Merging Digital and Physical Worlds into Cyber-Physical Systems Framework

David Wollman, PhD, NIST

Two worlds that have operated independently—the digital and physical worlds—are now merging, creating opportunities that will transform many sectors of our society. These new smart systems are based on engineered interacting networks of physical and computational components, and are described by names such as the Internet of Things (IoT), Cyber-Physical Systems (CPS), the Industrial Internet, Smart Cities, the Internet of Everything, and more. Regardless of the terminology, there is wide agreement that the economic and societal implications are enormous. Reports including a recent study by the McKinsey Global Institute, "The Internet of Things: Mapping the Value beyond the Hype," predict potential economic impacts of several trillions of dollars per year in ten years.

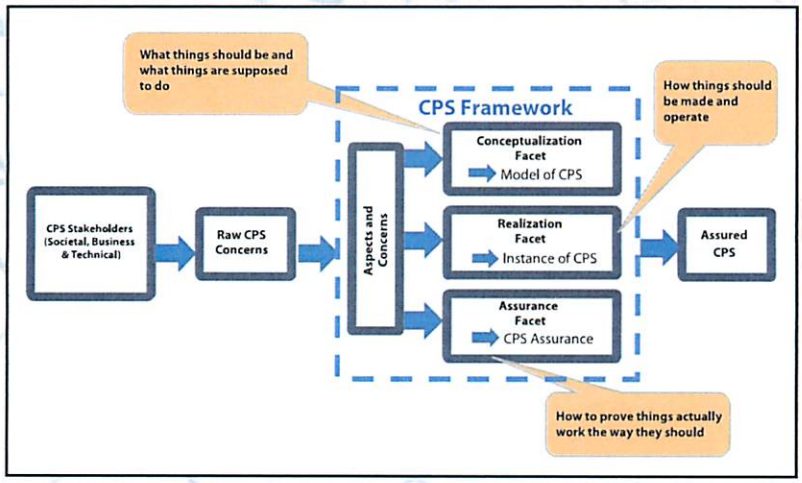

Figure 1. Analysis of CPS and Derivation of Framework

Interoperability Is Key

The same study identifies interoperability between IoT systems as a very critical issue, finding that "on average, interoperability is required for 40 percent of potential value across IoT applications and by nearly 60 percent in some settings." In other words, many of the benefits and much of the value will come from individual systems working together in systems of systems.

Enabling interoperability within this new cyber-physical realm is an important goal for the National Institute of Standards and Technology (NIST), the federal agency with a mission "to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life."

The NIST Cyber-Physical Systems Public Working Group

In mid-2014, NIST established the Cyber-Physical Systems Public Working Group, bringing together a broad range of experts from industry, academia, and government in an open public forum to help define and shape key characteristics of CPS. The objective is to develop a shared understanding of CPS and its foundational concepts and unique dimensions. The Public Working Group's goals have has been to promote progress through the exchange of ideas and integration of research across sectors and to support development of CPS with new functionalities. Five expert subgroups were formed, led by co-chairs from NIST, industry, and academia, to ensure that the following key perspectives were considered:

- Vocabulary and Reference Architecture
- Cybersecurity and Privacy
- Timing and Synchronization
- Data Interoperability
- Use Cases

Over the past 15 months, the Public Working Group and its five subgroups have been meeting regularly in face-to-face and virtual meetings, with information shared via the group's website, *www.cpspwg.org*. The first major product of the intense effort, "Framework for Cyber-Physical Systems," was released as a draft for public comment in late September 2015.

The CPS Framework presents a set of high-level concepts and their relationships, as well as 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 and analyzing interoperable CPS architectures in various domains so that these CPS can interoperate within and across domains and form systems of systems.

Figure 1 shows how the Framework is intended to help CPS stakeholders address their interests and concerns to create and implement assured solutions and systems.

A Common Language: Domains, Facets, and Aspects

From the most high-level view, the Framework discusses three types of elements: domains, facets, and aspects. See a visual depiction of this conceptual model in Figure 2.

Domains, probably the most familiar perspective from which to view CPS, refer to the areas of deployment, such as manufacturing, transportation, or cities. There are already dozens of domains, and the number will continue to grow. Domains answer the questions "Who?" and "Where?"

Facets answer the questions "What?" and "How?" The three facets, which can be applied to any system in any domain, include the following activities:

- Conceptualization Facet—what things should be and what things are supposed to do (e.g., functional decomposition, requirements, logical models).
- Realization Facet—how things should be made and operate (including detailed designs and engineering tradeoffs).
- Assurance Facet—how to achieve a desired level of confidence.

Aspects are groupings of cross-cutting concerns and answer the questions "Why?" and "When?" Nine aspects are currently identified in the Framework (see Figure 2).

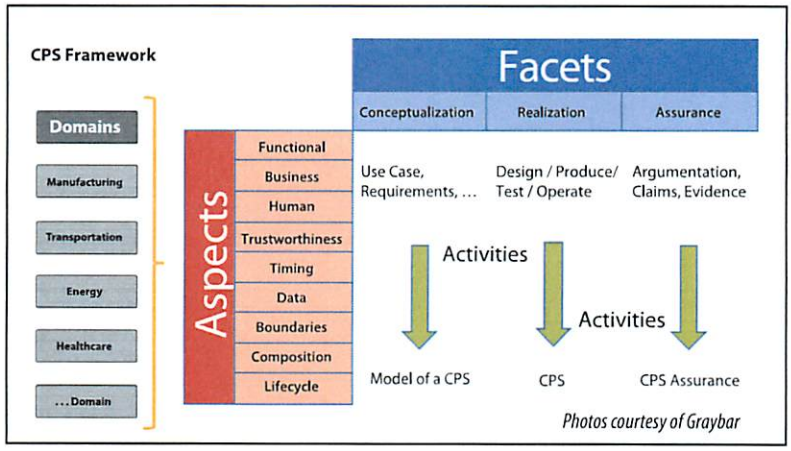

Figure 2. CPS Framework: Domains, Facets, Aspects

Using the Framework for Analysis

After defining and discussing these abstract terms, the Framework then shows how they can be used in a CPS analysis methodology. In this methodology, activities identified in the facets are implemented in a coordinated approach to address concerns within the aspects throughout the design, development, and implementation cycle, using a range of development approaches.

To illustrate how this approach can be applied in a real-world example, the Framework takes the reader through an analysis of a "smart traffic" system in an "emergency response" scenario.

A New Concept for CPS: "Trustworthiness"

Cyber-physical systems present a very wide range of cybersecurity challenges, and a significant section within the Framework document is devoted to this topic. The Framework outlines how CPS cybersecurity must expand its horizons from classic cybersecurity properties to evaluating cross-property risk management in a complicated system.

For CPS, there are five top-level properties of systems that risk managers must consider when performing risk management, as follows:

- Security (or cybersecurity)
- Privacy
- Safety
- Reliability
- Resilience

Taken together in the context of CPS, these five risk management properties support the "trustworthiness" of the system. Trustworthiness means that the CPS does what users and operators expect (and not something else) in the presence of various disruptions, errors, and attacks. Trustworthiness is a holistic concept, and it is not sufficient simply to assemble components that are themselves trustworthy. Integrating the components and understanding how the trustworthiness dimensions interact are central challenges in building trustworthy CPS. The close relationship between the five properties above provides both new challenges and opportunities, and designers and integrators should consider both the intended and unintended effects resulting from the combination of properties where the goals of each may contradict or be complimentary to their counterparts. Trade-off decisions should be considered in light of the system-of-systems objective, if known.

Next Steps and Your Involvement

The draft CPS Framework will be revised based on public comments, and a "final draft" will be released for an additional public comment period before completion of the CPS Framework in early 2016. Additional work is planned to evaluate the applicability of the new Framework concepts in example CPS domains, and to discover gaps that can be addressed in future roadmapping activities. The Public Working Group is open to all, and you are invited to join this important endeavor—please visit the CPS PWG website at *www.cpspwg.org* (or *nist.gov/cps/cpspwg.cfm*) for more information on how you can contribute.

Dr. Wollman is deputy director of NIST's Smart Grid and Cyber-Physical Systems Program Office.