NIST Special Publication 1500-201

Framework for Cyber-Physical Systems: Volume 1, Overview

Version 1.0

Cyber-Physical Systems Public Working Group
Smart Grid and Cyber-Physical Systems Program Office
Engineering Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1500-201

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

NIST Special Publication 1500-201

Framework for Cyber-Physical Systems: Volume 1, Overview

Version 1.0

Cyber-Physical Systems Public Working Group
Smart Grid and Cyber-Physical Systems Program Office
Engineering Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1500-201

June 2017

U.S. Department of Commerce
Wilbur L. Ross Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology (NIST) Special Publication 1500-201

79 pages (June 2017)

NIST Special Publication series 1500 is intended to capture external perspectives related to NIST standards, measurement, and testing-related efforts. These external perspectives can come from industry, academia, government, and others. These reports are intended to document external perspectives and do not represent official NIST positions.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1500-201
Natl. Inst. Stand. Technol. Spec. Publ. 1500-201, 79 pages (June 2017)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1500-201

Revision Tracking

Version	Date	Editor	Changes
1.0	20170320	Edward Griffor	First Release Version

Table of Contents

Table of Figures

Table of Tables

Disclaimer

This document has been prepared by the Cyber-Physical Systems Public Working Group (CPS PWG), an open public forum established by the National Institute of Standards and Technology (NIST) to support stakeholder discussions and development of a framework for cyber-physical systems. This document is a freely available contribution of the CPS PWG and is published in the public domain.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by the CPS PWG (or NIST), nor is it intended to imply that these entities, materials, or equipment are necessarily the best available for the purpose. All registered trademarks or trademarks belong to their respective organizations.

Acknowledgement

We would like to acknowledge the valuable leadership of the following individuals who helped guide the participants through the framework activity:

NIST Leadership:

Edward Griffor, David Wollman, Christopher Greer

Reference Architecture:

Industry Co-chairs:	Stephen Mellor, Shi-Wan Lin
Academic Co-chairs:	Janos Sztipanovits
NIST Co-chairs:	Abdella Battou

Security:

Industry Co-chairs:	Claire Vishik, Larry John
Academic Co-chairs:	Bill Sanders
NIST Co-chairs:	Victoria Pillitteri, Stephen Quinn

Use Cases:

Industry Co-chairs:	Stephen Mellor
Academic Co-chairs:	John Baras
NIST Co-chairs:	Eric Simmon

Data Interoperability:

Industry Co-chairs:	Peggy Irelan, Eve Schooler
Academic Co-chairs:	Larry Lannom
NIST Co-chairs:	Martin Burns

Timing:

Industry Co-chairs:	Sundeep Chandhoke
Academic Co-chairs:	Hugh Melvin
NIST Co-chairs:	Marc Weiss

Additionally, we would like to express our appreciation to all the participants from industry, government and academia that, through their generous donation of their intellect, experience and precious time, made this effort a success.

Executive Summary

Cyber-physical systems (CPS) are smart systems that include engineered interacting networks of physical and computational components. CPS and related systems (including the Internet of Things (IoT) and the Industrial Internet) are widely recognized as having great potential to enable innovative applications and impact multiple economic sectors in the worldwide economy.

In mid-2014, NIST established the CPS Public Working Group (CPS PWG) to bring together a broad range of CPS experts in an open public forum to help define and shape key characteristics of CPS, so as to better manage development and implementation within and across multiple "smart" application domains, including smart manufacturing, transportation, energy, and healthcare.

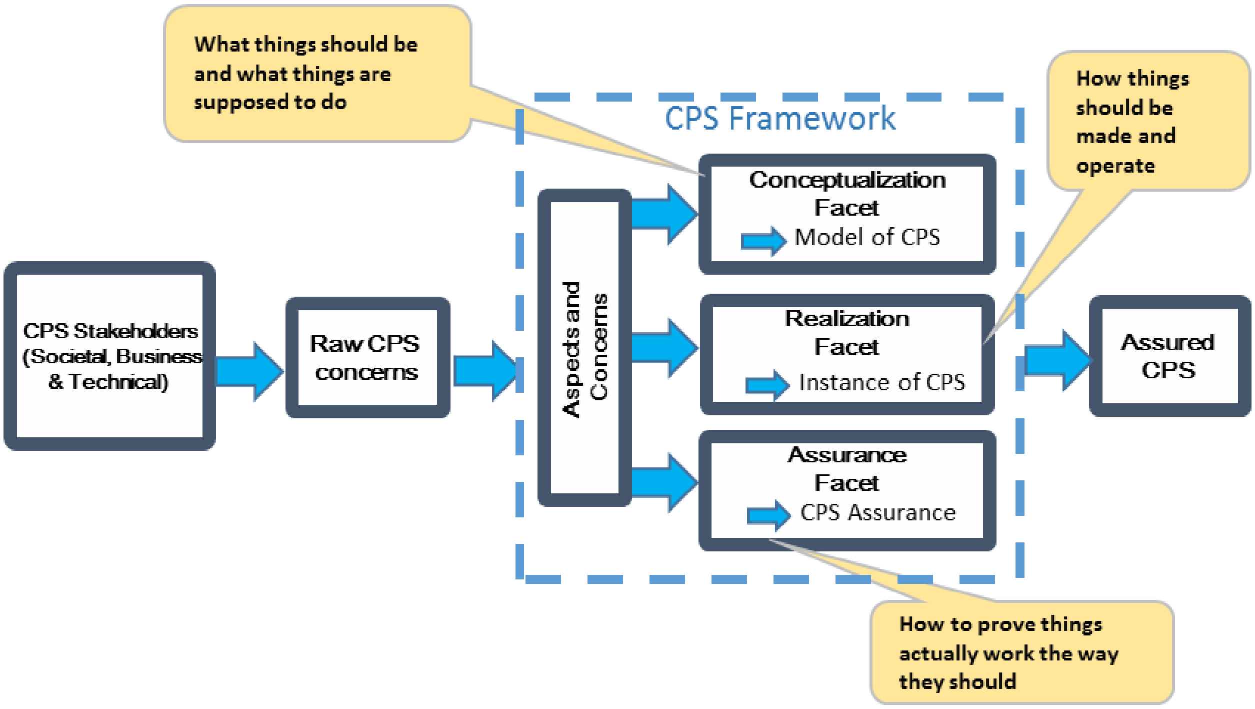
The objective of the CPS PWG is to develop a shared understanding of CPS and its foundational concepts and unique dimensions (as described in this "CPS Framework") to promote progress through exchanging ideas and integrating research across sectors and to support development of CPS with new functionalities. While in principle there are multiple audiences for this work, a key audience is the group of CPS experts, architects, and practitioners who would benefit from an organized presentation of a CPS analysis methodology based on the CPS Framework presented as *facets* and *aspects* in this document. The identified key concepts and issues are informed by the perspective of the five expert subgroups in the CPS PWG: Vocabulary and Reference Architecture, Cybersecurity and Privacy, Timing and Synchronization, Data Interoperability, and Use Cases. The CPS analysis methodology is designed as a framework to support the understanding and development of new and existing CPS, including those designed to interact with other CPS and function in multiple interconnected infrastructure environments. This foundation also enables further use of these principles to develop a comprehensive standards and metrics base for CPS to support commerce and innovation. As an example, the CPS Framework could support identification of the commonalities and opportunities for interoperability in complex CPS at scale. The broader audience for this work includes all CPS stakeholders, who may be interested in broadening individual domain perspectives to consider CPS in a holistic, multi-domain context.

The first stage in the three-stage work plan of the CPS PWG was to develop initial "Framework Element" documents in each of the five expert subgroups. In the second stage, these documents were combined into an initial draft CPS Framework and then revised and improved to create this draft document. The documented discussions of the subgroups have been included here as Appendices A through C. After public review and finalization of the CPS Framework Release 1, the applicability of this approach will be assessed in selected CPS domains, leading to a planned future road mapping activity to both improve the CPS Framework and develop understanding and action plans to support its use in multiple CPS domains.

With respect to this draft CPS Framework, the first goal was to derive a unifying framework that covers, to the extent understood by the CPS PWG participants, the range of unique dimensions of CPS. The second goal is to populate a significant portion of the CPS Framework with detail, drawing upon content produced by the CPS PWG subgroups and leadership team. It is important to note that there are sections of this draft CPS Framework that are not fully developed at this time. It is anticipated that additional content will be included in the future revisions to this document.

The diagram below shows this analysis proceeding in a series of steps as undertaken within the reference architecture activity:

1. **Identify** domains of CPS; these are the areas of deployment of CPS in which stakeholders may have domain-specific and cross-domain concerns.
2. **Identify** cross-cutting concerns, like societal, business, technical, etc. Stakeholders can have concerns that overlap or are instances of broader conceptual concerns.
3. **Analyze** cross-cutting concerns to produce aspects, or grouping of conceptually equivalent or related concerns.
4. **Address** concerns (aspects) through activities and artifacts organized within three fundamental facets of conceptualization, realization, and assurance.


What things should be and what things are supposed to do
CPS Framework
How things should be made and operate
Conceptualization Facet
Model of CPS
CPS Stakeholders (Societal, Business & Technical)
Raw CPS concerns
Aspects and Concerns
Realization Facet
Instance of CPS
Assured CPS
Assurance Facet
CPS Assurance
How to prove things actually work the way they should

Two iterations of integration and analysis produced the following Framework elements:

Domains. It is intended that the Framework can be applied to concrete CPS application domains, e.g., manufacturing, transportation, and energy, as both a specialization of these common conceptions and descriptions and a means for integrating domains for coordinated functions. Conversely, these specializations may validate and help to enhance the overarching CPS conceptions and descriptions. Within and across these domains, stakeholders have a variety of concerns or interests.

Facets. Facets are views on CPS encompassing identified responsibilities in the system engineering process. They contain well-defined activities and artifacts (outputs) for addressing concerns. There are three identified facets:

- The conceptualization facet captures activities related to the high-level goals, functional requirements, and organization of CPS as they pertain to what a CPS or its components should be and what they are supposed to do. It provides as its overarching output a conceptual model of the CPS.
- The realization facet captures the activities surrounding the detailed engineering design, production, implementation, and operation of the desired systems. These activities include tradeoff analyses, detailed engineering design and simulation(s), and more, that drive towards and are responsible for realization of a CPS.
- The assurance facet deals with obtaining confidence that the CPS built in the realization facet satisfies the model developed in the conceptualization facet. Its activities include evaluating the claims, argumentation, and evidence as required to address important (and sometimes mandatory) requirements of design, policy, law, and regulation.

Aspects. Aspects are high-level groupings of cross-cutting concerns. Concerns are interests in a system relevant to one or more stakeholders. The identified aspects are listed below:

- Functional
- Business
- Human
- Trustworthiness[1]
- Timing
- Data
- Boundaries
- Composability
- Lifecycle

Using the concepts of facets and aspects, this draft CPS Framework describes a CPS analysis methodology, in which the activities identified in the facets are implemented in a coordinated approach to address concerns throughout the entire life cycle, using a range of development approaches, such as waterfall, agile, spiral and iterative.

[1] Trustworthiness includes security, privacy, safety, reliability, and resilience.

In summary, this draft CPS Framework takes the foundation-building work done within the CPS PWG and integrates and reorganizes that work to form a cohesive document based on the identified concepts of facets and aspects.

It is hoped that this Framework will satisfy the need for a reference CPS description language on which tools, standards, and documented applications can be based.

Further input and comments from a broad audience will inform CPS PWG efforts to build out and improve this CPS Framework.

1 Introduction

This section provides an introduction for the document. It comprises the following:

- Section 1.1 provides a brief overview of cyber-physical systems.
- Section 1.2 defines the purpose of the document.
- Section 1.3 explains the scope of the document.
- Section 1.4 explains the organization of the rest of the document.

1.1 Overview

1.1.1 Background

Cyber-physical systems (CPS) are smart systems that include engineered interacting networks of physical and computational components. These highly interconnected and integrated systems provide new functionalities to improve quality of life and enable technological advances in critical areas, such as personalized health care, emergency response, traffic flow management, smart manufacturing, defense and homeland security, and energy supply and use. In addition to CPS, there are many words and phrases (Industrial Internet, Internet of Things (IoT), machine-to-machine (M2M), smart cities, and others) that describe similar or related systems and concepts.[2] There is significant overlap between these concepts, in particular CPS and IoT, such that CPS and IoT are sometimes used interchangeably; therefore, the approach described in this CPS Framework should be considered to be equally applicable to IoT.

The impacts of CPS will be revolutionary and pervasive; this is evident today in emerging autonomous vehicles, intelligent buildings, smart energy systems, robots, and smart medical devices. Realizing the full promise of CPS will require interoperability among heterogeneous components and systems, supported by new reference architectures using shared vocabularies and definitions. Addressing the challenges and opportunities of CPS requires broad consensus in foundational concepts, and a shared understanding of the essential new capabilities and technologies unique to CPS. NIST has established the CPS Public Working Group (CPS PWG) as an open forum to foster and capture inputs from those involved in CPS, both nationally and globally.

The CPS PWG was launched in mid-2014 with the establishment of five subgroups (Vocabulary and Reference Architecture, Use Cases, Cybersecurity and Privacy, Timing and Synchronization, and Data Interoperability)[3] Initial CPS PWG “Framework Element” documents were produced by each of the subgroups in December 2014, then integrated, reorganized, and refined to create this draft CPS Framework. The CPS

[2] CPS will be the focus of this document; however, terminology distinctions may be introduced to aid the reader where beneficial or informative.

[3] Additional information on the NIST CPS PWG is available at https://pages.nist.gov/cpspwg/ and http://www.nist.gov/cps/.

Framework is intended to be a living document and will be revised over time to address stakeholder community input and public comments; some sections of the document are incomplete and will be developed and extended over time.

The core of the CPS Framework is a common vocabulary, structure, and analysis methodology. As a process method, the CPS analysis methodology should enable and facilitate CPS systems engineering using a range of development approaches, such as waterfall, agile, spiral, and iterative. There are many well-documented system engineering process documents and flows – e.g., TOGAF [1] and CMMI [2]. This Framework, however, focuses on the detailed scope of CPS and the specific concerns implementers and analysts have in designing and understanding them. The concepts described in this document map cleanly to the more general methods and therefore are complementary to them rather than competitive.

The purpose of this CPS Framework is to allow for a comprehensive analysis of CPS. The CPS Framework captures the generic functionalities that CPS provide, and the activities and artifacts needed to support conceptualization, realization, and assurance of CPS. This analysis methodology includes addressing concerns that are specific to CPS and those that are applicable to any device or system. By this means, a complete methodology is proposed with common vocabulary and structure, which emphasizes CPS concerns but not to the exclusion of others.

1.1.2 What Is Different about CPS

CPS go beyond conventional product, system, and application design traditionally conducted in the absence of significant or pervasive interconnectedness. There are many reasons for this, including the following:

- **The combination of the cyber and the physical, and their connectedness, is essential to CPS.** A CPS generally involves sensing, computation and actuation. CPS involve traditional information technology (IT) as in the passage of data from sensors to the processing of those data in computation. CPS also involve traditional operational technology (OT) for control aspects and actuation. The combination of these IT and OT worlds along with associated timing constraints is a particularly new feature of CPS.

- **A CPS may be a System of Systems (SoS).** As such, it may bridge multiple purposes, as well as time and data domains, hence requiring methods of translation or accommodation among these domains. For example, different time domains may reference different time scales or have different granularities or accuracies.

- **Emergent behaviors are to be expected of CPS, due the open nature of CPS composition**. Understanding a behavior that cannot be reduced to a single CPS subsystem, but comes about through the interaction of possibly many CPS subsystems, is one of the key analysis challenges. For example, a traffic jam is a detrimental emergent behavior; optimal energy distribution by the smart grid where power consumers and producers work together is a desirable positive emergent effect.

- **CPS need a methodology to ensure interoperability, managing evolution, and dealing with emergent effects.** Especially in large scale CPS such as smart grid and smart city, many of the subsystems are the responsibility of different manufacturers.

- **CPS may be repurposed beyond applications that were their basis of design.** For example, a cell phone in a car may be used as a mobile traffic sensor, or energy usage information may be used to diagnose equipment faults.

- **CPS are noted for enabling cross-domain applications.** As an example, consider the intersection of the domains: manufacturing and energy distribution systems, smart cities, and consumer-based sensing.

- **CPS potential impact on the physical world and their connectedness bring with them heightened concern about trustworthiness.** There is a more urgent need for emphasis on security, privacy, safety, reliability, and resilience, and corresponding assurance for pervasive interconnected devices and infrastructures. As an example, CPS networks may have "brokers" and other infrastructure-based devices and aggregators that are owned and managed by third parties, resulting in potential trust issues – e.g., publish and subscribe messaging, certificate authorities, type and object registries.

- **CPS should be freely composable.** Components are available that may be combined into a system dynamically, and the system architecture may be modified during runtime to address changing concerns. There are challenges, however. For example, timing composability may be particularly difficult. Also, it may not always be necessary or desirable to purchase assets to build a system; instead, services can be purchased on a per-use basis, with users only paying for using the resources needed for a specific application and at the specific time of usage.

- **CPS must be able to accommodate a variety of computational models.** Each CPS application has computational and physical components and the range of platform and algorithm complexity is broad.

- **CPS must also support a variety of modes of communication.** CPS comprise systems that range from standalone to highly networked. They may use legacy protocols or anything up to more object exchange protocols. And they may be anywhere from power constrained to resource rich.

- **The heterogeneity of CPS leads them to display a wide range of complexity.** The complexity associated with the sensing and control loop(s) with feedback that are central to CPS must be well addressed in any design. This complexity must be accommodated by any framework for CPS, including sensors that range from basic to smart; static and adaptive sensors and control; single-mode and multi-faceted sensors; control schemes that can be local, distributed, federated, or centralized; control loops that rely on a single data source and those that fuse inputs; and so on. Interactions can be loosely coupled, as in repurposing of distributed sensing that is part of an existing CPS, as well as tightly coupled, as in telemedicine or smart grid operations. Coupling is both an opportunity to fulfill the vision of CPS and a challenge to CPS assurance. Emergent behaviors can become part of the intent of new services or may be unwanted. To mitigate complexity, CPS may be a product of co-design. In co-design, the design of the hardware and the software are considered jointly to inform tradeoffs between the cyber and physical components of the system.

- **There is typically a time-sensitive component to CPS, and timing is a central architectural concern.** A bound may be required on a time interval, i.e., the latency between when a sensor measurement event occurred and the time at which the data was made available to the CPS. The accuracy of event timestamps is a constraint on a time value, in this case between the actual time of the event and the value of the timestamp. Accurate time intervals are useful for coordinating actions in CPS of large spatial extent. Accurate timestamps in CPS are typically needed to facilitate better root cause analysis, and sometimes also for legal or regulatory reasons.

- **CPS are characterized by their interaction with their operating environment** (as indicated by the sensing and control loop(s) discussed above). CPS, together or individually, 'measure' and sense and then calculate and act upon their environment, typically changing one or more of the observed properties (thus providing closed loop control). The CPS environment typically includes humans, and humans function in a different way than the other components of a CPS. The architecture must support a variety of modes of human interaction with CPS to include: human as CPS controller or partner in control; human as CPS user; human as the consumer of CPS output; and human as the direct object of CPS to be measured and acted upon.

1.2 Purpose

The success of this CPS Framework can be assessed by its usefulness as guidance in designing, building, and verifying CPS and as a tool for analyzing complex CPS. It should aid users in determining the properties of a CPS, and provide guidance such that two CPS instance architectures, independently derived or tailored from this Framework, are in substantial alignment. That is, they can be mutually understood through the organizational and descriptive means of this Framework, and in doing so their real or potential interactions can be more easily understood.

By providing a framework for discussion of, design of, and reasoning about CPS, a common foundation will be established from which a myriad of interoperable CPS can be developed, safely and securely combined, verified, and delivered to the public, government, and researchers. If broadly adopted, this Framework will serve to enable activity in research and development that will produce reliable, well-designed, easily-integrated CPS-based products and services.

The framework uses many terms that have been defined in many other documents. We have provided definitions in Appendix B to indicate how we have used language in this document. Where possible we have drawn on documents in other standards, however some words are used differently in different standards and in different industries. There are also some words that are commonly used that we have not defined here. An example is the word precision or precise. This word is used in many contexts and in some cases with different meanings. It is hoped that such words are made clear by the context in which they are used.

This document defines a CPS as follows: Cyber-physical systems integrate computation, communication, sensing, and actuation with physical systems to fulfill time-sensitive functions with varying degrees of interaction with the environment, including human interaction.

A CPS conceptual model is shown in Figure 1. This figure is presented here to highlight the potential interactions of devices and systems in a system of systems (SoS) (e.g., a CPS infrastructure). A CPS may be as simple as an individual device, or a CPS can consist of one or more cyber-physical devices that form a system or can be a SoS, consisting of multiple systems that consist of multiple devices.

This pattern is recursive and depends on one’s perspective (i.e., a device from one perspective may be a system from another perspective). Ultimately, a CPS must contain the decision flow together with at least one of the flows for information or action. The information flow represents digitally the measurement of the physical state of the physical world, while the action flow impacts the physical state of the physical world. This allows for collaborations from small and medium scale up to city/nation/world scale.

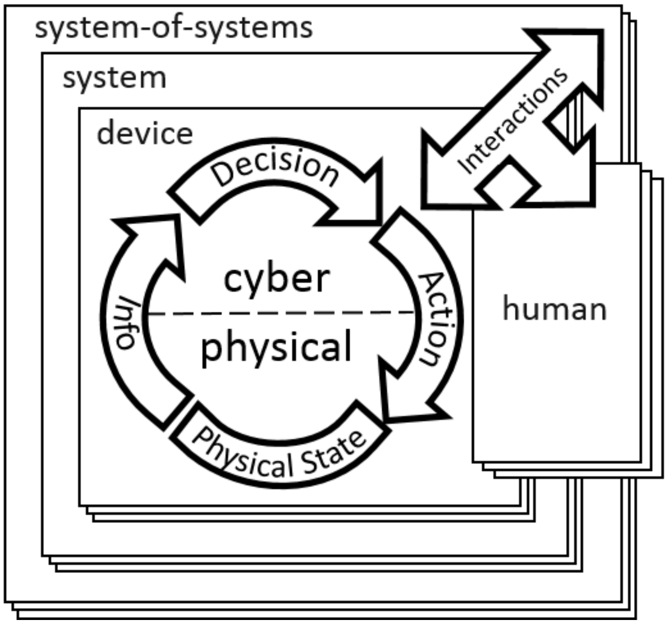


Figure 1: CPS Conceptual Model

1.3 Scope

The scope of CPS is very broad by nature, as demonstrated in the M2M sector map in Figure 2. There are large number and variety of domains, services, applications, and devices. This figure displays CPS focused on the IoT.[4] This broad CPS scope includes cross-cutting functions (i.e., functions that are derived from critical and overriding CPS concerns) that are likely to impact multiple interacting CPS domains. The CPS Framework will facilitate users' understanding of cross-cutting functions. Examples include safety, security, and interoperability.

[4] Note that the inclusion of Figure 2 is designed only to illustrate the scope of deployed, commercial CPS, but not a particular or preferred architecture for studying it.

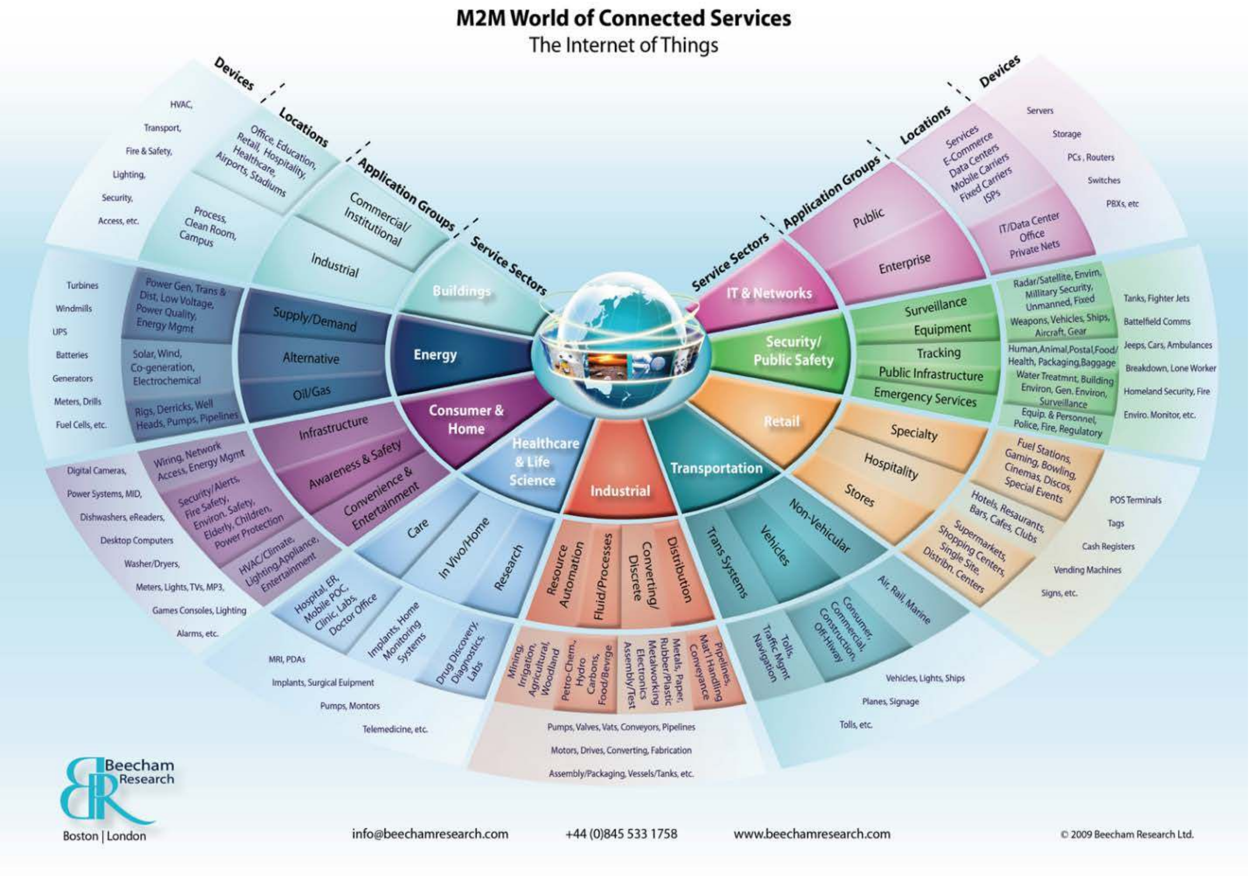

M2M World of Connected Services
The Internet of Things
Devices
Locations
Application Groups
Service Sectors
HVAC,
Transport,
Fire & Safety,
Lighting,
Security,
Access, etc.
Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums
Process, Clean Room, Campus
Commercial/ Institutional
Industrial
Buildings
Turbines
Windmills
UPS
Batteries
Generators
Meters, Drills
Fuel Cells, etc.
Power Gen, Trans & Dist, Low Voltage, Power Quality, Energy Mgmt
Solar, Wind, Co-generation, Electrochemical
Rigs, Derricks, Well Heads, Pumps, Pipelines
Supply/Demand
Alternative
Oil/Gas
Energy
Digital Cameras,
Power Systems, MID,
Dishwashers, eReaders,
Desktop Computers
Washer/Dryers,
Meters, Lights, TVs, MP3,
Games Consoles, Lighting
Alarms, etc.
Wiring, Network Access, Energy Mgmt
Security/Alerts, Fire Safety, Environ. Safety, Elderly, Children, Power Protection
HVAC/Climate, Lighting,Appliance, Entertainment
Infrastructure
Awareness & Safety
Convenience & Entertainment
Consumer & Home
MRI, PDAs
Implants, Surgical Euipment
Pumps, Montors
Telemedicine, etc.
Hospital, ER, Mobile POC, Clinic, Labs, Doctor Office
Implants, Home Monitoring Systems
Drug Discovery, Diagnostics, Labs
Care
In Vivo/Home
Research
Healthcare & Life Science
Pumps, Valves, Vats, Conveyors, Pipelines
Motors, Drives, Converting, Fabrication
Assembly/Packaging, Vessels/Tanks, etc.
Mining, Irrigation, Agricultural, Woodland
Petro-Chem., Hydro Carbons, Food/Bevrge
Metals, Paper, Rubber/Plastic Metalworking Electronics Assembly/Test
Pipelines, Mat'l Handling Conveyance
Resource Automation
Fluid/Processes
Converting/ Discrete
Distribution
Industrial
Vehicles, Lights, Ships
Planes, Signage
Tolls, etc.
Tolls, Traffic Mgmt Navigation
Consumer, Commercial, Construction, Off-Hiway
Air, Rail, Marine
Trans Systems
Vehicles
Non-Vehicular
Transportation
POS Terminals
Tags
Cash Registers
Vending Machines
Signs, etc.
Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events
Hotels, Resaurants, Bars, Cafes, Clubs
Supermarkets, Shopping Centers, Single Site, Distribn. Centers
Specialty
Hospitality
Stores
Retail
Tanks, Fighter Jets
Battelfield Comms
Jeeps, Cars, Ambulances
Breakdown, Lone Worker
Homeland Security, Fire
Enviro. Monitor, etc.
Radar/Satellite, Envirn. Millitary Security, Unmanned, Fixed
Weapons, Vehicles, Ships, Aircraft, Gear
Human,Animal,Postal,Food/ Health, Packaging,Baggage
Water Treatmnt, Building Environ, Gen. Environ, Surveillance
Equip. & Personnel, Police, Fire, Regulatory
Surveillance
Equipment
Tracking
Public Infrastructure
Emergency Services
Security/ Public Safety
Servers
Storage
PCs , Routers
Switches
PBXs, etc
Services E-Commerce Data Centers Mobile Carriers Fixed Carriers ISPs
IT/Data Center Office Private Nets
Public
Enterprise
IT & Networks
Beecham Research
Boston | London
info@beechamresearch.com
+44 (0)845 533 1758
www.beechamresearch.com
© 2009 Beecham Research Ltd.

Figure 2: Segmentation of M2M Market[5]

The scope of the CPS Framework includes the full dimensionality of CPS and the entire systems engineering process. That is, rather than address "selected topics," it intends to provide a comprehensive tool for the analysis and description of CPS. It is quite possible that this initial draft CPS Framework will have missed some important elements of CPS. With input from stakeholders including through a public review process, these gaps will be addressed in future releases.

As an example of the scope of CPS, consider the case of smart traffic systems (Figure 3). Smart traffic systems consist of smart traffic monitoring and control infrastructure, advanced traffic control centers powered by predictive analytics on real-time traffic data, autonomous vehicles interacting with peer vehicles in proximity, and traffic control systems. This section provides examples of how the use of CPS can impact a smart traffic system. This section also provides context for Appendix C, in which a

[5] Courtesy of Beecham Research, used by permission, http://www.beechamresearch.com/article.aspx?id=4, 2009

simplified traffic-related emergency response scenario is used as an analysis example to demonstrate how to exercise the CPS analysis methodology of this CPS Framework.

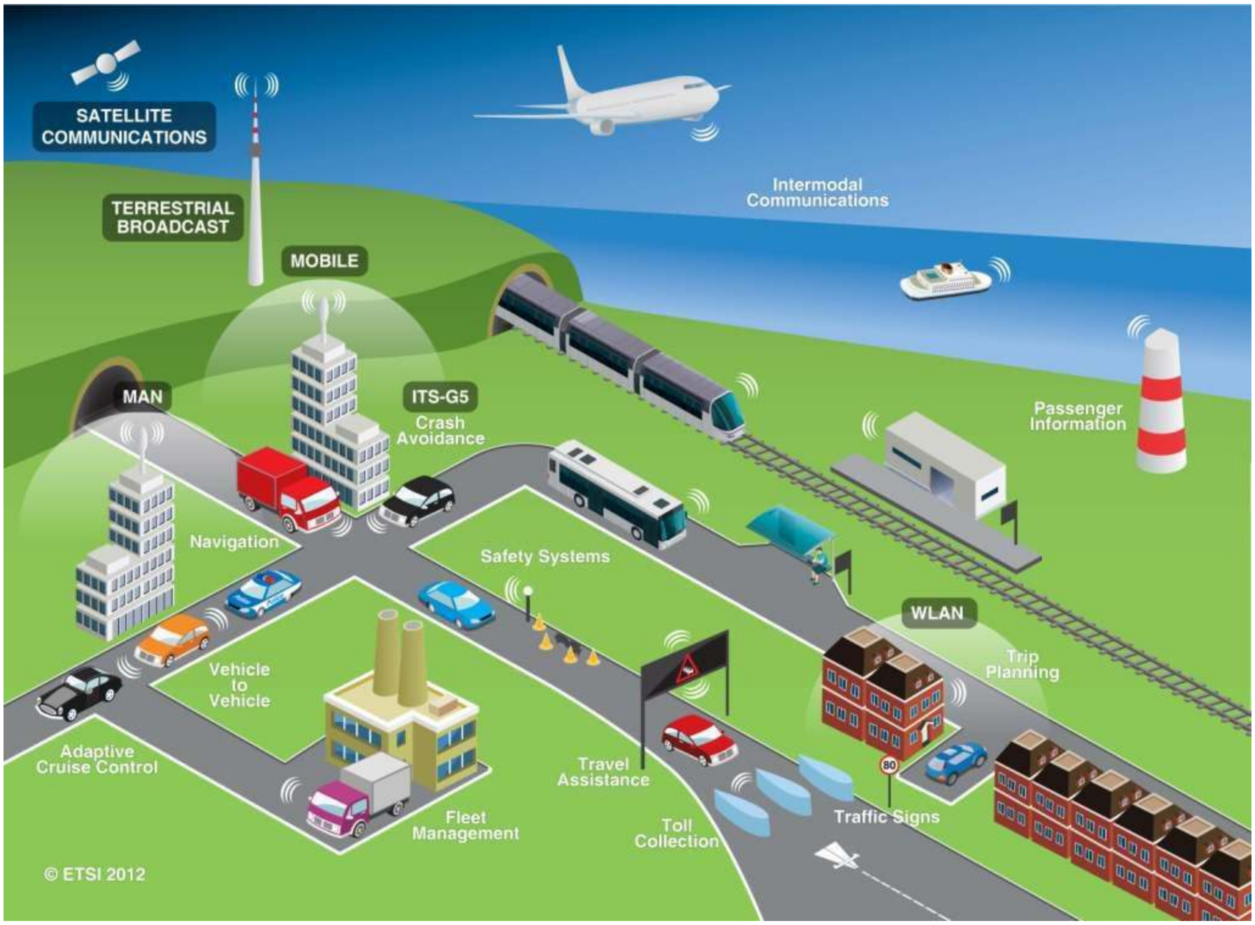


Figure 3: Smart Transportation[6]

CPS controls have a variety of levels of complexity ranging from automatic to autonomic. A prominent example of CPS in smart traffic is autonomous vehicles, which are themselves systems of CPS. The functions of CPS within an autonomous vehicle are orchestrated, collaborated, and coordinated to achieve the overall autonomous functions of the vehicle.

Another smart traffic CPS is an on-location smart traffic control system. Such systems are installed in street intersections to sense and measure local traffic patterns and conditions so they can apply commands to the traffic signals to orchestrate the movement of vehicles passing the intersections based on prescribed objectives. These on-location smart traffic control systems may be orchestrated by regional traffic control centers to optimize overall traffic flows.

[6] Courtesy of ETSI http://www.etsi.org/technologies-clusters/technologies/intelligent-transport, used with permission

CPS can collaborate with each other to produce effects that are greater than the sum of the parts. An example of collaboration of CPS is the collaboration of vehicles in proximity to avoid collisions. These vehicles communicate with each other in the cyber space, dynamically forming ad hoc communities to inform others of the actions each of them is taking that may affect the communities of vehicles. Examples of such actions include applying a brake or changing lanes. They also interact, albeit indirectly, in the physical space by continuously sensing and measuring the movement and trajectory of neighboring vehicles. The information gathered from both the cyber and physical spaces is then synthesized to gain an understanding of the state and intent of the vehicles in proximity. From this understanding, and based on prescribed objectives (e.g., to avoid collision, a physical effect), control decisions are continuously made to produce the desired physical effects in the vehicle in question, e.g., to slow down, stop, accelerate, or change course to avoid the undesired effects, such as collisions between vehicles or between vehicles and other objects.

CPS can be orchestrated by a cyber system that communicates logically with them. An example of this orchestration is the computational unit in an autonomous vehicle strongly orchestrating the activities between the steering, braking, and powertrain CPS. Another example of this is a traffic control unit using wireless signaling to orchestrate autonomous vehicles passing through a street intersection.

The SoS domain enables the complex management of CPS and supports emerging behavior. In smart traffic, traffic monitoring systems send data to the on-location traffic control units and to their respective regional traffic control centers. Vehicles also report driving data to the traffic Internet, which can in turn be routed to the relevant traffic control centers. The information component for the regional traffic control centers analyzes these data to understand the traffic conditions and patterns. The application component synthesizes this information with other information such as traffic patterns in the neighboring regions, current and forecast weather conditions, current and pending large public events, and road accident reports. It takes into account in its model the constraints imposed by the objectives, such as minimizing traffic delay, minimizing air and noise pollution, increasing safety and enhancing security, and reducing energy consumption. It optimizes the traffic routing patterns and sends high-level instructions to on-location traffic control units to orchestrate regional traffic patterns. It coordinates vehicle traffic flows by broadcasting advice to vehicles to suggest alternative routes. The application component may assist emergency response in locating accident sites for rescue and recovery. It may interact with the business component to plan road or facility repairs accounting for either or both material or work crews. It may interact with the business component to schedule predictive maintenance or repairs on the traffic control infrastructure based on information provided by the information and entity management component that manages the CPS in the traffic control infrastructure.

Furthermore, sensory data gathered from the vehicles correlated with geolocation, climate, and season data, as well as road construction and maintenance records, can be analyzed to derive information on road and bridge conditions at precise locations, and their relations to the interworking of climate, season, patterns of usage, construction materials and procedures, and maintenance frequency. Optimal preventive maintenance can be planned in relation to usage patterns, season, and cost. New materials and optimal procedures can be developed for specific usage patterns and climates.

1.4 Organization of This Document

Beyond the introductory material in this section, this Framework document is organized as follows:

Section 2: The CPS Framework – This section describes the CPS environment and stakeholder concerns, and provides an overview of the CPS Framework analysis methodology with its core concepts of *facets* (components of the systems engineering process with associated activities and artifacts) and *aspects* (groupings of cross-cutting concerns).

Section 2.2.2 describes facets as an activity-organized analysis of concerns and Section 2.2.3 describes the properties of the facets. Table 2 provides a description of each of the aspects. Uses of the Framework, an in-depth description, and related standards are described in Sections 2.3, 2.4, and 2.5, respectively.

Appendix A: References – This section provides references to a variety of CPS-related articles, standards, and other material cited in the text.

Appendix B: Definitions and Acronyms – This appendix provides a set of acronyms and definitions applicable to this document.

Appendix C: Applying the CPS Framework – This appendix uses a simplified "Emergency Response" scenario involving multiple CPS to illustrate how owners, designers, engineers, and operators can apply the Framework to analyze CPS in an operational context.

2 The CPS Framework

This section defines the CPS Framework at a high level. The components of the section are:

- Section 2.1 provides an overview of CPS and key CPS concepts.
- Section 2.2 explains the derivation of the CPS Framework.
- Section 2.3 describes potential uses of the CPS Framework.
- Section 2.4 contains the complete description of the CPS Framework.
- Section 2.5 discusses related standards and activities.
- Section 2.6 summarizes Section 2.

2.1 Overview

The focus of this Framework is to develop a CPS analysis methodology and a vocabulary that describes it. It includes the identification of CPS domains, facets, aspects, concerns, activities, and artifacts. These terms are defined in the context[7] of this Framework and are introduced later in this section.

To appreciate the scope of coverage that the CPS Framework addresses, this section briefly discusses the dimensionality of CPS. This presentation covers the entire scope of CPS as opposed to Section 1.1.2 which emphasized unique differences of highly connected systems versus conventional systems.

- CPS are frequently systems of systems (SoS), and the architectural constructs should be able to be applied recursively or iteratively to support this nested nature of CPS. The sensing/control and computational nature of CPS generally leads to emergent higher levels of behavior and system intelligence.

- CPS should be characterized by well-defined components. They should provide components with well-known characteristics described using standardized semantics and syntax. Components should use standardized component/service definitions, descriptions, and component catalogs.

- CPS should support application and domain flexibility. To do this, the definition of the components should be flexible and open ended. The architecture should support the provision of accurate descriptions of things to allow for flexibility in virtual system creation and adaption and to promote innovation. It should also support a large range of application size, complexity, and workload. The same components that are used in a very simple application should also be usable in a very large, complex, distributed system. Ideally the components can be assembled and scaled quickly, even during runtime. CPS architecture should allow composition from independent, decoupled components for flexibility,

[7] In a technology space as broad as CPS, a given term may have more than one meaning when used in practice by different audiences. Therefore, the definitions and usage in this Framework are intended for the scope of this Framework and are not proposed for universal meaning.

robustness, and resilience to changing situations. Decoupling should also exist between architectural layers, allowing each layer to be modified and replaced without unwittingly affecting the other layers. In order for the system to integrate different components, the interfaces to these components should be based on well-defined, interpretable, and unambiguous standards. Further, standardization of interfaces will allow for easy provisioning of various components by any systems envisioned today and into the future. By allowing internal component flexibility while providing external interoperability through standardized interfaces, customization can be achieved. This supports desirable diversity of application and scalability.

- CPS frequently perform critical applications, so the CPS architecture must support the level of reliability needed to meet requirements. It should provide the ability to resist change due to external perturbations or to respond to those changes in ways that preserve the correct operation of the critical application.

- Security is a necessary feature of the CPS architecture to ensure that CPS capabilities are not compromised by malicious agents, and that the information used, processed, stored and transferred has its integrity preserved and is kept confidential where needed. The nature of CPS not only increases the consequences of a breach but also introduces additional types of vulnerabilities. For example, timing in a CPS has unique vulnerabilities different from traditional data vulnerabilities considered in. Security needs to be built into CPS by design in order to be sufficiently flexible to support a diverse set of applications. This security should include component security; access control; as well as timing, data and communications security. Security must be considered in combination with other prioritized and potentially conflicting concerns, such as privacy, safety, reliability, and resilience, in a comprehensive risk management framework.

- Data exchange is a prominent dimension of CPS operation. The nature of data and its reliability, type, identity, and discovery are all key attributes that allow for a common understanding of data conveyed through communications in and among CPS. Often, data are “fused” or combined with other data to anonymize or enrich it or to summarize it for the benefit of users. Access to data is often constrained by “rights” or “privileges.”

- Components that contain sensors and/or actuators should have an appropriate level of awareness of physical location and time. For example, the accuracy requirement for location will change based upon the application. To support such applications, components may need the ability to access and/or report both location and the associated uncertainty of the location.

- Additionally, CPS architectures should support legacy component integration and migration. Legacy devices have physical artifacts, software, protocols, syntax, and semantics that exist due to past design decisions, and they may be inconsistent with the current architectural requirements. New components and systems should be designed so that present or legacy devices do not unnecessarily limit future system evolution. As even new components will become legacy in the future, a plan for adaptation and migration of legacy systems and standards should be created to avoid stranded investments, if possible. Legacy components should be integrated in a way that ensures that security and other essential performance and functional requirements are met.

2.2 Derivation of the Framework

A useful reference for the terminological and definitional conventions relating to systems architecture and systems architecture frameworks is ISO/IEC/IEEE 42010 [3]. For the purposes of this section, here are a few of these conventions:

- An *architecture framework* consists of the “conventions, principles and practices for the description of architectures established within a specific domain of application and/or community of stakeholders.”
- A *concern* is an “interest in a system relevant to one or more of its stakeholders.”
- An *architecture view* consists of “work product expressing the architecture of a system from the perspective of specific system concerns.”
- An *architecture viewpoint* consists of “work product establishing the conventions for the construction, interpretation and use of architecture views to frame specific system concerns.”

Another key reference relevant to the construction of this Framework is ISO/IEC/IEEE 15288 on System Life Cycle processes [4], which describes processes and outcomes to guide system engineering.

Building on these two references, this CPS Framework derives the core notions of facets, activities, artifacts, aspects, and concerns. Note that while these are two key references to general systems engineering principles, the Framework emphasizes the nature and function of CPS specifically.

2.2.1 Key Elements of the Framework

The key elements of the Framework are shown in Figure 4 and can be summarized as follows:

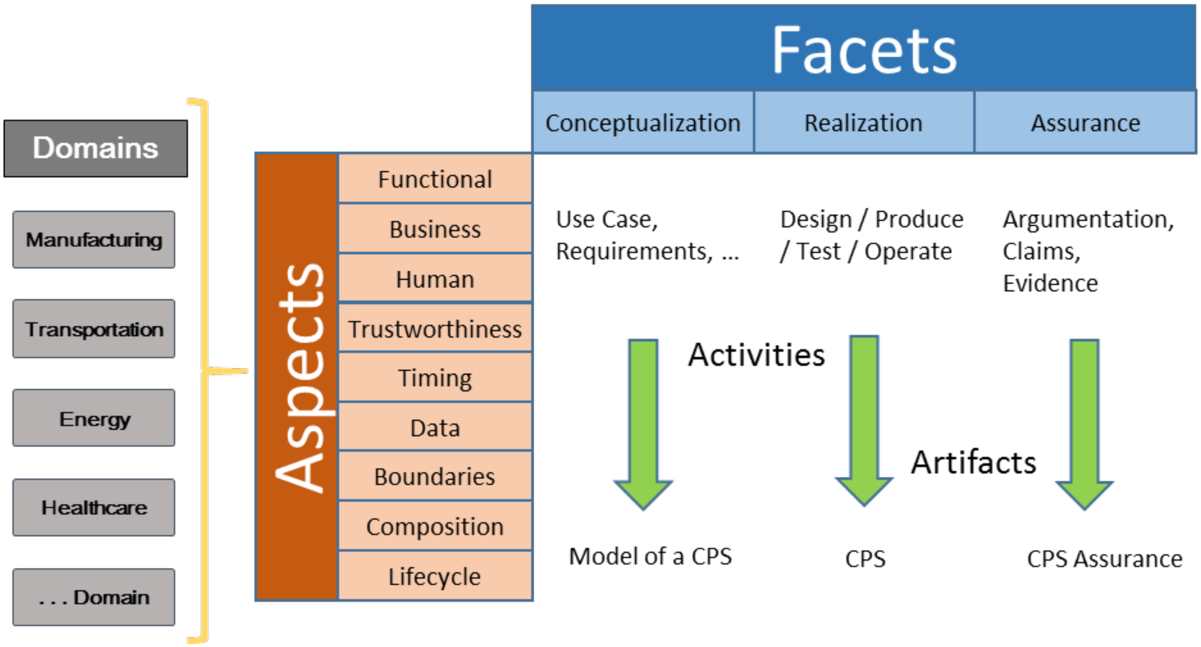


Figure 4: CPS Framework – Domains, Facets, Aspects

- *Domains* represent the different application areas of CPS as shown in Figure 4.
- *Concerns,* as expressed by many different stakeholders in their unique and collective viewpoints, are a fundamental concept that drives the CPS Framework methodology. They are addressed throughout the CPS development cycle. Concerns that are conceptually equivalent or related are grouped into Aspects, which are addressed by activities within the facets.
- *Properties* are the concrete assertions that address the concerns. They include requirements, design elements, tests, and judgments.
- *Aspects* consist of groupings of conceptually equivalent or related concerns. A listing of aspects is provided in Table 2. There may be modifications or other valid groupings of concerns that may benefit a particular application of the CPS Framework in a specific context. Note that aspects and concerns are not considered orthogonal. There are nine defined aspects: functional, business, human, trustworthiness, timing, data, boundaries, composition, and lifecycle.
- *Facets* are views on CPS encompassing identified responsibilities in the systems engineering process. Each facet contains a set of well-defined activities and artifacts (outputs) for addressing concerns. There are three identified facets: conceptualization, realization, and assurance.

The Framework was developed through an analysis process that followed a defined sequence of steps. Figure 5 shows this analysis, working in the context of identified CPS domain(s):

1. **Identify** domains of CPS; these are the areas of deployment of CPS in which stakeholders may have domain-specific and cross-domain concerns.

2. **Identify** cross-cutting concerns, like societal, business, technical, etc. Stakeholders can have concerns that overlap or are instances of broader conceptual concerns.
3. **Analyze** cross-cutting concerns to produce aspects, or grouping of conceptually equivalent or related concerns.
4. **Address** concerns (aspects) through activities and artifacts organized within three fundamental facets of conceptualization, realization, and assurance.

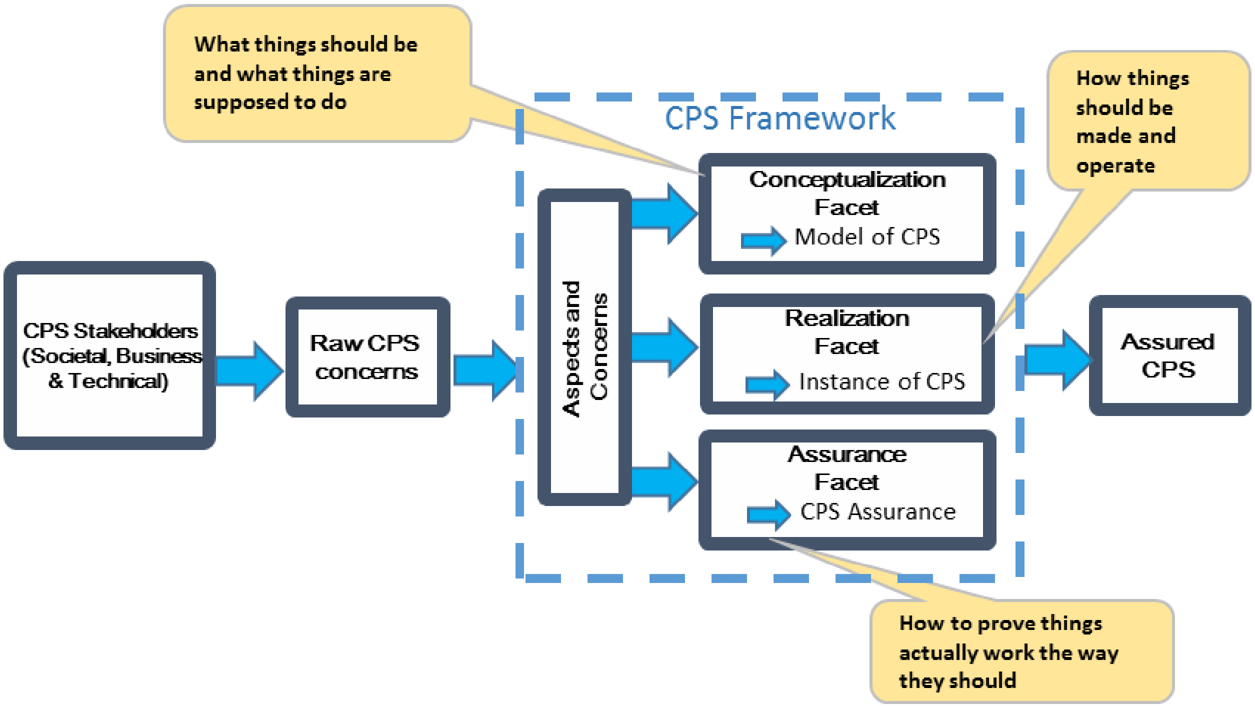

What things should be and what things are supposed to do
CPS Framework
How things should be made and operate
CPS Stakeholders (Societal, Business & Technical)
Raw CPS concerns
Aspects and Concerns
Conceptualization Facet
Model of CPS
Realization Facet
Instance of CPS
Assurance Facet
CPS Assurance
Assured CPS
How to prove things actually work the way they should

Figure 5: Analysis of CPS and Derivation of Framework

It is intended that the identification and description of the activities, methods, and artifacts in each of the facets can be applied within concrete CPS application domains (e.g., manufacturing, transportation, energy) as a specialization of these common conceptions and descriptions. Conversely, these specializations may validate and help to enhance these conceptions and descriptions.

2.2.2 The Facet as an Activity-Organized Analysis of Concerns

It is a primary goal of the CPS Framework to be *actionable*: to be useful to perform analyses of CPS. With that concern in mind, the prototypical model of a facet is shown in Figure 6:

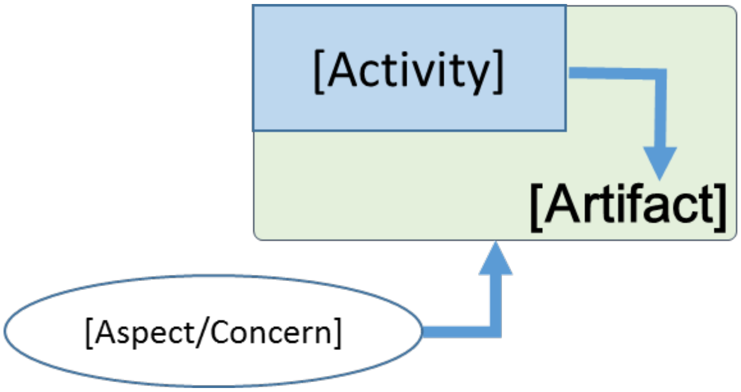


Figure 6: Model of a Facet

A *facet*, therefore, is a collection of activities that produce artifacts that are driven by aspects and their concerns for a CPS.

From this simple model, the three Framework facets are derived as shown in Figure 7:

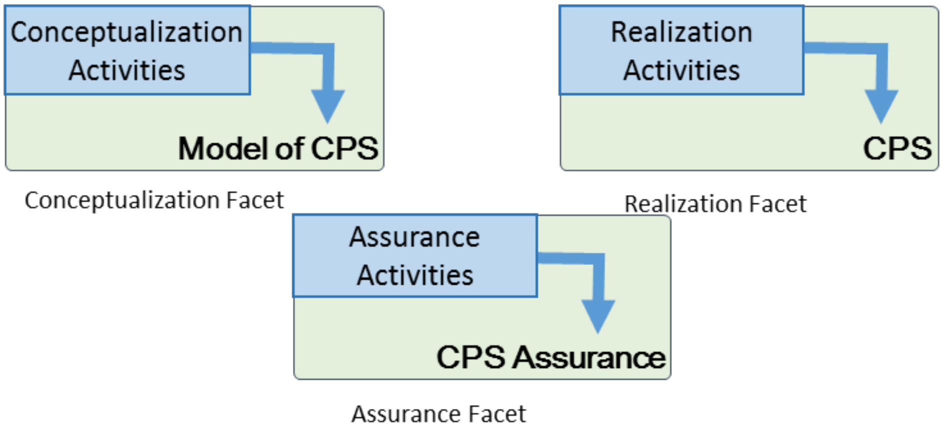


Figure 7: Three Primary Framework Facets

The three facets comprise the traditional systems engineering process (typified by the "VEE" model [5].) By analyzing each aspect within all facets, all cross-cutting concerns can be addressed at every stage of the design, creation and operation of a CPSThe . Figure 8 illustrates this concept:

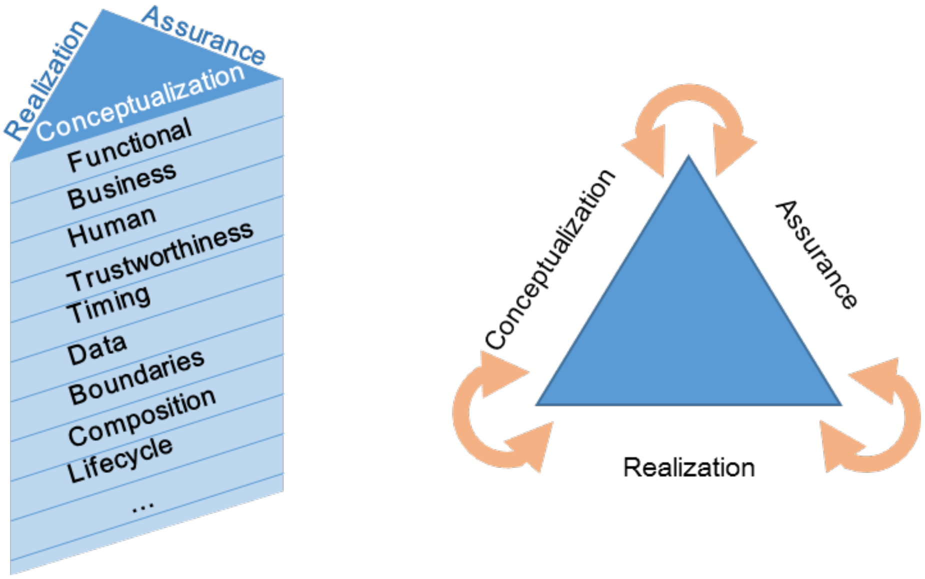


Figure 8: Facets and Aspects

On the left of the figure, the prism illustrates that aspects must be viewed through each face of the prism – the facets. Note that analysis of CPS can be viewed from any face and assembled by navigating one or more times through the faces to obtain the complete view of the CPS as shown on the right.
To emphasize that analysis of CPS need not (and is often not) a waterfall process, the facets should be considered as modes of analysis where transitions are valid at any time during the lifecycle of CPS concept.

2.2.3 Properties

The *conceptualization facet* comprises the set of activities and artifacts that produce a model of a CPS. This model is made up of distinct *properties of the CPS*. These properties are expressions of concerns held by the CPS stakeholders. There can be different kinds of such properties, for example, requirements and model elements. These properties put requirements or constraints on functions and behaviors of the CPS. They represent as well other attributes of the CPS associated with design and build practices and include properties of operation and disposal, i.e., the properties of a CPS span the entire lifecycle of a CPS.

A realized and assembled "CPS model" is an *instance of a CPS*. The *CPS model* is the theoretical ideal of the CPS. The *realization facet* and its activities strive to quantitatively satisfy the aspirational properties of the conceptualization facet. The *assurance facet* then provides the assurance that the conceptualization was realized *as intended*. The properties of the realization facet are made up of design elements and test elements.

CPS can be seen as extensions of human capabilities, including sensing, decision-making, and action. Many times human beings are more than aware of the limitation of their abilities, so assurance methodologies frequently provide both an extension of those abilities and an estimate of the uncertainty inherent in using these extensions. Humans maintain a certain level of situational awareness and many times need to be protected from errors in judgment.

Human beings' capabilities are enhanced through CPS, however CPS assurance and estimates of CPS assurance levels will be important to the success and adoption of CPS and will increase their benefit to mankind.

High on the list of CPS challenges are topics related to *human factors*. The assurance facet is intended to provide a methodology for understanding the scope and limits CPS capabilities. In doing this the interaction between operator and CPS may also be improved. Closer consideration of Figure 9 suggests that there is much research required to better understand the relationship between the cognitive cycle of a human operator and that of the CPS conceived, built, and operated by humans.

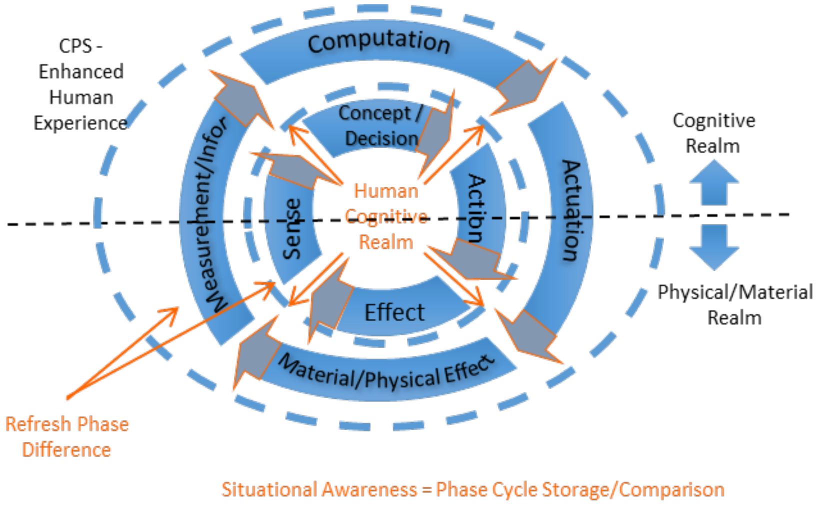


Figure 9: CPS Enhanced Cognitive Cycle

Elements of the *assurance case* of a CPS, developed using this Framework, consists of statements built from data produced during the activities of the first two facets of the framework, conceptualization and realization. The elements, shown in Figure 10, are:

- Claims
- Evidence
- Argumentation
- Estimate of confidence

The typical statement of assurance takes the form:

> "The [Evidence] is sufficient to conclude that the [Claims] are true based on the [Argumentation] with this [Estimate of Confidence]."

This is an *assurance judgment.* Judgments are properties of the assurance facet. Ultimately this relationship between evidence, claims, argumentation, and estimate of confidence can be formalized. In this formalization a judgment will have assumptions that are themselves judgments. *Derivation rules* can be used for deriving new judgments from given ones, i.e., one can apply formal reasoning to derive assurance judgments that themselves provide a justification for accepting the derived judgment. As an example, these rules may simply capture the reasoning suggested or dictated by a standard.

An added value of this approach is that such a derivation contains a mapping of all of the evidence used in deriving the judgment. It also provides guidance for how to re-construct the evidence used to conclude that a CPS has the desired properties.

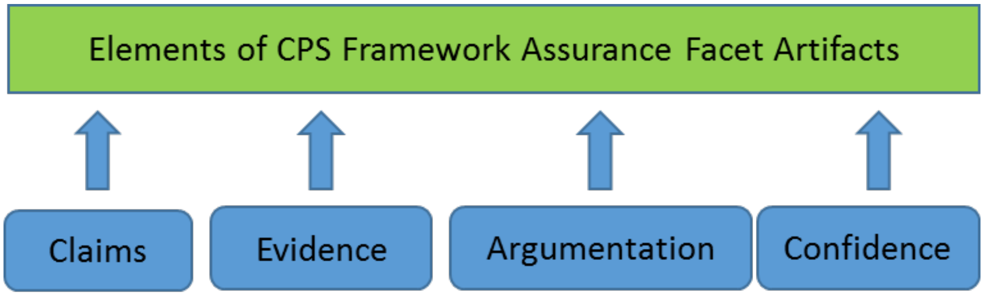


Figure 10: Elements of Assurance

The claims in the assurance facet are formed using the properties of the CPS developed during the conceptualization facet, i.e., the CPS Model. The CPS Model consists of the properties of the intended CPS. The claims in the assurance facet are the assertions that the CPS in question has or satisfies each of these properties. The CPS is said to *satisfy* the CPS Model if it satisfies or has each of the CPS Model properties. In the transportation domain, with ISO 26262 [6] examples, the high-level statement or judgement is that the CPS meets the requirements of the functional safety standard or that the processes of the organization that developed the CPS are ISO 26262 compliant.

The *evidence* in the assurance facet is formed from the artifacts of the realization facet, such as process documentation, design artifacts, test plans, and results, as depicted in Figure 11. They are determined by the specialization of the realization facet activities and artifacts to their domain and the applicable aspects.

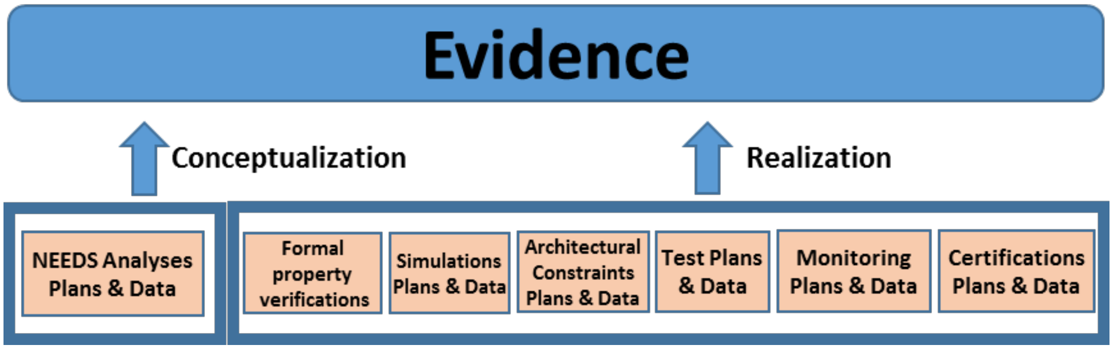

Evidence
Conceptualization
Realization
NEEDS Analyses Plans & Data
Formal property verifications
Simulations Plans & Data
Architectural Constraints Plans & Data
Test Plans & Data
Monitoring Plans & Data
Certifications Plans & Data

Figure 11: Evidence

As shown in Figure 12, the *argumentation* of the assurance facet is formed from a variety of things, including appeal to:

- Standards
- Best practices/consensus
- Formal methods
- Regulation (proscribed practices)
- Expert judgment (including criteria for being an expert in a domain)

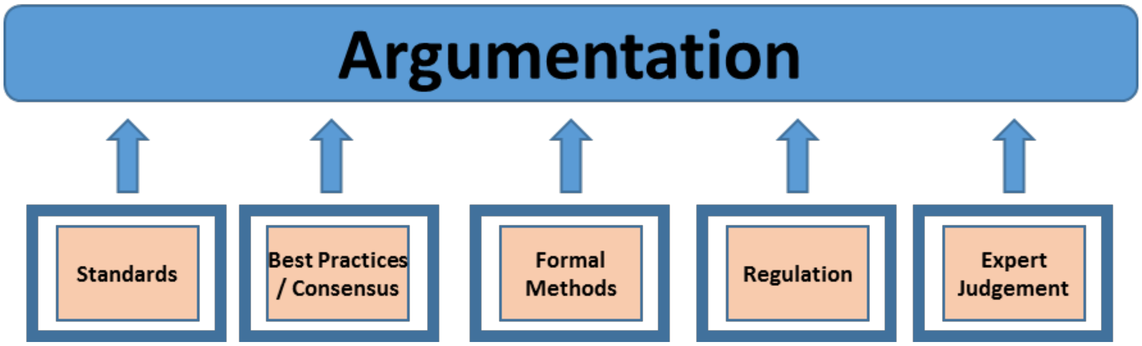
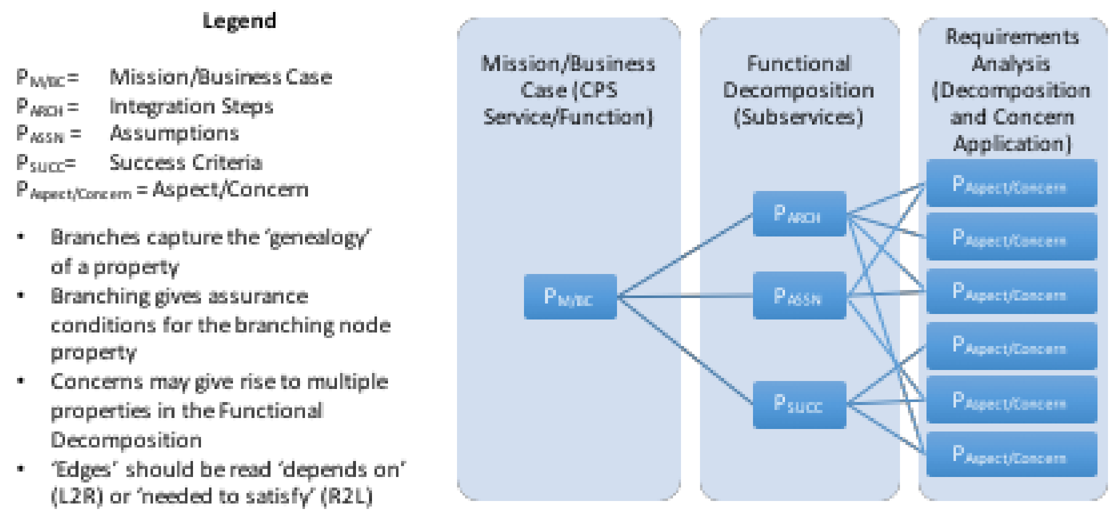


Figure 12: Argumentation

Application of the CPS Framework develops this information when each of the facet activities reviews each of the aspects of the Framework for impact on that activity. The output of that review is an updating of that activity and its artifacts. It is intended to provide criteria for evidence and supporting argumentation in the assurance facet to assure that the concerns in that aspect have been adequately addressed in the activity.

To facilitate addressing of the assurance for any of the properties in a CPS Model, we document the properties of the CPS developed during the conceptualization facet in the form of a tree of properties. Formally a tree is a partially ordered set with a unique root (all nodes trace back ultimately to the same node) and no *cycles* (a cycle corresponds to a node that can be reached from itself following a non-trivial path in the tree). The *property tree of a CPS*, consists of the properties of the CPS Model, ordered under the traceability ordering. The root is the property $P_{M/BC}$ with the successor relation outlined above.

Graphically this tree has the appearance shown in Figure 13:


Legend
P_M/BC= Mission/Business Case
P_ARCH = Integration Steps
P_ASSN = Assumptions
P_SUCC= Success Criteria
P_Aspect/Concern = Aspect/Concern
Mission/Business Case (CPS Service/Function)
Functional Decomposition (Subservices)
Requirements Analysis (Decomposition and Concern Application)
P_M/BC
P_ARCH
P_ASSN
P_SUCC
P_Aspect/Concern
P_Aspect/Concern
P_Aspect/Concern
P_Aspect/Concern
P_Aspect/Concern
P_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)

Figure 13: The Property Tree of a CPS

There are two types of assurance arguments, structural and empirical. Which one is applied depends on the types or sources of properties to be assured.

The 'branching type' assurance argument itself has a couple of different flavors, one for assurance of a logically compound property (containing propositional connectives) and one for properties that are compound due to the componentry of the CPS and its interactions.

The 'leaf type' assurance argument is one that relates to the design D and test T put in place in order to achieve a property of the CPS.

(1) $H_{Branching}$

(2) H_{Leaf}

The argument, "A", in this case may take the form that the test itself, the setup for the test, and the way in which test results are stored and managed is in compliance with a standard, and the argument would make reference to the standard, as an example.

(1) Structural (logical and architectural) for branching properties, P and Q:

$$A(P*Q) =_{Def} H_{Branching} (A(P), A(Q)),$$

for logically compound or architecture properties

(2) Empirical for the terminating properties or 'leaves' of the tree:

$$A(P, D, T) =_{Def} H_{Leaf} (P, D, T)$$

Each leaf represents the argumentation that "the design D and test T are sufficient to conclude that the property P is met." The argumentation H_{Leaf} makes reference to a certification, standard, or regulation where the test T is recommended or required to establish that property as well as provide an estimate of level of confidence.

The *assurance case* of a CPS consists of all of the assurance judgments for every property in the CPS Model.

2.2.4 Concerns to Aspects

The concerns are identified and further analyzed, producing a set of cross-cutting concern groupings called *aspects*. These aspects are “factored” from the work of the various working groups that produced this Framework – namely, the Vocabulary and Reference Architecture, Use Case, Cybersecurity and Privacy, Timing and Synchronization, and Data Interoperability subgroups.

Concerns and *aspects* are not orthogonal. That is, within the analysis of a given concern, consideration must also be given to related concerns. For example, in considering the trustworthiness aspect, the trustworthiness of timing should be considered.

2.2.5 Activities and Artifacts

In using the Framework to analyze and document CPS, a series of *activities* is performed. For example, a typical waterfall process includes use case development, functional decomposition, requirements analysis, design, etc.
These are generic activities and are identified for each facet. These activities can be considered activity groups which may be tailored during analyses of the aspects and concerns. For example, a Conceptualization facet activity “Requirements Analysis” may include a Trustworthiness requirements analysis, a Timing requirements analysis, etc.…
In this Framework, “activities” may refer to individual activities or activity groups.
Each activity produces one or more *artifacts*, which are the concrete technical components used to document the results.

2.3 Uses of the CPS Framework

As described in 2.2, the CPS Framework consists of *aspects* and *facets*. The *aspects* are categories of concerns. Each aspect represents a set of similar concerns and this is reflected in the name of the aspect. For example, the trustworthiness aspect includes concerns of security, privacy, safety, reliability and resilience. The CPS Framework facets are described in Section 2.4.2 and the aspects in Section 2.4.3.

Having clarity about the elements of each facet, the activities/artifacts lists, and how they interrelate is critically important to understanding the approach of this document. It is important to understand how the activities and their artifacts address concerns and aspects in all three facets.

Facet activities and artifacts are at the outset very general and relate to a generic high-level process needed to understand CPS conceptualization, realization, and assurance.

Hence these activities are in essence a template and need to be specialized to a CPS domain. The specialization of facet activities to a CPS domain involves the following:

- **Defining which of the CPS aspects apply to that domain:** People are often subject matter experts about a certain concern as it relates to a certain domain. Over time, they have built a consensus that a specific set of processes and tools must be applied in a specific way to adequately *address the concern.*
- **Updating the facet activities and artifacts for each applicable aspect:** this should be based on a review of the best practices for addressing each concern in the aspect.

The result of specializing facet activities to a CPS domain, and the attendant concerns, is a set of activities and artifacts that address the concerns that apply to that domain. For example, if the CPS performs or delivers safety-critical functions in the transportation domain, then there are multiple safety processes and test regimens that have become standards. For example, in the area of transportation that has to do with ground vehicles, the ISO/IEC 26262 document [6], has become a standard for shaping the approach of the commercial ground vehicle industry to establishing the software system safety of the vehicle systems.

Thus, the Framework can be used in different processes, depths, and scopes:
Processes:

- Waterfall (analyze conceptualization, then realization, then assurance.) This traditional system engineering flow allows for a requirements-driven process that leads to assured and verified function. Note that although this indicates a linear sequence through the facets, the ability to iterate and propagate changes discovered in one facet to the others is typically observed.
- Reverse engineering (analyze realization, then conceptualization, then assurance.) To understand a deployed CPS and perhaps to extend or enhance it, reverse engineering analyzes the realized CPS for its properties and observes its documentation to determine assurances. Once it is analyzed, modifications and enhancements can be made starting at any facet.
- Agile (do some conceptualization, then realization, then assurance, then iterate to greater depths of detail.) Analysis alone sometimes results in a reality other than what was originally envisioned at a high level, so an agile process seeks to take a minimal or “core” conceptualization to rapid realization and assurance. Once confirming initial assumptions about the CPS, the agile development process fills in additional detail in each facet to iteratively arrive at the completed set of artifacts.

- Service-based (analyze conceptualization, identify/fit advertised realizations, then assurance.) Dynamic services can be envisioned and deployed on top of existing CPS.

- Gap-analysis (analyze a set of CPS including systems of CPS and compare to discover gaps and overlaps for Pivotal Points of Interoperability (PPI)).

Understanding the opportunities for integration or gap-filling informs holistic tradeoff decisions about integrating systems and capabilities.

Depths:

- Critical tightly-coupled CPS: For critical infrastructures such as the energy grid, a deep and detailed process would be developed using the Framework. Emphasis on hard requirements and assurances, along with constraints from most aspects, would be evidenced.
- Loosely-coupled CPS: Especially appropriate for applications of CPS that repurpose capabilities of existing CPS and integrate them in new and novel ways, a lighter emphasis on hard requirements and a greater weight on functional goals are sought.
- Shallow analysis: For presenting concepts or talking about alternative approaches to CPS problems, small subsets of the Framework might be used. The use of the Framework structure and terminology allows the substance of the concept to be readily understood because the Framework sets a context for the discussion.

Scopes:

- Single CPS device: A device such as a video camera, robot, or thermostat. The focus of the analysis would emphasize the robustness of the design to enable it to become a valued component of a CPS.
- System or subsystem: A system of individual cyber, physical, and cyber-physical devices such as an HVAC system, which might consist of thermostat, air handler, compressor, and furnace.
- SoS: A system of interconnected systems, such as a power company demand response program interacting with individual HVAC systems to achieve a balanced energy system.

2.4 The Description of the CPS Framework

This section presents a detailed description of the CPS Framework. The Framework provides a taxonomy and organization of analysis that allow the complex process of studying, designing, and evolving CPS to be orderly and sufficiently encompassing.

A visual representation of the Framework was previously shown in Figure 4 in terms of domains, facets, and aspects.

The rest of this section presents the elements of the Framework in tabular form, providing only the taxonomy.

2.4.1 Domains

The domains of CPS are the areas of deployment of CPS in which stakeholders may have domain-specific and cross-domain concerns. Table 1 provides examples of CPS domains considered by the Public Working Group in its analysis.

Table 1: Examples of CPS Domains

Domains	
Advertising	Entertainment/sports
Aerospace	Environmental monitoring
Agriculture	Financial services
Buildings	Healthcare
Cities	Infrastructure (communications, power, water)
Communities	Leisure
Consumer	Manufacturing
Defense	Science
Disaster resilience	Social networks
Education	Supply chain/retail
Emergency response	Transportation
Energy	Weather

2.4.2 Facets

Table 2 lists and defines the facets.

Table 2: Facets

Facet	Description
Conceptualization	What things should be and what things are supposed to do: the set of activities that produce a model of a CPS (includes functional decomposition, requirements, and logical models.)
Realization	How things should be made and operate: the set of activities that produce, deploy, and operate a CPS (includes engineering tradeoffs and detailed designs in the critical path to the creation of a CPS instance.)
Assurance	How to achieve a desired level of confidence that things will work the way they should: the set of activities that provide confidence that a CPS performs as specified (includes claims, evidence, and argumentation.)

2.4.3 Aspects and Concerns

Table 3 lists and defines the aspects.

Table 3: Aspects

Aspect	Description
Functional	Concerns about function including sensing, actuation, control, communications, physicality, etc.
Business	Concerns about enterprise, time to market, environment, regulation, cost, etc.
Human	Concerns about human interaction with and as part of a CPS.
Trustworthiness	Concerns about trustworthiness of CPS including security, privacy, safety, reliability, and resilience.
Timing	Concerns about time and frequency in CPS, including the generation and transport of time and frequency signals, timestamping, managing latency, timing composability, etc.
Data	Concerns about data interoperability including fusion, metadata, type, identity, etc.
Boundaries	Concerns related to demarcations of topological, functional, organizational, or other forms of interactions.
Composition	Concerns related to the ability to compute selected properties of a component assembly from the properties of its components. Compositionality requires components that are composable: they do not change their properties in an assembly. Timing composability is particularly difficult.
Lifecycle	Concerns about the lifecycle of CPS including its components.

Table 4 lists and defines the concerns.

Table 4: Concerns

Aspect	Concern	Description
Functional	**actuation**	Concerns related to the ability of the CPS to effect change in the physical world.
Functional	**communication**	Concerns related to the exchange of information internal to the CPS and between the CPS and other entities.
Functional	**controllability**	Ability of a CPS to control a property of a physical thing. There are many challenges to implementing control systems with CPS including the non-determinism of cyber systems, the uncertainty of location, time and observations or actions, their reliability and security, and complexity. Concerns related to

Aspect	Concern	Description
		the ability to modify a CPS or its function, if necessary.
Functional	**functionality**	Concerns related to the function that a CPS provides.
Functional	**manageability**	Concerns related to the management of CPS function. For example, Managing Timing in complex CPS or SoS is a new issue with CPS that did not exist before. It is being developed with new standards
Functional	**measurability**	Concerns related to the ability to measure the characteristics of the CPS.
Functional	**monitorability**	Concerns related to the ease and reliability with which authorized entities can gain and maintain awareness of the state of a CPS and its operations. Includes logging and audit functionality.
Functional	**performance**	Concerns related to the ability of a CPS to meet required operational targets.
Functional	**physical**	Concerns about purely physical properties of CPS including seals, locks, safety, and EMI.
Functional	**physical context**	Concerns relating to the need to understand a specific observation or a desired action relative to its physical position (and uncertainty.) While this information is often implied and not explicit in traditional physical systems, the distributed, mobile nature of CPS makes this a critical concern.
Functional	**sensing**	Concerns related to the ability of a CPS to develop the situational awareness required to perform its function.
Functional	**states**	Concerns related to the states of a CPS. For example, the functional state of a CPS is frequently used to allow for variation in the CPS response to the same set of inputs. Variation in response based on state is sometimes referred to as functional modes.
Functional	**uncertainty**	Managing the effects of uncertainties is a fundamental challenge in CPS. Sources of uncertainty in CPS can be grouped into statistical (aleatoric), lack of knowledge (epistemic) uncertainty, or systematic uncertainty. In CPS, statistical uncertainty is caused by randomness of accuracy of sensing and actuation, often caused by uncertainty of

Aspect	Concern	Description
		manufacturing processes. Systematic uncertainty is caused by incomplete knowledge either due to limits of acquired knowledge or due to simplification in modeling. Typical manifestations of epistemic uncertainty are limited validity of models of physical processes or limits of computability of properties of mathematical models.
Business	**enterprise**	Concerns related to the economic aspects of CPS throughout their lifecycle.
Business	**cost**	Concerns related to the direct and indirect investment or monetary flow or other resources required by the CPS throughout its lifecycle.
Business	**environment**	Concerns related to the impacts of the engineering and operation of a CPS on the physical world.
Business	**policy**	Concerns related to the impacts of treaties, statutes, and doctrines on a CPS throughout its lifecycle.
Business	**quality**	Concerns related to the ease and reliability of assessing whether a CPS meets stakeholder (especially customer) expectations.
Business	**regulatory**	Concerns related to regulatory requirements and certifications.
Business	**time to market**	Concerns related to the time period required to bring a CPS from need realization through deployment.
Business	**utility**	Concerns related to the ability of a CPS to provide benefit or satisfaction through its operation. Utility reflects a business concern, especially when considered as the numerator when computing value, which equals utility divided by costs.
Human	**human factors**	Concern about the characteristics of CPS with respect to how they are used by humans.
Human	**usability**	Concerns related to the ability of CPS to be used to achieve its functional objectives effectively, efficiently, and to the satisfaction of users (adapted from ISO 9241-210.) The combination of physical and cyber into complex systems creates challenges in meeting usability goals. Complexity is a major issue. The diversity of interfaces creates a significant learning curve for human interaction.

Aspect	Concern	Description
Trustworthiness	**privacy**	Concerns related to the ability of the CPS to prevent entities (people, machines) from gaining access to data stored in, created by, or transiting a CPS or its components such that individuals or groups cannot seclude themselves or information about themselves from others. Privacy is a condition that results from the establishment and maintenance of a collection of methods to support the mitigation of risks to individuals arising from the processing of their personal information within or among systems or through the manipulation of physical environments.
Trustworthiness	**reliability**	Concerns related to the ability of the CPS to deliver stable and predictable performance in expected conditions.
Trustworthiness	**resilience**	Concerns related to the ability of the CPS to withstand instability, unexpected conditions, and gracefully return to predictable, but possibly degraded, performance.
Trustworthiness	**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 stakeholders and the physical environment.
Trustworthiness	**security**	Concerns related to the ability of the CPS to ensure that all of its processes, mechanisms, both physical and cyber, and services are afforded internal or external protection from unintended and unauthorized access, change, damage, destruction, or use. Confidentiality: Preserving authorized restrictions on access and disclosure. Integrity: Guarding against improper modification or destruction of system, and includes ensuring non-repudiation and authenticity Availability: Ensuring timely and reliable access to and use of a system.
Timing	**logical time**	Concerns related to the order in which things happen (causal order relation) or event driven.
Timing	**synchronization**	Concerns for synchronization are that all associated nodes have timing signals traceable to the same time scale with accuracies as required. There are three kinds of synchronization that might be required: time, phase, and frequency synchronization, although

Aspect	Concern	Description
		frequency synchronization is also called syntonization.
Timing	**time awareness**	Concerns that allow time correctness by design. The presence or absence of time explicitly in the models used to describe, analyze, and design CPS and in the actual operation of the components. This is a life-cycle concern as well as a concern for the ability to build devices without the need for extensive calibration of the timing properties.
Timing	**time-interval and latency**	Specifying requirements for timing generally involves requirements for time-intervals between pairs of events. A time-interval is the duration between two instants read on the same timescale. CPS timing requirements are generally expressed as constraints on the time intervals (TI) between pairs of system significant events. These can be categorized in terms of bounded TIs or latency, deterministic TIs, and accurate TIs.
Data	**data semantics**	Concerns related to the agreed and shared meaning(s) of data held within, generated by, and transiting a system.
Data	**identity**	Concerns related to the ability to accurately recognize entities (people, machines, and data) when interacting with or being leveraged by a CPS.
Data	**operations on data**	Concerns related to the ability to create/read/update/delete system data and how the integrity of CPS data and behaviors may be affected.
Data	**relationship between data**	Concerns related to how and why sets of data must, may, or may not be associated with each other and the value or harm that can be derived from those associations.
Data	**data velocity**	Concerns related to the speed with which data operations are executed.
Data	**data volume**	Concerns related to the volume or quantity of data associated with a CPS' operation.
Boundaries	**behavioral**	Concerns related to interdependence among behavioral domains. Concerns related to the ability to successfully operate a CPS in multiple application areas.
Boundaries	**networkability**	Concerns related to the ease and reliability with which a CPS can be incorporated within a (new or existing) network of other systems.

Aspect	Concern	Description
Boundaries	**responsibility**	Concerns related to the ability to identify the entity or entities authorized to control the operation of a CPS.
Composition	**adaptability**	Concerns related to the ability of the CPS to achieve an intended purpose in the face of changing external conditions such as the need to upgrade or otherwise reconfigure a CPS to meet new conditions, needs, or objectives.
Composition	**complexity**	Concerns related to our understanding of the behavior of CPS due to the richness and heterogeneity of interactions among its components, such as existence of legacy components and the variety of interfaces.
Composition	**constructivity**	Concerns related to the ability to combine CPS modular components (hardware, software, and data) to satisfy user requirements.
Composition	**discoverability**	Concerns related to the ease and reliability with which a CPS component can be observed and understood (for purposes of leveraging the component’s functionality) by an entity (human, machines). Concerns related to the ease and reliability with which a CPS component’s functions can be ascertained (for purposes of leveraging that functionality) by an entity (human, machines).
Lifecycle	**deployability**	Concerns related to the ease and reliability with which a CPS can be brought into productive use.
Lifecycle	**disposability**	Concerns related to the impacts that may occur when the CPS is taken physically out of service.
Lifecycle	**engineerability**	Concerns related to the ease and reliability with which a CPS design concept can successfully be realized via a structured engineering process.
Lifecycle	**maintainability**	Concerns related to the ease and reliability with which the CPS can be kept in working order.
Lifecycle	**operability**	Concerns related to the operation of the CPS when deployed.
Lifecycle	**procureability**	Concerns related to the ease and reliability with which a CPS can be obtained.
Lifecycle	**producibility**	Concerns related to the ease and reliability with which a CPS design can be successfully manufactured.

2.4.4 Composition of Concerns

Concerns are applied in the CPS Framework in general to all of the activities of all of the facets. This is one sense in which they are potentially ‘cross-cutting’. For a particular CPS one may decide to apply certain of the concerns and may view others as not being relevant. This is one of the ways that the CPS Framework can be tailored to the development of a CPS. At the same time, once the set of relevant concerns has been determined, the application of a concern must take into account its interactions with other relevant concerns. For example, action taken in a design to address the cyber-security concern may adversely affect the safety of the CPS. Corrective action then taken to bolster its safety may then reduce the effectiveness of the actions for cyber-security, resilience or reliability. In other words, there will be trade-offs between concerns.

Thus, one needs to explain how a set of more than one concern, deemed as relevant to a CPS, is applied to the CPS in question. This is referred to as the *composition of concerns* and explains how it is to be understood and used.

The effect of applying a concern to a CPS depends on the facet and activity being considered. Generally, that application can be associated with the *set of properties or requirements* that the concern requires of the CPS. Hence applying two or more concerns amounts to requiring *all of the properties required by the set of concerns*.

If one denotes formally the set of properties of a CPS required by a concern as:

$$\bar{C}^{CPS} = \{properties\ of\ the\ CPS\ required\ by\ the\ concern\ C\}$$

then the composition of concerns C_1 and C_2 can be expressed as follows:

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

The interpretation of the composition of multiple concerns is defined in terms of binary composition. The composition of a set of concerns is interpreted as the *union of the properties required by each concern in the set*. This notion of composition is clearly *commutative* and *associative*.

This *set-theoretic semantics* of the CPS Framework can be extended to all of the concepts of the framework and will be worked out in detail in future works.

An example of composition of concerns is *timing security*. The composition of *timing* and *security* results in the collection of all the properties of CPS that are required by the timing and the security concerns. Resolving ‘conflicts’ between properties is one of the tasks of *requirements analysis*.

Consider since timing requires both a physical signal and data about that signal, timing security includes the security of the data in much the same way as traditional cyber-security, plus the security of the physical signal. Many CPS will require timing reliability, both for the local system and for the traceability of the timing. For example, GPS jamming is the timing equivalent of a cyber denial-of-service attack. Resilience will appear as fault-tolerance in timing, whether the fault is intentional or unintentional. Timing safety will depend on the CPS. Certainly in some systems a timing failure can lead to a lack of safety. Privacy will not be a timing concern in many systems, because timing is generally intended to be public information. However, there may well be cases where the timing requires privacy.

So assume that it is desired to present the concerns that apply to the exchange of GNSS ("GPS") timing. You would simultaneously have to satisfy concerns of the form:

- Trustworthiness.Reliability – "message delivery shall be reliable"
- Trustworthiness.Security – "availability shall not be interfered with through Denial Of Service"
- Trustworthiness.Resilience - "the system shall be fault-tolerant"
- Trustworthiness.Safety – "message exchange failure shall not lead to hazard or harm"
- Trustworthiness.Confidentiality – "message exchange shall only be understood by the intended recipient"
- Trustworthiness.Privacy – "message shall not contain PII"
- Data.DataSemantics – "shall have a representation of time"
- Trustworthiness.Security.Cybersecurity – "message exchange must not be tampered with"

This expresses the above outlined example as a set of concerns which taken together corresponds to the union of the properties given by each concern.

2.4.5 Activities and Artifacts

Table 5 lists the activities (groups) and artifacts related to the conceptualization facet.

Table 5: Conceptualization Facet: Activities and Artifacts

Activity and Artifacts
Mission and Business Case Development **Artifact: Business use cases**
Functional Decomposition **Artifact: Detailed use cases, actors, information exchanges**
Requirements Analysis **Artifact: Functional and non-functional requirements**
Requirements Allocation **Artifact: HW/SW configuration Items**
Interface Requirements Analysis **Artifact: Interface requirements**

Table 6 lists the activities (groups) and artifacts related to the realization facet.

Table 6: Realization Facet: Activities and Artifacts

Activity and Artifacts
Business Case Analysis **Artifact: Trade studies, lifecycle cost analysis, return on investment, and interdependencies with requirements, regulations, and incentives**
Lifecycle Management **Artifact: Lifecycle management and sustainability plan, integrated lifecycle management monitoring**
Design **Artifact: Design documentation, tradeoff analyses, requirement verification, virtual prototypes**
Manufacturing/Implementation **Artifact: Manufactured, integrated products, testing plans, and test results**
Operations **Artifact: Performance, quality, and product evolution tracking**
Disposal **Artifact: Reuse, sustainability and energy recovery assessments, disposal manifests**
Cyber-Physical Abstraction Layer Formation **Artifact: Domain (and product)-specific ontologies, modeling languages, and semantics specifications used in all phases of the lifecycle**
Physical Layer Realization **Artifact: Physical substrates of the CPS used in all phases of the lifecycle.**

Table 7 lists the activities (groups) and artifacts related to the assurance facet.

Table 7: Assurance Facet: Activities and Artifacts

Activity and Artifacts
Identify Assurance Objectives **Artifact: Assurance objectives/analysis report**
Define Assurance Strategy **Artifact: Strategy document/plan**
Control Assurance Evidence **Artifact: Control documentation**
Analyze Evidence **Artifact: Analysis report**
Provide Assurance Argument **Artifact: Assurance argument report**
Provide Estimate of Confidence **Artifact: Confidence estimate**
Configuration Audit **Artifacts: Product configuration assessment**
Requirements Verification **Artifact: Requirements and test results assessment**

Activity and Artifacts
Product Certification and Regulatory Compliance Testing **Artifact: Certifications**

2.5 Related Standards and Activities

The purpose of this section is to highlight some, though far from all, related standards, organizations and working groups that are relevant to the NIST CPS PWG effort.

From 2010 to 2013, the European Lighthouse Integrated Project “Internet of Things – Architecture” (IoT-A) developed and proposed an architectural reference model for the IoT, referred to as the IoT Architectural Reference Model (IoT ARM) [7]. The goal of the project was to introduce a common language for fostering the interoperability between vertical “silos” (domains) in emerging IoT applications. The IoT ARM introduces top-down architectural principles and design guidelines.

IoT-A explicitly separates itself in scope from CPS. The IoT-ARM’s functional view is organized in service layers (including communication, services, management, and security) on top of CPS. CPS, in IoT-A’s terminology, are IoT devices (devices) and IoT resources (software), and their architecting guidelines are not covered by the IoT ARM. It is important for the NIST CPS PWG Vocabulary and Reference Architecture subgroup to determine possible interactions with the IoT ARM.

The IEEE P2413 working group [8] was formed in 2014 to promote cross-domain interaction, aid system interoperability, and provide functional compatibility in the IoT. The IEEE P2413 also defines an architectural framework for the IoT, including abstractions and a common vocabulary. It emphasizes a “blueprint for data abstraction and the quality quadruple (protection, security, privacy, and safety.)”

The IoT ARM and IEEE P2413 share a few important characteristics that are worth noting. Both initiatives adhere to the ISO/IEC/IEEE 42010 standard, their functional models are inspired by the OSI reference model, and they explicitly take into consideration architecture divergence. Also, both identify architecture divergence as a major topic. It is important for the NIST CPS PWG to find similarities and key differences between the scopes of IoT-related activities and CPS. This will help readers of this document to distinguish between CPS and IoT and use the NIST CPS Reference Architecture to define CPS-specific architectures that may be compatible with IoT services and standards.

OneM2M [9] is intended to be an interoperability enabler for the entire CPS, M2M and IoT Ecosystem. The purpose and goal of OneM2M is to develop Technical Specifications and Technical Reports, which address the need for a common IoT Service Layer that can be readily realized through an API embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with IoT application servers worldwide. A critical objective of OneM2M is to enable users to build platforms, regardless of existing sector or industry solutions, to enable wider integration and cross-system value to be derived than is currently possible. OneM2M aims to attract and actively involve a wide variety of organizations from IoT-related business domains such as: telematics and intelligent transportation, healthcare, utilities, industrial automation, smart homes, etc.

Cybersecurity Research Alliance (CSRA) [10] is an industry-led, non-profit consortium focused on research and development strategy to address evolving cybersecurity environment through partnerships between government, industry, and academia. This effort was established in response to the growing need for increased public-private collaboration to address R&D issues in cybersecurity.

CPS Voluntary Organization (supported by the National Science Foundation) [11] is an online site to foster collaboration among CPS professionals in academia, government, and industry.

The Networking and Information Technology Research and Development (NITRD) CPS Senior Steering Committee [12] coordinates programs, budgets, and policy recommendations for CPS research and development (R&D). This includes identifying and integrating requirements, conducting joint program planning, and developing joint strategies for the CPS R&D programs conducted by agency members of the NITRD Subcommittee. CPS includes fundamental research, applied R&D, technology development and engineering, demonstrations, testing and evaluation, technology transfer, and education and training; and "agencies" refers to Federal departments, agencies, directorates, foundations, institutes, and other organizational entities.

NIST Privacy Engineering [13] focuses on providing guidance that can be used to decrease privacy risks, and to enable organizations to make purposeful decisions about resource allocation and effective implementation of controls in information systems. This NIST privacy engineering work targets specifically how government agencies are to address privacy and may not be adequate for the private sector.

The goal of making time an integral part of networks is being advanced in foundational standards that define both wired and wireless networks. IEEE 802.1 [14] [15][8], [9] has a time sensitive networking (TSN) working group defining various standards that will enable determinism in local area wired networks using synchronized clocks. The method of synchronizing clocks is based on the IEEE 1588 standards that have invented the Precision Time Protocol (PTP) [16]. The Internet Engineering Task Force (IETF) is planning to leverage the building blocks defined by IEEE 802.1 and IEEE 1588 to enable determinism in wide area networks (routable wired networks). Similar initiatives in the IEEE 802.11 [15] standards body have resulted in the development of Timing Measurement and Fine Timing Measurement protocols that enable precise clock

[8] IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards/ieee.org/).

[9] The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

synchronization in WiFi networks. International Telecommunications Union (see ITU-T standard G.8265.1-July 2014[10]) has also leveraged the work done in 1588 and applied it to telecommunication networks. Enhancements to the IEEE 802.15.4 standards have resulted in the development of a time-slotted communication model for low power personal area networks. This work has been created by the IETF task group called 6TISCH, RFC 7554 [17].

AVnu Alliance [18] is a community for creating an interoperable ecosystem servicing precise timing and low latency requirements of diverse applications using open standards like Time-Sensitive Networking (TSN). This alliance focuses on creating interoperability tests and certification for products used in applications requiring bounded latency, reserved bandwidth, and synchronized time.

Industrial Internet Consortium (IIC) [19] brings together the organizations and technologies necessary to accelerate growth of the Industrial Internet by identifying, assembling, and promoting best practices. This goal of the IIC is to drive innovation through the creation of new industry use cases and testbeds for real-world applications; define and develop the reference architecture and frameworks necessary for interoperability; influence the global development standards process for Internet and industrial systems; facilitate open forums to share and exchange real-world ideas, practices, lessons, and insights; and build confidence around new and innovative approaches to security.

National Security Telecommunications Advisory Committee (NSTAC) [20] brings together up to 30 industry chief executives from major telecommunications companies, network service providers, information technology, finance, and aerospace companies. These industry leaders provide the President with collaborative advice and expertise, as well as robust reviews and recommendations. The NSTAC's goal is to develop recommendations to the President to assure vital telecommunications links through any event or crisis, and to help the US Government maintain a reliable, secure, and resilient national communications posture.

The European Telecommunications Standards Institute's (ETSI's) standardization group dedicated to Low Throughput Networks (LTN) [21] technology has released the first three specifications of an Internet of Things (IoT) network dedicated to low throughput communications. These new requirements provide a breakthrough in the machine to machine business, allowing object connection for a few euros per year, with a few milliwatts for transmission and a modem costing less than 1 euro. The key to the success of IoT standardization and implementation, these assumptions are the basis for many new and innovative applications. Low Throughput Network (LTN) technology is a wide area bidirectional wireless network with key differentiators compared to existing networks. It enables long-range data transmission (distances around 40 km in open

[10] ITU-R publications are available from the International Telecommunications Union, Place des Nations, 1211 Geneva 20, Switzerland (http://www.itu.in/).

field) and/or communication with buried underground equipment and operates with minimal power consumption allowing several years of operation even with standard batteries. This technology also implements advanced signal processing that provides effective protection against interference.

The Internet of Things (IoT) is one of the new, convergent technologies addressed by Open Platform 3.0™ [22] The Open Group IoT standards aim to do for the IoT what HTML/HTTP did for the Web, enabling everything to be connected on the fly. Vendors will be able to collect information from products in the field throughout their lifecycle. This will allow the optimization of maintenance operations, providing increased safety at lower cost. Enterprises will be able to monitor and control installed equipment, and integrate it into intelligent solutions, for example, to ensure the health of buildings and machinery, or to improve energy efficiency.

2.6 SUMMARY

The CPS Framework presents a set of high-level concepts, their relationships, and a vocabulary for clear communication among stakeholders (e.g., architects, engineers, users). The ultimate goal of the CPS Framework is to provide a common language for describing interoperable CPS architectures in various domains so that these CPS can interoperate within and across domains and form systems of systems.

The CPS Framework includes the identification of foundational goals, characteristics, common roles, and features across CPS domains, while considering cybersecurity, privacy, and other cross-cutting concerns. The CPS Framework is an abstract framework, or meta-model, for understanding and deriving application domain-specific CPS architectures. Work remains to be done to further specify this high-level architecture independent from specific application domains, problems, standards, technologies, protocols, and implementations, and to identify interfaces to facilitate cross-sector CPS interoperability.

The CPS Framework consists of three facets – conceptualization, realization, and assurance. Each facet is presented and understood from its set of activities and artifacts. The activities in turn address aspects and concerns throughout the CPS development cycle.

The artifacts consist of properties discovered and modeled in the conceptualization facet, implemented and deployed in the realization facet, and verified and validated in the assurance facet.

Appendix A. References

This section provides references to a variety of CPS-related articles, standards, and other material cited in the text.

[1] TOGAF, The Open Group Architecture Forum, Open Group Standard Version 9.1, 2011, http://pubs.opengroup.org/architecture/togaf9-doc/arch/

[2] CMMI, Capability Maturity Model Integration, Version 1.3, November 2010, https://resources.sei.cmu.edu/asset_files/TechnicalReport/2010_005_001_15287.pdf

[3] ISO/IEC/IEEE 42010, "Systems and software engineering – architecture description," 2011, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6129467

[4] ISO/IEC/IEEE FDIS 15288:2014(E), "Systems and software engineering - System life cycle processes," http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6994196

[5] Forsberg, K. and Mooz, H. "The Relationship of System Engineering to the Project Cycle," in Proceedings of the First Annual Symposium of National Council on System Engineering, link, October 1991.

[6] ISO 26262-1:2011(en), Road vehicles – Functional safety, https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:ed-1:v1:en

[7] Internet of Things – Architecture (IoT-A), "Final architectural reference model for the IoT v3.0," http://www.iot-a.eu/public/public-documents/d3.1, 2013.

[8] IEEE P2314, "Standard for an Architectural Framework for the Internet of Things (IoT)," Webinar, June 13, 2014. http://standards.ieee.org/develop/project/2413.html

[9] Standards for M2M and the Internet of Things, OneM2M, http://www.onem2m.org/technical/published-documents

[10] The Cybersecurity Research Alliance, http://www.cybersecurityresearch.org/about_us.html

[11] The Cyber-Physical Systems Virtual Organization, http://cps-vo.org/

[12] The Networking and Information Technology Research and Development (NITRD) Program, https://www.nitrd.gov/nitrdgroups/index.php?title=Cyber_Physical_Systems_(CPS_SSG)#title

[13] Computer Security Division Computer Security Resource Center, NIST, http://csrc.nist.gov/projects/privacy_engineering/index.html

[14] IEEE 802.1 Time Sensitive Networking Task Group, http://www.ieee802.org/1/pages/tsn.html

[15] IEEE 802.11, "Wireless Local Area Networks," Working Group for WLAN Standards, http://www.ieee802.org/11/

[16] IEEE Instrumentation and Measurement Society, IEEE 1588-2008 IEEE Standard for Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, 24 July 2008,. https://standards.ieee.org/findstds/standard/1588-2008.html

[17] 6TISH, "RFC 7554 on Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement," IETF, 14th May 2015, https://tools.ietf.org/html/rfc7554

[18] The Avnu Alliance, www.avnu.org

[19] The Industrial Internet Consortium, http://www.industrialinternetconsortium.org/

[20] The National Security Telecommunications Advisory Committee, Department of Homeland Security, http://www.dhs.gov/nstac

[21] ETSI specification for Internet of Things and Machine to Machine Low Throughput Networks, ETSI, http://www.etsi.org/news-events/news/827-2014-09-news-etsi-new-specification-for-internet-of-things-and-machine-to-machine-low-throughput-networks

[22] The Open Group Internet of Things (IoT) Work Group, http://www.opengroup.org/getinvolved/workgroups/iot

[23] ISO/IEC 27000:2014, Information technology — Security techniques — Information security management systems — Overview and vocabulary https://www.iso.org/standard/63411.html

[24] ISO/IEC 16500-8:1999, Information technology -- Generic digital audio-visual systems -- Part 8: Management architecture and protocols and concepts, https://www.iso.org/standard/31016.html

[25] ISO/IEC 24760-1:2011 **,** Information technology — Security techniques — A framework for identity management — Part 1: Terminology and Concepts, https://www.iso.org/standard/57914.html

[26] ISO/IEC DIS 18834-1:2016, RA SOA – Information technology -- Reference Architecture for Service Oriented Architecture (SOA RA) -- Part 1: Terminology and concepts for SOA, https://www.iso.org/standard/63104.html

[27] ISO TS 19104:2008, Geographic information – Terminology, https://www.iso.org/standard/45020.html

[28] ISO 9000:2015, Quality management systems – Fundamentals and vocabulary, https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v1:en

[29] Industrial Internet Reference Architecture v1.8, Industrial Internet Consortium, https://www.iiconsortium.org/IIRA.htm

[30] ISO/IEC 24791-1:2010, Information technology — Radio frequency identification (RFID) for item management — Software system infrastructure — Part 1: Architecture, https://www.iso.org/standard/46137.html

[31] CNSSI 4009 Committee on National Security Systems (CNSS) Glossary, Release Date: 04/06/2015, https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[32] ISO/IEC 2382-1:1993, Information technology -- Vocabulary -- Part 1: Fundamental terms, https://www.iso.org/standard/7229.html

[33] European Commission Community Research and Development Information Service, Internet of Things Architecture [IOT-A] project, http://cordis.europa.eu/project/rcn/95713_en.html

[34] ISO/TR 14252:1996, Information technology -- Guide to the POSIX Open System Environment (OSE), https://www.iso.org/standard/23985.html

[35] ISO 7498-2:1989, Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture https://www.iso.org/standard/14256.html

[36] ISO/IEC 14814:2006, Road transport and traffic telematics — Automatic vehicle and equipment identification — Reference architecture and terminology, https://www.iso.org/standard/37046.html

Appendix B. Definitions and Acronyms

The following definitions and acronyms are presented as a ready reference to the intended meaning of their use in the text of this document. It is recognized that within various technical domains, many of these terms and acronyms have multiple meanings. The intent is to provide clarity for the interpretation of this framework and not to make a definitive statement about the "universal" definition of the terms and acronyms. In some cases, canonical references were not identified and the "source" column lists "this document" as the context for the definition.

B.1 Selected terms used in this document are defined below.

Term	Definition	Source
access control	A means to ensure that access to assets is authorized and restricted based on business and security requirements Note: Access control requires both authentication and authorization	[23]
accuracy	Closeness of the agreement between the result of a measurement and the true value of the measurand.	ITU-R Rec. TF.686
actors	A person or system component who interacts with the system as a whole and who provides stimulus which invoke actions.	[24]
ageing	The systematic change in frequency with time due to internal changes in the oscillator. NOTE 1 – It is the frequency change with time when factors external to the oscillator (environment, power supply, etc.) are kept constant.	ITU-R Rec. TF.686
architecture view	An 'architecture view' consists of 'work product expressing the architecture of a system from the perspective of specific system concerns'.	[3]
architecture viewpoint	An 'architecture viewpoint' consists of work product establishing the conventions for the construction, interpretation and use of architecture views to frame specific system concerns'.	[3]
aspect	Conceptually equivalent concerns, or major categories of concerns. Sometimes called "cross-cutting" concerns.	This document
assurance	The level of confidence that a CPS is free from vulnerabilities, either intentionally designed into it or accidentally inserted during its lifecycle, and that the CPS functions in the intended manner.	This document
attribute	A characteristic or property of an entity that can be used to describe its state, appearance, or other aspects.	[25]
calibration	The process of identifying and measuring offsets between the indicated value and the value of a reference standard used as the test object to some determined level of uncertainty. NOTE 1 – In many cases, e.g., in a frequency generator, the calibration is related to the stability of the device and therefore its	ITU-R Rec. TF.686

Term	Definition	Source
	result is a function of time and of the measurement averaging time.	
certificate	A set of data that uniquely identifies an entity, contains the entity's public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key to the entity. Additional information in the certificate could specify how the key is used and its cryptoperiod.	SP 800-21
clock	A device that generates periodic signals for synchronization. Note: Other definitions are provided in different references that are tailored to particular applications. Suitable references include ITU-T Rec. G.810, ITU-R Rec. TF.686 and IEEE Std. 1377-1997.	IEEE Std. 1377-1997
collaboration	Type of composition whose elements interact in a non-directed fashion, each according to their own plans and purposes without a predefined pattern of behavior.	[26]
component	Modular, deployable, and replaceable part of a system that encapsulates implementation and exposes a set of interfaces.	[27]
composition	Result of assembling a collection of elements for a particular purpose.	[26]
CPS architecture	A concrete realization of a reference CPS architecture designed to satisfy use-case-specific constraints.	This document
CPS Framework	Abstract framework and analysis methodology for understanding and deriving application-domain-specific CPS architectures. Activities and outputs to support engineering of CPS.	This document
CPS network manager	A work-station or CPS node connected to a CPS domain that manages and monitors the state and configuration of all CPS nodes in one or more CPS domains.	This document
CPS time domain	A CPS time domain is a logical group of CPS nodes and bridges which form a network with their own timing master.	This document
cross-cutting concern	See aspect	This document
cryptographic (encryption) certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes	SP 800-32
cryptographic key	A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification	SP 800-63
cyber-physical device	A device that has an element of computation and interacts with the physical world through sensing and actuation.	This document
data	Re-interpretable representation of information in a formalized manner suitable for communication, interpretation, or processing. NOTE Data can be processed by humans or by automatic means.	[28]
device	A physical entity embedded inside, or attached to, another physical entity in its vicinity, with capabilities to convey digital information from or to that physical entity.	[29]

Term	Definition	Source
element	Unit that is indivisible at a given level of abstraction and has a clearly defined boundary. Note: An element can be any type of entity	[26]
endpoint	One of two components that either implements and exposes an interface to other components or uses the interface of another component.	[30]
entity	Item inside or outside an information and communication technology system, such as a person, an organization, a device, a subsystem, or a group of such items that has recognizably distinct existence	[25]
epoch	Epoch signifies the beginning of an era (or event) or the reference date of a system of measurements.	ITU-R Rec. TF.686
facet	Facets are perspectives on CPS that each express a distinct set of well-defined processes, methods and tools to support the CPS development process and for expressing the architecture of a system. The Framework identified facets are conceptualization, realization and assurance.	This document
frequency	If T is the period of a repetitive phenomenon, then the frequency f = 1/T. In SI units the period is expressed in seconds, and the frequency is expressed in hertz (Hz).	ITU-R Rec. TF.686
functional requirement	Functional requirements define specific behavior (functions) or particular results of a system and its components, what the system is supposed to accomplish.	This document
hash	Value computed on data to detect error or manipulation. See Checksum.	[31]
identification	A process of recognizing an entity in a particular identity domain as distinct from other entities.	[25]
identifier	Identity information that unambiguously distinguishes one entity from another one in a given identity domain.	[25]
identity authentication	Formalized process of identity verification that, if successful, results in an authenticated identity for an entity.	[25]
identity domain	An environment where an entity can use a set of attributes for identification and other purposes.	[25]
identity information	A set of values of attributes optionally with any associated metadata in an identity. Note: In an information and communication technology system an identity is present as identity information.	[25]
industrial internet	An Internet of things, machines, computers and people, enabling intelligent industrial operations using advanced data analytics for transformational business outcomes.	[29]
information	Knowledge concerning objects, such as facts, events, things, processes or ideas, including concepts, that within a certain context has a particular meaning	[32][32]
jitter	The short-term phase variations of the significant instants of a timing signal from their ideal position in time (where short-term implies here that these variations are of frequency greater than or equal to 10 Hz). See also “wander”.	ITU-R Rec. TF.686

Term	Definition	Source
latency	The latency of a device or process is the time delay introduced by the device or process.	This document
master data	Data held by an organization that describes the entities that are both independent and fundamental for that organization, and that it needs to reference in order to perform its transactions.	[28]
network time protocol (NTP)	The network time protocol (NTP) is used to synchronize the time of a computer client or server to another server or reference time source, such as a terrestrial or satellite broadcast service or modem. NTP provides distributed time accuracies on the order of one millisecond on local area networks (LANs) and tens of milliseconds on wide area networks (WANs). NTP is widely used over the Internet to synchronize network devices to national time references. See www.ntp.org. See also IETF documents (e.g., RFC 5905).	ITU-R Rec. TF.686
non-functional requirement	Non-functional requirements specify criteria useful to evaluate the qualities, goals or operations of a system, rather than specific behaviors or functions of a system.	This document
orchestration	The type of composition where one particular element is used by the composition to oversee and direct the other elements. Note: the element that directs an orchestration is not part of the orchestration.	[26]
oscillator	An electronic device producing a repetitive electronic signal, usually a sine wave or a square wave.	ITU-R Rec. TF.686
phase coherence	Phase coherence exists if two periodic signals of frequency M and N resume the same phase difference after M cycles of the first and N cycles of the second, where M/N is a rational number, obtained through multiplication and/or division from the same fundamental frequency.	ITU-R Rec. TF.686
phase synchronization	The term phase synchronization implies that all associated nodes have access to reference timing signals whose significant events occur at the same instant (within the relevant phase accuracy requirement). In other words, the term phase synchronization refers to the process of aligning clocks with respect to phase (phase alignment). NOTE 1 – Phase synchronization includes compensation for delay between the (common) source and the associated nodes. NOTE 2 – This term might also include the notion of frame timing (that is, the point in time when the timeslot of an outgoing frame is to be generated). NOTE 3 – The concept of phase synchronization (phase alignment) should not be confused with the concept of phase-locking where a fixed phase offset is allowed to be arbitrary and unknown. Phase alignment implies that this phase offset is nominally zero. Two signals which are phase-locked are implicitly frequency synchronized. Phase-alignment and phase-lock both imply that the time error between any pair of associated nodes is bounded	ITU-T Rec. G.8260

Term	Definition	Source
precision time protocol (PTP)	A time protocol originally designed for use in instrument LANs now finding its way into WAN and packet based Ethernet network applications. PTP performance can exceed NTP by several orders of magnitude depending on the network environment. See IEEE 1588.	ITU-R Rec. TF.686
reference timing signal	A timing signal of specified performance that can be used as a timing source for a slave clock.	ITU-T Rec. G.810
second	The SI unit of time, one of the seven SI base units. The second is equal to the duration of 9 192 631 770 periods of the radiation corresponding to the transition between the two hyperfine levels of the ground state of the cesium-133 atom. Note: The symbol for second, the SI unit of time, is s.	found in IEEE Std 270-2006 (Revision of IEEE Std 270-1966); IEEE Standard Definitions for Selected Quantities, Units, and Related ... |
sensor	A sensor is a special device that perceives certain characteristics of the real world and transfers them into a digital representation.	[33]
service	A distinct part of the functionality that is provided by an entity through interfaces.	[34]
stability	Property of a measuring instrument or standard, whereby its metrological properties remain constant in time.	ITU-R Rec. TF.686
subsystem	A discrete part of a system that groups some functionality that is part of the whole.	
system	A system is a composite set of logical components that together satisfy a concrete set of Use Cases.	This document
system function	What the system does. Formalized requirements.	This document
time awareness	The extent to which a device or system has an appropriate ability to sense and response to timing signals and information. Also the extent to which a model can appropriately use time accurately for design, including time semantics, visual design, and time correctness once applied to operational systems.	This document
time interval	The duration between two instants read on the same timescale.	ITU-R Rec. TF.686
time scale (timescale; time-scale)	A system of unambiguous ordering of events. NOTE – This could be a succession of equal time intervals, with accurate references of the limits of these time intervals, which follow each other without any interruption since a well-defined origin. A time scale allows to date any event. For example, calendars are time scales. A frequency signal is not a time scale (every period is not marked and dated). For this reason "UTC frequency" must be used instead of "UTC".	ITU-T Rec. G.810

Term	Definition	Source
timing	A general term for the field or discipline, including time and frequency sources, signals, measurement methods, timestamp methods, specification methods, and metrics.	This document
timing signal	A nominally periodic signal, generated by a clock, used to control the timing of operations in digital equipment and networks. Due to unavoidable disturbances, such as oscillator phase fluctuations, actual timing signals are pseudo-periodic ones, i.e., time intervals between successive equal phase instants show slight variations.	ITU-T Rec. G.810
traceability	The property of a result of a measurement whereby it can be related to appropriate standards, generally international or national standards, through an unbroken chain of comparisons. (ISO/IEC 17025:2005). Ability to compare a calibration device to a standard of even higher accuracy. That standard is compared to another, until eventually a comparison is made to a national standards laboratory. This process is referred to as a chain of traceability.	found in IEEE Std 1159-1995; IEEE Recommended Practice for Monitoring Electric Power Quality; also ITU-R Rec. TF.686
universal time (UT)	Universal time is a measure of time that conforms, within a close approximation, to the mean diurnal motion of the sun as observed on the prime meridian. UT is formally defined by a mathematical formula as a function of Greenwich mean sidereal time. Thus UT is determined from observations of the diurnal motions of the stars. The timescale determined directly from such observations is designated UT0; it is slightly dependent on the place of observation See Recommendation ITU-R TF.460. UT0: UT0 is a direct measure of universal time as observed at a given point on the Earth’s surface. In practice, the observer’s meridian (position on Earth) varies slightly because of polar motion, and so observers at different locations will measure different values of UT0. Other forms of universal time, UT1 and UT2, apply corrections to UT0 in order to establish more uniform timescales. See “universal time”, “UT1” and “UT2” and Recommendation ITU-R TF.460. UT1: UT1 is a form of universal time that accounts for polar motion and is proportional to the rotation of the Earth in space. See “universal time” and Recommendation ITU-R TF.460. UT2: UT2 is a form of universal time that accounts both for polar motion and is further corrected empirically for annual and semi-annual variations in the rotation rate of the Earth to provide a more uniform timescale. The seasonal variations are primarily caused by meteorological effects. See “universal time” and Recommendation ITU-R TF.460. NOTE 1 – The UT2 timescale is no longer determined in practice.	ITU-R Rec. TF.686

Term	Definition	Source
UTC : coordinated universal time	The time scale, maintained by the Bureau International des Poids et Mesures (BIPM) and the International Earth Rotation Service (IERS), which forms the basis of a coordinated dissemination of standard frequencies and time signals. See Recommendation ITU R TF.460. It corresponds exactly in rate with TAI, but differs from it by an integer number of seconds. The UTC scale is adjusted by the insertion or deletion of seconds (positive or negative leap seconds) to ensure approximate agreement with UT1. See “universal time” and Recommendation ITU R TF.460.	ITU-T Rec. G.810 and ITU-R Rec. TF.686
wander	The long-term phase variations of the significant instants of a timing signal from their ideal position in time (where long-term implies here that these variations are of frequency less than 10 Hz). See “jitter”. Note: there is work in ITU-T SG15/Q13 to address wander/jitter associated with time signals such as 1PPS where the 10Hz breakpoint is not meaningful.	ITU-R Rec. TF.686

B.2 Selected acronyms used in this document are defined below.

Acronym	**Expansion**
ACM	Association for Computing Machinery
ANSI	American National Standards Institute
API	Application programming interface
ARINC	Aeronautical Radio, Incorporated
BIPM	Bureau International des Poids et Mesures
CHESS	Center for Hybrid and Embedded Software
COAST	Copper/Optical Access, Synchronization, and Transport Committee
CPS PWG	Cyber-Physical Systems Public Working Group
CRIS	Critical Infrastructures
DIS	Draft International Standard
EMI	Electromagnetic interference
EPRI	Electric Power Research Institute
ERM	Enterprise resource management
EU	European Union
FDIS	Final Draft International Standard
FIPP	Fair Information Practice Principles
GNSS	Global navigation satellite system
GPS	Global positioning system
HIPAA	Health Insurance Portability and Accountability Act
HTTPS	Hypertext Transfer Protocol over TLS
HVAC	Heating, ventilating, and air conditioning
HW	Hardware
I/O	Input/output
ICNRG	Information Centric Networking
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IF-Map	Interface for Metadata Access Points
IIC	Industrial Internet Consortium
IJSWIS	International Journal on Semantic Web and Information Systems
IoT	Internet of Things
IoT ARM	Internet of Things Architectural Reference Model
IoT-A	Internet of Things – Architecture
IP	Internet Protocol
IPsec	Internet Protocol Security

Acronym	**Expansion**
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization
ISPCS	International IEEE Symposium on Precision Clock Synchronization for Measurement, Control, and Communication
IT	Information technology
ITU	International Telecommunication Union
ITU-R	International Telecommuncation Union – Radiocommunication Sector
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
JDL	Joint Director of Laboratories
KPI	Key performance indicator
LNCS	Lecture Notes in Computer Science
M2M	Machine-to-machine
MAC	Media Access Control
MACsec	Media Access Control Security
NISO	National Information Standards Organization
NIST	National Institute of Standards and Technology
NITRD	Networking and Information Technology Research and Development
NSTAC	National Security Telecommunications Advisory Committee
NTP	Network Time Protocol
OEM	Original equipment manufacturer
OMG	Object Management Group
OT	Operational technology
OWL	Web Ontology Language
PALS	Physically-Asynchronous Logically-Synchronous
PII	Personally identifiable information
PKI	Public key infrastructure
POSIX	Portable Operating System Interface
PROFINET	Process Field Net
PTIDES	Programming Temporally Integrated Distributed Embedded Systems
PTP	Precise Time Protocol
R&D	Research and development
RA	Reference architecture
RDF	Resource Description Framework
RFC	Request for Comments
RFID	Radio-frequency identification
SDH	Synchronous digital hierarchy
SOA	Service-oriented architecture

Acronym	**Expansion**
SoS	System-of-systems
SPARQL	SPARQL Protocol and RDF Query Language
SW	Software
TAI	International Atomic Time (Temps Atomique International)
TLS	Transport Layer Security
TNC	Trusted Network Communications
TTA	Time-Triggered Architecture
UAV	Unmanned Aerial Vehicle
URL	Universal Resource Locator
US	United States
UTC	Coordinated Universal Time
W3C	World Wide Web Consortium
XEP	XMPP Extension Protocol
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

Appendix C. Applying the CPS Framework: An Emergency Response Use Case

In this appendix, as a simplified example to illustrate the use of the CPS Framework concepts, the CPS Framework is applied to analyze an example CPS use case for Emergency Response. The use case has been limited in scope in order to make this example use of the Framework more clearly expressed.

C.1 Perspective for Applying the Framework

There are many variations, alternative scenarios, and critical features that would make this a comprehensive use case. However, the purpose of the exercise is to demonstrate how to use the Framework, as opposed to how to design emergency response.

The activity, therefore, limited the scope to the initial use case with no elaborations beyond a refinement of the success criteria. It can be expected that this constrained scope will result in significant limitations to the actual value of the analysis to offer insight into emergency response. On the other hand, the concepts presented will be readily recognized by the reader and should enhance the understanding of how the Framework was applied.

The goals for analyzing this problem are to convey an understanding of the *mechanics* of the CPS Framework. To this end the discussion is further limited to:

- The interfaces to the CPS devices and systems involved in the scenario and not the architecting of these systems and devices.
- The *properties* exposed during the Framework analysis of this CPS. For the complete analysis the reader should refer to section 2 of the CPS Framework. A complete analysis of this and its component systems would include all the properties, full design, and full assurance cases of the component systems and this system.
- As offered in section 2.3 Uses of the CPS Framework, this analysis will be of "shallow depth."

C.2 Workflow for Analyzing the Emergency Response Use Case

The Framework section 2.4, The Description of the CPS Framework, suggests a workflow that starts with the development of a template containing the Domains/Facets/Activities/Aspects/Concerns and allows for a tailoring based on the identified use of the framework from section 2.3.

With a decision to follow a waterfall process, the work in analyzing a use case using the CPS Framework has the following high-level steps:

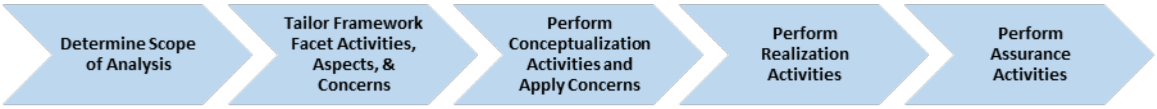

Determine Scope of Analysis
Tailor Framework Facet Activities, Aspects, & Concerns
Perform Conceptualization Activities and Apply Concerns
Perform Realization Activities
Perform Assurance Activities

Figure 14: Workflow for Framework Application Sample

C.3 Emergency Response Use Case Original

The following is the use case that was the basis of the exercise. The input provided to the exercise as a starting point is as follows:

> **"Injured person needs help – 1st responders on the way"**
>
> A person has been injured. The injured person sends a text to e-911 for help. An ambulance is dispatched. A smart GPS combines map data with traffic flow data to route the ambulance. Traffic signals are triggered to assist ambulance in navigation (or negotiating) the route.
>
> **Systems**
>
> - Smart phone
> - E-911 system (includes dispatch system)
> - Ambulance (includes smart GPS subsystem)
> - Traffic Control System
> - GPS System
> - Cellular Phone Network
>
> **Steps**
>
> - A person becomes injured.
> - Person uses cell phone to text for help.
> - The E-911 system gets the person's location from the GPS if available and Cell Tower if not.
> - The cell phone provides the location through the cellular system to the E-911 system.
> - A request is sent to the closest ambulance.
> - The ambulance uses map data + traffic flow data to determine best route.
> - The route is sent to the traffic control system.
> - Traffic control system changes the lights to green as the ambulance proceeds towards the destination (based on ambulance GPS).
> - Light status is fed back to the ambulance (including intersections with no lights).

- The ambulance progress is sent by text to the injured person and the dispatch system (i.e. E-911 system)

Success

- Ambulance arrives at injured person in a timely fashion and in line with the urgency indicated by the injury information.

Variations (not analyzed in this Appendix but noted for future work)

- A power line falls while the ambulance is on route, and the ambulance needs to take a different route.
- A UAV drone support system is used to augment the "smart GPS" of the ambulance.

C.4 Determine Scope of Analysis

Section 2.3 provides for the tailoring of the overall analysis. The following table was used to choose among the possibilities (note that an ‘x’ in the left column selects an item for inclusion):

Table 8: Tailoring the Analysis

What kind of analysis is this?	
	Processes
x	Waterfall
	Reverse Engineer
	Agile
	Service-Based
	Depth
	Critical-tightly coupled
	Loosely coupled
x	Shallow analysis
	Scopes
	Single CPS Device
	System or subsystem
x	System of systems

Then, the CPS Application Domains directly related to the use case are identified:

Table 9: CPS Application Domains Relevant to Use Case

	Domain
	Advertising
	Aerospace
	Agriculture
	Buildings
x	Cities
	Communities
x	Consumer
	Defense
	Disaster resilience (includes preparedness and crisis management activities)
	Education
x	Emergency response
	Energy (included in “infrastructure”, but this is a very broad category)
	Entertainment/sports
	Environmental monitoring (e.g., weather, greenhouse gas emission tracking)
	Financial services
	Healthcare
x	Infrastructure (communications, power, water)
	Leisure
	Manufacturing
	Science
	Social networks
	Supply chain/retail
x	Transportation

C.5 Tailor Framework Facet Activities, Aspects & Concerns

The Conceptualization Facet was tailored to three activities:

Table 10: Tailoring the Conceptualization Facet

Conceptualization Facet	
	Activities and Artifacts
x	Mission and Business Case Development Artifact: Business use cases
x	Functional Decomposition Artifact: Detailed use cases, actors, information exchanges

Conceptualization Facet	
x	Requirements Analysis Artifact: Functional and non-functional requirements
	Interface Requirements Analysis Artifact: Interface requirements

The Realization Facet was tailored to a single activity. Also note that this activity was limited to resolving two Conceptualization properties that arose from concerns.

Table 11: Tailoring the Realization Facet

Realization Facet	
	Activities and Artifacts
	Business Case Analysis Artifact: Trade studies, lifecycle cost analysis, return on investment, and interdependencies with requirements, regulations, and incentives
	Lifecycle Management Artifact: Lifecycle management and sustainability plan, integrated lifecycle management monitoring
x	Design Artifact: Design documentation, requirement verification, virtual prototypes
	Manufacturing/Implementation Artifact: Manufactured, integrated products, testing plans, and test results
	Operations Artifact: Performance, quality, and product evolution tracking
	Disposal Artifact: Reuse, sustainability and energy recovery assessments, disposal manifests
	Cyber-Physical Abstraction Layer Formation Artifact: Domain (and product)-specific ontologies, modeling languages, and semantics specifications used in all phases of the lifecycle
	Physical Layer Realization Artifact: Physical substrates of the CPS used in all phases of the lifecycle.

The Assurance Facet was tailored to two activities:

Table 12: Tailoring the Assurance Facet

Assurance Facet	
	Activities and Artifacts
	Configuration Audit Artifacts: Product configuration assessment

Assurance Facet	
	Requirements Verification Artifact: Requirements and test results assessment
	Product Certification and Regulatory Compliance Testing Artifact: Certifications
x	Identify Assurance Objectives Artifact: Assurance objectives/analysis report
x	Define Assurance Strategy Artifact: Strategy document/plan
	Control Assurance Evidence Artifact: Control documentation
	Analyze Evidence Artifact: Analysis report
	Provide Assurance Argument Artifact: Assurance argument report
	Provide Estimate of Confidence Artifact: Confidence estimate

The Aspects were tailored as follows:

Table 13: Tailoring of Aspects

	Aspects
x	Functional
	Business
x	Human
x	Trustworthiness
x	Timing
x	Data
x	Boundaries
x	Composition
	Lifecycle

C.6 Perform Conceptualization Activities and Apply Concerns

The Conceptualization Facet has as its artifact the CPS Model which consists of the properties of the intended CPS.

C.6.1 Conceptualization Activity 1: Mission and Business Case Development

This activity involved the analysis of the Use Case and the derivation of an overarching business case and key assumptions and success metrics. The materials started with were broken down into “properties” for further use in the functional decomposition and the requirements analysis.

Note that each of the following could be further broken down into more primitive components. However, that will be left to a future activity.

P_{BC} Business Case:

The goal of this service is to provide medical attention to an injured person. It is assumed for this exercise that the value of human life justifies the expenditures needed to make this service viable.

P_{UC} Use Case:

A person has been injured. The injured person sends a text to E-911 for help. An ambulance is dispatched. A smart GPS combines map data with traffic flow data to route the ambulance. Traffic signals are triggered to assist the ambulance in navigation (or negotiating) the route.

P_{ASSN} Assumptions:

The existence of a set of system components is assumed (see below). They are assumed to be functioning as expected. Organizational responsibilities are pre-existing and functioning as expected. No other extraordinary event is occurring at the same time.

P_{SUCC} Success Metric:

The ambulance arrives at the injured person in a timely fashion and in line with the urgency indicated by the injury information.

C.6.2 Conceptualization Activity 2: Functional Decomposition

The use case is analyzed to identify additional properties: system components, information exchanges, and general information about the networks they utilize.

P_{SC} System Components

- Smart phone [cell]
- E-911 system (includes dispatch system) [E911]
- Ambulance (includes smart GPS subsystem) [ambulance]
- Traffic Control System [TCS]
- GPS System [GPS]

P_{NW} Assumptions

- Person's cell phone and ambulance are on a cellular network.
- The TCS and E911 are on a high speed enterprise network.

P_{ARCH} Use Case Steps (how the system should function)

Table 14: Emergency Response Use Case Steps

Data Exchange Messaging for Use Case				
	Step	**from Actor**	**to Actor**	**data**
1	A person becomes injured			
2	Person uses cell phone to text for help	cell	E911	text help message
3	The cell phone gets the person's location from the GPS if available and Cell Tower if not	GPS	cell	location
4	The cell phone provides the location through the cellular system to the E-911 system	cell	E911	location
5	A request is sent to the response (closest) ambulance	E911	ambulance	dispatch
6	The ambulance uses map data + traffic flow data to determine best route	TCS	ambulance	TCS status
7	The route is sent to the traffic control system	ambulance	TCS	route
8	Traffic control system changes the lights to green as the ambulance proceeds towards the destination (based on ambulance GPS).	ambulance	TCS	location
9	Other vehicles move out of the way	TCS	other vehicles	emergency status
10	Light status is fed back to the ambulance (including intersections with no lights)	TCS	ambulance	light status
11	The ambulance progress is sent by text to the injured person and the dispatch system (i.e. E-911 system)	ambulance	cell, TCS, E911	progress

C.6.3 Conceptualization Activity 3: Requirements Analysis

The results of Activity 1 and 2 were studied with respect to each Aspect and their subsidiary Concerns to identify the properties that would comprise the CPS Model. Each property discovered is listed in the corresponding cell for an aspect/concern. Multiple properties are separated by semicolon/line feeds. Aspects that were profiled out (see earlier section) or had no elucidated properties are indicated by 'N/A'.

It is likely additional property elaboration would be appropriate to be a complete result to the depth of this CPS analysis. However, the properties identified provide a good guide to the nature and abstraction of such properties for this kind of effort.

Table 15: Emergency Response Requirements Analysis

Aspect	Concern	Requirements Analysis
Functional	actuation	ambulance gets sent; ambulance proceeds unimpeded; vehicles move out of the way;

Functional	communication	deliver text message to E911;
		location delivered;
		texting (cell to E911);
		E911 to ambulance;
		GPS identification of cell location;
		GPS sends cell location to ambulance;
		ambulance sends route to TCS;
		TCS to all vehicles;

Functional	controllability	E911 identify and dispatch ambulance;
		TCS light control;
		E911 monitors progress;
		optimal route;

Functional	functionality	Use Cases; Business Cases; success criteria; assumptions;
Functional	measurability	successful arrivals of the ambulances; average time to get to person;
Functional	monitorability	timestamped sequence of events; status of all systems;
Functional	performance	ambulance arrives within target time; vehicles are informed in time to move;
Functional	physical	N/A[11]
Functional	physical context	location of ambulance relative to traffic, intersections and destination at a given time; location of person;

Functional	sensing	location of ambulance, person;
		time for stamping;
		traffic flows;

Functional	uncertainty	route uncertainty better less than road dimension; location uncertainty small enough to determine location of person and ambulance; systems are time synchronized to establish reliable sequence of events;
Business	enterprise	N/A

[11] N/A indicates concerns that were profiled out or had no elucidated properties.

Aspect	Concern	Requirements Analysis
Business	cost	N/A
Business	environment	N/A
Business	policy	N/A
Business	quality	N/A
Business	regulatory	N/A
Business	time to market	N/A
Human	human factors	N/A
Human	usability	emergency text should be sent from a simple unambiguous behavior (no dialog/navigation/typing); other vehicle interpretation of guidance to get out of ambulance way should be unambiguous;
Human	utility	N/A
Trustworthiness	privacy	personally identifiable information (PII) from the emergency response is protected in flight;
Trustworthiness	reliability	ambulance, cell, TCS, E911, and GPS have an acceptable combined reliability (e.g. 95% assurance that the ambulance arrives in the timely fashion).
Trustworthiness	resilience	failure of ambulance is detected and another ambulance dispatched; in order to maintain the acceptable combined performance, redundant or backup systems are available to maintain timely response for any emergency response; the ambulance, TCS, E911 timing physical and messaging signals have resilience;
Trustworthiness	safety	TCS avoids creating hazardous conditions in managing lights with respect to cross streets; E911, TCS, GPS are designed to fail functional; Directions to the ambulance does not create hazard to the ambulance operation; Route should convey the ambulance safely;

Aspect	**Concern**	**Requirements Analysis**
Trustworthiness	security	Messaging is not confidential; Records of the emergency response are protected at rest; Source and destination of messages are validated; Messages received have not been tampered with; All messaging with guaranteed delivery; All components protect against physical tamper; The ambulance, TCS, and E911 timing, physical and messaging signals have integrity; The ambulance, TCS, and E911 timing, physical and messaging signals have availability;
Timing	logical time	The sequence of events is as described in the Use Case;
Timing	managing timing and latency	cell network delivers text message in a timely manner (e.g. <10 seconds); TCS/E911 network have minimum message latency (e.g. <1 seconds);
Timing	synchronization	TCS, E911, ambulance must have a common time scale (e.g. UTC)
Timing	time awareness	TCS, E911, ambulance can give a timely response;
Timing	time-interval and latency control	time interval from sending text message to E911 and ambulance arrival is timely (e.g. <6 minutes); timing of TCS must perform relevant to the movement of the ambulance, and other vehicles and cross-traffic to effect rapid progress of ambulance and minimize impact to cross-traffic (e.g. predicted progress of the ambulance accurate to 1s);

Data	data semantics	text help message;
		location;
		dispatch;
		TCS status;
		route;
		emergency status;
		light status;
		progress;
		text help message is encoded as a "text message";

Data	identity	personal phone, ambulance, TCS system(s), E911 system, intersections, response event;
Data	operations on data	fuse data from various sources to determine best route; evaluate ambulance characteristics and availability to optimize allocation;
Data	relationship between data	locations of ambulances, person, route, traffic must be analyzed and correlated;

Aspect	Concern	Requirements Analysis
Boundaries	cross-domain	emergency response interacting with traffic control and, … see domain list
Boundaries	connectivity	cell phone can connect with cell phone towers -- one hop to cell tower, GPS network receive broadcast
Boundaries	responsibility	TCS is the responsibility of municipal government traffic management; The holder of the phone has the ability to participate in the scenario; The E911 is the responsibility of the government e-response; The ambulance is part of the emergency response function and may be fire/police/private;
Compositio n	adaptability	work with different cell phone technologies; use cell towers or GPS for location;
Compositio n	complexity	work with older (flip phones); deal with different kinds and managements of ambulance services; "green lighting" can cause impact on other existing flows;
Compositio n	constructivity	Emergency response requires E911 system, the diversity of cell phones, cell phone networks, and ambulance services; coordination between neighbor TCS;

Compositio n	discoverability	ambulance location and capability;
		cellphone location;
		traffic need to be determined;
		pertinent TCS identity and capability;

Lifecycle	deployability	N/A
Lifecycle	disposability	N/A
Lifecycle	engineerability	N/A
Lifecycle	maintainability	N/A
Lifecycle	operatability	N/A
Lifecycle	procureability	N/A
Lifecycle	producibility	N/A

C.7 Perform Realization Activities

This exercising of the realization activities produced two example design/test pairs.

During this analysis, an accelerated design process reviewed some on-line literature and derived a first level design for two properties enumerated in the Conceptualization activities.

These designs were provided with hypothetical test plans that could verify the successful performance of the design.

Table 16: Realization Activity

Aspect/Concern: Property	Design	Test Format: Test ID (TID) Test Description
Functional/Performance: 2.6.1.1 ambulance arrives within target time	$D_{\text{scenario timing}}$ Steps[12] 1 – start 2 – 10 s high confidence that SMS gets through to target 3 – 60 s maximum GPS location acquisition time 4 – 10 s same as 2 5 – 10 s E911 has situational awareness of all ambulances locations and metrics 6 – 3 s ambulance is enabled to rapid routing 7 – 3 s high quality of service to TCS from ambulance 8 – 4.5 m drive time to cell phone 6 minutes target response time location accuracy 50-300 m maximum distance for ambulance to travel 5, 35 mph	$T_{\text{scenario timing}}$ TID 1. Measure SMS propagation over 1000 messages and verify <10 s TID 2. Measure GPS location acquisition time from a selected set of locations and cell phone start conditions and verify <60 s in all cases TID 3. Measure ambulance routing capability and verify < 3 s over 100 random locations within 4 mile radius TID 4. Measure transit time of message from ambulance to TCS and verify <3 s over 100 locations throughout territory. TID 5. From a set of 100 test locations and different traffic conditions, verify that test response driving times are < 4.5 minutes
Composition/Adaptability 2.6.1.2 work with different cell phone technologies	$D_{\text{cell phone technologies}}$ Rely on SMS and cellular location as a minimum requirement	$T_{\text{cell phone technologies}}$ TID1. Measure SMS transfer and locational accuracy for each available cell phone on the market and several legacy phones including flip phones. Verify 10 s SMS. Verify 30 m location accuracy

C.8 Perform Assurance Activities

The conceptualization facet produces the CPS Model that consists of properties of the CPS. Some of these properties result from interpreting the initial business case and the impact of the relevant aspects and concerns on the business case.

[12] Some metrics presented in this analysis were obtained from the following article: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4288957/

Two of the activities of the Assurance Facet were undertaken. Refer to Section 2 for definition of terminology.

To identify Assurance Objectives, we turn back to the properties that were defined as the artifacts of the Conceptualization Facet and we identify as an objective the assurance of those properties. There were two properties defined in the requirements analysis activity for which all three facets were exercised – corresponding to the *performance concern of the functional aspect* and the *adaptability concern of the composition aspect*:

Functional Aspect/Performance Concern driven property:

$$P_{\text{Ambulance shall arrive within target time}}$$

Composition Aspect/Adaptability Concern driven property:

$$P_{\text{Shall function with different cell phone technologies}}$$

These two properties comprise the assurance objective.

The assurance strategy for these two properties makes use of the design and test artifacts called out in the Realization Facet. The strategy is to provide argumentation to the effect that the successful execution of the test suffices to make the judgment that the properties are met:

H_{Leaf} is the argumentation that says that the test, design, and tracing to the property is sufficient to conclude that the property in question has been met:

$$A(P, D, T) =_{\text{Def}} H_{\text{Leaf}}\,(P_{\text{Ambulance shall arrive within target time}}, D_{\text{scenario timing}}, T_{\text{scenario timing}})$$

$$A(P, D, T) =_{\text{Def}} H_{\text{Leaf}}\,(P_{\text{Shall function with different cell phone technologies}}, D_{\text{cell phone technologies}}, T_{\text{cell phone technologies}})$$