A Prototype Architecture for Cyber-Physical Systems

Ying Tan, Steve Goddard
Computer Science and Engineering
University of Nebraska–Lincoln
Lincoln, NE 66588
{yingtan, goddard}@cse.unl.edu

Lance C. Pérez
Electronic Engineering
University of Nebraska–Lincoln
Lincoln, NE 66588
lperez@unl.edu

Abstract

Cyber-Physical Systems (CPS) is an exciting emerging research area that has drawn the attention of many researchers. Although the question of "What is a CPS?" remains open, widely recognized and accepted attributes of a CPS include timeliness, distributed, reliability, fault-tolerance, security, scalability and autonomous. In this paper, a CPS definition is given and a prototype architecture is proposed. It is argued that this architecture captures the essential attributes of a CPS and lead to identification of many research challenges.

1 Introduction

The current technologies that integrate computations and interactions with the physical world typically emanate from the fields of Embedded Systems and Real-Time Systems. Figure 1 shows a typical architecture used in embedded systems. In this architecture, sensor and actuator units are tightly coupled with a higher level control unit, and *timing properties* are carefully measured at each system level so that control loops perform correctly (both functionally and temporally).

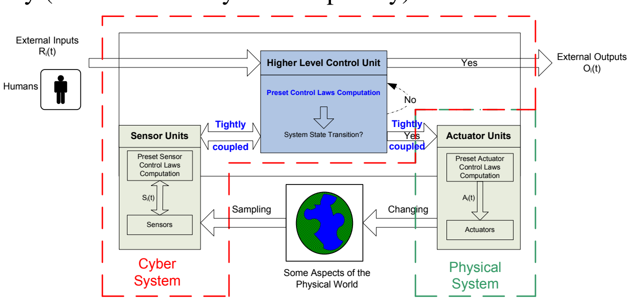

Figure 1. Typical Architecture of Embedded Systems

Traditional embedded system design has made tremendous progress in the past decades. As system complexity increases, however, this centralized and tightly coupled architecture becomes problematic. In contrast, human society provides an example of a system that has successfully bridged the complexity gap. Humans have been successfully interacting and changing the physical world for thousands of year, and might be one of the most sophisticated systems to ever exist. In addition to interacting with the physical world, human society also interacts well with the cyber-world. In fact human society has many of the identified attributes of a CPS. Thus, it is worth taking a closer look at human society to identify the factors that make the system successful. Below are some basic observations:

- A global reference time is the foundation for all system components to communicate and work correctly. As a result, although system components may be interacting with the physical world concurrently and asynchronously, communicating system components can still achieve a correct partial ordering of behaviors and events.
- Human society is an event/information driven system. Events/information are abstractions of the physical world made by system components. In addition, these abstractions have a life-span property; live events/information reflect some current status of the physical world, while out-of-date events/information reflect some past status of the physical world. By their very nature, events/information have a confidence property.
- Different system components (e.g., human individuals) may assign different trustworthiness and dependability values to different input sources based on their personal likes/dislikes, past experience and knowledge. As a result, even for the same input abstractions, different system components might produce totally different outcomes/behaviors.
- Publish and Subscribe are two basic communication schemes used in human society. By using a global reference time (implicitly or explicitly), anyone can publish their abstraction of the physical world, which can then be subscribed to and interpreted correctly by other interested human individuals.

2 Fundamental Gaps

One often asked question is: "Why are today's embedded system's technologies and real-time theories not sufficient for future CPSs?" For any time-sensitive distributed system, the first step in system design requires a global reference time (either logical or physical) that will help achieve a global (partial) ordering of events. That way any system component will correctly interpret information produced by other system components. However, today's embedded systems are still built with isolated system-level time. Thus, every time we build a complex system, we need to re-test the timing property for all system components. This process is expensive, time consuming, and error-prone, which represents a major obstacle towards developing future CPSs.

The second question is: "If all system components are provided with a global reference time, is the problem solved?" Unfortunately, the answer is still "No". The reason is a lack of a unified mechanism to quantify the confidence of a system com-

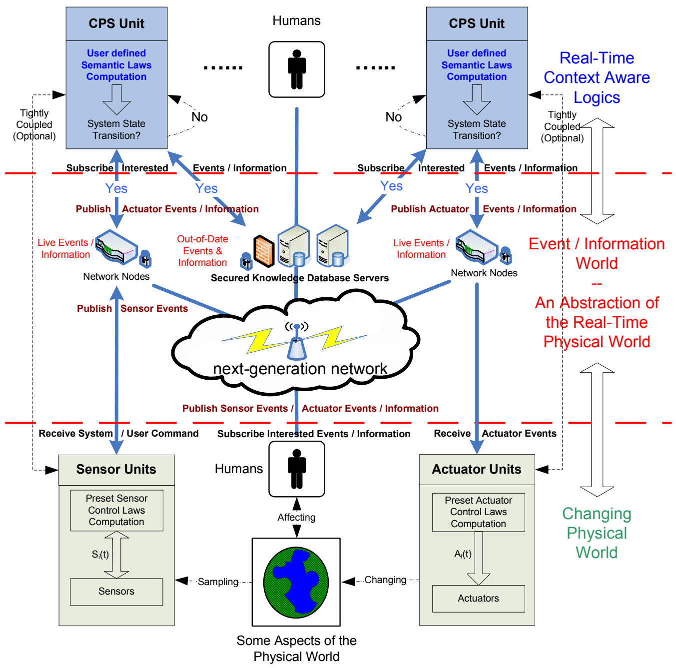

Figure 2. A Prototype Architecture of CPSs

ponent's output at any time point.

The third problem is a lack of public and private communication mechanisms for all system components to publish/subscribe event/information, which limits the scalability of the system.

In summary, fundamental gaps between today's technology and the needs of future CPSs require us to *reconsider today's system design in a fundamental way. This includes a unified abstraction of time, quantified confidence, and communication mechanisms at all system levels.*

3 CPS Definition and Architecture

Cyber-Physical Systems are a next-generation network-connected collection of loosely coupled distributed cyber systems and physical systems monitored/controlled by user defined semantic laws. Here, cyber systems are collections of control logic and sensor units, while physical systems are collections of actuator units. A prototype architecture of a CPS is shown in Figure 2. The highlights of this architecture include:

• Global Reference Time, which is provided by the next-generation network. This should be accepted by all system components, including humans, physical devices, and cyber logic in this architecture.

• Event/Information Driven. Just as human society is Event/Information Driven, future CPSs should also use a similar communication mechanism. Moreover, we differentiate between Events and Information. *Events* are either "raw facts" reported by sensor units/humans (called *Sensor Events*) or "actions" made by actuator units/humans (called *Actuator Events*). *Information* is the abstraction of the physical world made either by CPS control units or humans through event processing.

• Quantified Confidence. This design goal is archived by a Unified Event/Information model. Any event/information in this architecture should contain the following built-in properties. *Global reference time* – records the event/information occurrence/detected time. *Life-span* – specifies how long until that event/information's confidence level drops to zero. *Confidence and confidence fading equation* – specifies the event/information confidence level and how it fades over time. The confidence level and equation are decided by a particular device and control logic to provide a standard method for the subscriber to calculate the confidence of the subscribed event/information at any point in time. *Digital signature and authentication code* – specifies who published and who can access the event/information. *Trustworthiness* – specifies how much the subscriber trusts a particular publisher. *Dependability* – specifies the subscriber's dependence on event/information provided by a publisher in order to produce a particular outcome/information. *Criticalness* – specifies the critical urgency of each event/information so the subscriber can allocate its system resources based on different system design goals.

• Publish/Subscribe Scheme. Using this scheme, each CPS Control Unit acts like a human being in that it only subscribes to interesting events/information based on its system goal, and publishes event/information when necessary.

• Semantic Control Laws. Usually defined in an Event-Condition-Action like form, they form the core of each CPS control unit. With the abstraction of the real-time physical world shown in Figure 2, we can precisely control system behaviors related to the environment context according to user defined conditions/scenarios.

• New Networking Techniques. In addition to providing a global reference time, the next-generation network should also provide new event/information routing and data management schemes. Each network node should use a "publish-like" scheme for passing event/information to its neighbor nodes based on current confidence. Once the confidence of the event/information drops to zero (or below a certain threshold), the value of letting this event/information continue to "live" in the network is zero. The Secured Network Knowledge Database Servers only accept the data when it expires, and serves as a knowledge backup.

4 Conclusion and Future Work

This paper provides a definition for Cyber-Physical Systems, and proposes a prototype architecture. It argues that this definition and architecture not only meet all the currently identified CPS requirements and characteristics, but also unifies the current human-only computation model and machine-only computation model.

There are many open research challenges for this architecture. For example, how can a global reference time be provided in a large scale heterogenous system? How should the Publish/Subscribe scheme be formulated? How should the formalized Event/Information Model be specified? How is network routing achieved using Event/Information confidence (lifespan)? Knowledge data management and dispatching are other challenges, while security issues pose a challenge for any system.