NIST Cyber-Physical Systems Public Working Group (CPS PWG)

UPDATE WEBINAR

January 15, 2015

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

The CPS PWG is a key component of the NIST CPS program

- NIST mission: to promote U.S. innovation and industrial competitiveness to enhance security and improve the quality of life (working in partnership with industry, academia and gov't)
  - NIST provides a neutral perspective, technical expertise, and convening capability, with CPS activities in several NIST Labs
- Significant progress in 3 areas led by NIST Engineering Laboratory's Smart Grid and Cyber-Physical Systems Program Office:
  - **CPS Public Working Group (CPS PWG)**
    - **Update Webinar today, and F2F meeting April 7-8, 2015 NIST G'burg**
  - Smart America & NIST's Global Cities Team Challenge
    - GCTC TechJam, February 12-13, 2015 at NIST Gaithersburg
  - CPS Testbed Development – future R&D
    - CPS Testbed Workshop, February 24-25, 2015 at NIST Gaithersburg

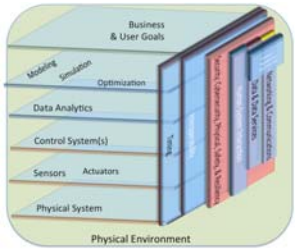
CPS PWG Goal:
CPS Framework and Roadmap(s) to support CPS research, development and deployment

- Need multi-domain perspective baked in
  - Applicable within all CPS domains
  - Supports cross-CPS domain applications

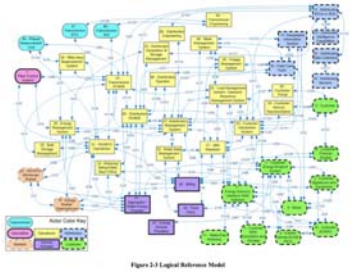
CPS Framework

Smart infrastructure (grid, water, gas, …)

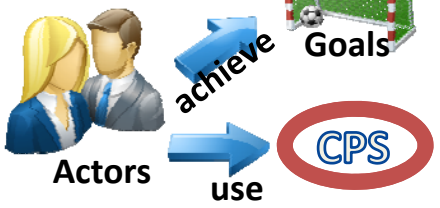
Smart buildings



Smart emergency response



Smart healthcare



Many more!!

Smart manufacturing

Smart transportation

CPS PWG outputs

The output of the CPS PWG are documents developed in three sequential phases:

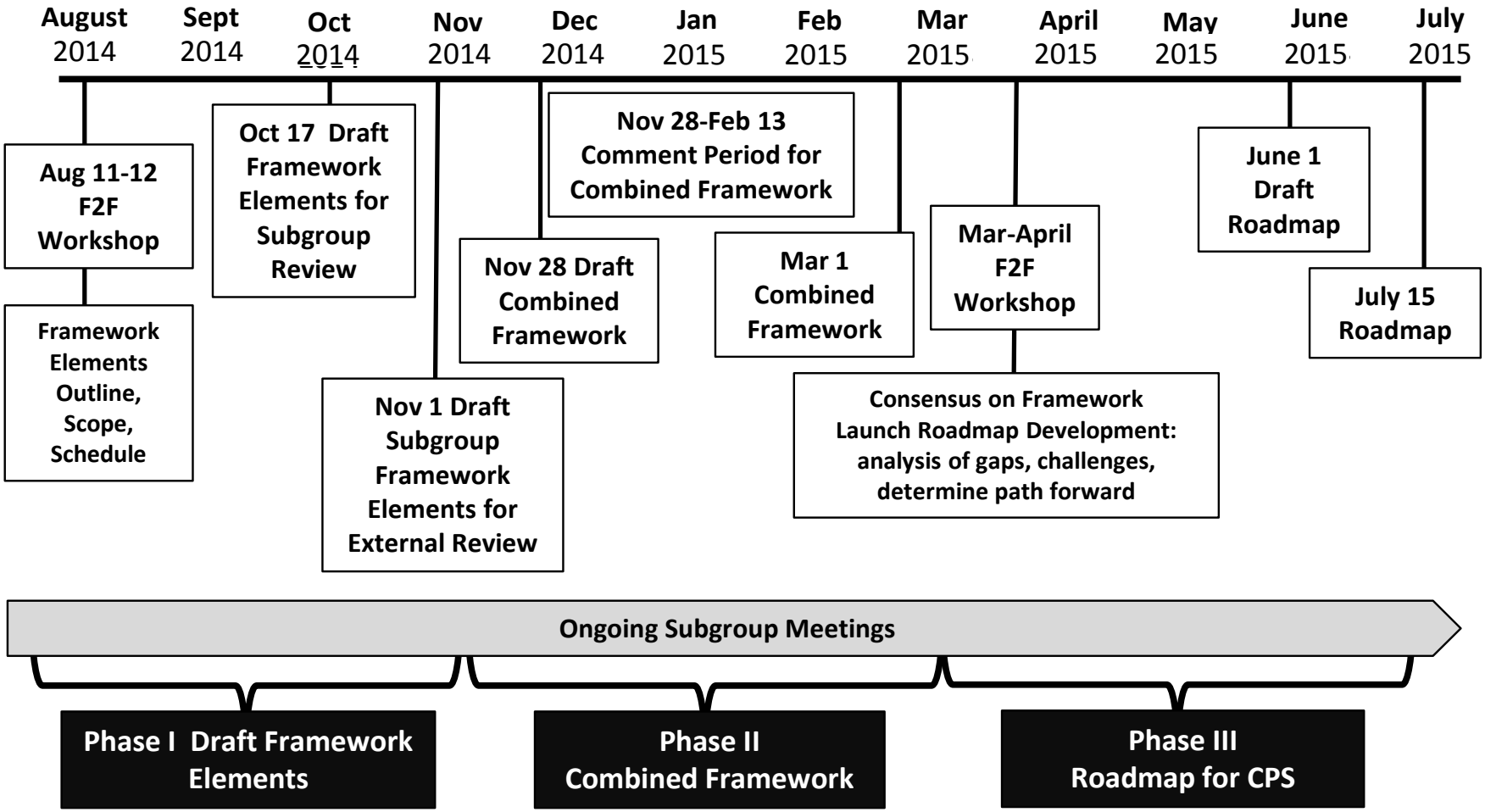
- **Phase I**: Initial "Framework Element" reports from each of the five subgroups – Reference Architecture, Use Cases, Cybersecurity, Timing, and Data Interop.
- **Phase II**: CPS Framework document created by integrating the subgroup reports and subsequent refining
- **Phase III**: CPS Technology Roadmap identifying opportunities and desired time schedule for a coordinated effort on key technical challenges

Key characteristics of CPS PWG outputs: open use, freely available online, technology-neutral and business-model neutral, representative of consensus (but not necessarily unanimous) tech perspective/group

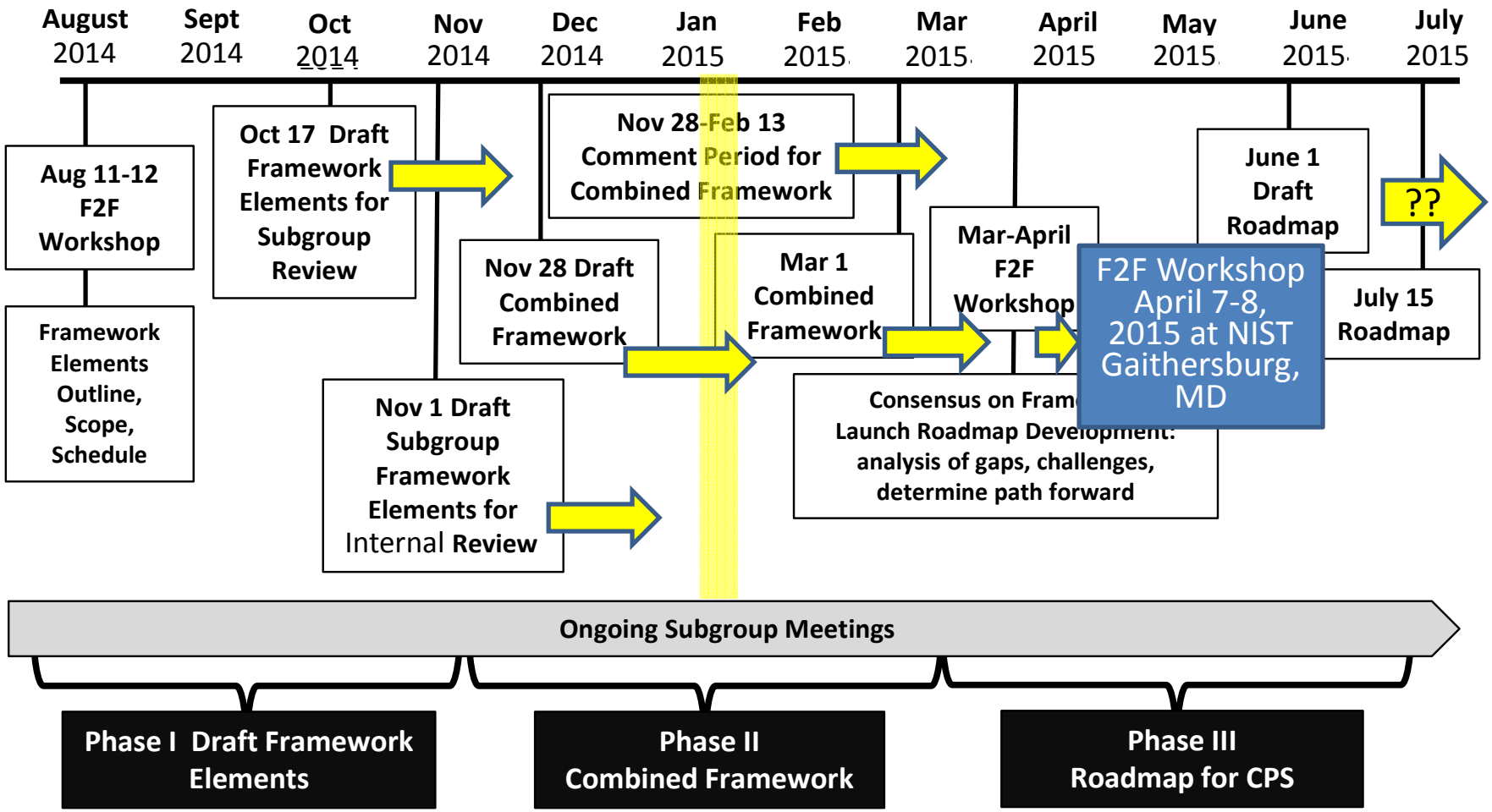
CPS PWG progress

- **We have come a long way in a short time!** Starting with the CPS PWG kickoff webinar (June 30, 2014) and our first Face-to-Face meeting (August 11-12, 2014) to launch Phase I, the five subgroups initiated email list discussions and regular teleconferences with content/notes on www.cpspwg.org for subgroup members.
- With the help of a little extra time in Nov/Dec 2014, **all five CPS PWG subgroups have completed their initial CPS "Framework Element" documents … CONGRATS!**
- We have now started Phase II, in which the **Framework Element documents have been being combined into an initial draft integrated CPS Framework document**—currently being circulated with the subgroup cochairs. Working on review process …
- Looking ahead, our **upcoming CPS PWG F2F meeting (April 7-8, 2015 at NIST, Gaithersburg, Maryland)** will conclude Phase II and launch the Phase III Roadmapping activity... Save the Date and join us!

Original timeline for CPS PWG outputs



Modified timeline for CPS PWG outputs



CPS PWG Subgroup Co-Chairs

CPS PWG Chairs: David Wollman and Chris Greer (NIST)

Co-Chairs	Reference Arch	Use Cases	Security	Timing	Data Interop
NIST	Abdella Battou	Eric Simmon	Vicky Pillitteri	Marc Weiss	Marty Burns
Academia	Janos Sztipanovits	John Baras	Bill Sanders	Hugh Melvin	Larry Lannom
Industry	Stephen Mellor	Stephen Mellor	Claire Vishik	Sundeep Chandhoke	Peggy Irelan

NIST has contracted with Energetics to provide support for the CPS PWG and its subgroups and collaboration website. NIST has also contracted with Trusted Security Alliance, LLC (G2, Inc.) to provide SME support.

CPS PWG: Reference Architecture

Co-chairs: Abdella Battou, Janos Sztipanovits, Stephen Mellor

Presenters:
Edward Griffor
Janos Sztipanovits
Shi-Wan Lin

CPS Framework Intent

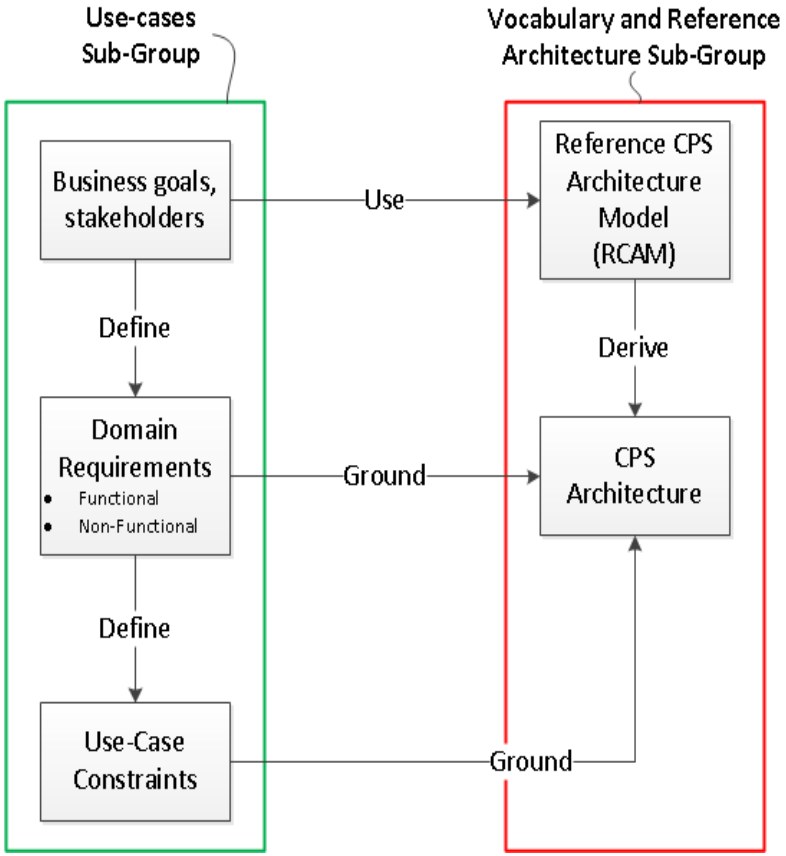
This 'CPS Reference Architecture' intends to provide guidance that will allow a broad range of smart devices to work together to provide functions that will drastically improve quality of life.

Cyber-physical systems (CPS):

- smart systems that include co-engineered interacting networks of physical and computational components.
- intentionally cross product in their conception, design, and execution and will …
- provide and enable collaborative and emergent functions that can drastically improve 'quality of life' (personalized health care, emergency response, traffic flow management, smart manufacturing, defense and homeland security, energy and more)

Ref Arch: Document Methodology

- Assemble high level concepts that capture all of key elements present in a variety of current applications of CPS
- Capture the interactions and relationships between these elements
- Categorize them relative to their role in the system
- Partition into ***architecture layers*** with a common type of interactions
- Determine the interactions and correspondences between layers
- Provide a common language and common constructs, the ***framework***, to facilitate the future development and maintenance of CPS
- Use this common framework to identify critical, ***cross-cutting concerns*** and ***cross-cutting functions*** that address them such as safety and security



CPS Framework as Guidance

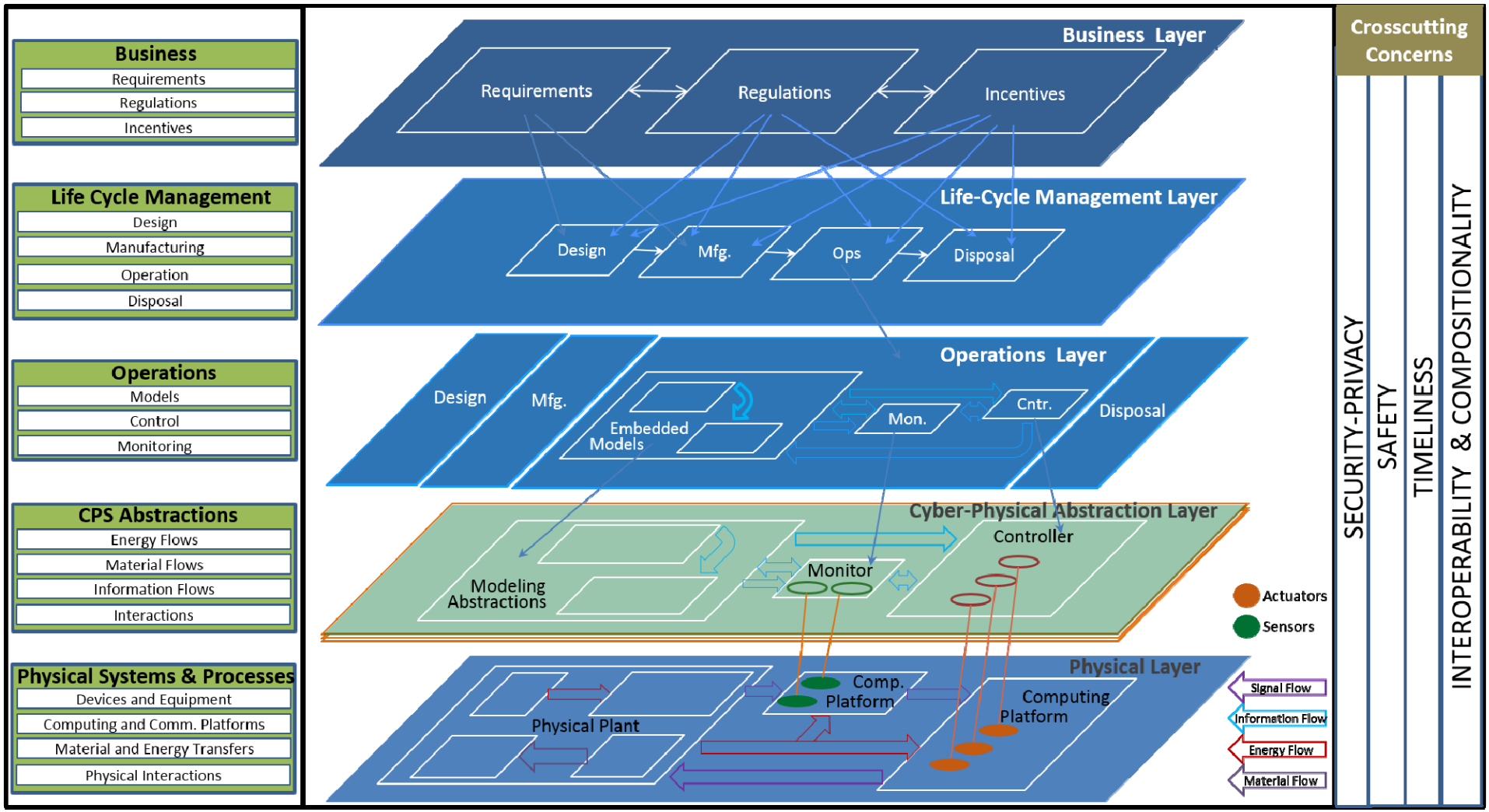
I. CPS architecture is a concrete realization of a CPS Reference Architecture designed to satisfy use-case-specific constraints (domain and implementation specific)

II. Use cases cascade into Functional and Non-Functional Requirements to Constraints

Ref Arch: Framework Document Elements

- Purpose and Scope: Background, Use, Key Concepts, Definitions, Applications and Requirements, Framework
- Reference Architecture
  - Overview
  - Key Architectural Concepts for CPS
  - Cyber-Physical System Layers (Business, Life Cycle Management, Operations, Cyber Physical Abstraction and Physical Layers)
  - Towards a Cross-Sector Reference Architecture Model
    - Bootstrapping the CPS Reference Architecture
    - Other Standards and Activities
    - References
  - CPS Functional Framework
    - Conceptual Functional View: Systems of Systems
    - A Functional Decomposition of the cyber-physical systems
    - Crosscutting Functions
- Annex: The Reference Architecture Function View

CPS Engineering Viewpoint



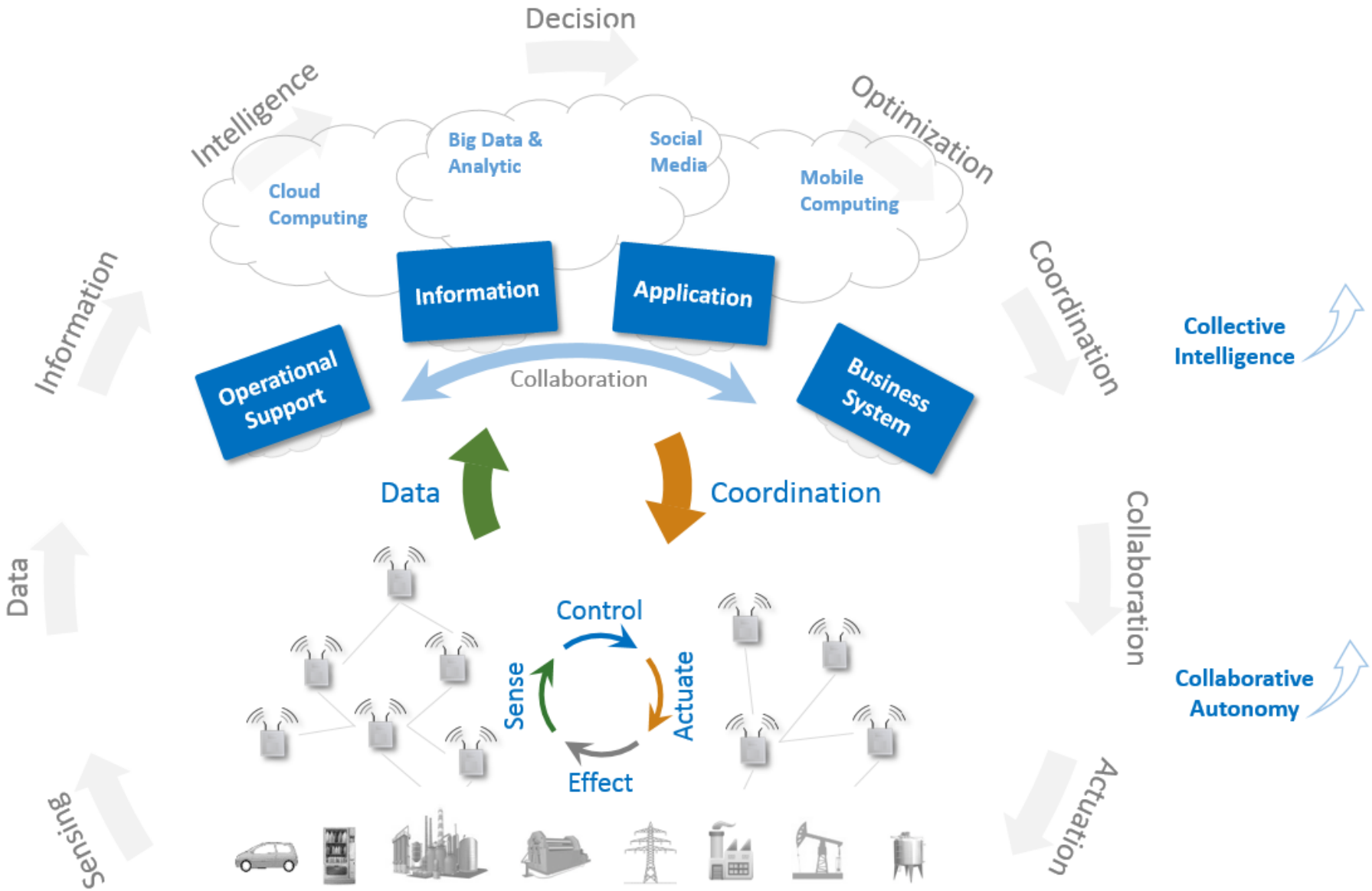
Engineering Viewpoint Highlights

- **The engineering viewpoint defines conceptual layers** that are essential in engineering CPS. Each layer defines concepts, relationships, notional architectures and technology infrastructure that can be instantiated into layer and domain specific CPS architectures
- **Layers in the engineering viewpoint are not structured according to 'cyber' and 'physical' system types.** They are equally relevant to either implementation technologies. For instance, the Physical Layer includes physical substrates and processes related to computation and communication. Accordingly, direct physical interactions (e.g. RF interference or heat flow) among computing devices and other physical devices may be subject to design, manufacturing or operational considerations.
- The **CPS Abstraction Layer(s)** extend to both cyber and physical aspects and enable modeling, analysis, synthesis and verification of CPS without early commitment to specific implementation technologies. The primary goals in formulating suites of abstractions for different CPS categories are enabling co-design, supporting design tradeoffs across disciplinary boundaries, understanding operational implications of faults and cyber attacks, optimization of operation characteristics across system layers and much more.
- **Crosscutting concerns** in the engineering viewpoint represent system level properties that have manifestations on each layer.

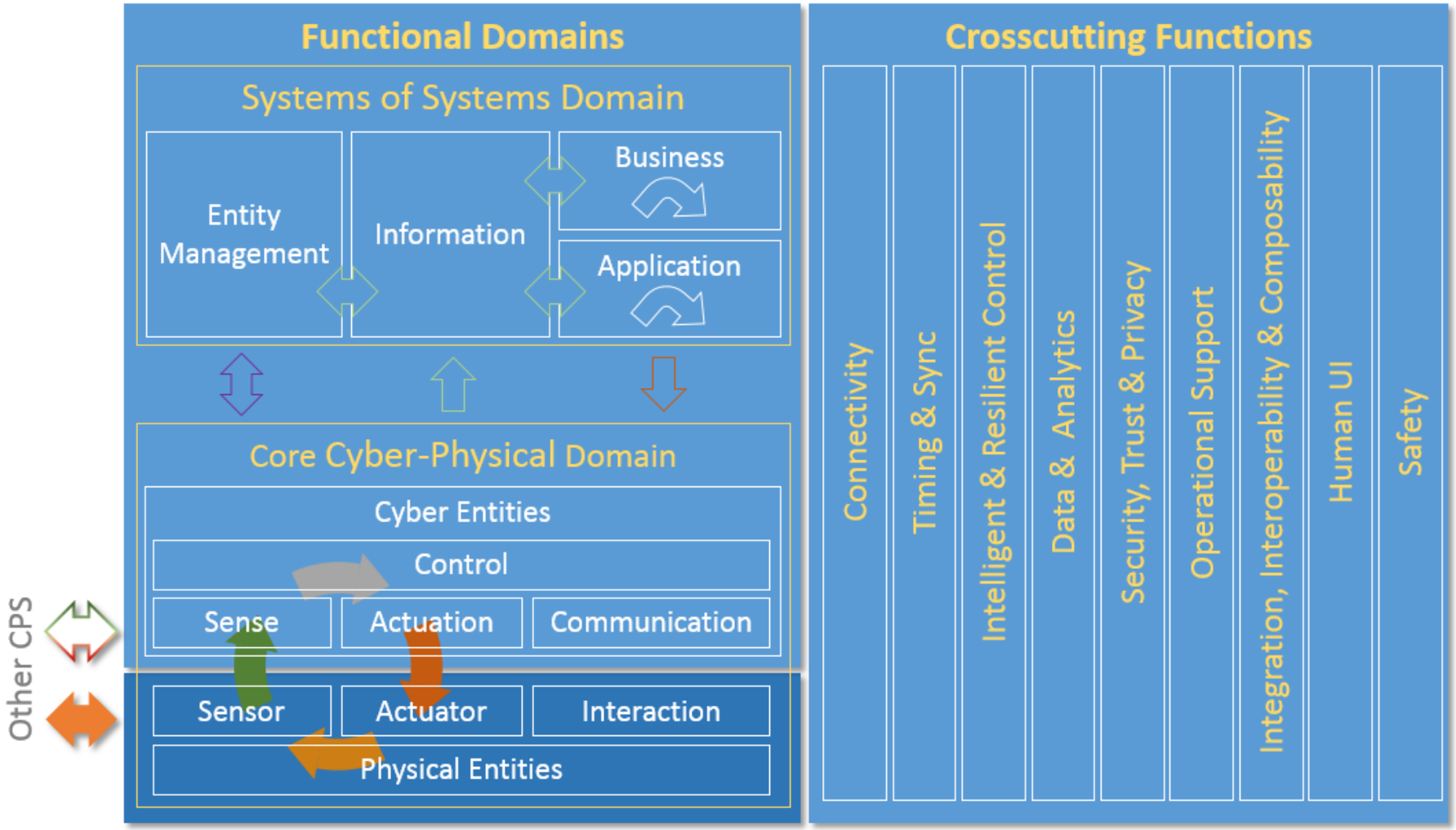
CPS Functional Viewpoint

- An architectural description of
  - basic and common high-level functions of CPS
  - functional decomposition of a CPS
  - structure, relations and interactions of CPS components
- An functional reference architecture
  - abstract & generic – inspired by known usecases and informed by technology roadmaps but not constrained by either
  - applicable to various industrial sectors
  - common starting point for system conception
  - promote interoperable and compostable functional building blocks
- Guided by considerations of broad technology trends & their potential impacts on the evolution of CPS
- Consists of
  - Functional Domains
  - Crosscutting Functions

CPS Environment



CPS Functional Domains & Crosscutting Functions



Ref Arch: Future Steps

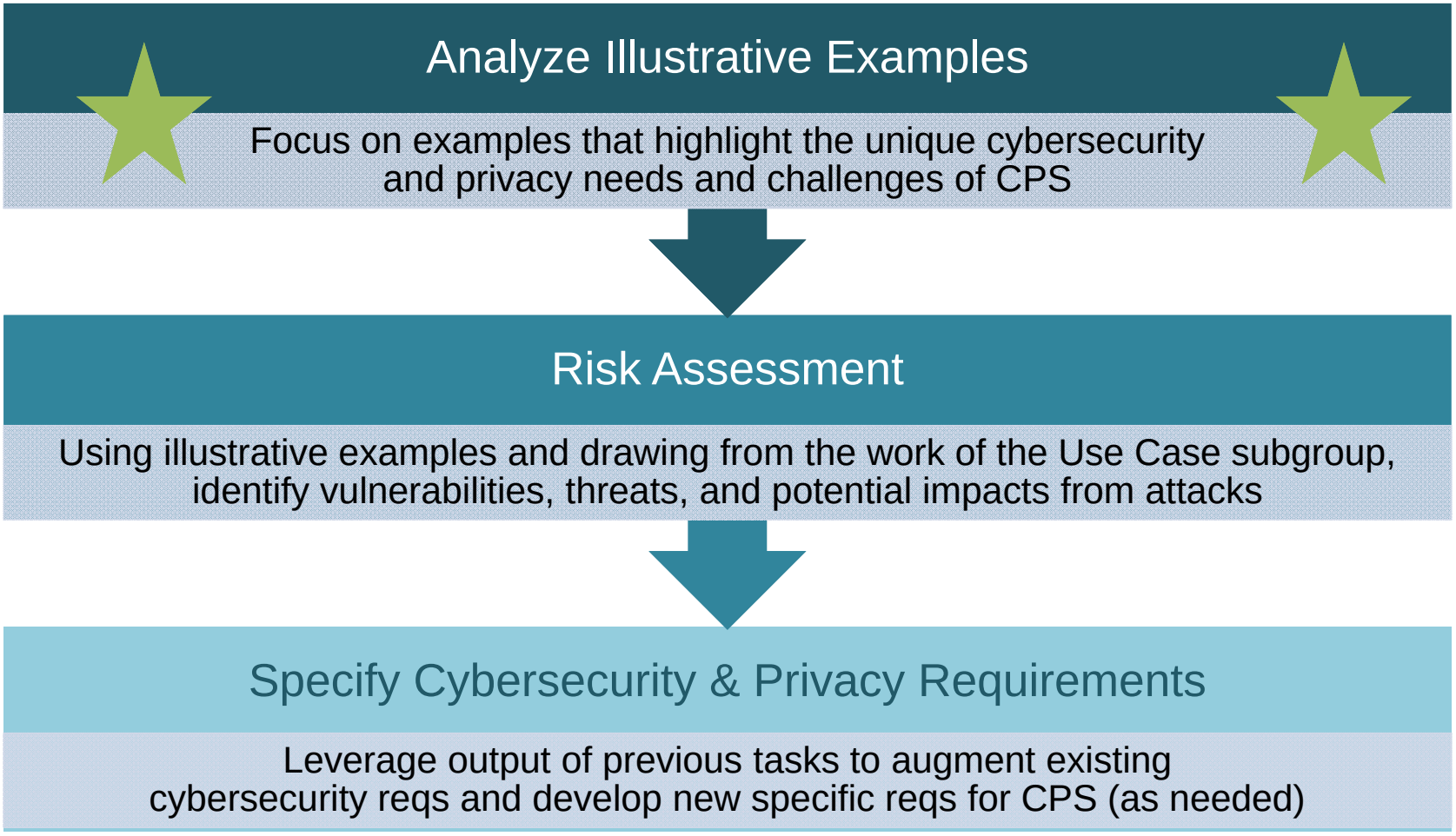
- **Establishing synergy across the different subgroup documents.** This will be a quite significant effort. Probably a smaller team would need to go through in depth the materials and raise flags where inconsistencies are obvious. After this the document owners need to find resolution. A possible alternative is that the small review team also proposes a resolution and the document owners accept or reject it.
- **Enrich the document with illustrative examples.** E.g. showing how use cases can be mapped on the reference architecture; how co-design can be utilized; etc…These could be included in the Appendix and referenced only in the core material.
- **A discussion on the level of autonomy of system(s) of systems**
- **Validation by means of a case study** of appropriate size or at minimum develop a CPS development work flow for a specific domain based on the RA.

CPS PWG: Cybersecurity and Privacy

Co-chairs: Vicky Pillitteri, Bill Sanders, Claire Vishik

Presenter: Claire Vishik

CPS PWG: Cybersecurity & Privacy Methodology



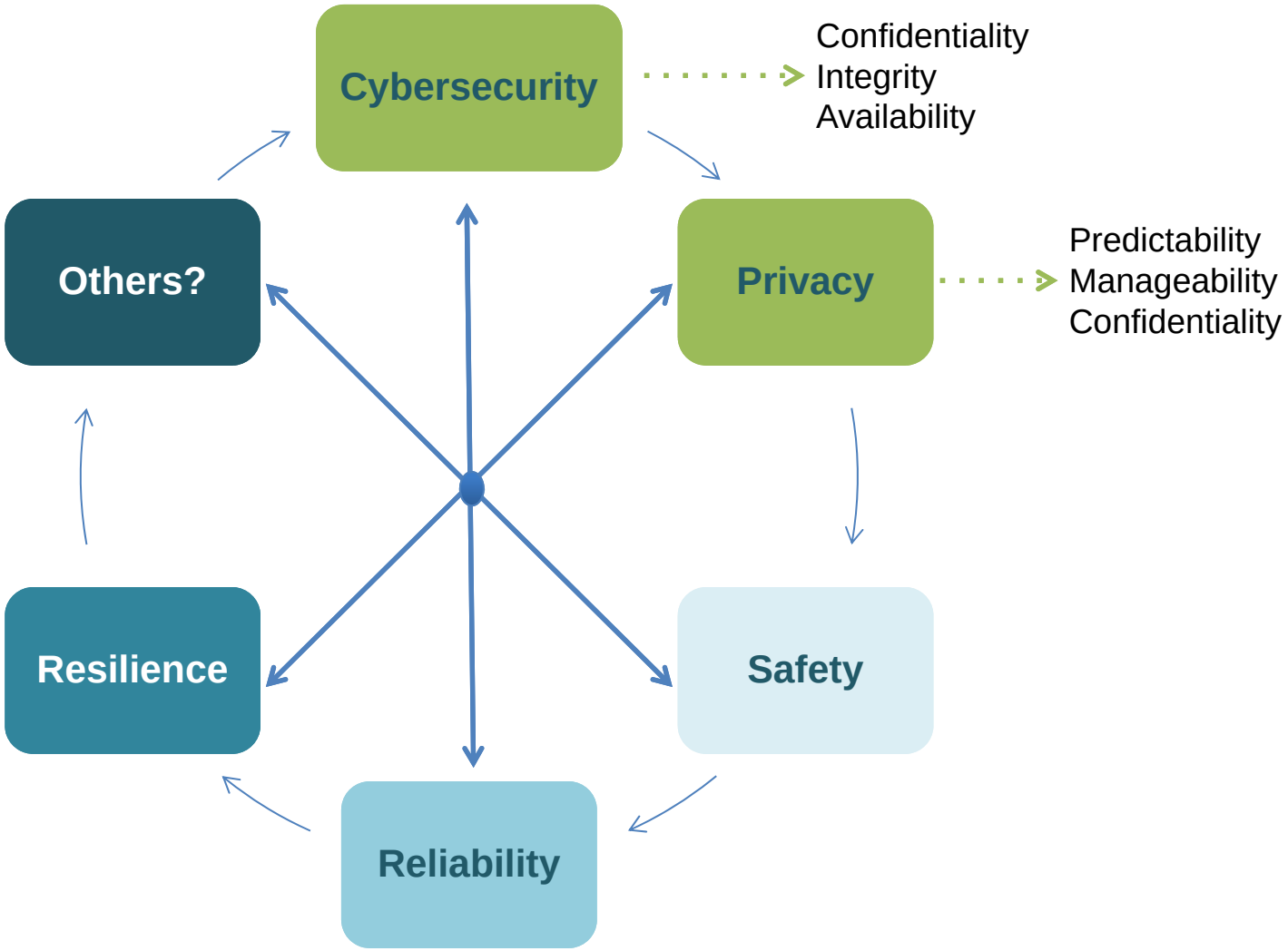
Input from Working Draft

Properties relevant for cybersecurity and privacy

- Wide range of contexts and operational conditions
- “Systems of systems”
- Impact on physical world and cyber world
- Time-aware operations
- Resource constrained platforms
- Stringent “Always on” and resilience requirements
- Lifecycle challenges
- Diversity of privacy contexts
- Safety controls
  - Could provide non-cyber solutions for cybersecurity problems

Input from Working Draft

The Relationship to other Domains such as Safety, Reliability, and Resilience



Input from Working Draft

Future Work and Roadmap Needs

- Next CPS Cybersecurity & Privacy Subgroup Virtual Meeting: January 29 at 4 PM Eastern

- Ongoing work on evolving the discussion of the relationship to other domains such as safety, reliability, and resilience
- Begin discussion of roadmap areas for CPS Cybersecurity

CPS PWG: Timing and Synchronization

Co-chairs: Marc Weiss, Hugh Melvin, Sundeep Chandhoke

Presenter: Sundeep Chandhoke

Methodology for Developing Framework for Timing and Synchronization in CPS

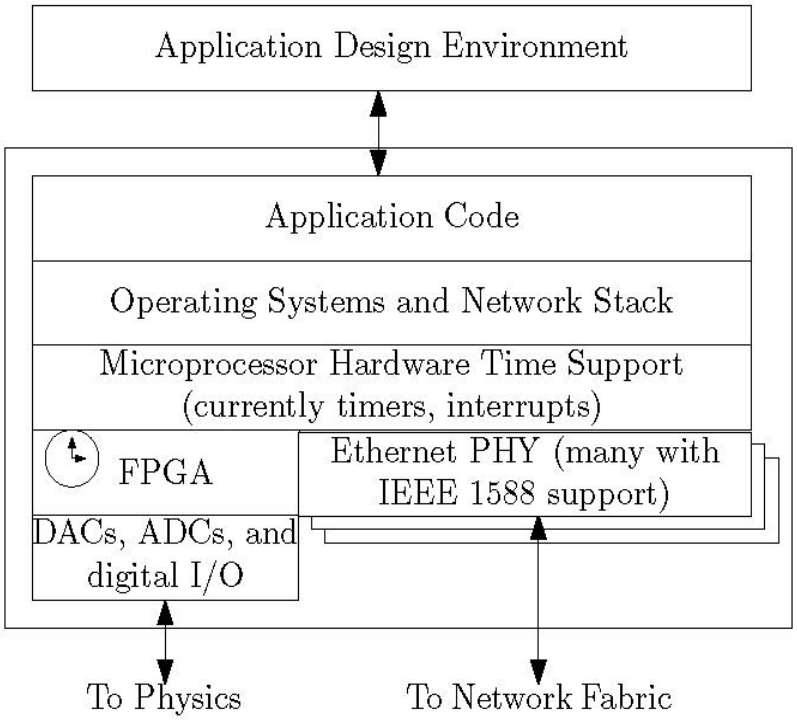
1. Fundamental concepts regarding timing and synchronization in CPS
   a. Timing has a fundamental challenge in CPS that is not well-understood
   b. Timing can enable more than is currently used in CPS
2. Need for and status of time-awareness in system elements of a CPS
   a. Time-awareness is needed for CPS operation
   b. Current status of time-awareness in systems needs to grow
3. Timing and latency in CPS
   a. A convergence of timing with cyber-systems is growing out of CPS
4. Special security issues that arise with timing in CPS
   a. CPS require both cyber-security *and* security of physical timing signals
   b. This latter creates unique security requirements for timing

1. Fundamental concepts regarding timing and synchronization in CPS

- Precise timing in a CPS can
  - Enable better implementation of control systems,
  - More robust correlation of acquired data for measurement applications
  - Permit CPS that have large spatial extent and/or higher degrees of complexity
  - Facilitate new application domains and approaches
- Important aspects of timing in a CPS are:
  - Timing Predictability
  - Temporal Determinism
  - Concept of a time-interval (TI) that is characterized by
    - Epoch (which marks the origin)
    - Rate at which time advances
    - Ability to correlate to an internationally defined time-scale like TAI or UTC (traceability)

2. Need for and Status of time-awareness in system elements of a CPS

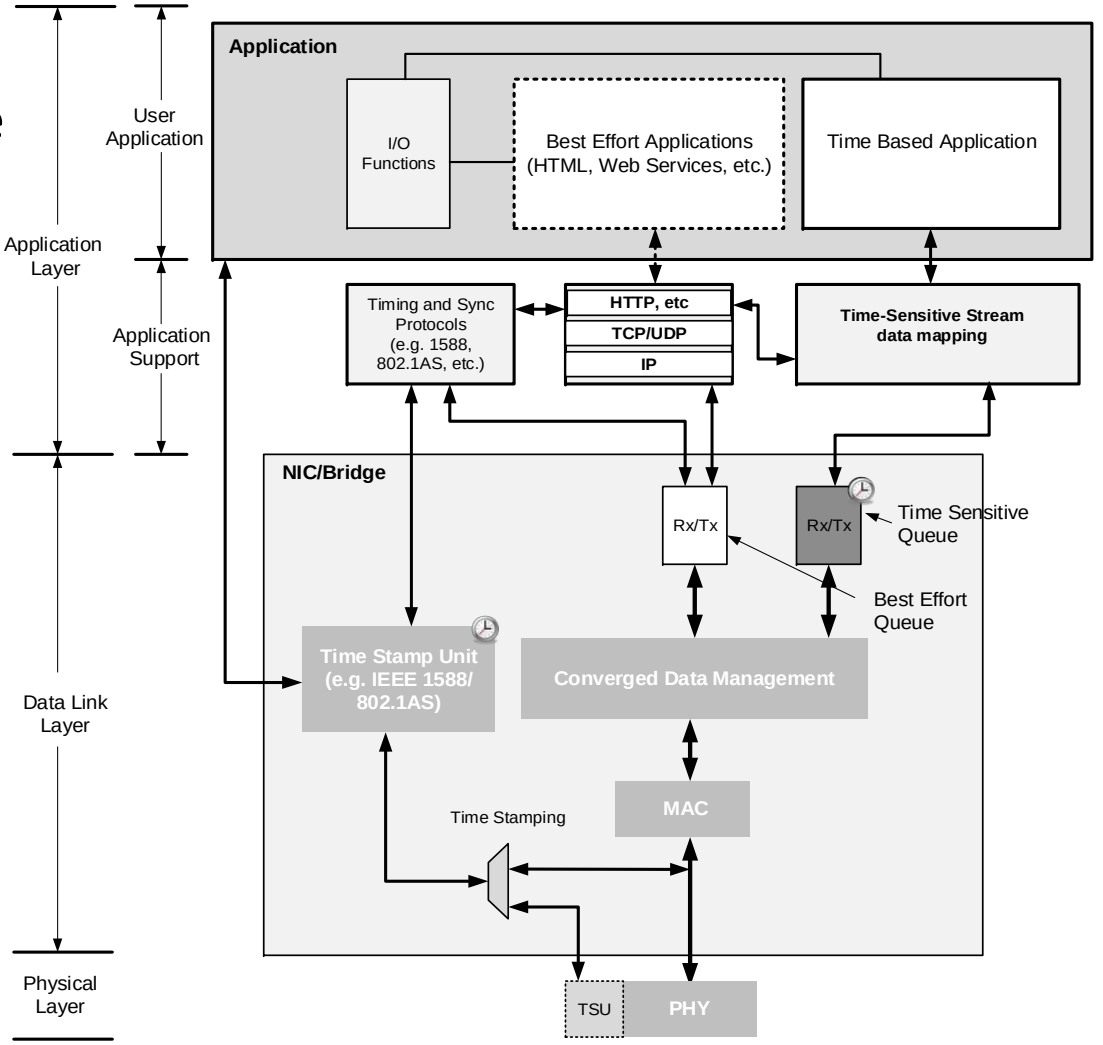
- Methodology to determine needs:
  - Examine components of a CPS from the perspective of the presence or absence of explicit time
  - Define constraints based on degree of time-awareness needed



- Current status of time-awareness in CPS today:
  - Time-based synchronization not universally implemented for accurate timing at the interface to the "physics"
  - Hardware-assist mechanisms available for establishment of system-wide time to high levels of accuracy (sub microseconds)
  - Universal adoption will result in "Time correctness by design"

3. Timing and latency in CPS

- Proposes a reference architecture on how to build time-aware CPS in the future
- Describes a model based on the current ongoing efforts in standard bodies like IEEE to make time-synchronization fundamental part of Ethernet
- This enables a converged network where both best-effort and time-sensitive streams can co-exist without impacting performance



4. Special security issues that arise with timing in CPS

- Discusses how time is impacted by both cyber and physical security architectures
- Lists both assurance (data and channel) and resilience attributes
- Contains a survey of current time distribution methods regarding both data and channel assurance attributes
- Lists the attack vectors in Time Networks
  - Replay attacks, jamming, spoofing etc.
- Suggests mechanisms to achieve secure time
  - Redundant timing sources, Redundancy in time-data paths etc.

Timing: Future Vision and Roadmap

Sub-sections 3 and 4 both list future research topics to build secure time-aware CPS:

- Standards work that is in incubation
  - To build large scale converged networks
  - Alternative sources to traceable national standard reference time
  - Timing network topologies to support diverse and redundant paths
  - Cybersecurity measures that minimize impact of timing performance
- New research in time-based scheduling tools to enable large converged networks
- New research in mechanisms to detect timing compromises sufficiently early so that there is no performance impact to the CPS
- Information Technology (IT) and Operation Technology (OT) working together for configuration of CPS both from timing and latency as well as security

CPS PWG: Data Interoperability

Co-chairs: Marty Burns, Larry Lannom, Peggy Irelan
Presenter: Marty Burns

Data Interop: Methodology

1. Developed Scope Statement
2. Developed Proposed Outline
3. Recruited Volunteers to Populate Outline
4. Review and Revise

Data Interop: Framework Elements

- **Data Interoperability Topics from the CPS Viewpoint**
  - **Data Fusion**
    - **Data fusion from multiple sensor or source types or use of such data for diverse purposes**
    - **Data fusion of streaming data and predictive analytics capabilities**
  - **Complex data exchange and other management issues for interoperability across heterogeneous systems**
  - **Data-driven interactions between dependent and independent cyber physical systems**
  - **Privacy-protecting data infrastructures**

Data Interop: Framework Elements

- **Traditional data interoperability issues**
  - Data Models, Relationships between Data and Data Type
    - Data Models
    - Relationships between Data
    - Data Type
  - Identification of type and instance
  - Data quality and provenance
  - Governance
  - Privacy and cybersecurity
  - Data about Timing and Timestamps
  - Safety and Configuration Assurance
- Issues section with outstanding topics for resolution

Data Interop: Key Issues

- Scope
  - Are we missing key data interoperability dimensions or do we have them all?
- Coverage
  - Breadth
    - The topics are broad and there are many protocols, standards, and moving parts
    - Many topics, especially in “Data Interoperability Topics from the CPS Viewpoint” section are written from the perspective of a single set of exemplary standard sets
  - Depth
    - Framework vs treatise

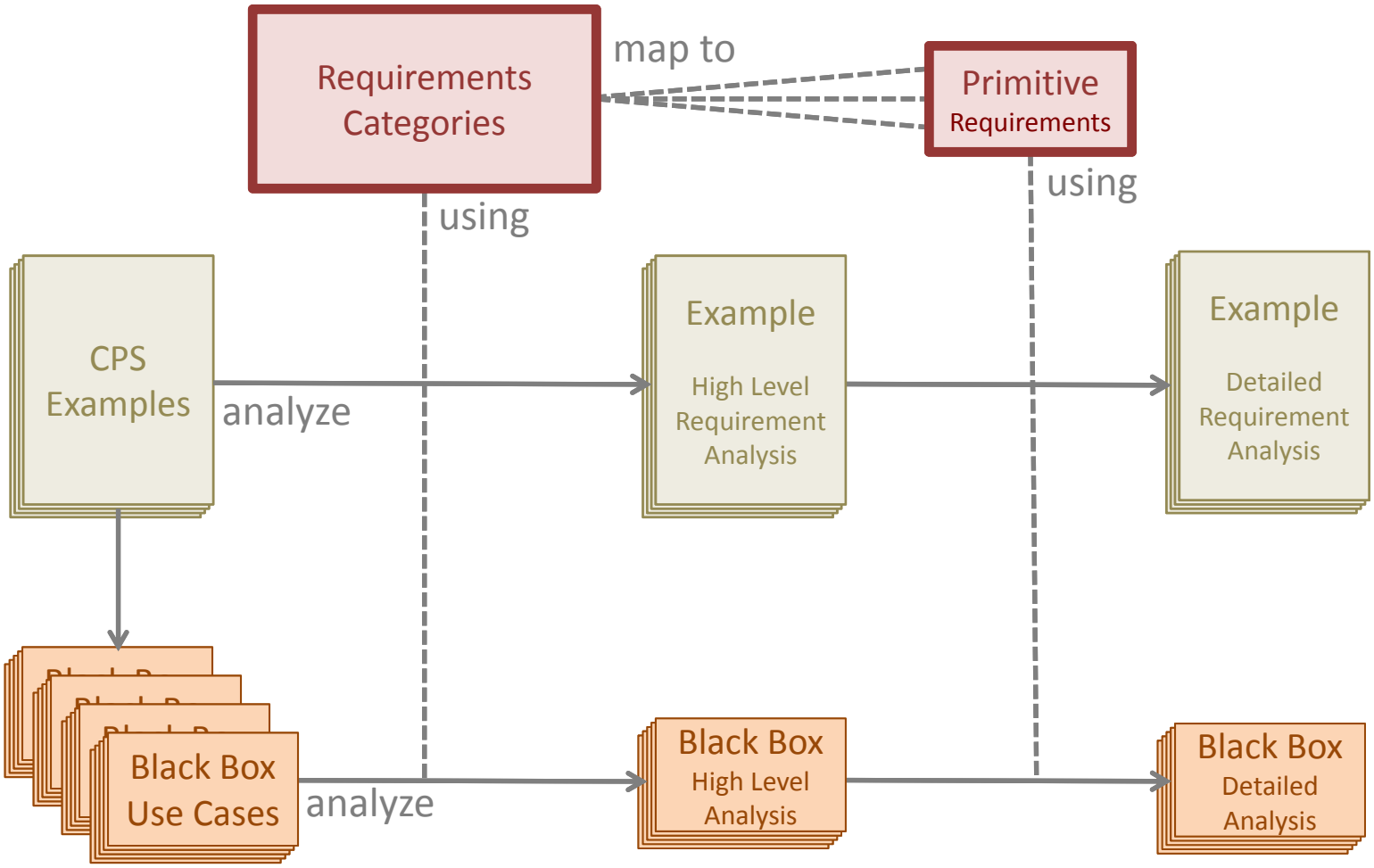
Data Interop: Future Work

- Refine introductory sections to better predict the contents
- Resolve issues in issue section
- Either draw out clearly distinction between standard suites discussed or summarize some alternatives
- Meeting biweekly at 11:00A Thursdays starting 1/15/2015

CPS PWG: Use Cases

Co-chairs: Eric Simmon, John Baras, Stephen Mellor
Presenter: Stephen Mellor

Use Cases: Methodology



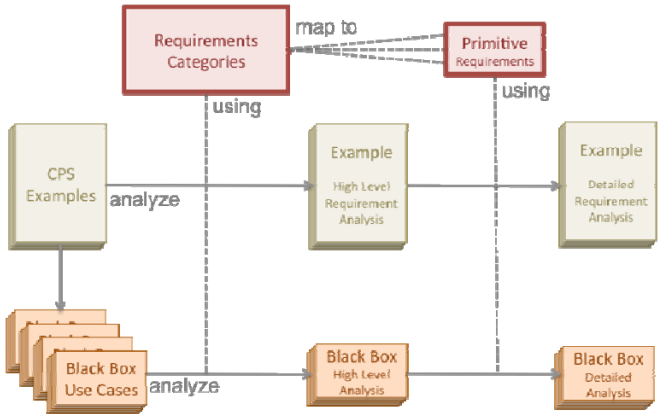
CPS PWG Document

NIST CPS Public Working Group

V1.0

Use Case Chapter

describes



Use Cases: Document Organization

- Background
  - Requirements
  - Relationship with other subgroups
  - Overview
    - Stakeholders
    - Application Categories
- Analysis Method
- Supporting CPS Examples
  - Monitoring Energy Efficiency of Manufacturing System
  - Grain/Produce Monitoring and Delivery
- Black-box use cases

Use Cases: Highlights

- Face to Face Meeting in November was very productive.
- Language/terminology still an issue
- Need more variety of examples (for more application categories)
- Focus will be on analyzing what we have now (and expanding as we go), and on developing requirements for the Ref Arch subgroup

Use Cases: Future work

- Gather more CPS Examples
- Perform high-level analysis on Examples
- Develop low-level primitive requirements list
- Develop actor, system, use cases for each CPS Example
- Perform low-level analysis on each use case
- Align language with Ref-Arch subgroup

CPS PWG phases

- Phase I: COMPLETE
  (Framework Elements from all 5 working groups)
- Phase II: UNDERWAY
  (integrated CPS Framework Document)
- Phase III: UPCOMING
  (CPS Roadmap)
  - Roadmap development process is primary focus of April 7-8, 2015 CPS PWG F2F meeting at NIST G'burg

Phase II review process

- Work in progress ….
- Goal is to focus review/comments and improvements on the integrated CPS Framework document rather than Framework Element documents
- Need to solicit feedback on applicability within example domains and cross-domain interactions
- We will provide details on review process when ready via the cps_pwgcomprehensive announcement mailing list
- Potential for CPS PWG-branded document and subsequent NIST Special Publication

CPS PWG Face-to-Face meeting on April 7-8, 2015

- Location: NIST campus in Gaithersburg, Maryland
- We will work with subgroup co-chairs and others on work plan and full agenda, and website/registration
- First portion of meeting will conclude Phase II with review/agreement on CPS Framework and some illustrative examples of its potential and applications
- Majority of meeting will focus on CPS Roadmapping, and will include breakouts focused on specific topics and action plans

Questions and Answers

David Wollman, moderator

- Please type questions into the webinar chat window, and our team of presenters will select questions and respond verbally with answers (depending on level of questions and available time)

Websites and Meetings

- Collaboration website: www.cpspwg.org
  - Public-facing information on CPS PWG
  - Subgroup members documents management system
  - Meeting calendar for all CPS PWG subgroups
- Web Sites
  - NIST CPS: www.nist.gov/cps/ (general questions to nistcps@nist.gov)
  - NIST CPS PWG: http://www.nist.gov/cps/cpspwg.cfm
- Meetings:

Subgroup	Email list	Meetings
Ref Architecture	cps_arch@nist.gov	Biweekly, Tuesday 1:00P EST (Next 1/27/2015) https://attendee.gotowebinar.com/register/120988656
Use Cases	cps_usecase@nist.gov	Biweekly, Thursday 10:00A 1/15/2015 https://www1.gotomeeting.com/join/610492473
Cybersecurity	cps_cyber@nist.gov	Biweekly, Thursday 4:00P EST (Next 1/29/15) https://attendee.gotowebinar.com/register/6501970071277836545
Timing	cps_sync@nist.gov	Biweekly, Friday 12:00P EST (Next 1/16/15) Register: https://www1.gotomeeting.com/register/784073528 Call: 1-888-513-3298; PIN Code: 73714001
Data Interop	cps_datainterop@nist.gov	Biweekly, Thursday 11:00A EST (Next 1/29/2015) https://attendee.gotowebinar.com/register/6651369512060232450

Thank you for attending this CPS PWG Update Webinar!

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