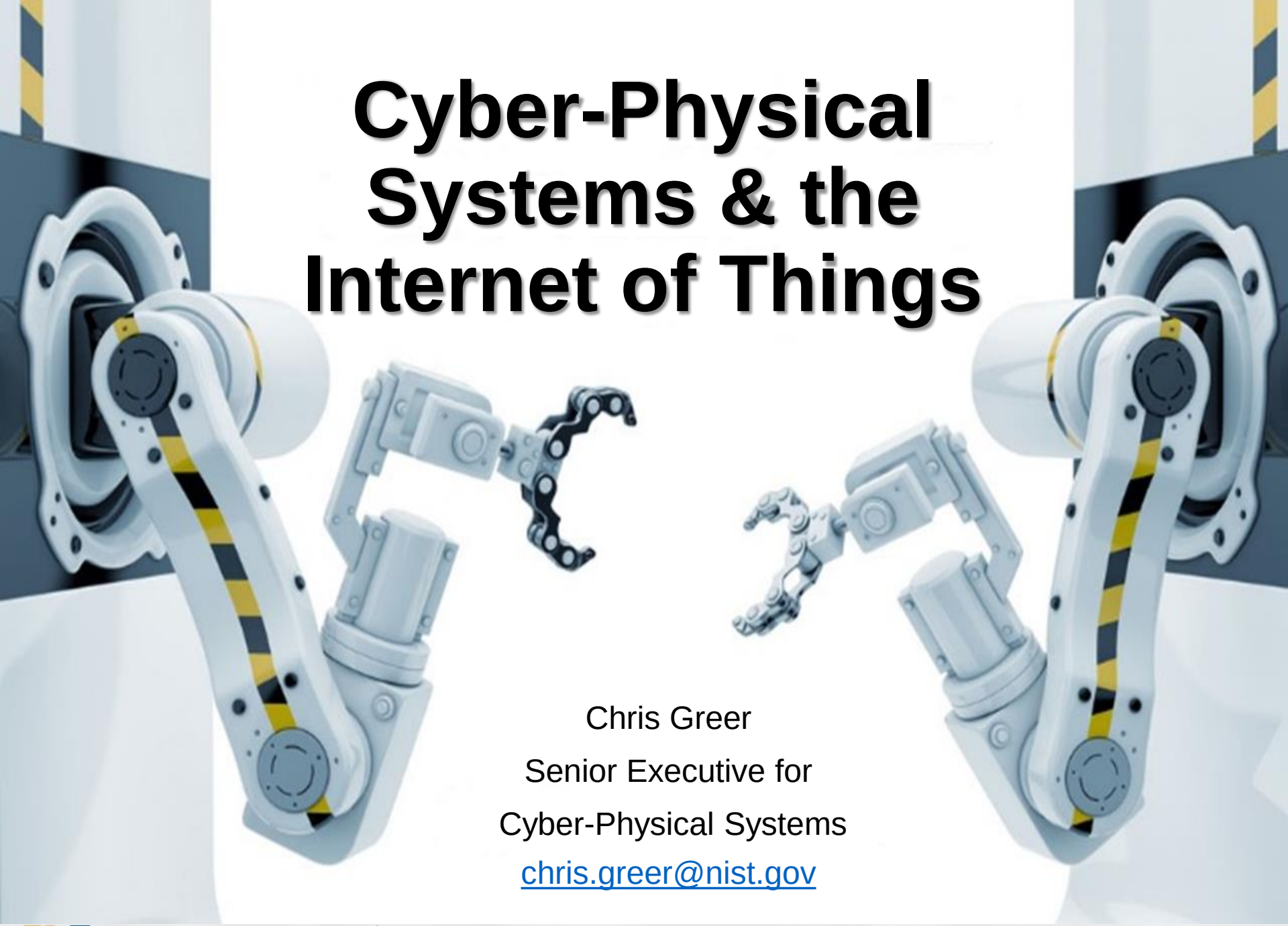
Cyber-Physical Systems & the Internet of Things



Chris Greer

Senior Executive for

Cyber-Physical Systems

chris.greer@nist.gov

NIST's Mission

- To promote U.S. innovation and industrial competitiveness by advancing **measurement science, standards**, and technology in ways that enhance economic security and improve our quality of life

NIST: Basic Stats and Facts

- Bureau within the Department of Commerce
- Major assets
  - ~ 3,000 employees
  - ~ 2,800 associates and facilities users
  - Two main locations: Gaithersburg, Md., and Boulder, Colo.
  - Nobel Prize Winners: 1997, 2001, 2005, 2007, 2013

Cyber-Physical Systems (CPS)

- Integrated, hybrid networks of cyber (IT) and engineered physical (OT) elements
- Co-designed and co-engineered OT and IT systems
- Adaptive and predictive to enhance performance

IoT = Subset of CPS focused on:

- Devices that are not traditionally networked
- Device-to-device communications
- New data streams

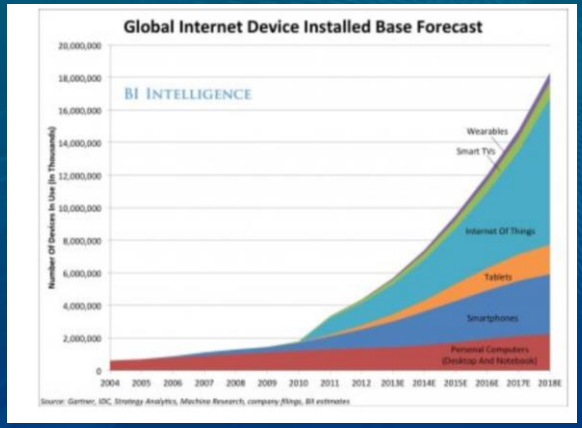
Internet of Things

If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste, loss and cost.

— Kevin Ashton, That 'Internet of Things' Thing, RFID Journal, July 22, 2009

The Opportunity – CPS/IoT by the Numbers

- Number of devices
  - 12 billion devices connected to the Internet today
  - 200 billion devices in just 5 years (IDC, Intel, UN)
- Global IoT Market
  - $756.8 billion in 2014 (VisionGain Research)
  - 17.5% CAGR through 2020 (IDC)
  - $19 trillion by 2020 (Cisco)
- Range of applications
  - Near to far: Smart spoon to Mars rover
  - Small to large: Medical nanobot to A380
  - Local to global: Home area network to global Internet
  - Etc.



The Opportunity - CPS/IoT Verticals

SAP: Industrial Internet technologies will provide $500 billion in annual savings in manufacturing costs by 2020.

Navigant Research: The worldwide installed base of smart meters will grow from 313 million in 2013 to nearly 1.1 billion in 2022.

Foster Research: Innovations in autonomous systems will save $1.5 trillion in global transport costs by 2025.

SAP: Internet of Things technologies have the potential to provide for a 67% increase in global agricultural productivity.

Internet of Things

What are the key dimensions of the “Internet of Things?”

- Scale
- Capability
- Reach

Internet of Things

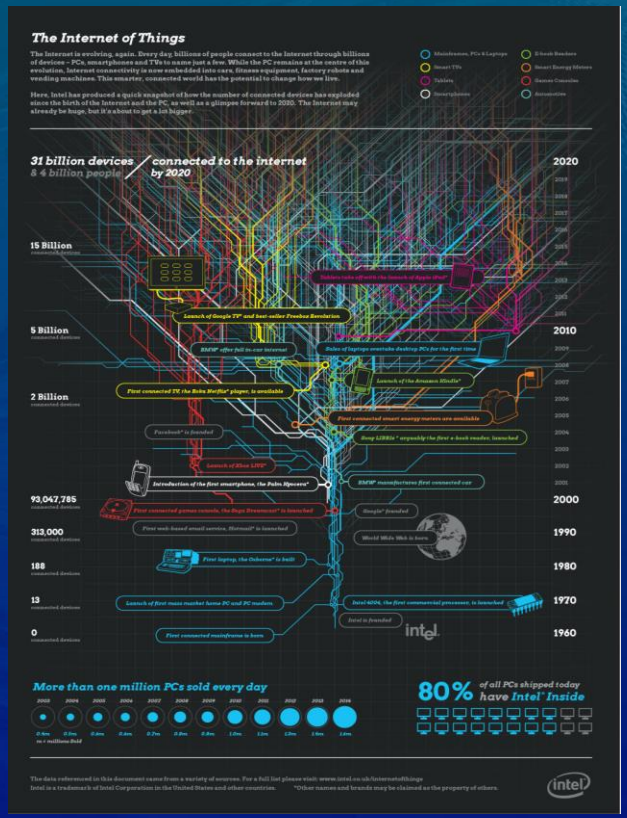
What are the key dimensions of the “Internet of Things?”

- Scale
- Capability
- Reach

Internet of Things - Scale

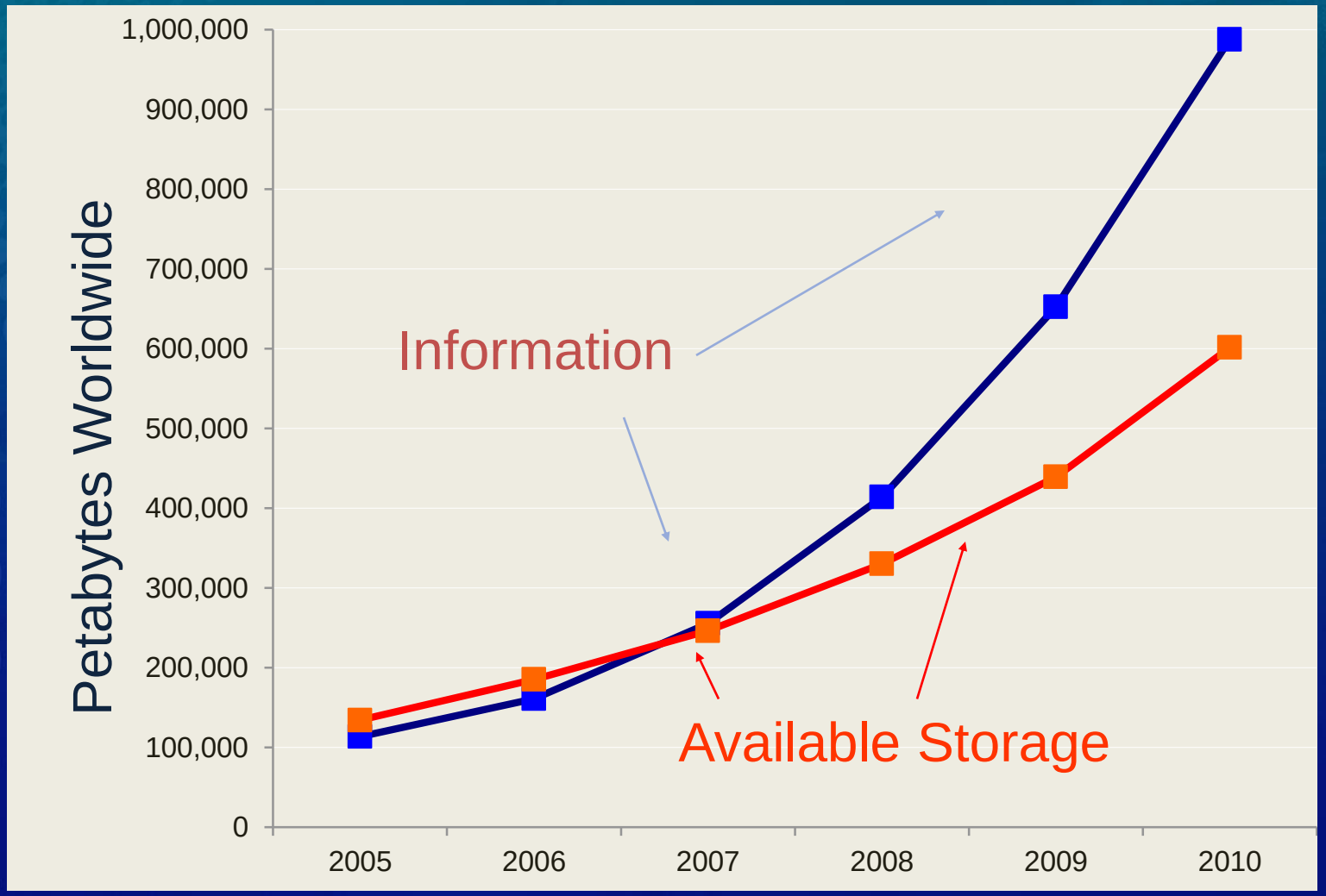
Devices connected to the Web:

- 1970 = 13
- 1980 = 188
- 1990 = 313,000
- 2000 = 93,000,000
- 2010 = 5,000,000,000
- 2020 = 31,000,000,000



Source: Intel

Big Data - Quantitative



Source: John Gantz, IDC Corporation, *The Expanding Digital Universe*

Big Data - Qualitative

Things You Don't Know

Questions You're Asking

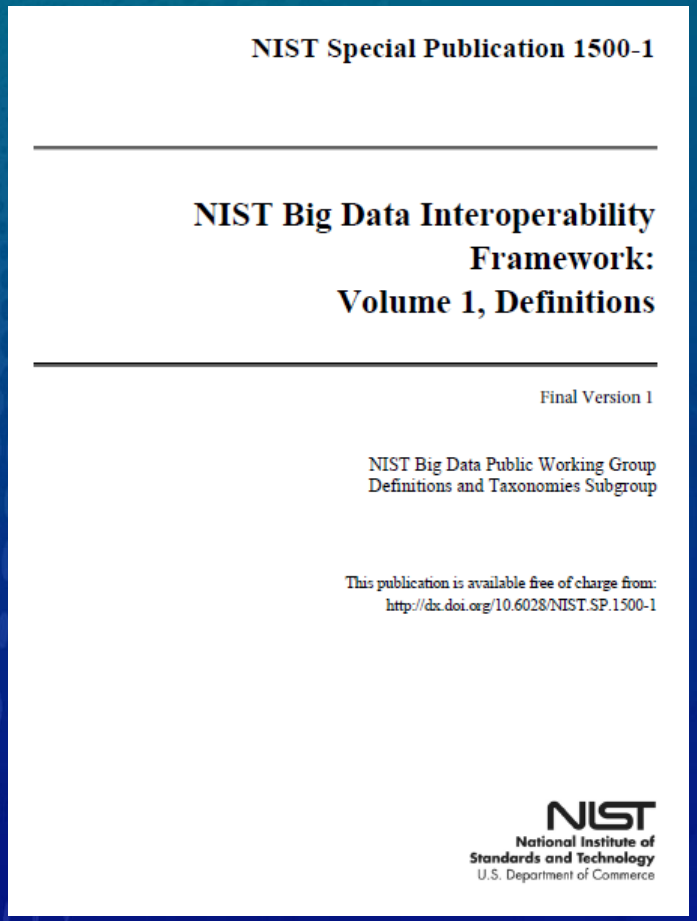
Data Acquisition	BIG DATA
Conventional Data Analytics	Data-enabled Exploration

Questions You Haven't Thought Of

Things You Know

Credit: Jason Kolb, Applied Data Labs; Modified from the original at: www.applieddatalabs.com/content/new-reality-business-intelligence-and-big-data

NIST Big Data Working Group


NIST Special Publication 1500-1

NIST Big Data Interoperability Framework:
Volume 1, Definitions

Final Version 1

NIST Big Data Public Working Group
Definitions and Taxonomies Subgroup

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.1500-1

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

7 Volumes:

- Definitions
- Taxonomies
- Use Cases & Req'ts
- Security & Privacy
- Architecture
- Standards Roadmap

Available at:
www.nist.gov/el/cyber-physical-systems/big-data-pwg

Internet of Things

What are the key dimensions of the “Internet of Things?”

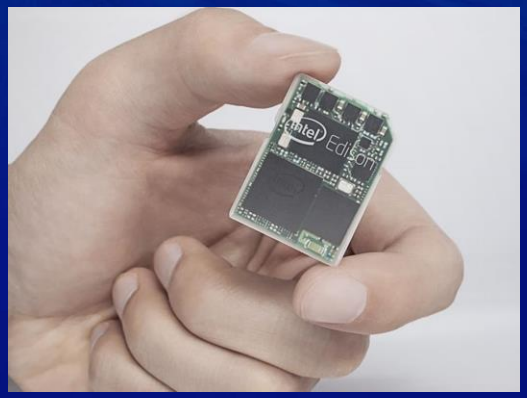
- Scale
- Capability
- Reach

Internet of Things - Capability

Intel Edison:

"It's a full Pentium-class PC in the form factor of an SD card,"

Intel CEO Brian Krzanich



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

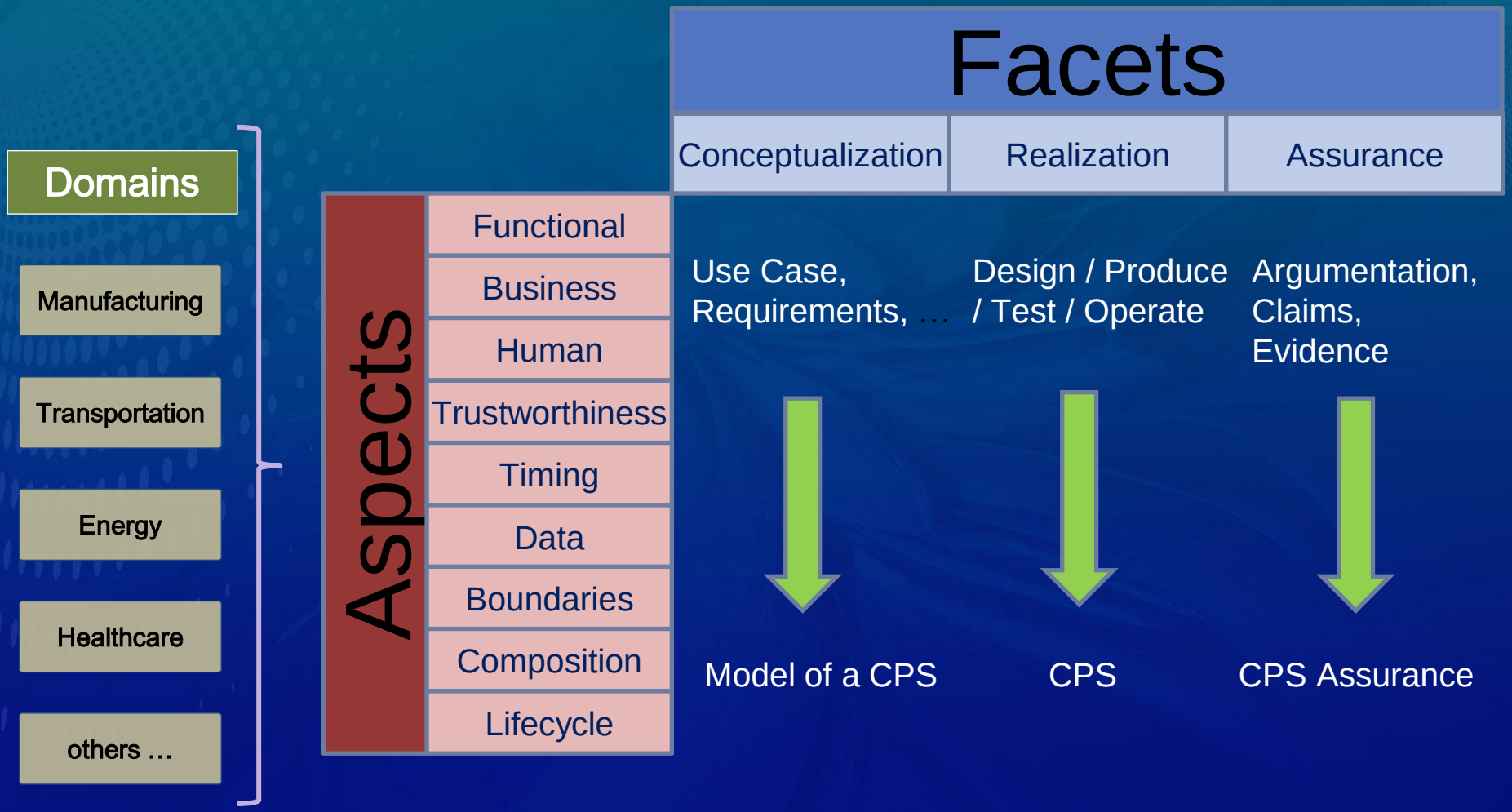
Framework for Cyber-Physical Systems

Release 1.0

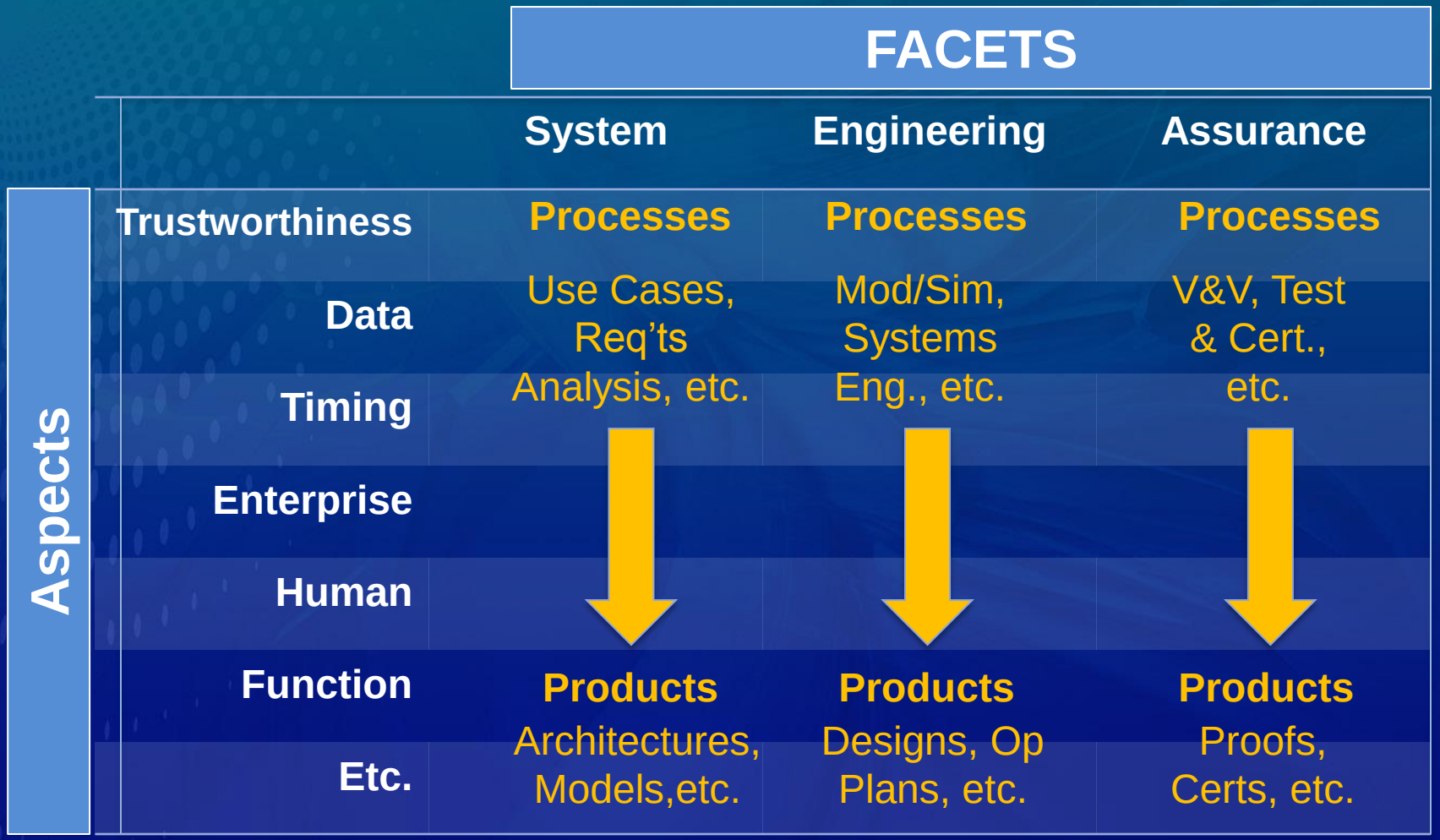
May 2016

Cyber Physical Systems Public Working Group

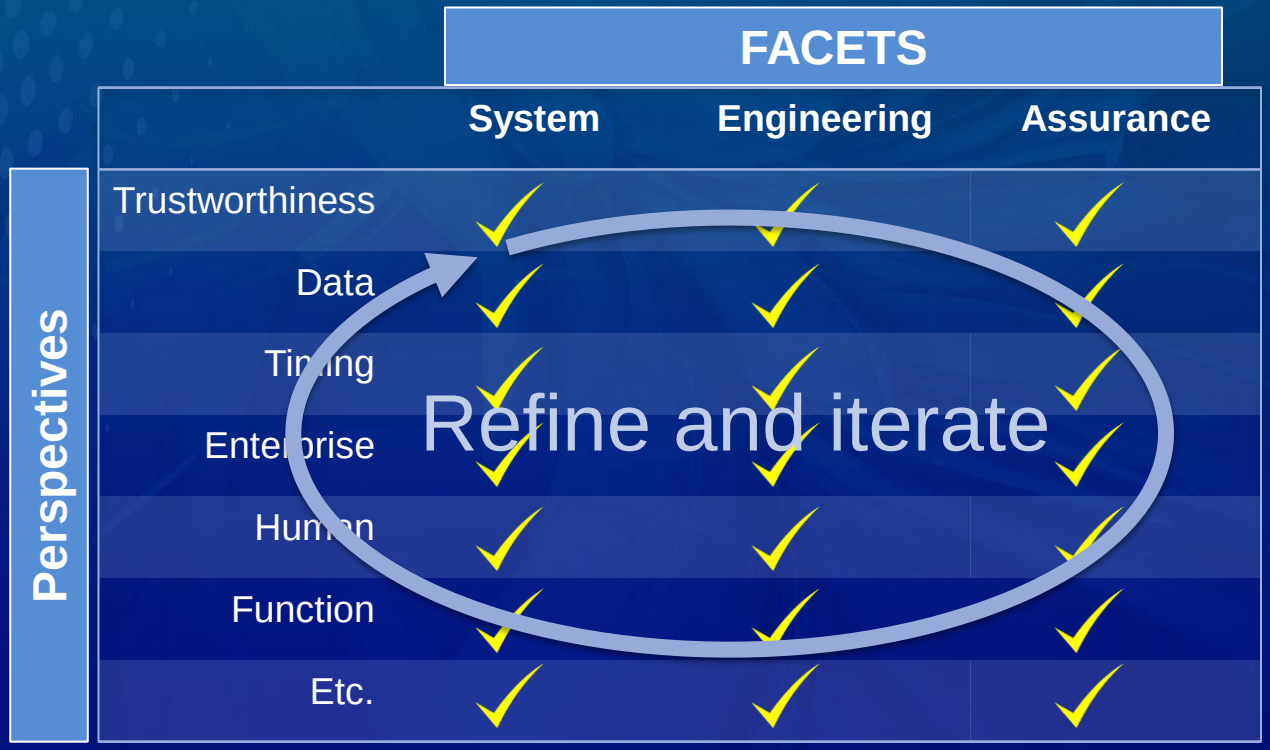
CPS Framework Structure



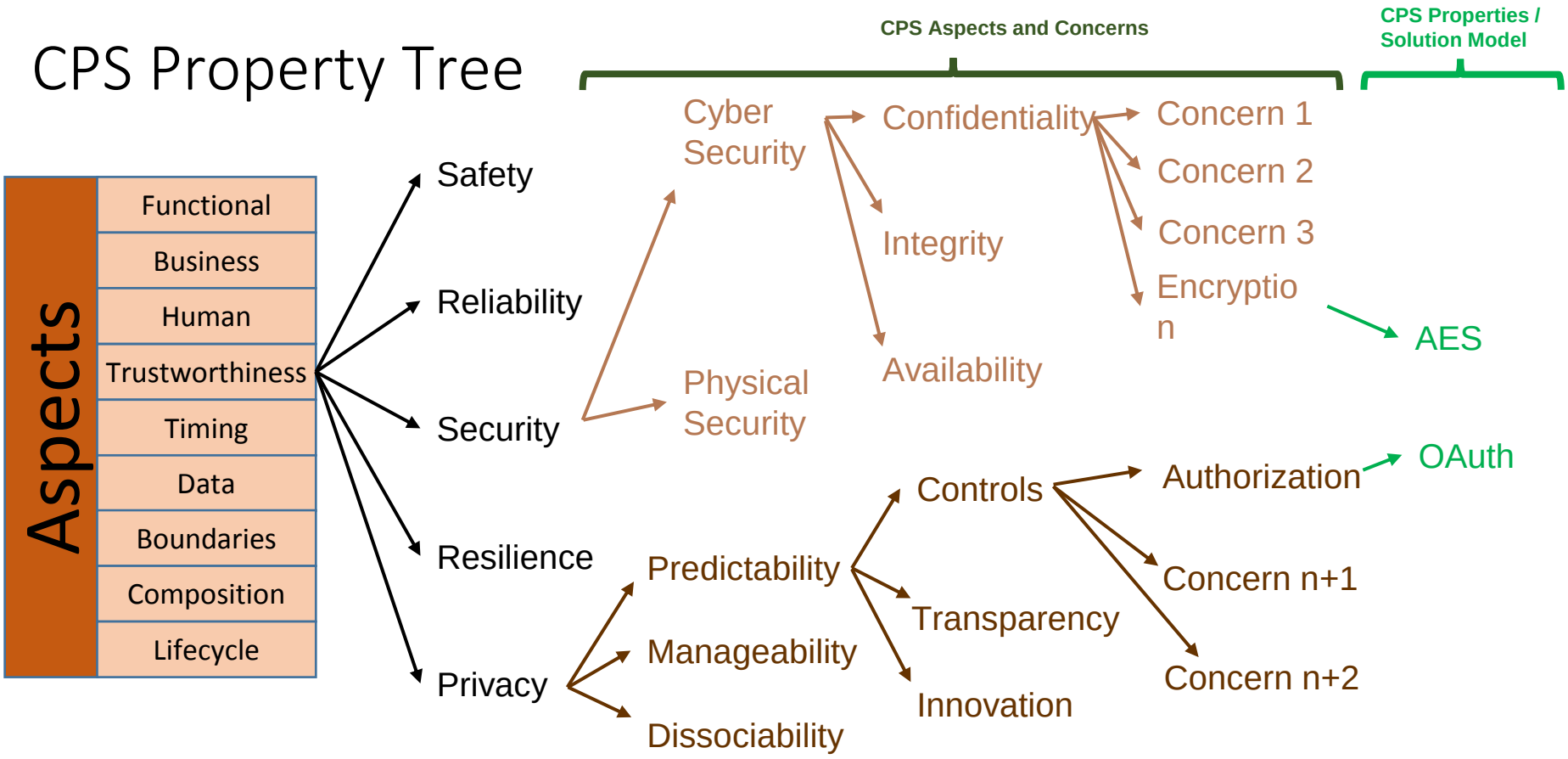
CPS Analytics



CPS Analytics: Agile Development



CPS Property Tree



Constructing Traceable Properties

Concern (Requirement)

A privacy protected message exchange might consist of the simultaneous set of properties:

Design Provision

{Trustworthiness.Security.Cybersecurity.Confidentiality.Encryption.AES}

{Trustworthiness.Privacy.Predictability.Controls.Authorization.OAuth}

Aspects

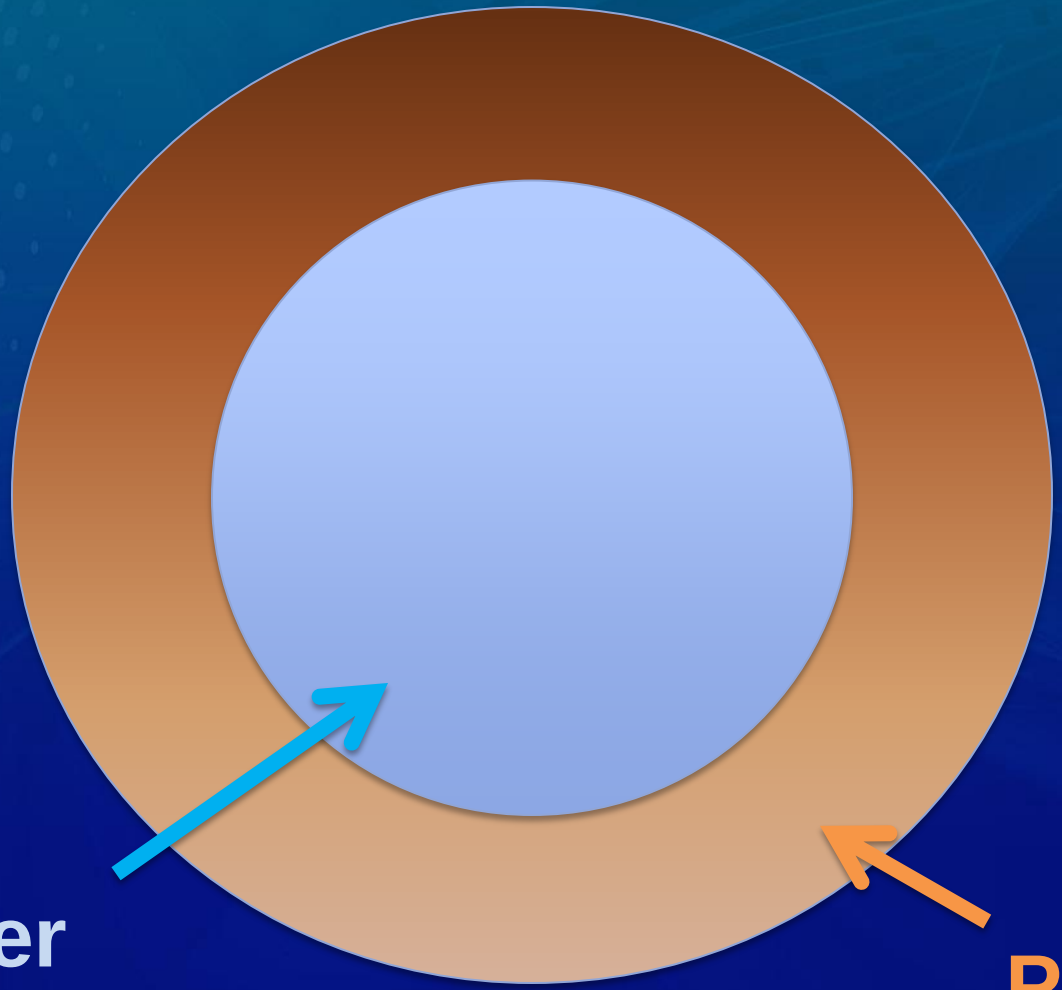
Functions

Internet of Things

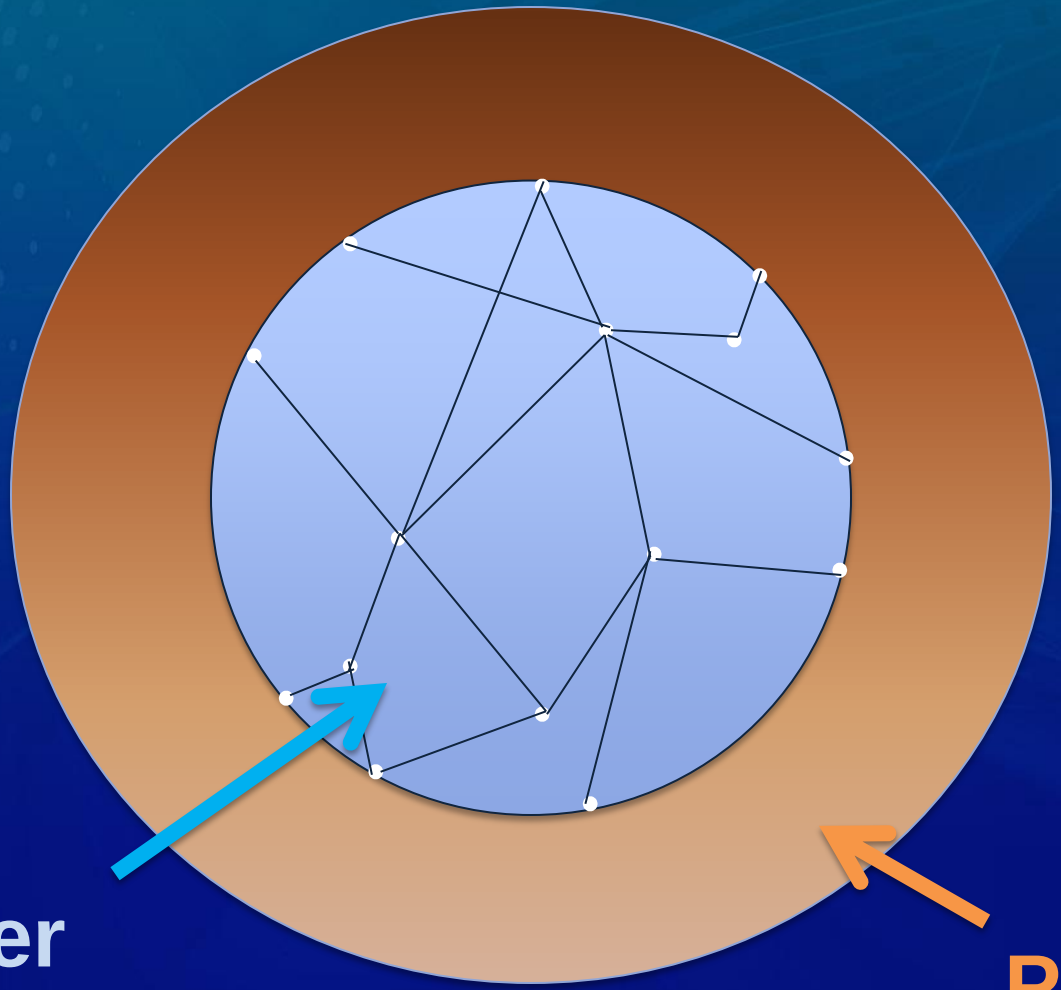
What are the key dimensions of the “Internet of Things?”

- Scale
- Capability
- Reach

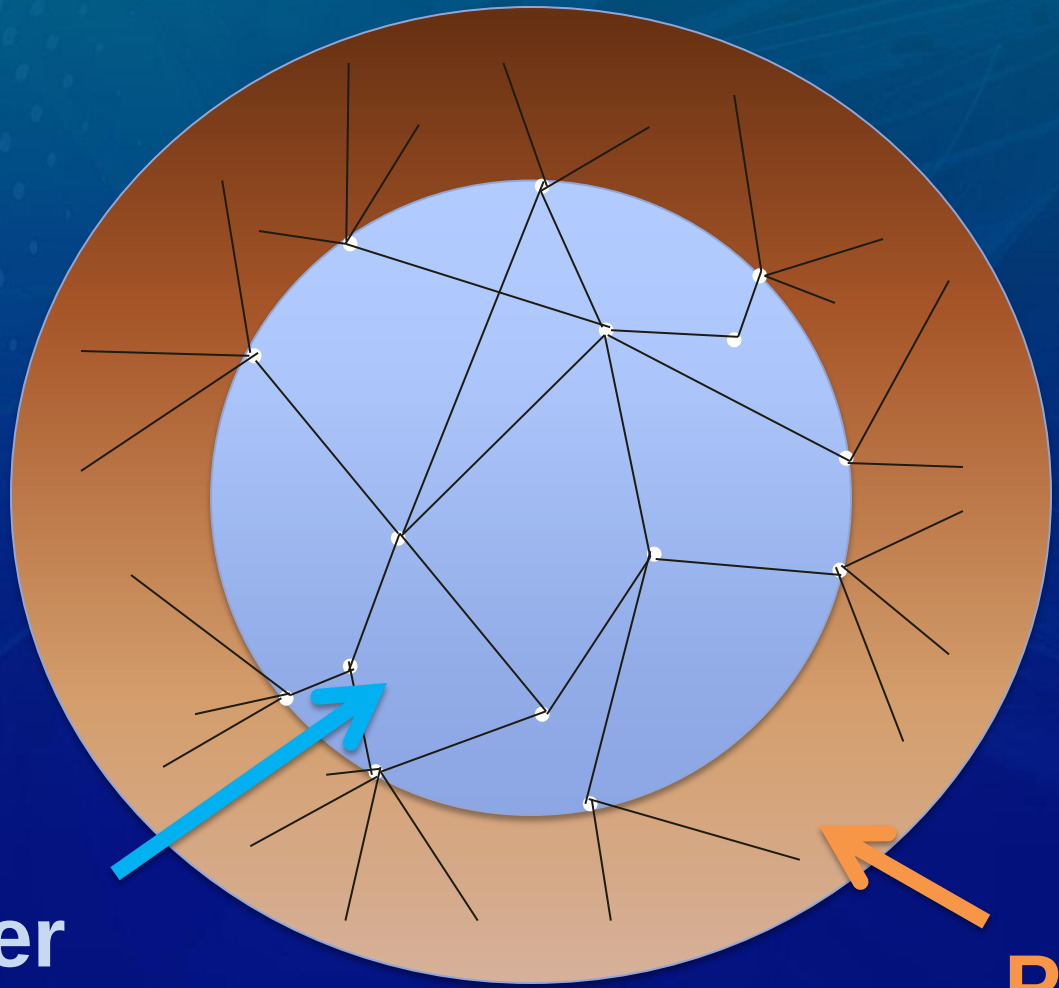
Reach Map



Internet – Reach Map



Internet of Things – Reach Map



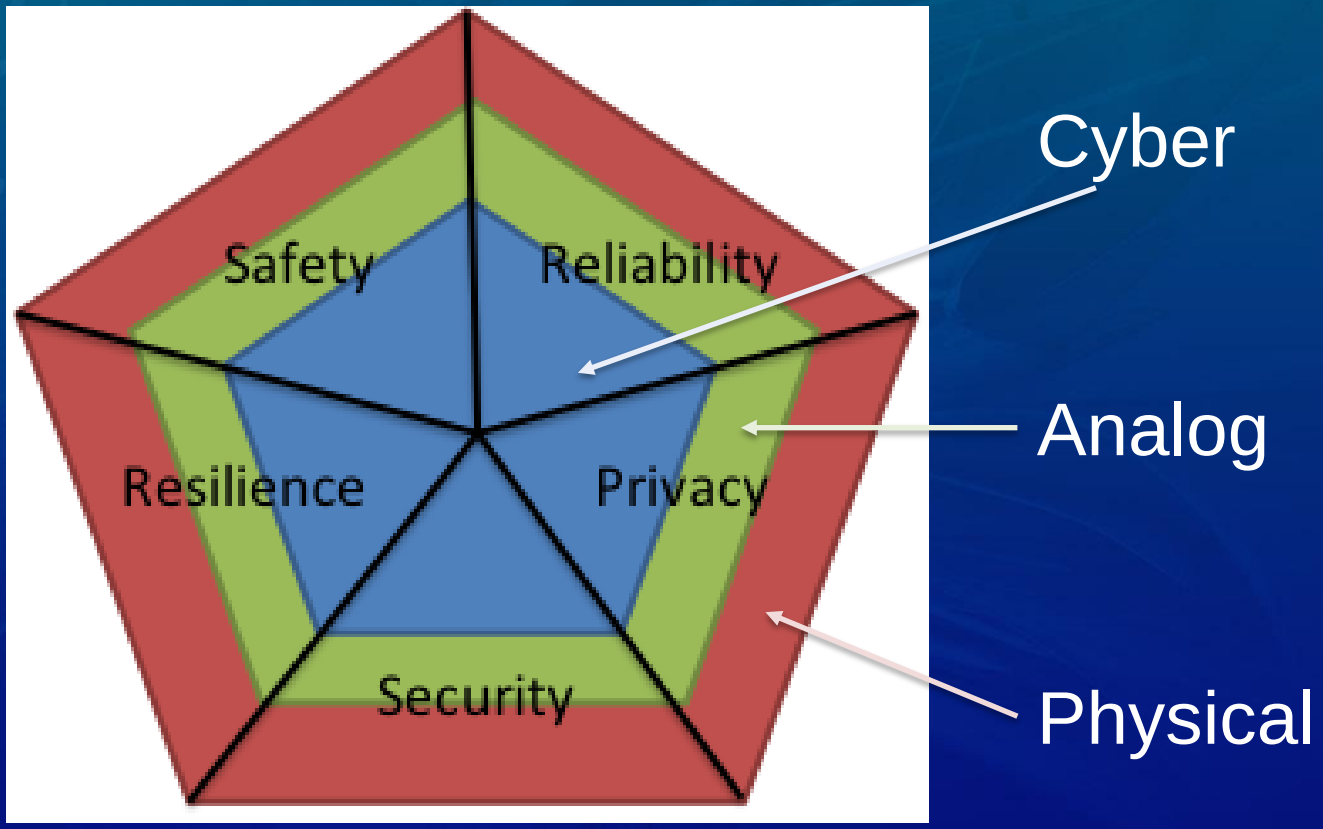
CPS Challenges: Measurement Science and Standards

- Integrating OT and IT Trust
- Integrating Physics-based and System Time
- Integrating IT, Engineered, and Human Elements
- Enabling Scalability and Compositionality

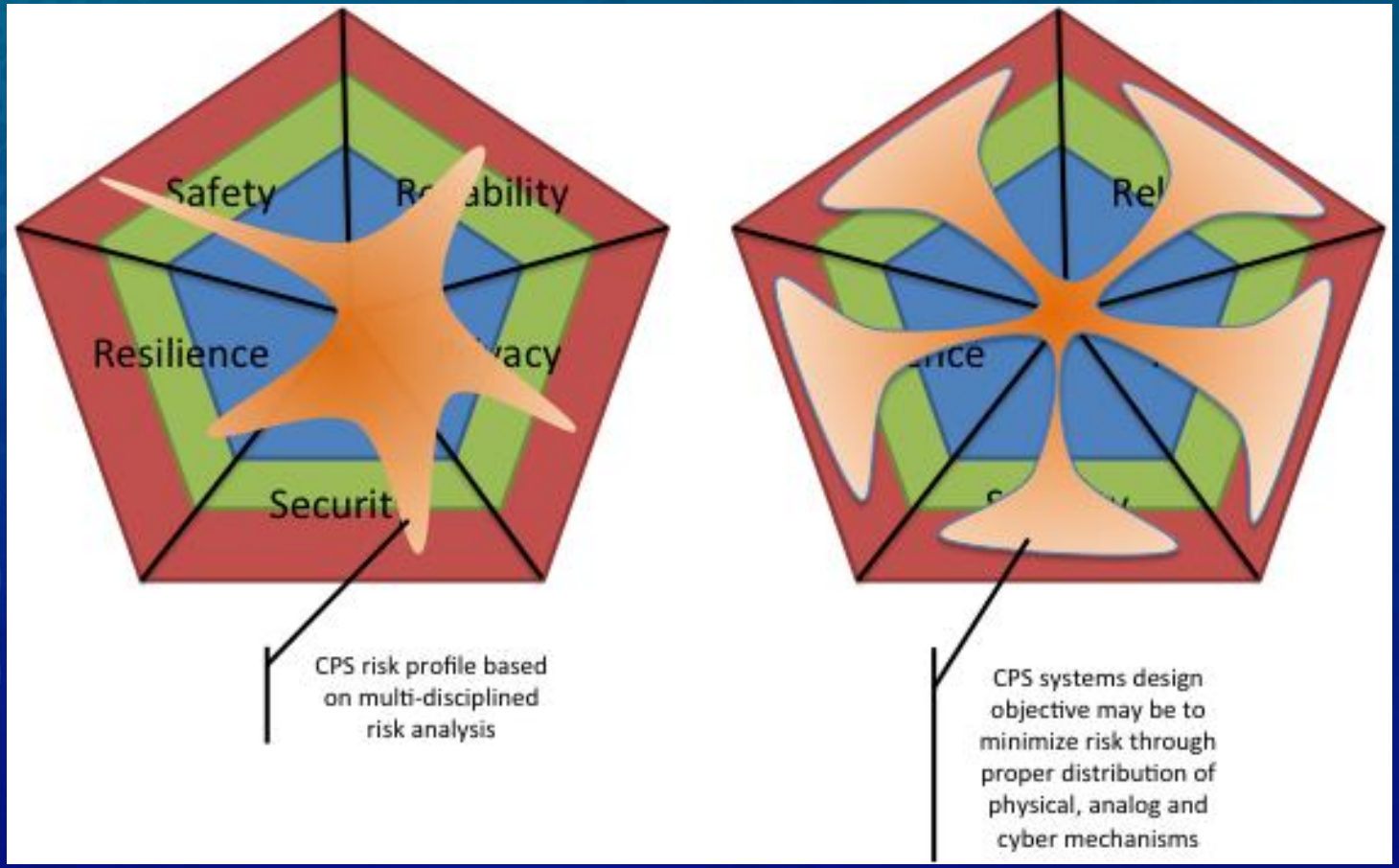
CPS Challenges: Measurement Science and Standards

- Integrating OT and IT Trust
- Integrating Physics-based and System Time
- Integrating IT, Engineered, and Human Elements
- Enabling Scalability and Compositionality

Integrating Operational and Information Technology Trust



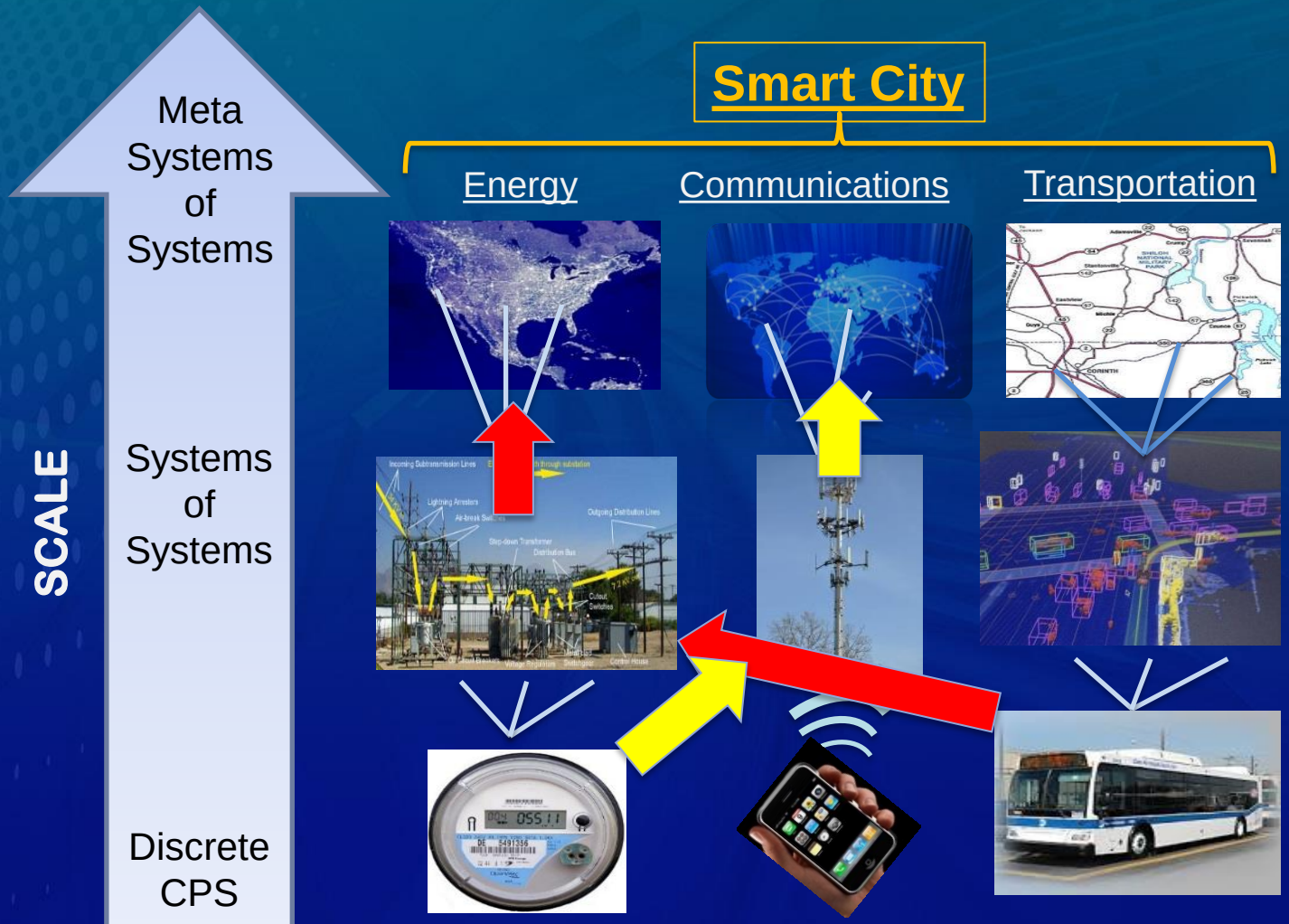
Integrating Operational and Information Technology Trust



CPS Challenges:
Measurement Science and Standards

- Integrating Physics-baseIntegrating OT and IT Trus
- Integrating Physics-based and System Time
- Integrating IT, Engineered, and Human Elements
- Enabling Scalability and Compositionality

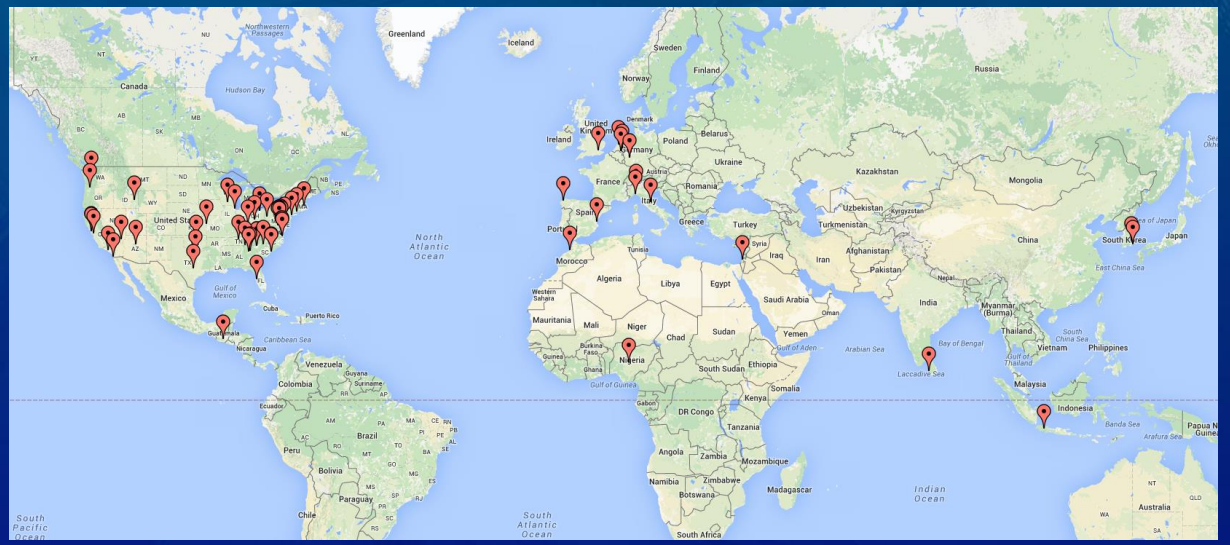
CPS: Scalability and Compositionality



GCTC Stats

Photo Credits: NIST / US-Ignite

- GCTC 2015 and 2016
  - 100+ teams have been identified/incubated
  - 300+ companies/organizations involved
  - 120+ municipal governments across the globe



GCTC 2016 Partners include:

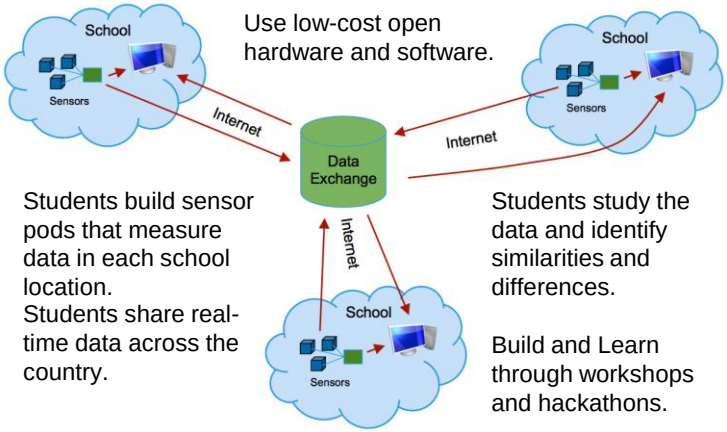
- NSF, ITA, Census, DoT, State Department, GSA, NCO/NITRD
- Governments of Netherlands, Italy, and South Korea
- AT&T, Intel, IBM, US Ignite, FIWARE, WeGO, IIC

Tech Jam: March 22-23, 2016, NIST

- 2016 Action Clusters to present their projects, add partners, form new teams

Bringing Internet of Things Know-How to High School Students

Today's students will be building the smart cities and communities of tomorrow.
The time to start learning is now.



Why?

- Strengthen STEM education and interest
- Learn about open hardware and software
- Learn to program hardware and sensors
- Learn how to share and analyze data
- Consider ways to leverage high-speed connectivity where available

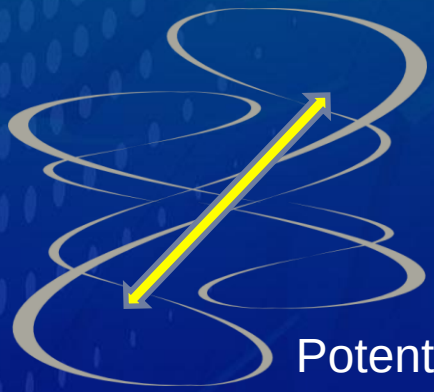
IoT DC Internet of Things DC | IoT Dev Labs | Arlington Virginia | VirginiaTech National Capital Region | Innovation Program Montgomery County, Maryland | + Students, High Schools, Educators and Volunteers

Internet of Things-Enabled Smart Cities Framework IES-City ("Yes-City")

Partners

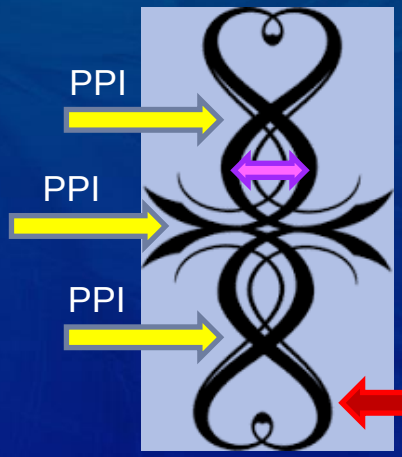
Pivotal Points of Interoperability (PPI)

Independent technology deployments



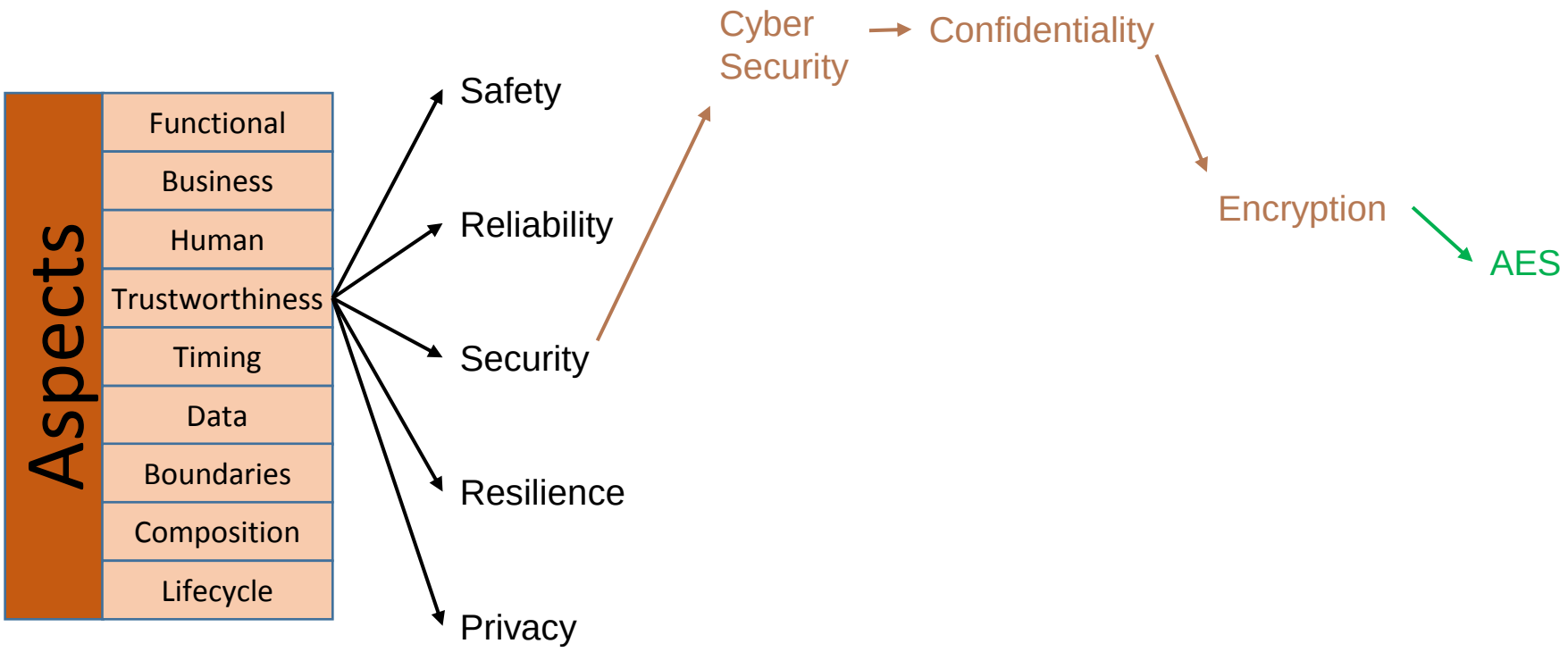
Potentially large distance to interoperability

With Pivotal Points of Interoperability



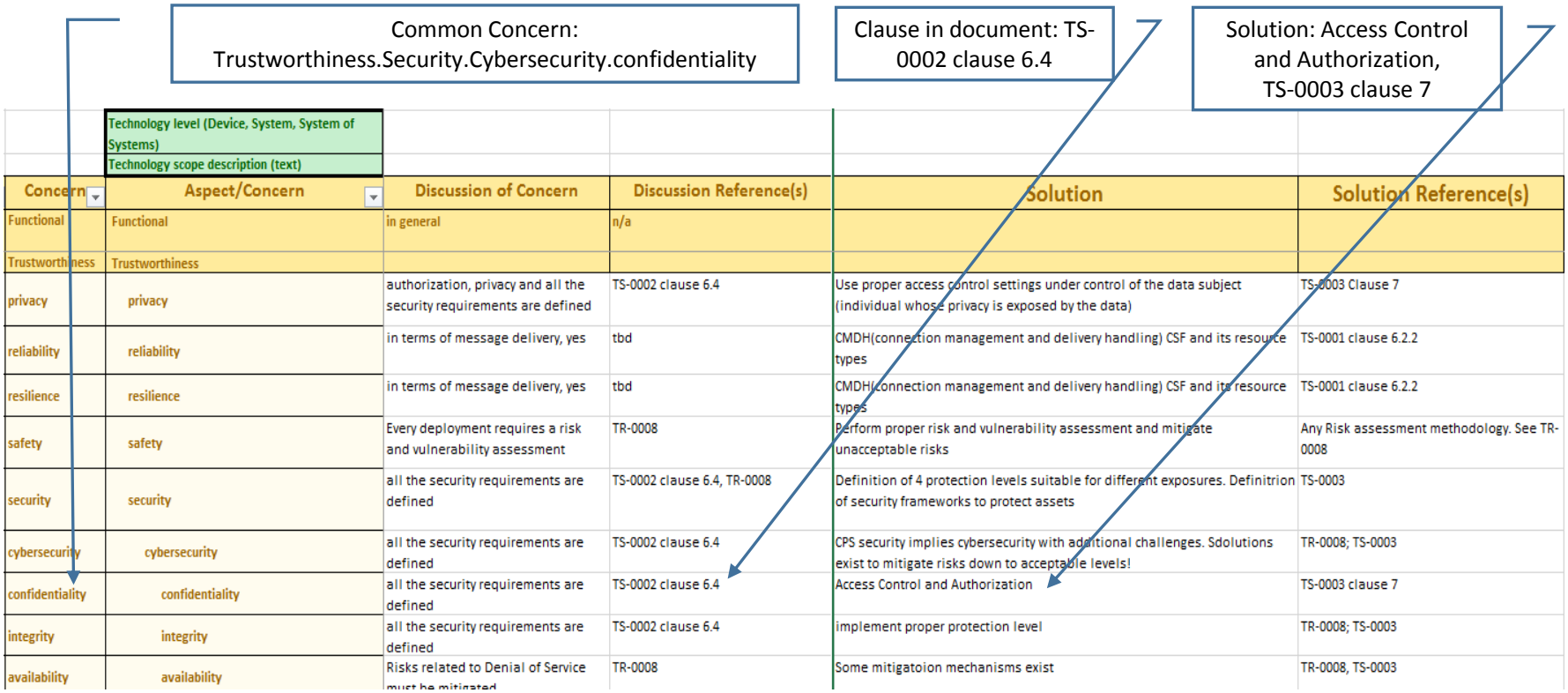
Minimize distance to interoperability

CPS Property Tree



{Trustworthiness.Security.Cybersecurity.Confidentiality.Encryption.AES}

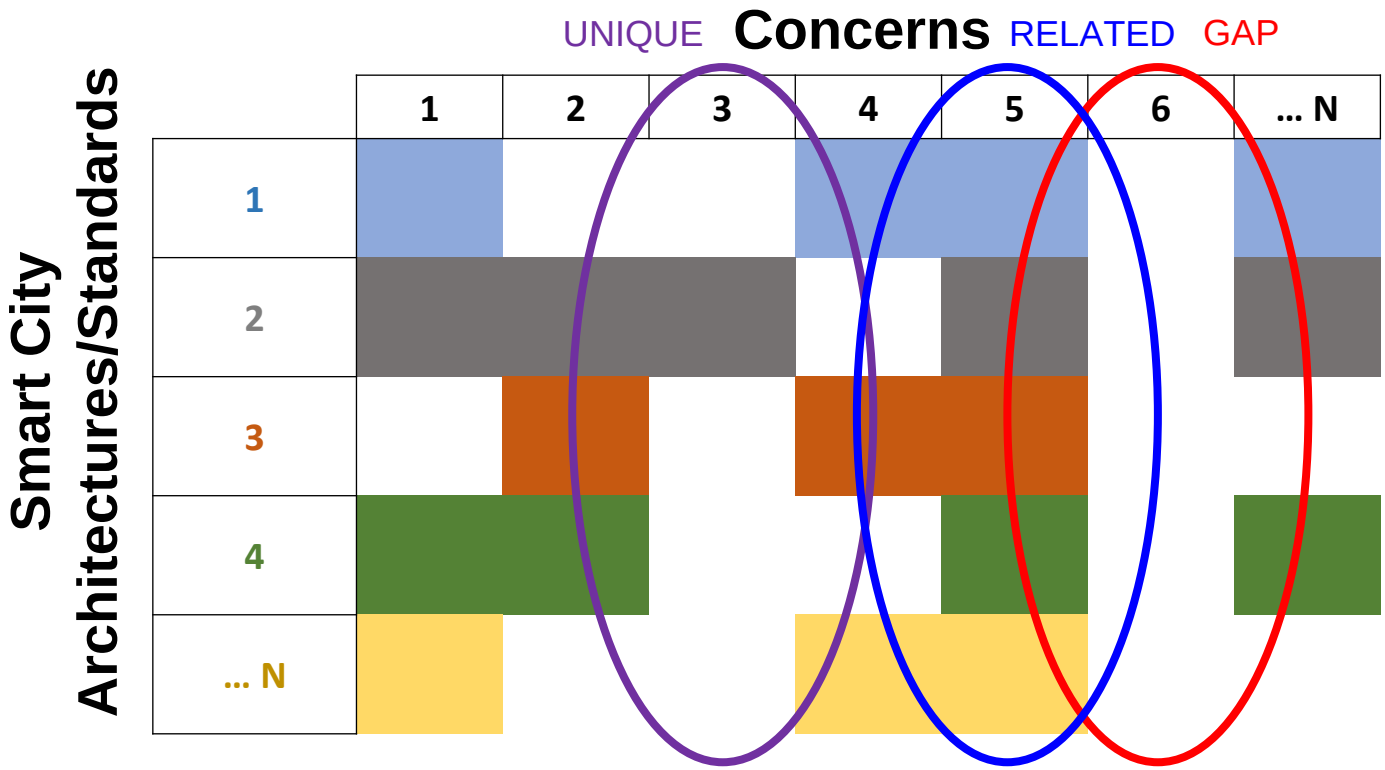
Concern-Driven Analysis of a Standard



	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



Internet of Things

What are the key dimensions of the “Internet of Things?”

- Scale
- Capability
- Reach

Privacy Engineering

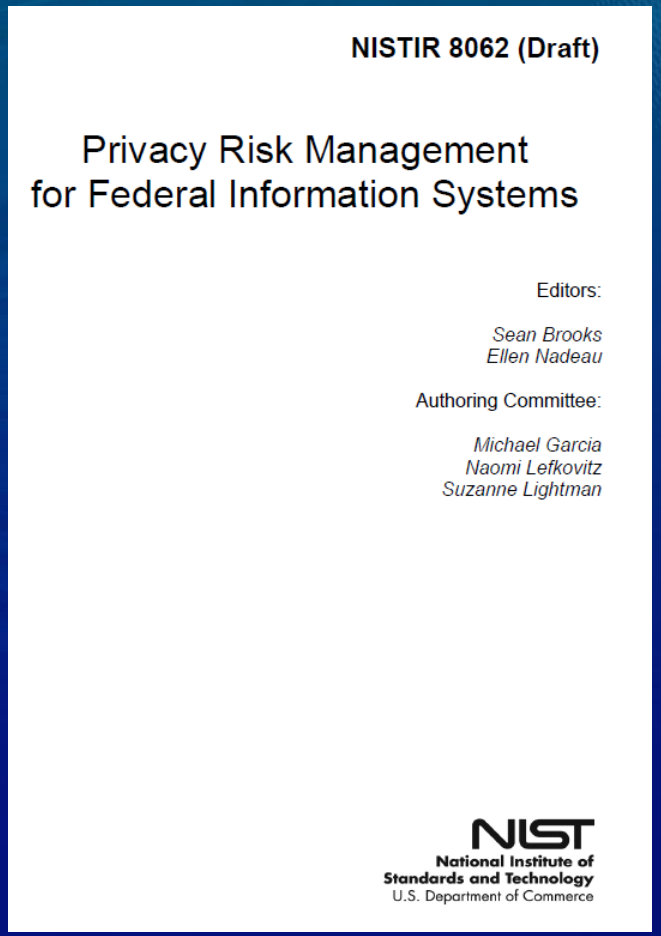
NIST's privacy engineering work is focused on providing guidance to developers and designers of information systems that handle personal information. The privacy engineering effort is primarily directed at mitigating risks arising from unanticipated consequences of normal system behavior.

See csrc.nist.gov/projects/privacy_engineering/

Draft Privacy Risk Management Framework

Draft NISTIR 8062 Includes:

- Common vocabulary
- Objectives to facilitate Privacy Engineering
- Risk model for assessing privacy risk in information systems



Internet of Things

What are the key dimensions of the “Internet of Things?”

- Scale
- Capability
- Reach

Contact Info

Chris Greer
Senior Executive for
Cyber Physical Systems

chris.greer@nist.gov
301 975 5919

Engineering Laboratory
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899-8600

www.nist.gov