expanded vulnerability to both **physical and cyber attack** and so to failure
- The grid must invest also in security and privacy, i.e. ***trustworthiness***

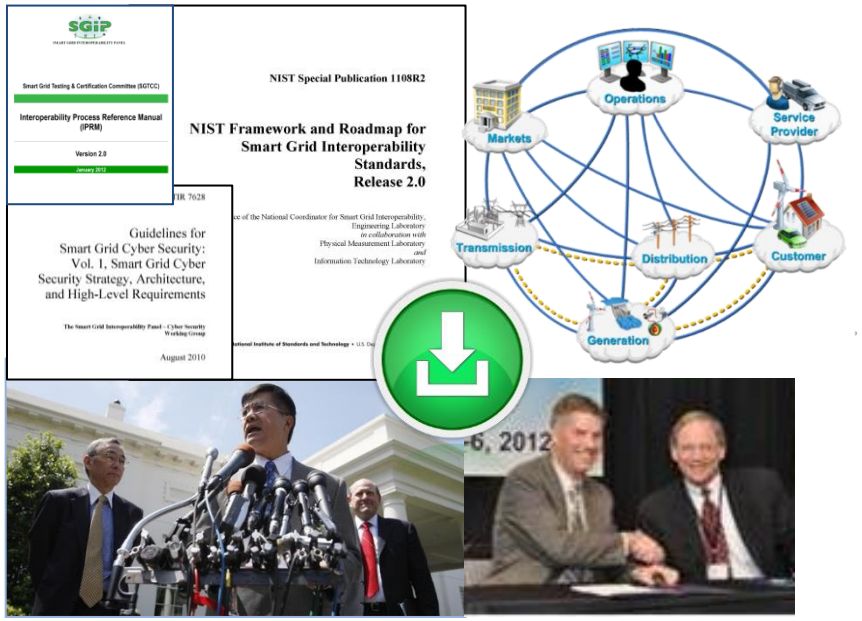
Outline

- Background
- CPS Framework – Aspects and Facets
- Interactions Across Aspects and Facets
- Expanded Mitigation Surface
- SAE Collaborative Agreement – Trustworthy Autonomous Vehicles
- Overview of the CPS Framework Open Source Project
- Open Source Project: Models and Tools

NIST Smart Grid Program

Energy Independence and Security Act (2007)

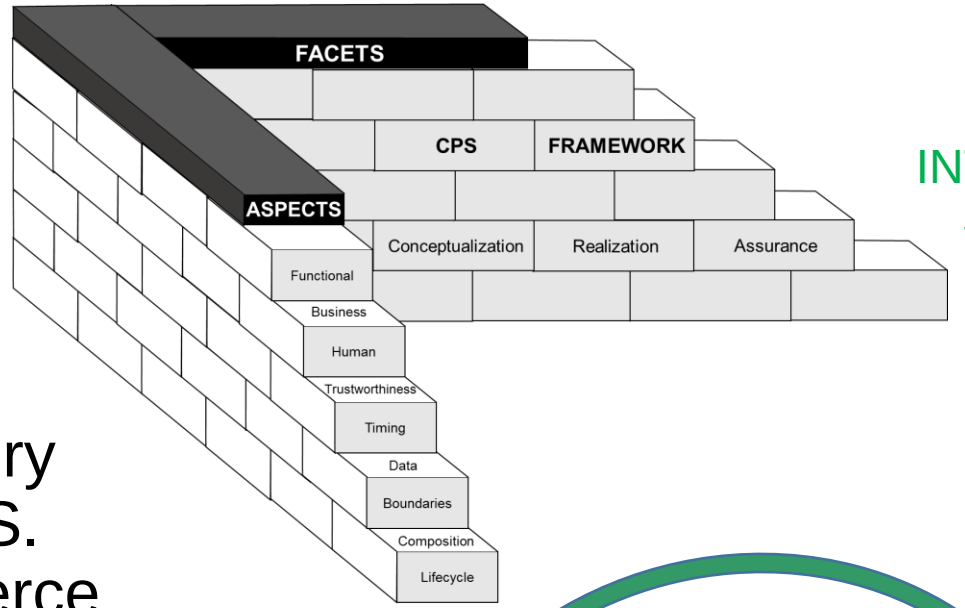
- NIST: to work with stakeholders to coordinate development of a consensus-based framework for smart grid interoperability standards: initial workshops, Smart Grid Interoperability Panel (SGIP), continued engagement…
- Smart Grid Interoperability Standards Coordination, R&D, Testbed



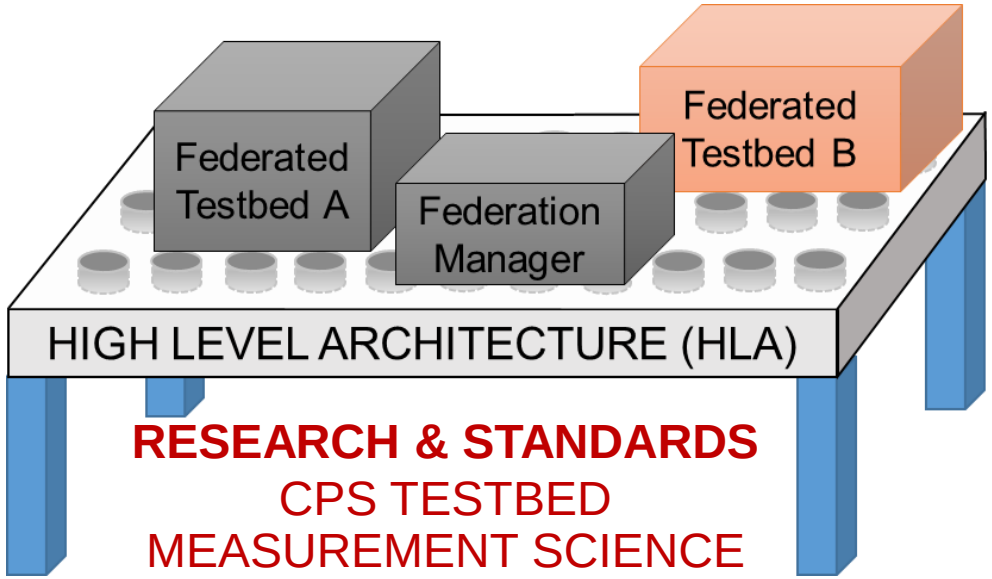
NIST smart grid testbed(s)

NIST CPS (IoT) Program

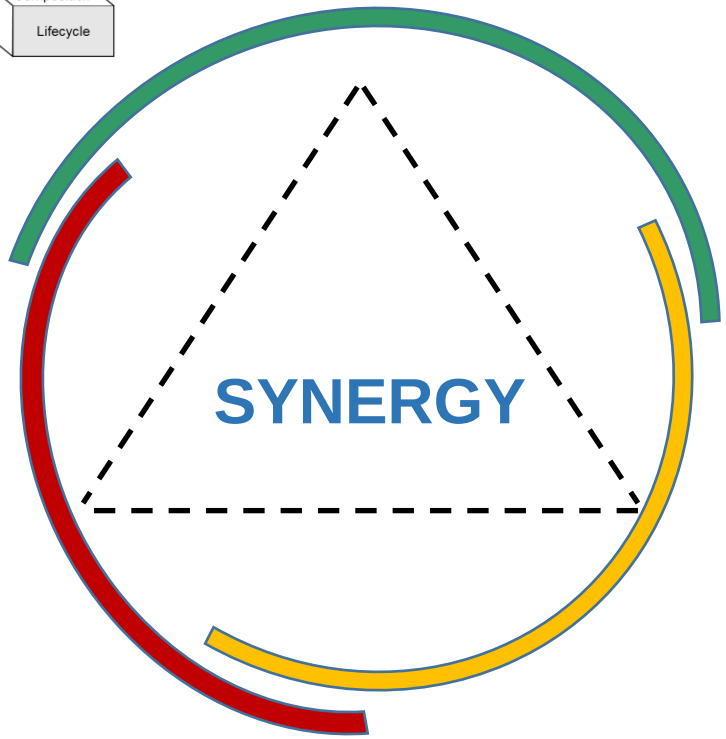
NIST is a non-regulatory R&D agency in the U.S. Department of Commerce

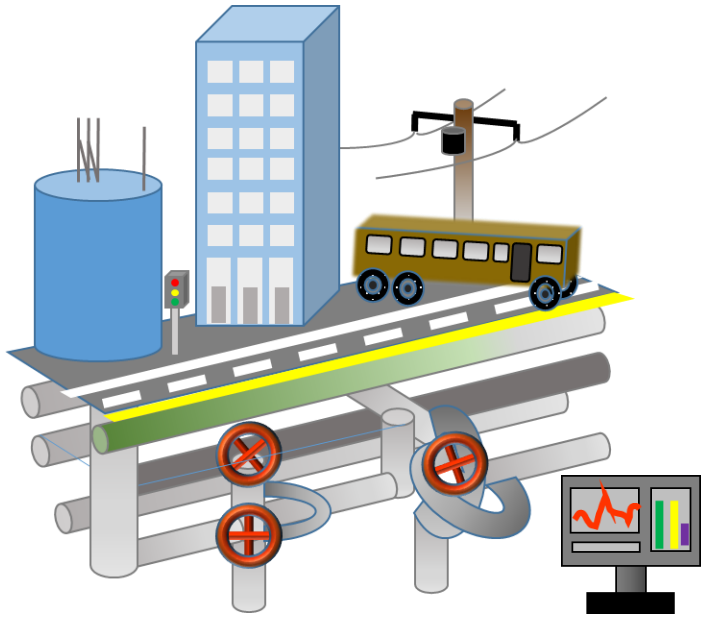


FOUNDATIONS:
CPS FRAMEWORK &
INTERNET-OF-THINGS-ENABLED
SMART CITY (IES-'YES' CITY)
FRAMEWORK



RESEARCH & STANDARDS
CPS TESTBED
MEASUREMENT SCIENCE
Federated Testbeds





APPLICATIONS:
GLOBAL CITIES TEAMS
CHALLENGE 2016-2017

Frameworks – NIST Convening of Stakeholders

2008 2009 2010 2011 2012 2013 2014 2015 2016

Smart Grid
Dec 2007
EISA SG Legislation

Cloud Computing
2010

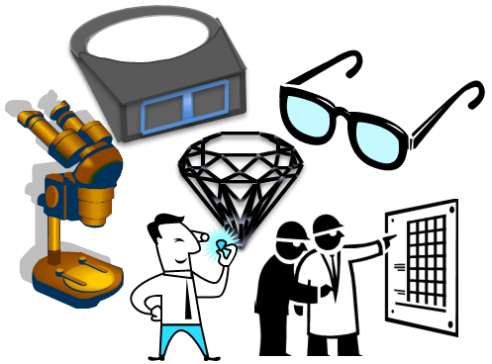
Cybersecurity
Feb 2013
Executive Order

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

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

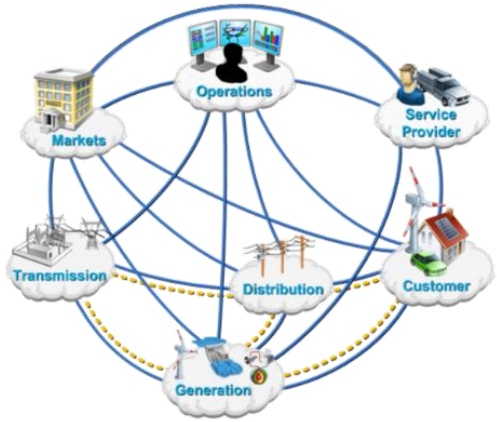
June 2014

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)



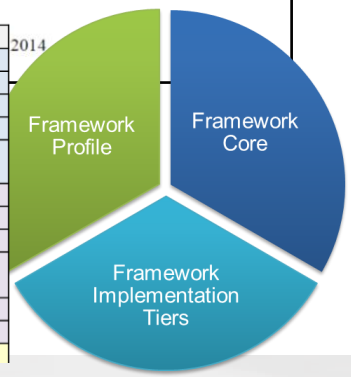
Framework for Improving Critical Infrastructure Cybersecurity

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



NIST Special Publication 1500-4

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

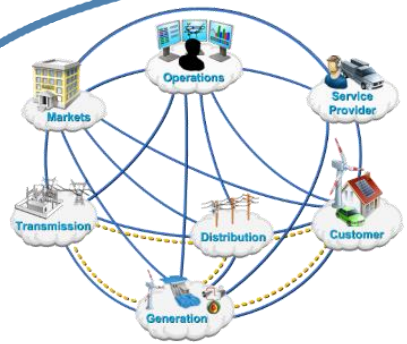
Final Version 1

NIST Big Data Public Working Group
Security and Privacy Subgroup

NIST CPS Public Working Group

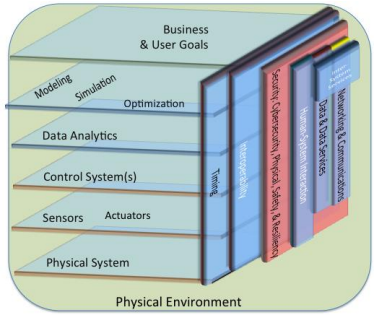
- Goal: create CPS Framework to support CPS research, development and deployment (applicable to CPS and Internet of Things IoT)
- Need: multi-domain perspective baked in
  - Applicable within all CPS domains, supports cross-CPS domain applications

CPS Framework



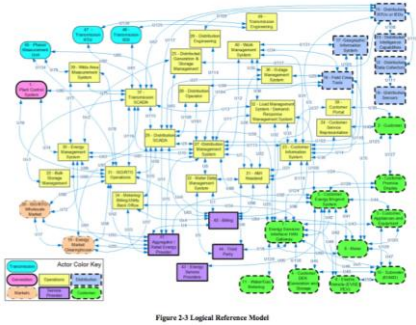
Smart infrastructure (grid, water, gas, …)

Smart buildings



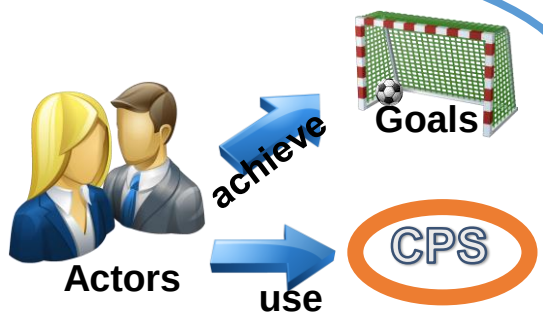
Smart emergency response

Smart healthcare



Many more!!

Smart manufacturing



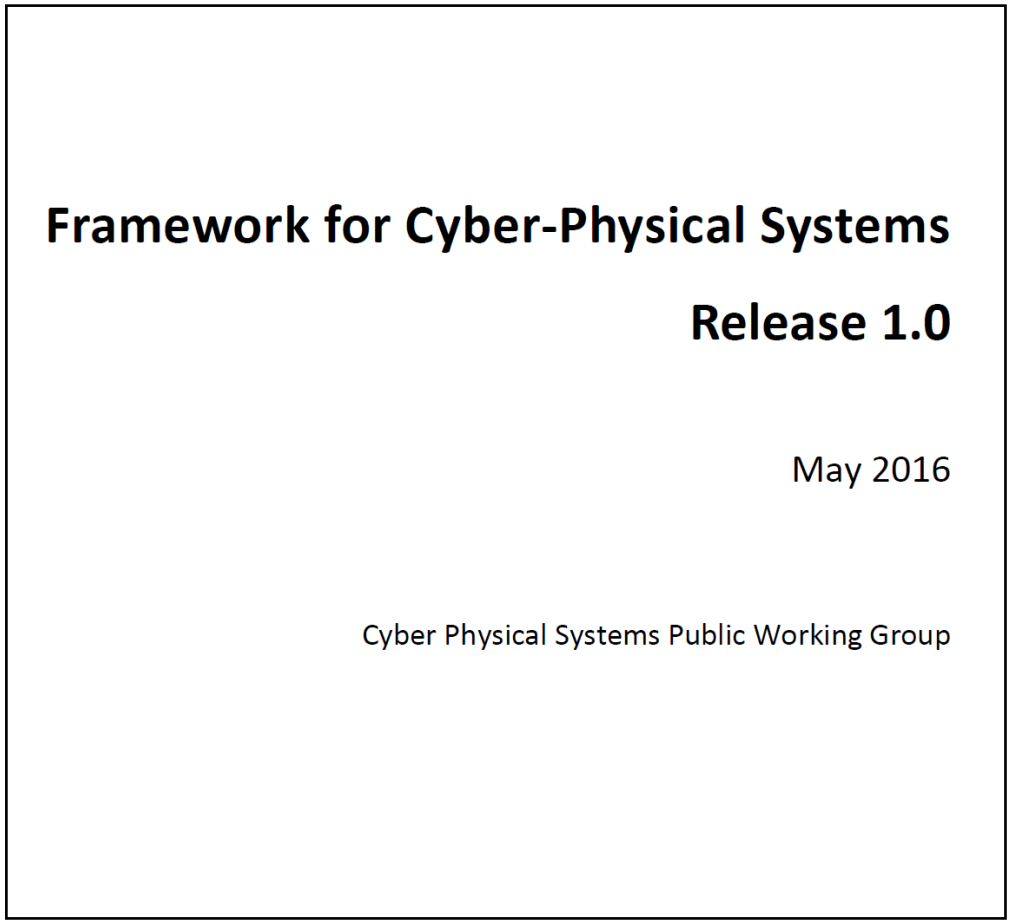
Smart transportation

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

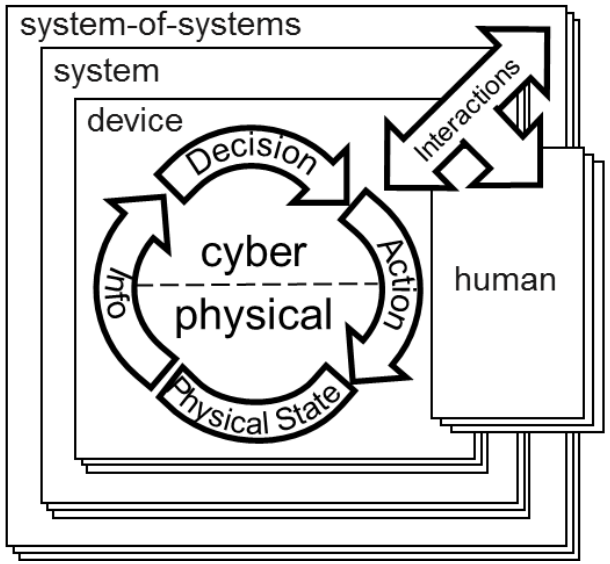
pages.nist.gov/cpspwg



NIST CPS Public Working Group - CPS Framework

- **CPS Framework Release 1.0 (May2016)** provides technical, concern-driven foundation and analysis methodology for CPS/IoT
- NIST leadership w/industry, academia, government; https://pages.nist.gov/cpspwg/

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



Cyber-Physical System

CPS Framework Structure

Domains

- Manufacturing
- Transportation
- Energy
- Healthcare
- others …

Aspects

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

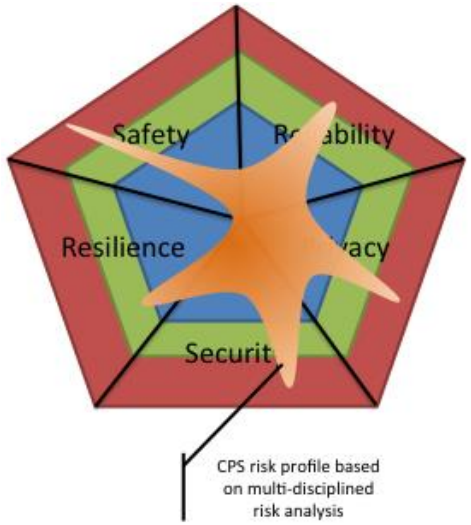
Facets

Conceptualization	Realization	Assurance
Use Case, Requirements, …	Design / Produce / Test / Operate	Argumentation, Claims, Evidence

Activities and their Artifacts

Model of a CPS	CPS	CPS Assurance

Trustworthiness concerns: Security, Privacy, Safety, Reliability, Resilience

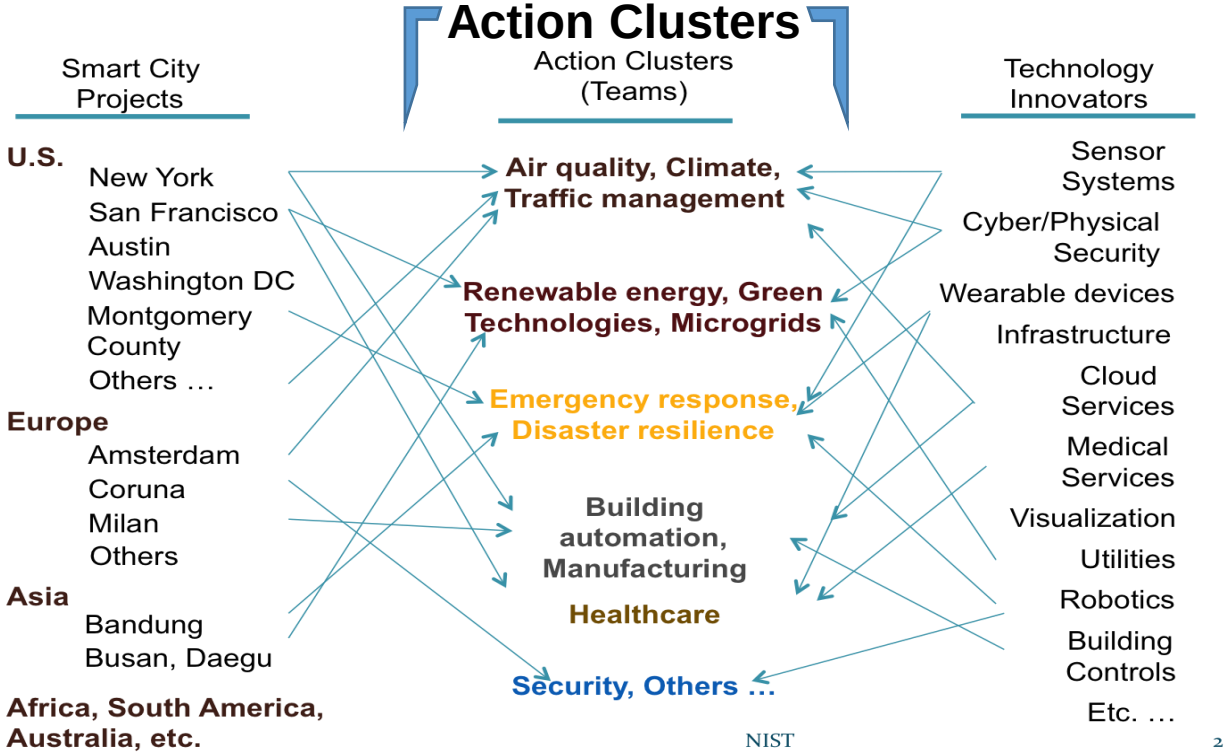


NIST Global Cities Teams Challenge (GCTC)

GLOBAL CITY TEAMS CHALLENGE

usignite

- Establish and demonstrate replicable, scalable and sustainable models for incubation and deployment of interoperable, standard-based IoT solutions and demonstrate their *measurable* benefits in Smart Communities/Cities



http://www.nist.gov/cps/sagc.cfm

NIST Global Cities Teams Challenge (GCTC)

- GCTC Expo 2016 (Austin, TX): 100+ action clusters represented
- Teams: 120+ local governments and 300+ companies/orgs working to deploy replicable and interoperable solutions in multiple cities.
- Each team creates at least one Key Performance Indicator (KPI) of the *tangible and direct* impacts to the local governments and the residents. Teams will report final results by June 2017.
- Suggested KPIs include:
  - Productivity/planning efficiency (e.g. frequency)
  - Environmental impacts (e.g. CO2 level)
  - Energy usage (e.g. kWh)
  - Traffic congestion (e.g. time to commute, number of cars)
  - Crime (e.g. reported number of incidents)

Internet of Things-Enabled Smart (IES) City Framework

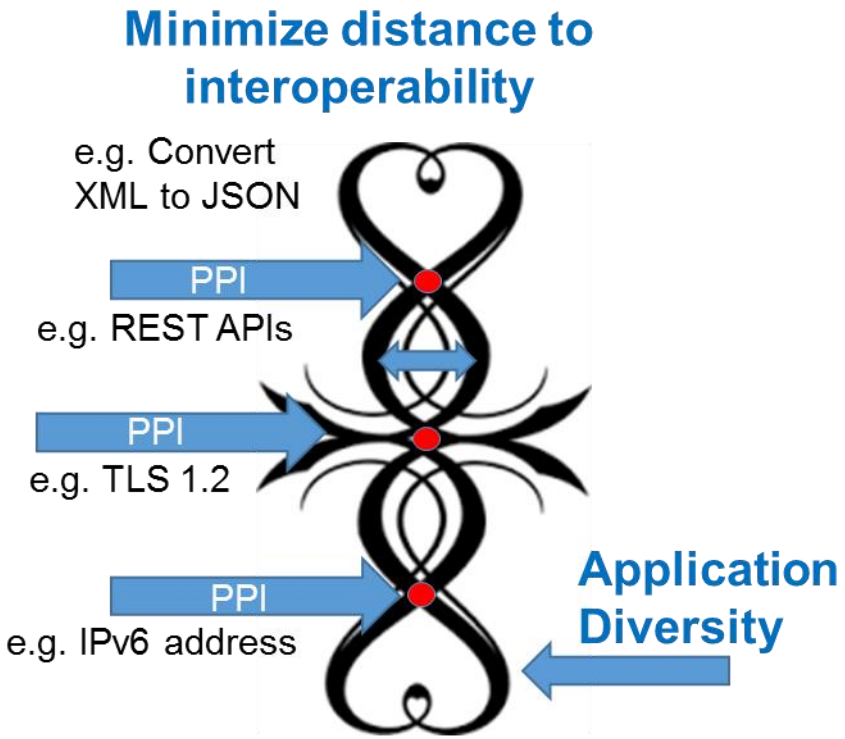
- **IES-City Framework Int'l Working Group**
  NIST and its partners have convened a public working group to distill a common set of smart city architectural features and identify "Pivotal Points of Interoperability"
  - 3 working groups, collaboration site: https://pages.nist.gov/smartcitiesarchitecture/
  - First drafts fall 2016, completion 2017

Goal: A reference framework for the development of architectures for incremental and composable Smart Cities

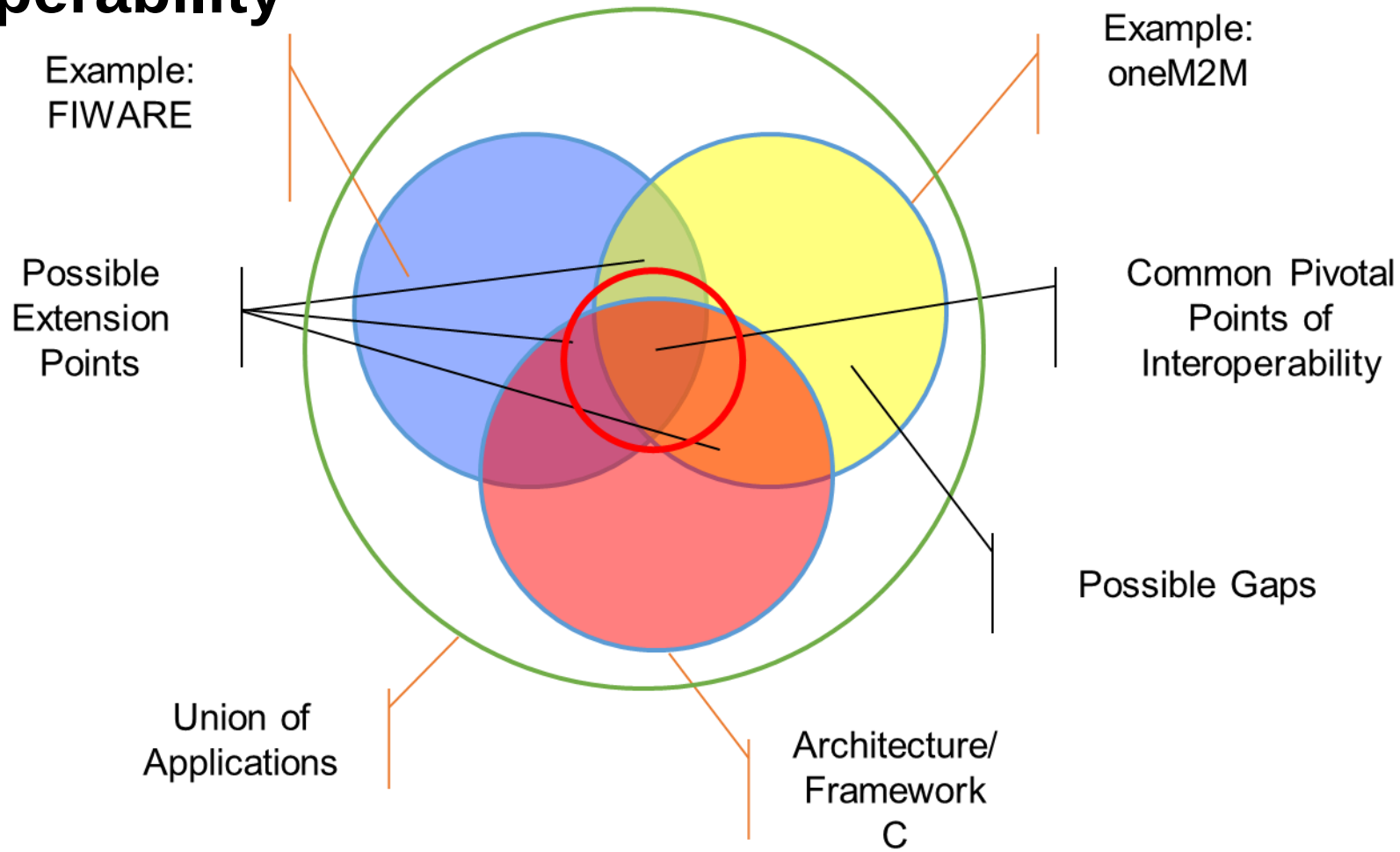
FIWARE MSIP NIST National Institute of Standards and Technology U.S. Department of Commerce ETSI World Class Standards ANSI U.S. Green Building Council USGBC ENEA Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile

Internet of Things-Enabled Smart (IES) City Framework

- **Pivotal Points of Interoperability**



Systems factor into PPI and Application Diversity



Concern-Driven Analysis of a Standard

Common Concern: Trustworthiness.Security.Cybersecurity.confidentiality

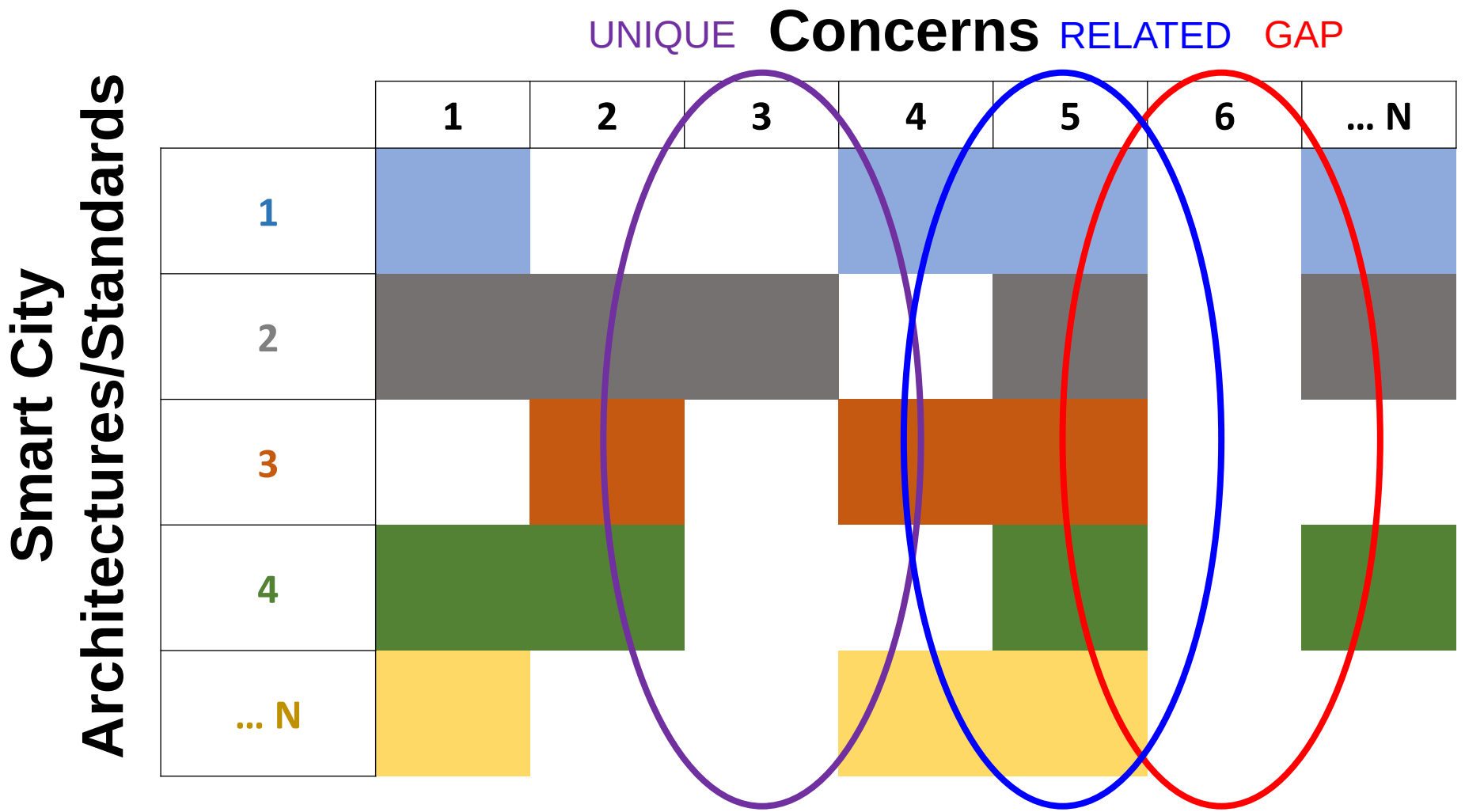
Clause in document: TS-0002 clause 6.4

Solution: Access Control and Authorization, TS-0003 clause 7

	Technology level (Device, System, System of Systems) Technology scope description (text)				
Concern	Aspect/Concern	Discussion of Concern	Discussion Reference(s)	Solution	Solution Reference(s)
Functional	Functional	in general	n/a		
Trustworthiness	Trustworthiness				
privacy	privacy	authorization, privacy and all the security requirements are defined	TS-0002 clause 6.4	Use proper access control settings under control of the data subject (individual whose privacy is exposed by the data)	TS-0003 Clause 7
reliability	reliability	in terms of message delivery, yes	tbd	CMDH(connection management and delivery handling) CSF and its resource types	TS-0001 clause 6.2.2
resilience	resilience	in terms of message delivery, yes	tbd	CMDH(connection management and delivery handling) CSF and its resource types	TS-0001 clause 6.2.2
safety	safety	Every deployment requires a risk and vulnerability assessment	TR-0008	Perform proper risk and vulnerability assessment and mitigate unacceptable risks	Any Risk assessment methodology. See TR-0008
security	security	all the security requirements are defined	TS-0002 clause 6.4, TR-0008	Definition of 4 protection levels suitable for different exposures. Definitrion of security frameworks to protect assets	TS-0003
cybersecurity	cybersecurity	all the security requirements are defined	TS-0002 clause 6.4	CPS security implies cybersecurity with additional challenges. Sdolutions exist to mitigate risks down to acceptable levels!	TR-0008; TS-0003
confidentiality	confidentiality	all the security requirements are defined	TS-0002 clause 6.4	Access Control and Authorization	TS-0003 clause 7
integrity	integrity	all the security requirements are defined	TS-0002 clause 6.4	implement proper protection level	TR-0008; TS-0003
availability	availability	Risks related to Denial of Service must be mitigated	TR-0008	Some mitigatoion mechanisms exist	TR-0008, TS-0003

Concern **Description** **Solution** **Reference**

Foundation for Cooperation



Outline

- Background
- CPS Framework – Aspects and Facets
- Interactions Across Aspects and Facets
- Expanded Mitigation Surface
- SAE Collaborative Agreement – Trustworthy Autonomous Vehicles
- Overview of the CPS Framework Open Source Project
- Open Source Project: Models and Tools

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 hold of the design artifacts according to an accepted, consensus mode of argumentation.

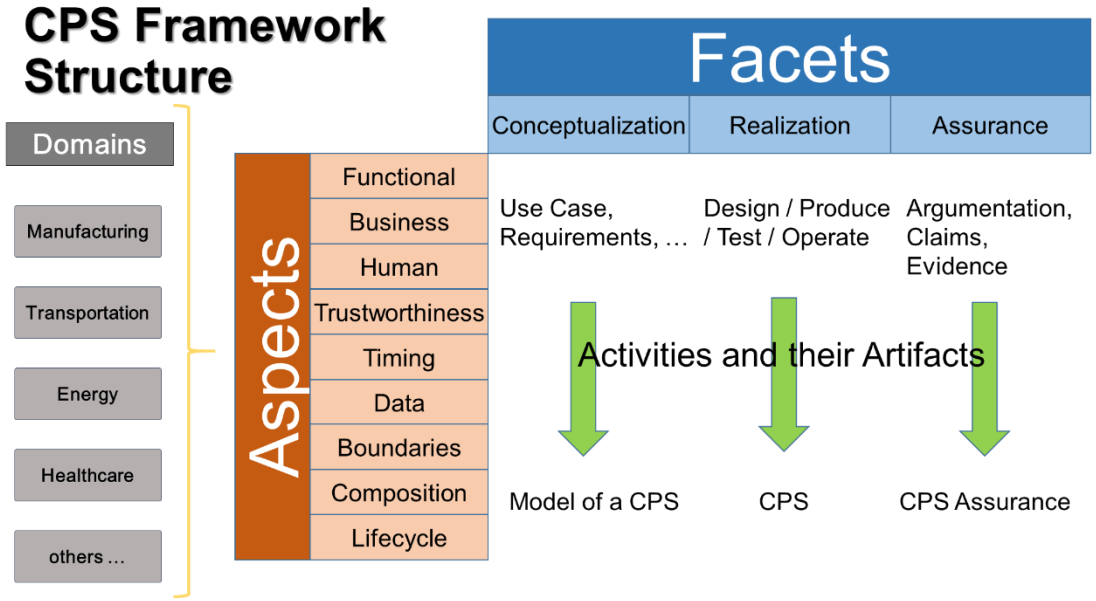
Outline

- Background
- CPS Framework – Aspects and Facets
- Interactions Across Aspects and Facets
- Expanded Mitigation Surface
- SAE Collaborative Agreement – Trustworthy Autonomous Vehicles
- Overview of the CPS Framework Open Source Project
- Open Source Project: Models and Tools

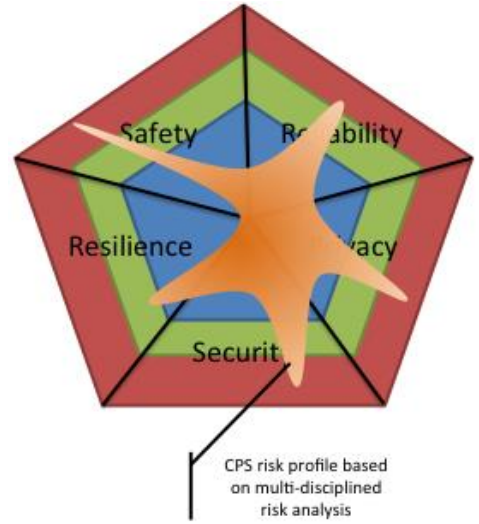
CPS Public Working Group

- 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': integrated approach to dimensions of a CPS



Concerns as Dimensions of CPS Measurement



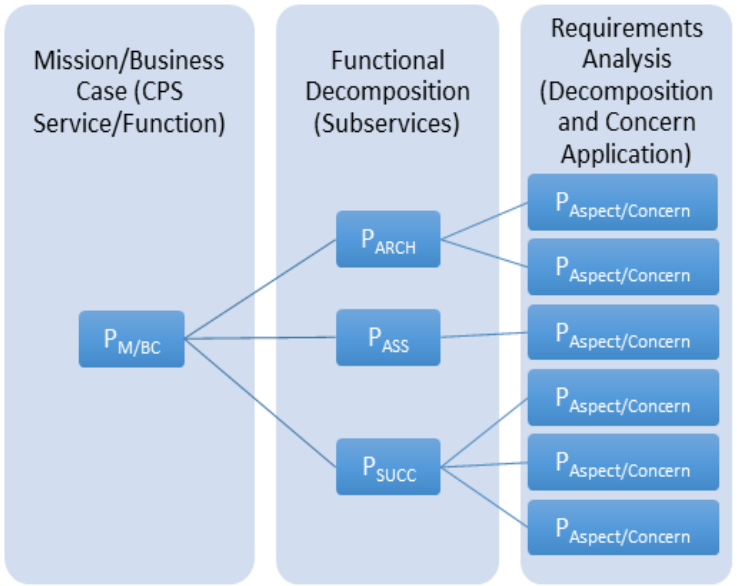
CPS Framework Mathematics

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

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

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

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

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

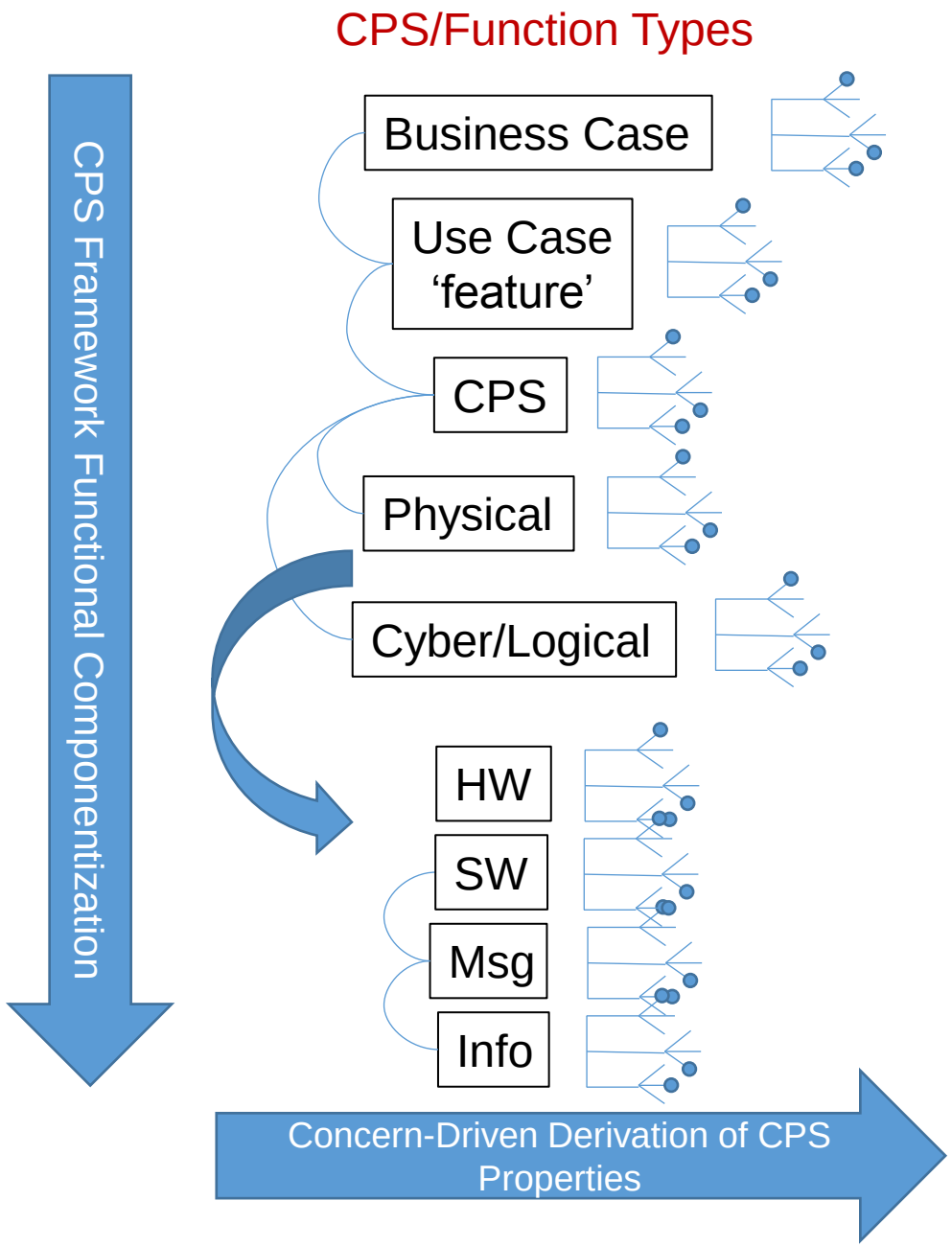
… defines **composition of concerns**

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

formal methods for assurance of a CPS

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

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



Decomposing a CPS in the CPS Framework

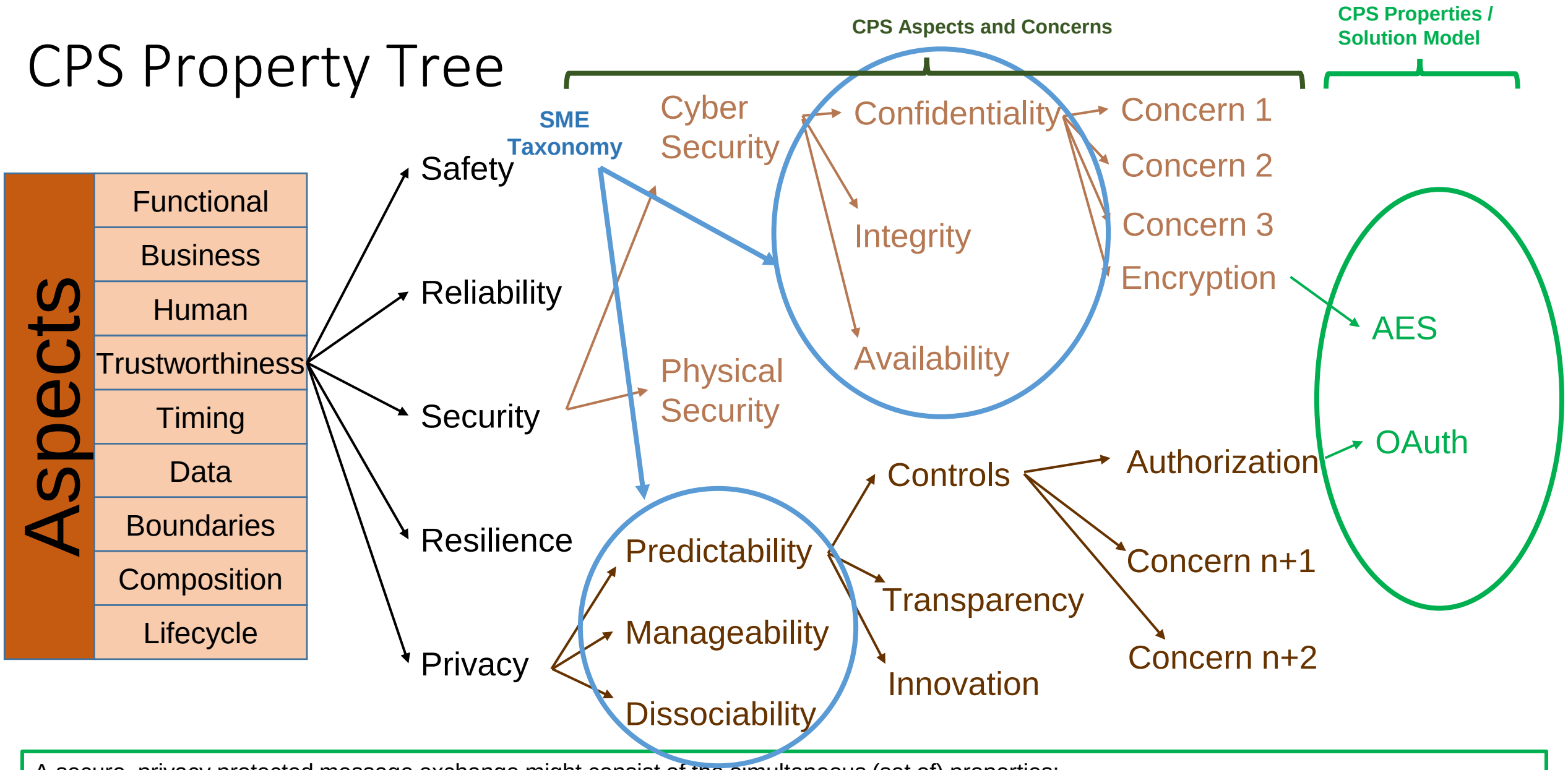
Function Types correspond to:

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

Including:

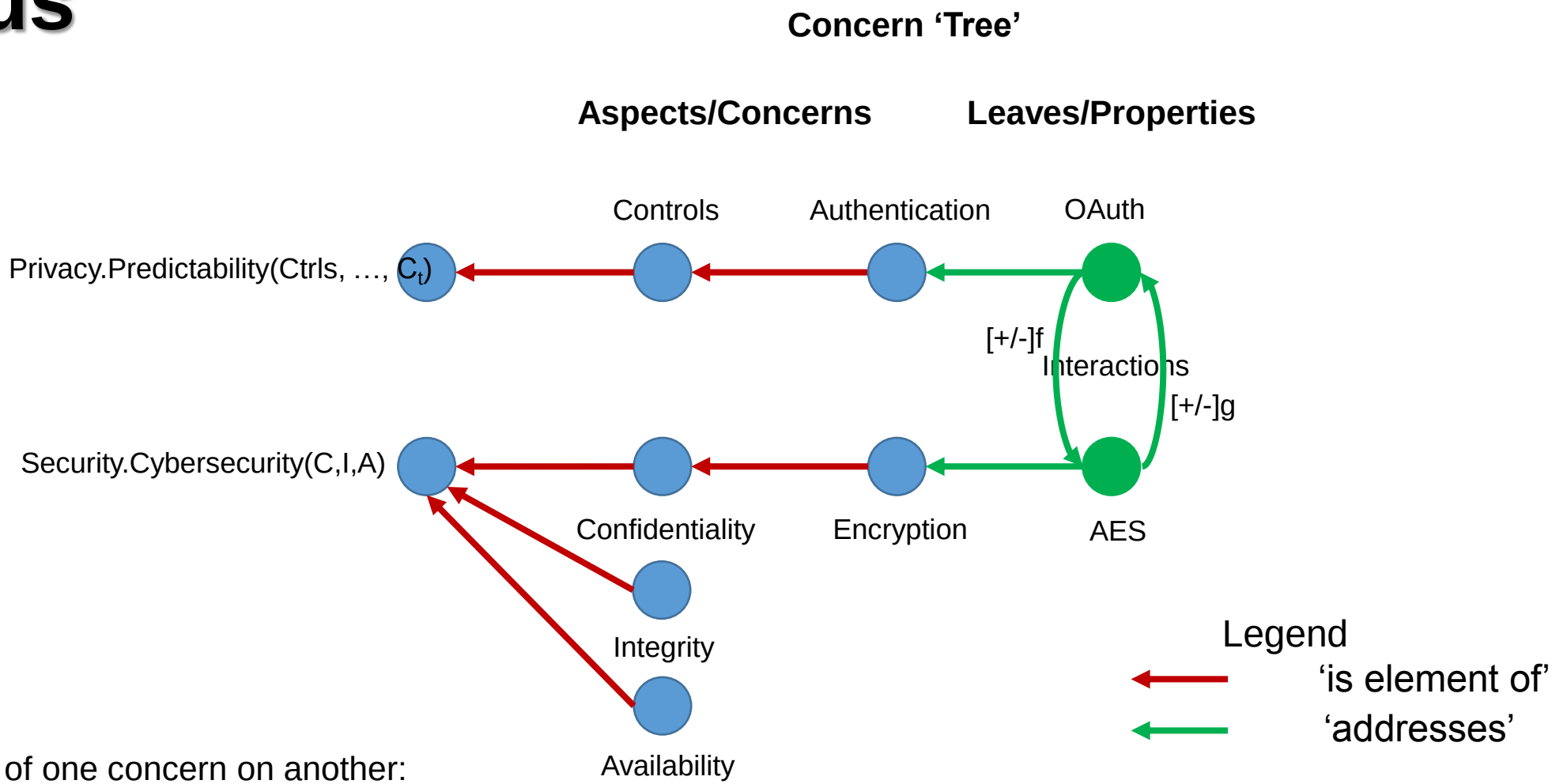
- Business Case (content and constraints)
- Use Case (feature/function)
- CPS (cyber-physical subsystems)
- Physical functions
- Cyber/logical functions
- Allocation to SW/HW
- Message and Signal

CPS 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}

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'
- Impact is the 'integral' over all pathways

Outline

- Background
- CPS Framework – Aspects and Facets
- Interactions Across Aspects and Facets
- Expanded Mitigation Surface
- SAE Collaborative Agreement – Trustworthy Autonomous Vehicles
- Overview of the CPS Framework Open Source Project
- Open Source Project: Models and Tools

IT vs IoT/CPS Threats

	Primary Impact of Failure		Mitigation Mechanisms		
	Digital	Physical	Digital	Analog	Physical
IT Syster	✓		✓		
IoT/CP	✓	✓	✓	✓	✓

Better Cybersecurity Through Physics

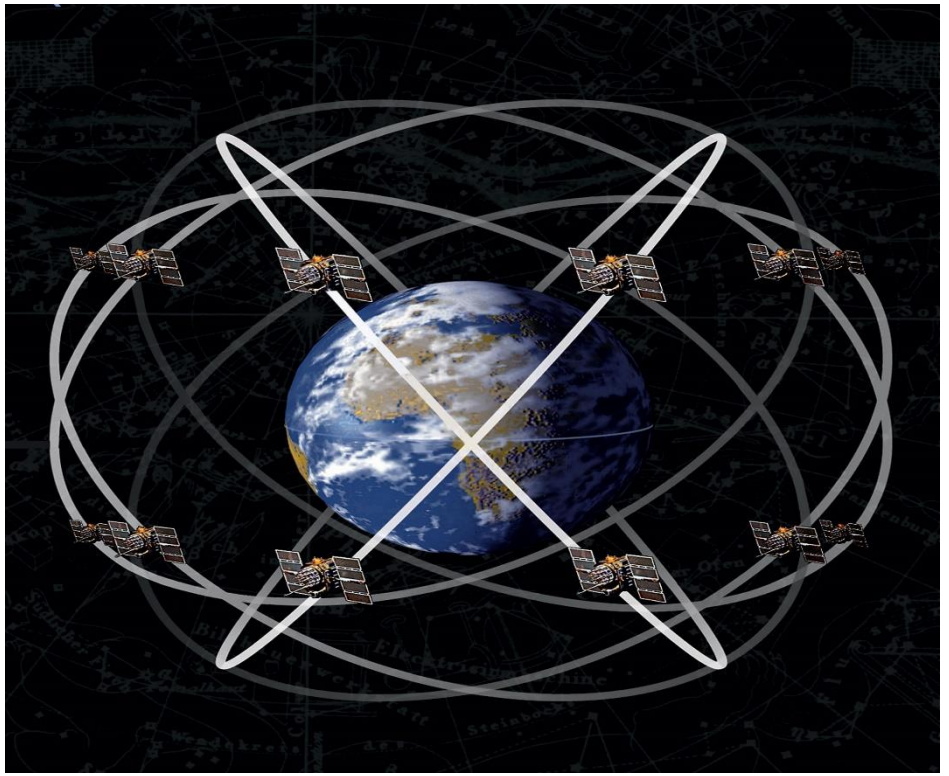
GPS is vulnerable to spoofing attacks. Here's how we can defend these important navigation signals

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

Physics and Engineering Attestation of the 'Logical'



Outline

- Background
- CPS Framework – Aspects and Facets
- Interactions Across Aspects and Facets
- Expanded Mitigation Surface
- SAE Collaborative Agreement – Trustworthy Autonomous Vehicles
- Overview of the CPS Framework Open Source Project
- Open Source Project: Models and Tools

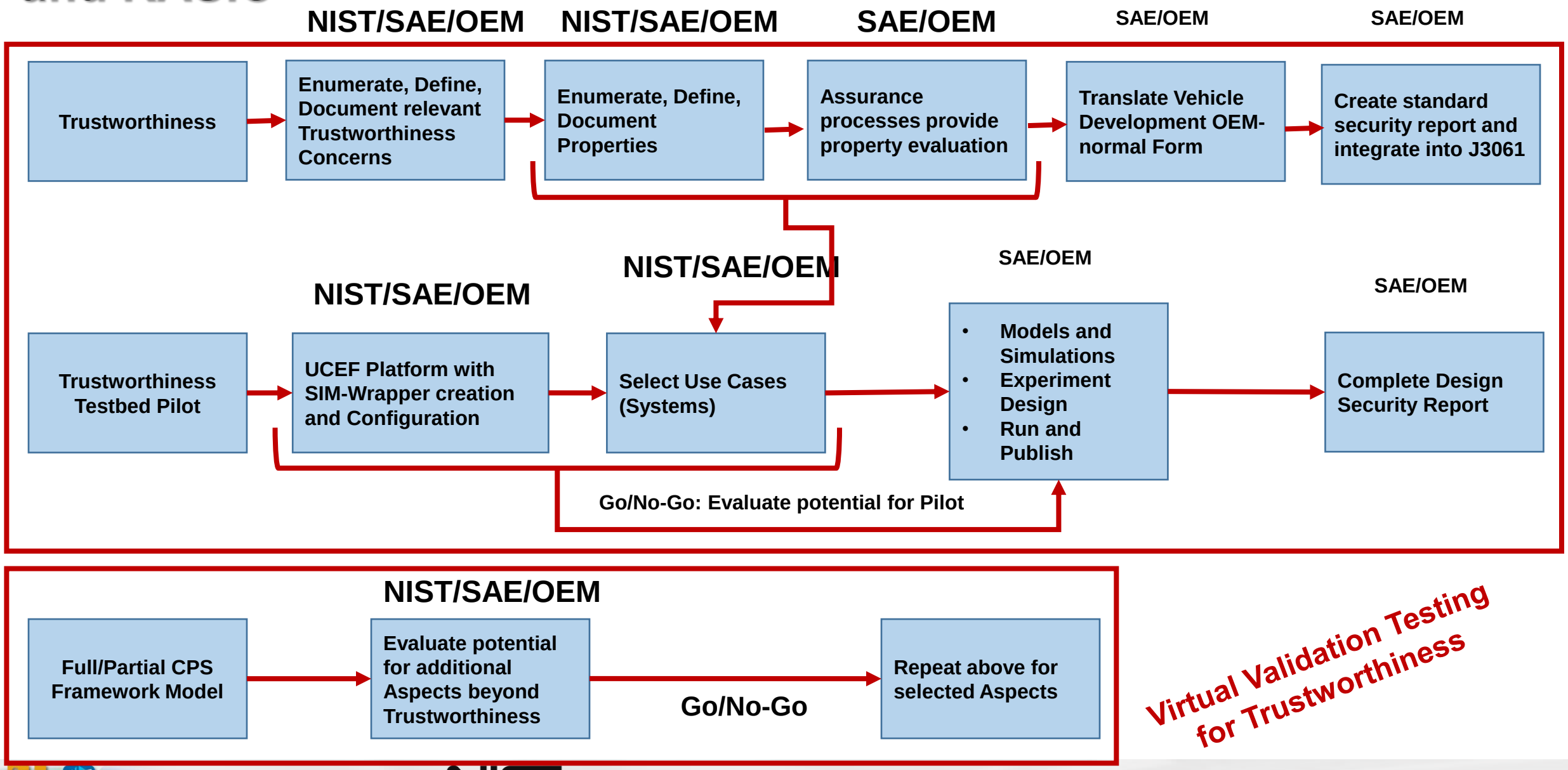
SAE INTERNATIONAL NIST National Institute of Standards and Technology

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. 301-975-4743

Item	Required	Lead	
1. Welcome and Introductions.	I	SAE Staff	10 10
2. Agenda changes/additions, Anti-trust, Patent Disclosure, Transparency, and IP statements are reviewed.	I	SAE Staff	10 10
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.	I	SAE Staff	10: 10
4. Scoping The Work- covers items 5-12	I	Ed Griffor, NIST, Lisa Boran, Ford	10: 2:
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	I	Ed Griffor, NIST, Lisa Boran, Ford	10 11
6. Break			11: 11
7. Automotive Trustworthiness Concerns a. Background material from the CPS Framework's trustworthiness aspect- Ed presentation b. DISCUSSION: Elaborate, deepen, document the automotive trustworthiness concerns, including any directions/ideology	I	Ed Griffor, NIST	11 12
8. Working Lunch			12 1:
9. Automotive Trustworthiness Requirements a. DISCUSSION: Rough in the high-level, functional objectives for the chosen trustworthiness concerns and their metrics	I	Lisa Boran- Ford	12 12
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	I	Ed Griffor, NIST	12: 1:
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	I	Lisa Boran- Ford	1: 1:
12. Work Breakdown/Approach	I	SAE Staff	1: 2:

Trustworthiness Development/Testing/Reporting Form - Plan and RASIC



Agenda

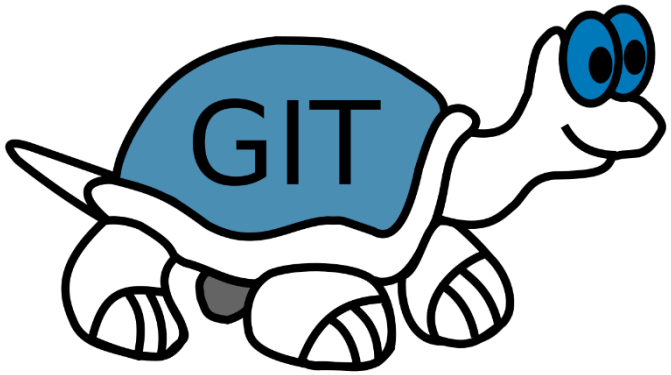
- Background
- CPS Framework – Aspects and Facets
- Interactions Across Aspects and Facets
- Expanded Mitigation Surface
- SAE Collaborative Agreement – Trustworthy Autonomous Vehicles
- Open Source Project: Models and Tools
- Overview of the CPS Framework Open Source Project

Tools for Modeling the CPS Framework

Enterprise Architect: UML Editor

XMLSpy: XML/XMLSchema Editor

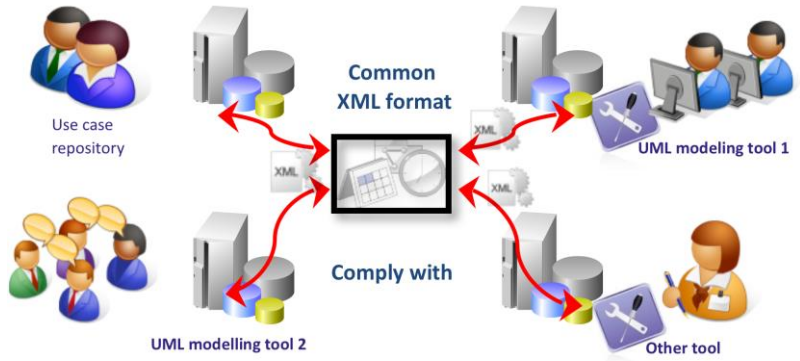
TortoiseGit: Windows GitTool



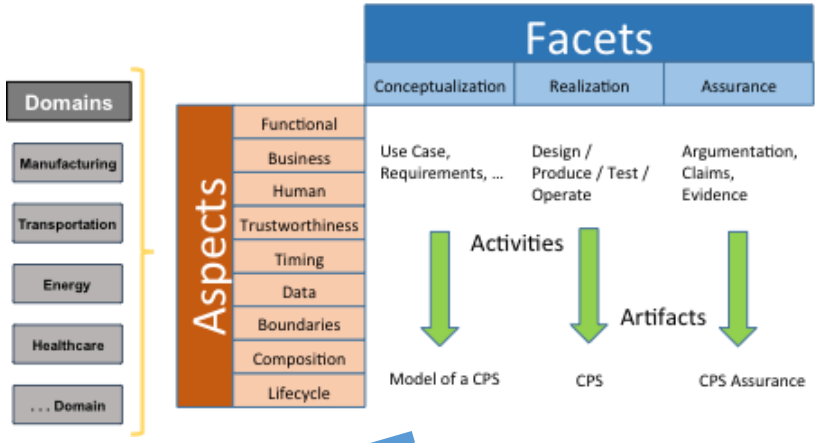
Notepadd++: Programmers Editor

Building a Model of a System in the Framework

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

Agenda

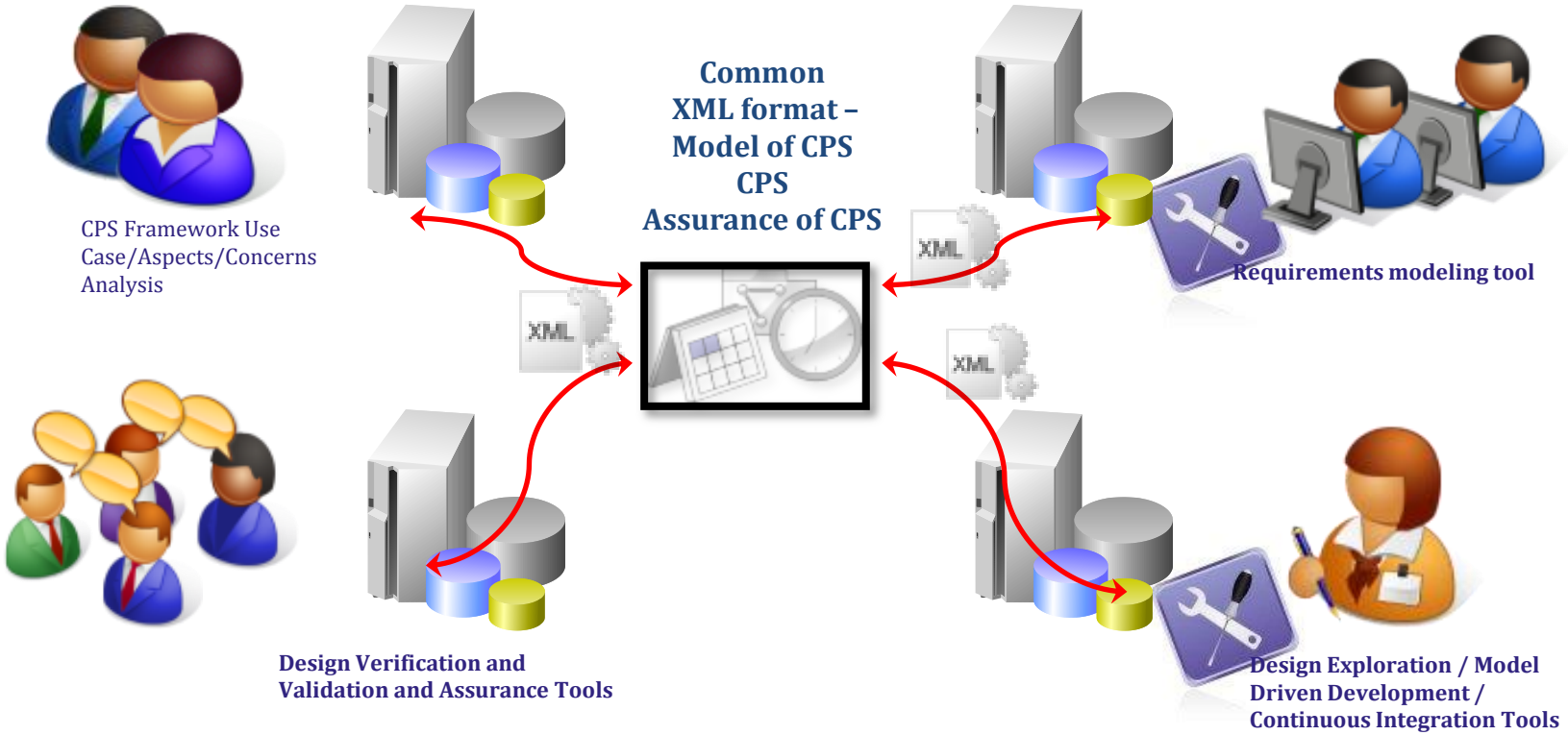
- Background
- CPS Framework – Aspects and Facets
- Interactions Across Aspects and Facets
- Expanded Mitigation Surface
- SAE Collaborative Agreement – Trustworthy Autonomous Vehicles
- Open Source Project: Models and Tools
- The CPS Framework Open Source Project

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.

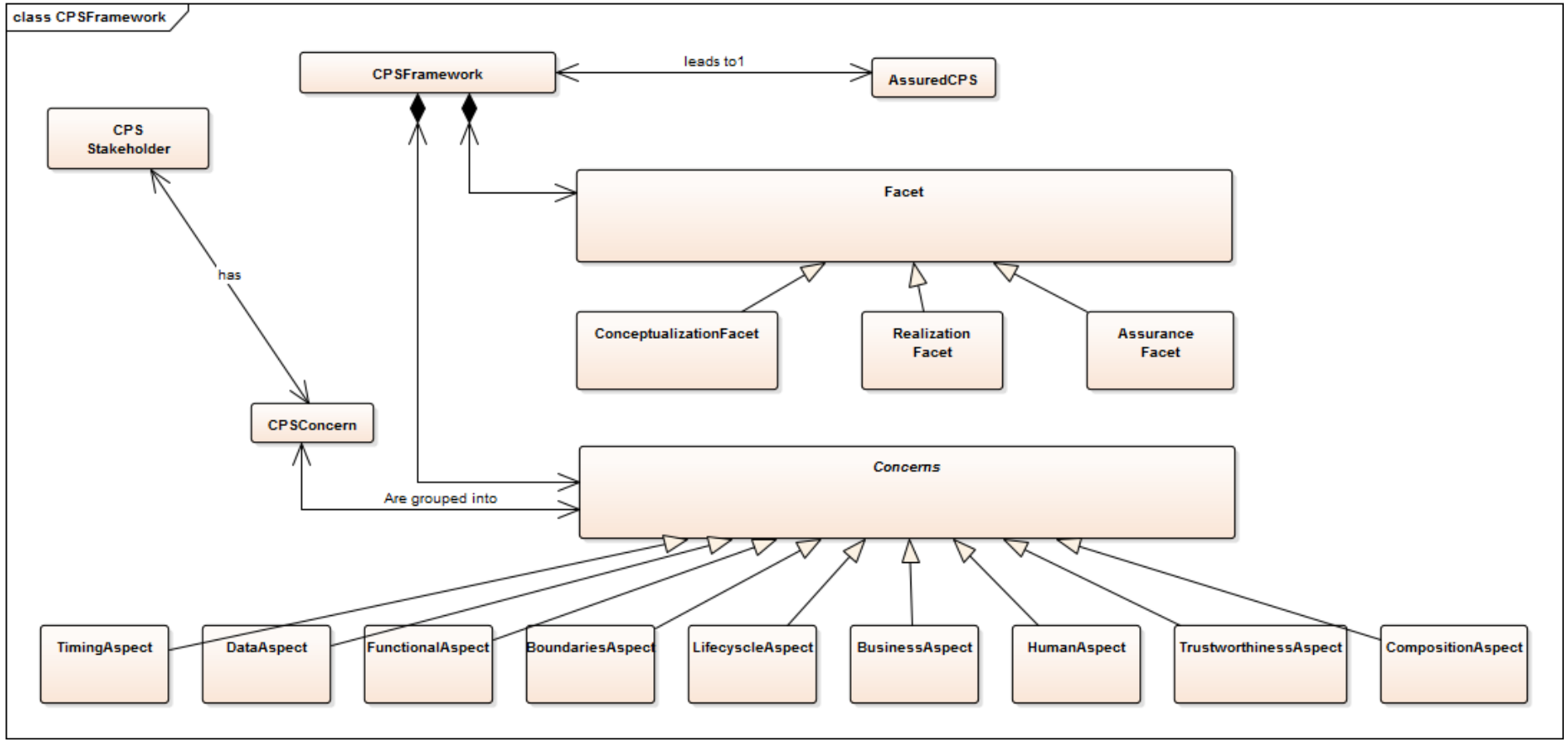
CPS Framework is NOT A PROCESS!!
It is a *method for integrating concerns into systems engineering processes*!

Engineering in the CPS Framework: One system representation, multiple views

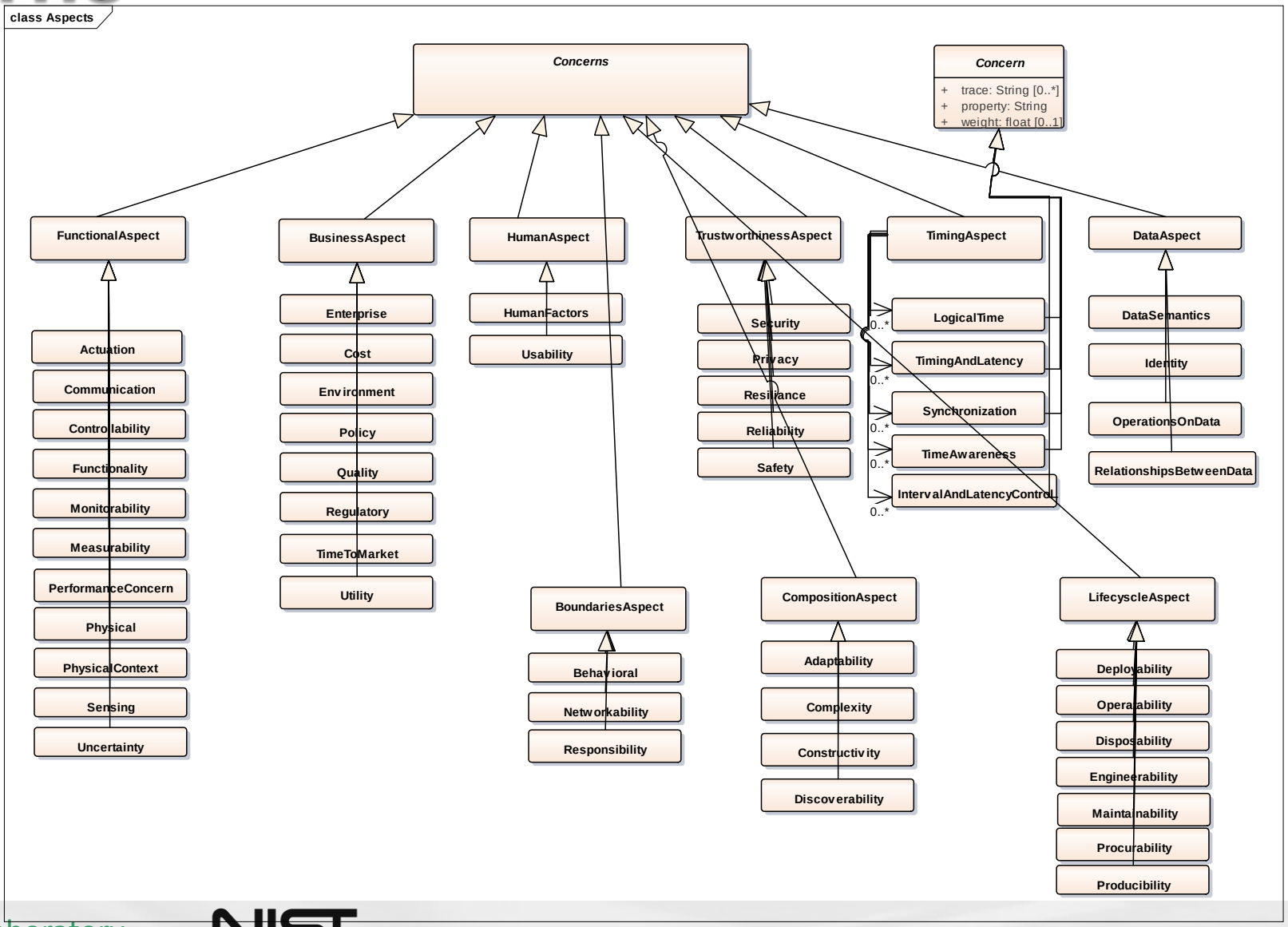


XML as the Design and Engineering Data Exchange standard.

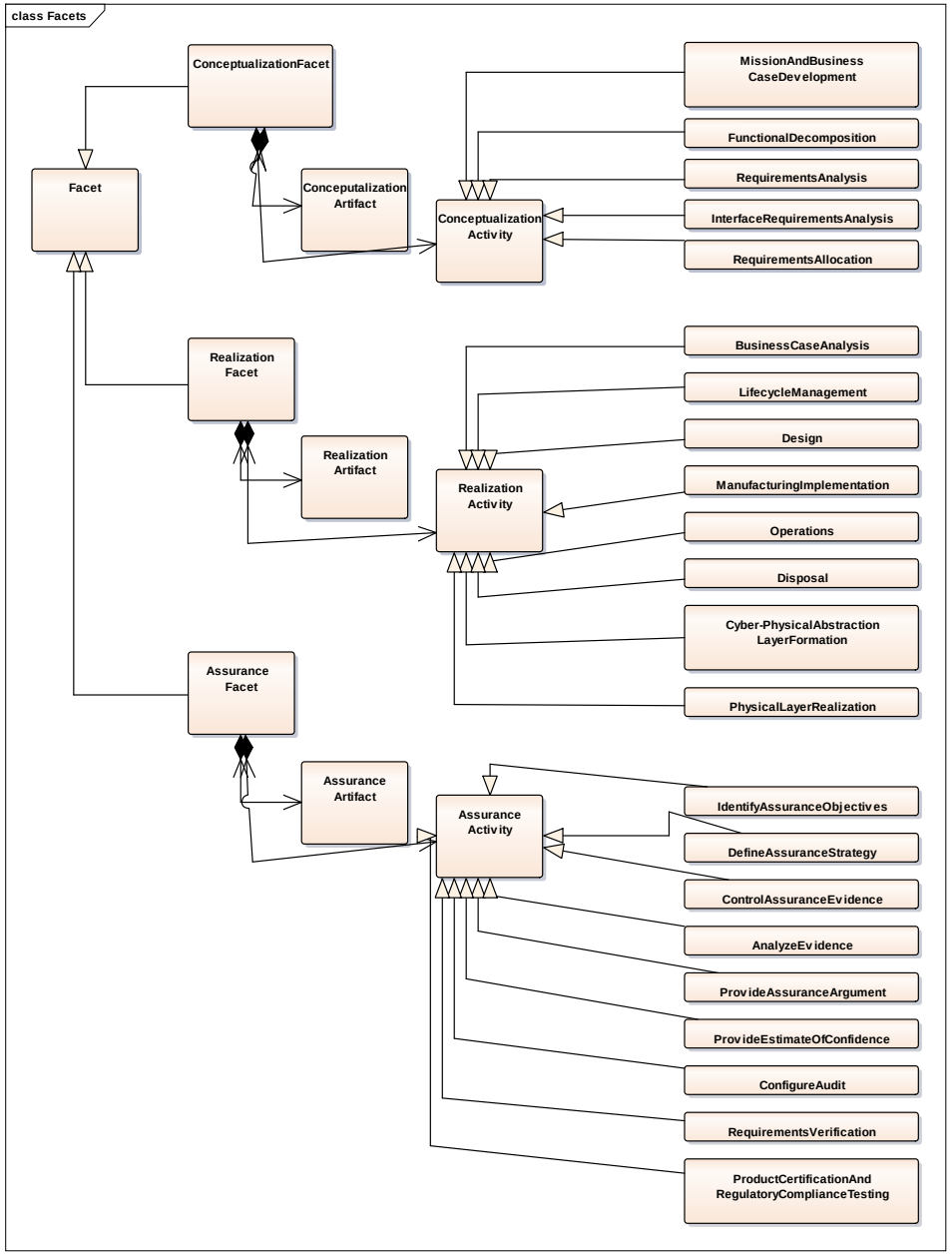
Modeling the CPS Framework: Aspects and Facets



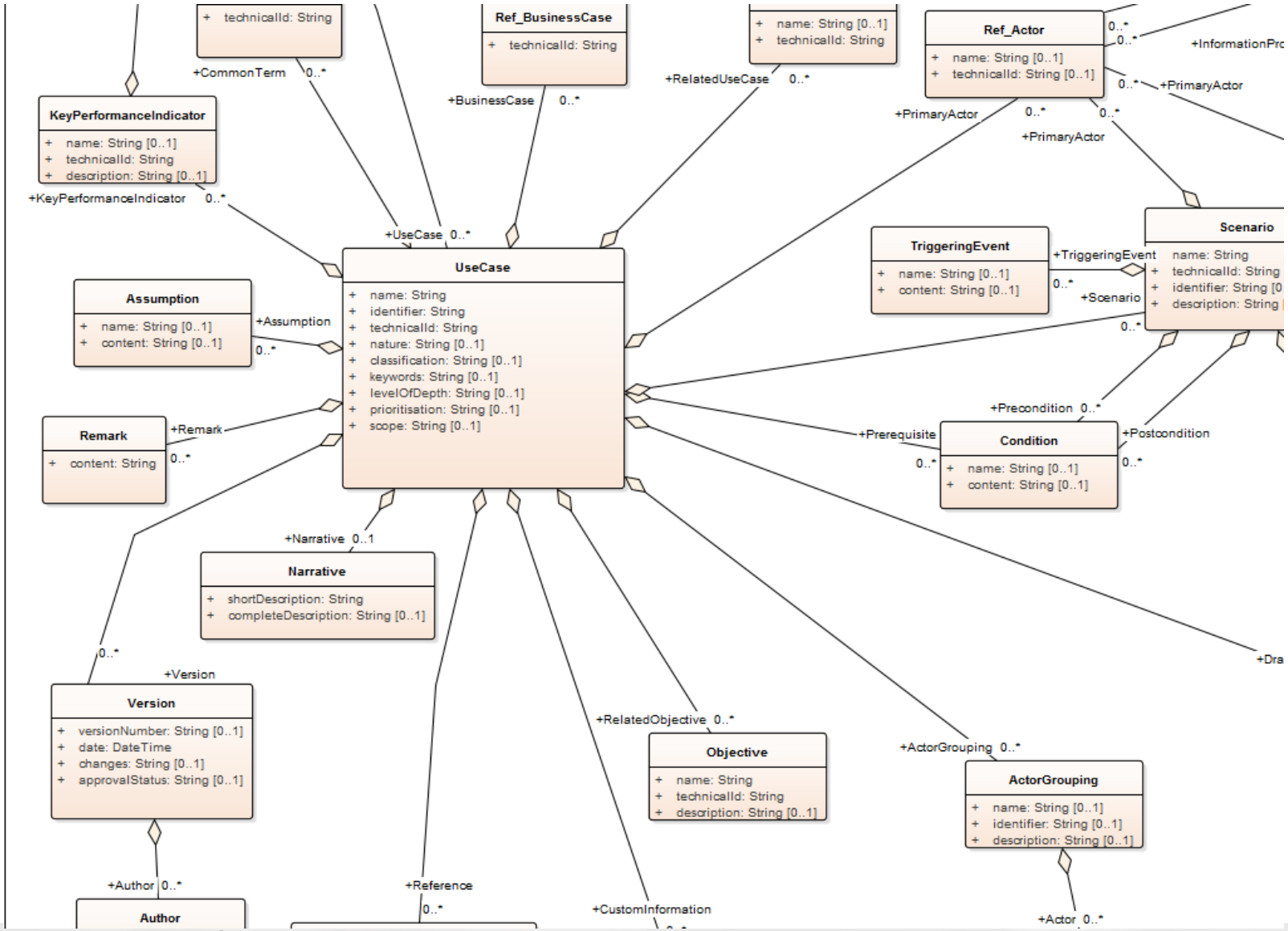
Modeling the Framework: Aspects and Concerns



Modeling the Framework: Facets and Activities

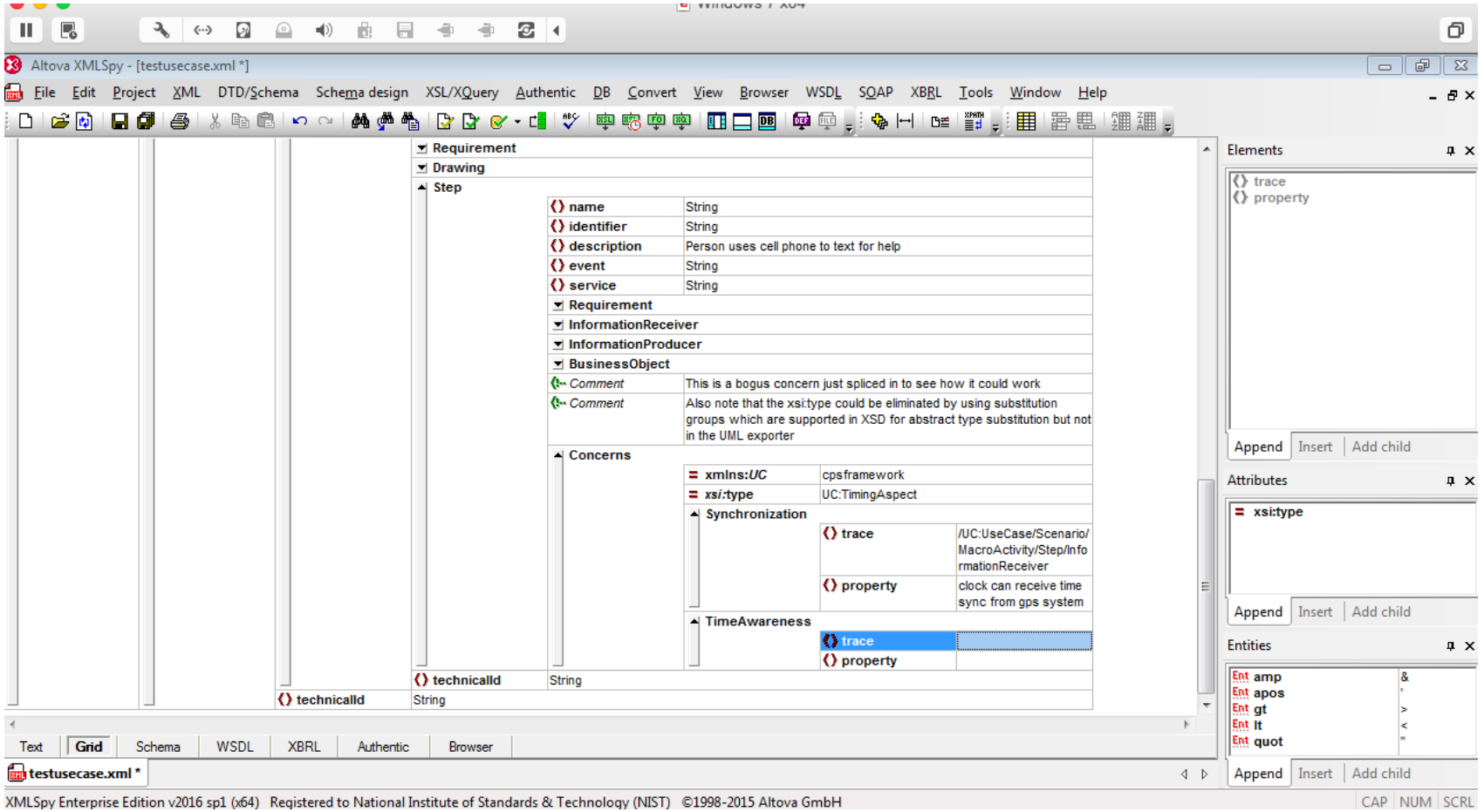


Modeling a Use Case*/System and Feature



*IEC 62559 Use Case Model

Concern-structured Requirements Development (XML)



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