Computer Communications 36 (2012) 1–7

Contents lists available at SciVerse ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Editorial

Cyber-physical systems: Milestones and research challenges

1. Introduction

In the past decade, we have witnessed an unparalleled success of information and communication technologies (ICT), which is expected to be even more proliferating and ubiquitous in the future. Among many ICT applications, ICT components embedded into various devices and systems have become a critical one. In fact, embedded systems with communication capability span virtually every aspect of our daily life.

An embedded system is defined as a computer system designed to perform dedicated specific functions, usually under real-time computing constraints. It is called "embedded" because it is embedded as a part of a complete device or system. By contrast, a general-purpose computer is designed to satisfy a wide range of user requirements. Embedded systems range from portable devices such as smart phones and MP3 players, to large installations like plant control systems.

Recently, the convergence of cyber and physical spaces [1] has further transformed traditional embedded systems into cyber-physical systems (CPS), which are characterized by tight integration and coordination between computation and physical processes by means of networking. In CPS, various embedded devices with computational components are networked to monitor, sense, and actuate physical elements in the real world.

Examples of CPS encompass a wide range of large-scale engineered systems such as avionics, healthcare, transportation, automation, and smart grid systems. In addition, the recent proliferation of smart phones and mobile Internet devices equipped with multiple sensors can be leveraged to enable mobile cyber-physical applications. In all of these systems, it is of critical importance to properly resolve the complex interactions between various computational and physical elements.

In this guest editorial, we first provide an overview of CPS by introducing major issues in CPS as well as recent research efforts and future opportunities for CPS. Then, we summarize the papers in the special section by clearly describing their main contributions on CPS research.

The remainder of the editorial is organized as follows: In Section 2, we provide an overview of CPS. We first explain the key characteristics of CPS compared to the traditional embedded systems. Then, we introduce the recent trend in CPS research with an emphasis on major research topics in CPS. We introduce recent CPS-related projects in Section 3. Summary of the papers in the special section follows in Section 4 by focusing on their contributions on CPS research. Finally, our conclusion follows in Section 5.

2. Overview of CPS

The term of cyber-physical systems (CPS) has emerged as a promising research paradigm, which is the confluence of control, communication, and computation [2–13]. Though it is somewhat difficult to provide an exact definition due to its broadness, CPS can be generally characterized as "physical and engineered systems whose operations are monitored, controlled, coordinated, and integrated by a computing and communication core" [6]. More specifically, the importance of interaction between physical and cyber elements in CPS is emphasized as follows [9]:

> CPS is an integration of computation with physical processes. Embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa. As an intellectual challenge, *CPS is about the intersection, not the union, of the physical and the cyber*. It is not sufficient to separately understand the physical components and the computational components. We must instead understand their interaction.

In summary, unlike traditional embedded systems that primarily focus on computing elements, CPS mainly take into account the interaction between the physical elements in the real world and the computing elements in the cyber space. Therefore, a key element in CPS is an ICT component as a communication medium, which connects the computing and physical elements by information exchange. Examples of CPS encompass a broad range of complex man-made systems such as avionics, transportation, factory automation, electronic healthcare, and smart grid systems.

CPS are expected to exceed the traditional embedded systems in various aspects such as efficiency, safety, reliability, robustness, adaptability, and a lot more. In other words, CPS promise systems that can respond more quickly, more precisely, more reliably, and more efficiently. For example, by a quick response, we can possibly avoid fatal car accidents. With a better precision, we can have better robotic surgery. We can further have so-called zero net energy buildings with improved efficiency, just to name a few. Consequently, research on CPS will significantly improve the fundamental performance of almost every engineered systems, and eventually the quality of our daily life. Some key characteristics of CPS can be summarized as follows:

1. System of systems: Unlike individual embedded systems, CPS is typically referred to as a complex system, which consists of many subsystems that can stand alone in an individual manner.

0140-3664/$ - see front matter
http://dx.doi.org/10.1016/j.comcom.2012.09.006

Consequently, due to the complex interactions among subsystems, the overall complexity of CPS is extremely higher than that of typical embedded systems.
2. Novel interactions among control, communication, and computation: CPS need to be highly automated, and every control loop in the system should close at any scale. Therefore, the non-technical human factor in the control loop should be removed as much as possible in order to expedite autonomous operation. Consequently, the computing element as a controller, the physical system, and the communication and network element as a medium should be considered at the same time in the system design.
3. Application-driven cyber and physical coupling: By carefully incorporating the key characteristics of each application domain, the computing element in the cyber world should be tightly coupled with the physical systems in the real world. To this end, large scale wired and wireless networking becomes critical at multiple and extreme scales.

In the US, the President's Council of Advisors on Science and Technology (PCAST) has recommended CPS as a top priority for federal research investments [3]. As a result, the CPS program was initiated at the National Science Foundation (NSF) with a funding level around 30 M USD per year in 2009. The NSF CPS program focuses on grand challenges in a number of sectors including automotive, energy, healthcare, aerospace, transportation, civil infrastructure, and manufacturing. Some examples of grand challenges are as follows [5,6]:

1. Blackout-free electricity generation and distribution;
2. Zero net energy buildings and cities;
3. Safe and rapid evacuation in response to disasters;
4. Perpetual assistance to busy, older, and disabled people;
5. Extreme-yield agriculture;
6. Location-independent access to world-class healthcare service;
7. Near-zero automotive traffic fatalities and significantly reduced traffic congestion;
8. Significant reduction of testing and integration time and costs of complex CPS systems, such as in avionics.

By abstracting these application domains, the NSF CPS program aims to identify cross-cutting fundamental scientific and engineering principles that support the integration of cyber and physical elements across all the application sectors.

Furthermore, the NSF CPS program also supports the development of methods and tools, hardware and software components, run-time substrates in order to expedite the realization of CPS in a wide range of application domains. The program further implements the CPS Virtual Organization (http://www.cps-vo.org/) in order to build up a research and education community committed to the study and application of CPS innovations.

In addition to the NSF CPS program, there have been various workshops and conferences on CPS from the research community during the past few years. Most prominently, in 2010, the ACM and the IEEE have jointly launched the first International Conference on Cyber-Physical Systems (ICCPS), which was very successful with an impressive number of submitted papers. A summary of CPS events in presented in Fig. 1.

So far, most of these initial research efforts on CPS have been made by the real-time and embedded system community. For example, the ICCPS was co-sponsored by the ACM Special Interest Group on Embedded Systems (SIGBED) and the IEEE Technical Committee on Real-Time Systems (TCRTS). As mentioned above, since one salient feature of CPS is the tight integration between the cyber and physical components, it is obvious that networking plays a key role in coordination between cyber and physical elements of CPS. Consequently, CPS research is awaiting significant inputs from the communication and networking community.

2.1. CPS research challenges

In this section, we discuss several CPS research challenges.

1. *Real-time system abstraction.* Because of the tremendous number of sensors and actuators as well as computers with information exchange of various types of data, it is of critical importance to develop a new framework that can enables us to abstract the salient features of systems in real time. For example, the network topology of CPS may dynamically change due to physical environments. Consequently, there is a need for research on novel distributed real-time computing and communication mechanisms that can properly reflect the key interaction among elements in CPS and eventually provide the required level of performance such as safety, security, robustness, and reliability.
2. *Robustness, safety, and security.* Unlike logical computation in the cyber systems, the interaction with physical world inevitably exhibits a certain level of uncertainty due to problems such as randomness in the environment, errors in physical devices, and possible security attacks. Hence, it is critical to ensure overall system robustness, security, and safety in CPS. To this end, the intrinsic nature of CPS can be leveraged by exploiting the physical information on location and timing of the system.
3. *Hybrid system modeling and control.* The fundamental difference between physical and cyber is that the former evolves in continuous real time while the latter changes according to discrete logic. As a result, a careful hybrid system modeling and control mechanism is needed for CPS design, which incorporates both the physical and cyber elements. For example, a new theoretical framework is needed that can merge continuous-time systems with event-triggered logical systems for closing the feedback control loop. In this framework, both the various time scales (from micro-seconds to months or years) and dimensional orders (from on-chip level to possibly planetary scale) should be carefully addressed.
4. *Control over networks.* The design and implementation of networked control in CPS pose several challenges with respect to issues such as time-driven and event-driven computation, time-varying delays, transmission failures, and reconfiguration of the system [14,15]. In particular, design of network protocols in CPS research has the following challenges: guarantee of mission-critical quality-of-service over wireless networks, tradeoff between control law design and real-time computation constraints, bridging the gap between continuous and discrete time systems, and reliability and robustness of large-scale systems.
5. *Sensor-actuator networks.* Wireless sensor networks have been extensively studied for more than a decade. Nevertheless, wireless sensor-actuator networks (WSAN) [16] is an emerging area that has not been properly investigated, especially from the CPS perspective. The interaction among the sensors, actuators, physical systems, and the computing elements should be carefully incorporated into the design of sensor-actuator networks. In particular, the physical details and effects of actuators on the overall system have not been fully considered in the system design so far.
6. *Verification and validation.* From the perspective of verification and validation of the system, hardware and software components, operating systems, and middleware are required to go through complete compositional verification and testing to guarantee the overall CPS requirements. In particular, CPS need to go beyond existing cyber infrastructure in terms of its trustworthiness. As an example, in the aviation industry, it is known

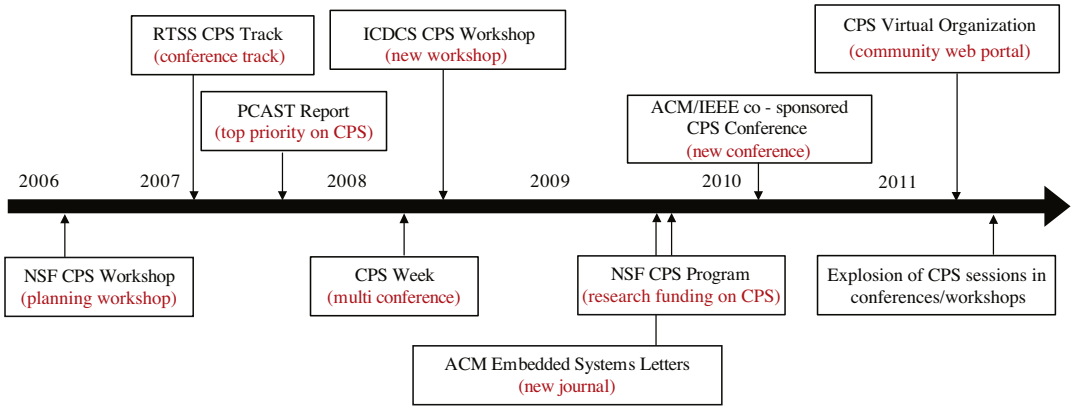

Fig. 1. CPS timeline.

that the certification process consumes more than a half of the resources to develop new systems. In this domain, overdesign is the best known methodology in order to develop safe system certification. However, with the today's large-scale complex systems, it is becoming intractable to simply apply the overdesign approach. As a consequence, we need new models, algorithms, and tools that can incorporate compositional verification and validation of software as well as other elements at the design stage.

7. *Control and scheduling co-design.* Control and scheduling co-design is in fact a well-studied area in the real-time and embedded systems community. However, with the advent of CPS, co-design issues are reconsidered in various aspects. For example, since CPS are typically networked control systems, the effect of the network delay on system stability has recently been studied in terms of the tradeoff between stability and real-time schedulability [17]. The outcome of this research is a non-periodic control approach that can guarantee the overall system stability with the minimum usage of the computational resource.
8. *Computational abstraction.* Physical properties, such as the laws of physics and chemistry, safety, real-time and power constraints, resources, robustness, and security characteristics should be captured in a composable manner by programming abstractions.
9. *Architecture.* CPS architectures must be consistent at a meta-level and capture a variety of physical information. New network protocols must be designed for large-scale CPS. An innovative paradigm can be built around the notion of being "globally virtual, locally physical."

2.2. Major application domains of CPS

2.2.1. Healthcare

CPS research has opened new opportunities as well as challenges in healthcare such as intelligent operating rooms and hospitals, real-time image-guided surgery, and model-driven implementation of a patient-controlled analgesia infusion pump [18]. The key challenge in so-called medical CPS is to develop systems as well as control methodologies that are safe, secure, reliable in a certifiable manner. In particular, some trends in medical CPS, which act as opportunities and challenges at the same time, include: wireless connectivity in medical devices, seamless monitoring, patient modeling and simulation, physiological close-loop control, model-based design, security and safety, medical-device integration and interoperation, and verification, validation, and certification.

From the networking perspective, today's hospitals use numerous devices over wires for various medical applications such as patient monitoring, diagnosis, treatment, and medical alarms. In order to reduce the deployment cost and time for plugging in more medical devices, there is a surge of demand for replacing wires by wireless technologies. Furthermore, by introducing wireless connectivity in medical devices, we can overcome the shortcoming of standalone devices and significantly increase the connectivity of the medical systems. For example, a standalone medical telemetry system in a patient room is practically not very helpful unless medical personnel is present in the room. Hence, the connectivity of medical devices in healthcare facilities is crucial for the overall performance of the medical systems [19,20].

By introducing wireless technologies, we not only improve the connectivity of medical devices, but also enhance the system-level reliability. We expect that wireless technologies can significantly improve the safety of medical systems; current massive communication over wires in healthcare environments often results in the so-called "malignant spaghetti" (a crisscross of cables from various devices), which is a serious potential hazard for patient safety [21].

Since the reliability of the system is the top priority in medical CPS, the main trends are targeting how to increase the overall system reliability by introducing appropriate theories as well as technologies. We expect that the medical CPS approach can significantly change the medical and healthcare community by bringing in proper technologies, especially from the ICT community.

2.2.2. Automotive

Today's automotive systems are far from pure mechanical systems [22–24]. There are about 30 to 90 processors per car; most of the subsystems such as engine control, break system, airbag deployment system, windshield wiper, and door locks are operated in a networked manner. In addition, cars can communicate with each other either via the Internet, cellular networks, or even vehicle-to-vehicle networks. Under these circumstances, significantly advanced design approaches are needed to guarantee a specified level of safety, security, and reliability for complex software, as well as its interactions with automotive hardware and human drivers.

Automotive CPS is one of the most prevalent safety–critical applications that has a great impact on our daily life. Currently, in the US, car accidents account for about 42,000 fatalities per year and an estimated 18% of healthcare expenditures [23]. Current technologies for collision avoidance are passive, and heavily depend on driver's interaction. Consequently, the automation of

collision avoidance is of great interest. With advanced technologies for onboard sensing and in-vehicle computation, as well as with global positioning systems (GPS) and inter-vehicle information exchange, we expect to achieve the grand challenge of near-zero automotive traffic fatalities and significantly reduced traffic congestion.

To this end, one of the most difficult technical obstacles is how to assure that the implementation really matches all the key system requirements [23]; in order to ensure that all the major properties are properly maintained throughout the whole lifecycle of the automotive system, we need to develop appropriate metrics that can assess the safety, security, and reliability qualities of the implementation.

2.2.3. Smart power grid

Recently, research on smart power grid has gained tremendous interests [6,10]. Development of smart power grids has been of great public interest, which results in a high priority for policy makers. In particular, the significance of investment on smart grids are evident from the following facts [10]: (i) Electricity demand is expected to increase more than 75% by the year of 2030; (ii) the cost of generating 1 KWh is four times greater than the cost of saving 1 KWh.

The main goal in this line of research is to improve energy efficiency by introducing advanced technologies in the energy infrastructure. At the same time, it is also a top priority to protect the energy infrastructure from failure as well as outside attacks. For example, under certain unexpected situations, a failure in one location of the electric power grid can propagate across the grid, which leads to a cascading failure and wide-spread blackouts. In addition, it is an open research challenge how to coordinate the various resources of energy generation to meet the required demand.

The key objective is to design a robust power grid network by introducing real-time control in the composition of cyber and physical elements in the grid. In particular, the following aspects should be carefully considered [6]: (i) Power grid and their cyber control need to be modeled for correctness in a uniform way. Bridge theories may also be necessary to accommodate multiple models; (ii) resilience is required to maintain correctness in improperly coordinated control of cyber and physical elements; (iii) security policy, intrusion detection, and mitigation must counter possible outside attacks; (iv) the existing power grid infrastructure needs to transition to the advanced power network grid with required technologies.

2.2.4. Aerospace

CPS research has a significant impact on the design of aircrafts as well as on air traffic management with the aim to significantly improving aviation safety [25,26,10].

Some key research issues in aerospace CPS are as follows [10]: (i) New functionalities to achieve higher capacity, greater safety, and more efficiency as well as tradeoffs among their possibly conflicting goals; (ii) integrated flight deck systems, moving from displays and concepts for pilots to future autonomous systems; (iii) vehicle health monitoring and management; (iv) safety research relative to aircraft control systems.

One of the main challenges is design verification and validation of extremely complex flight systems. Since the complexity of flight systems is ever increasing, the cost to verification and validation also increases. The research on verification and validation of aviation flight-critical systems include how to provide methodologies for rigorous and systematic high-level validation of various system safety properties and requirements, in the all phases, ranging from initial design through implementation, maintenance, and modification; it is also highly required to understand tradeoffs between complexity and verification methods for supporting robustness and fault tolerance [10].

3. CPS-related projects

In this section, we present some projects that are representative of the recent progress in CPS in the following domains: aviation, smart grid, transportation, and healthcare.

ActionWebs [27]@the University of California-Berkeley – principal investigators include Claire Tomlin, Edward Lee, S. Shankar Sastry, David Culler, and Hamsa Balakrishnan. In order to provide efficient coordination among multiple decision makers, this research project aims to develop a theory, called "ActionWebs", which uses stochastic hybrid systems to identify the interaction between continuous dynamical physical models and discrete state machines. To show the advantages of ActionWebs, this project takes into account two application scenarios: i.e., Intelligent Buildings and Air Traffic Control.

A Network Architecture for Localized Electrical Energy Reduction, Generation and Sharing (LoCal) [28]@the University of California-Berkeley – principal investigators include Randy Katz, Seth Sanders, David Culler, and Eric Brewer. The objective of this research is to explore and exploit the pervasive information to optimize energy production, distribution and use. With the aid of a cyber overlay on the energy distribution system, this project can construct a scalable and flexible electric infrastructure to significantly decrease the usage of energy and offer energy-aware management.

Autonomous Transportation Systems [29–31]@CMU – principal investigators include Raj Rajkumar, David Wettergreen, John Dolan, Paul Rybski, and Christopher Urmson. Automotive accidents often lead to many fatalities and injuries together with severe costs. In order to address this problem and facilitate autonomous driven cars, this research aims to develop and implement a comprehensive set of CPS techniques. CPS can control autonomous vehicles, providing the best possible routes and alleviating driving chores from humans, thus significantly reducing accidents, deaths and injuries.

Center for Energy Efficient Electronics Science (Center for E3S) [32] – principal investigators include Eli Yablonovitch, Jeff Bokor, Constance Chang-Hasnain, Tsu-Jae King, and Ming Wu. Since the underlying physics, chemistry, and materials science construct the foundation of information processing technologies, this project addresses the fundamental physical limits and implementation of electronic devices and systems, investigated by an interdisciplinary team of scientists from UC Berkeley, MIT and Stanford University.

Architecture and Distributed Management for Reliable Megascale Smart Grids [33]@the University of Illinois at Urbana-Champaign and Arizona State University – principal investigators include P.R. Kumar, Shobha Vasudevan, Junshan Zhang, and Vijay Vittal. This projet aims to build a framework for smart grids in order to support penetration of renewable distributed energy resources and provide flexible deployments of plug-and-play applications. By using networked sensing, control and verification schemes, distributed computation tasks can be executed in multiple levels, such as component, system and application. The grid hence becomes an adaptive optimizer to efficiently handle system-wide problems. The proposed framework can allow intelligent control, communication, and computation mechanisms to be configured into real-world physical systems.

Assuring the Safety, Security and Reliability of Medical Device Cyber Physical Systems [18]@the University of Pennsylvania – principal investigators include Insup Lee, Oleg Sokolsky, Rajeev Alur, George Pappas, and Clarence Hanson. This project aims to offer effective design, implementation and certification for medical

CPS devices. By using new design and certification techniques, patient safety can be improved. The overall costs of health care can be reduced by enabling closed-loop scenarios into clinical practice.

Networked Sensor Swarm of Underwater Drifters [34]@the University of California-San Diego – principal investigators include Jules Jaffe and Peter Franks, and Curt Schurgers, Thomas Bewley, and Ryan Kastner. By using networked, sensor-equipped underwater drifters, this project aims to establish a coastal observing system to allow dense and 4D spatio-temporal sensing. Many autonomous buoyancy controlled drifters are deployed to sample the data from real-world applications and further support the analysis of scientific and environmental questions.

Addressing Design and Human Factors Challenges in Cyber Transportation Systems [35]@SUNY at Buffalo – principal investigators include Chunming Qiao, Adel Sadek, Kevin Hulme, and Changxu Wu. The objectives of this project are twofold. One is to evaluate cyber transportation systems (CTS) applications when considering traffic safety and related operations. The other is to develop a simulator that integrates traffic-driven networks. In order to reduce the response time and the workload from drivers, and avoid conflicting warnings and false alarms, this project designs new algorithms and protocols that take into account the techniques of prioritization, delivery and fusion, thus significantly improving the safety and efficiency in the transportation systems.

4. Papers in the special section

The first paper of the special section, entitled "A Comprehensive Co-Simulation Platform for Cyber-Physical Systems," builds a simulation tool for CPS, which is crucial for modeling and analyzing various CPS applications. CPS feature the tight integration and coordination between the computational and physical components. The physical world is not entirely predictable. CPS will not be operating in a fully-controlled environment and must be robust to unexpected conditions. To evaluate and improve the technologies and designs, it is crucial to develop co-simulation platforms that can capture both the cyber and physical dynamics.

The main obstacles for developing such a co-simulation platform is how to synchronize the cyber and physical simulators. The proposed architecture in the paper significantly differs from the traditional approaches that either solely extend physical simulators or network simulators in that it merges the existing physical simulator, Modelica, with the widely used network simulator, ns-2 in a very effective manner.

The authors present a solid and effective method for synchronizing Modelica and ns-2. In particular, by considering the non-deterministic nature of the networks such as packet drops and transmission delays, the proposed platform allows ns-2 to dominate time synchronization and communication between the two simulators. The key idea for time synchronization is to pause ns-2 while Modelica is progressing, when there is no ns-2 event and Modeilca does not have any event requiring communication with ns-2. In addition, for communication, messages are divided into two groups, i.e., read and write, and each corresponding ports are opened for message transmission. Since the two simulators are loosely coupled with each other, it is simple to update the component in each simulator without interrupting the other. The authors further validate the proposed co-simulation platform by several convincing examples.

The second paper, "Dependable and Secure Computing in Medical Information Systems," proposes an attribute-based secure data sharing scheme for dependable and secure medical information systems, which is one of the main research domains in CPS, i.e., medical CPS applications. In medical environments, accessing patient data must be monitored, controlled, and granted only to the authorized users. Many medical applications require increased protection of private and confidential patient data including access control methods that are cryptographically enforced.

In this paper, the proposed scheme realizes reliable communications between medical devices by exploiting the storage node managed by the device controller. In addition, a general framework of the escrow-free key issuing protocol is proposed. Contrasting with previous schemes, the proposed protocol requires the key authority and the device controller to generate different private key components of a user by performing secure two-party computation (2PC) protocol between them. The 2PC protocol prevents them from obtaining any master secret information of each other so that any of them can by no means generate the whole private keys of users alone.

Thus, patient privacy is preserved by resolving the key escrow problem such that any curious device controller or key authority cannot decrypt the private medical data. Since the access control policy can be defined over a set of attributes using any monotone access structure, fine-grained data access control is also achieved. Additionally, the proposed scheme enables the medical devices to delegate most laborious tasks of decryption to the device controller without leaking any confidential information to it. Therefore, the computation and storage overhead at each medical device are greatly reduced in the proposed scheme.

The third paper of this special section, entitled "A Holistic Approach to Decentralized Structural Damage Localization Using Wireless Sensor Networks," deals with structural health monitoring (SHM) technologies that are crucial for monitoring the condition of various types of civil structures. With the ability to gain real-time and pertinent information about the condition of a civil structure, SHM technologies have the revolutionary potential to improve public safety while decreasing the cost associated with maintenance and repair. Different types of sensors can be utilized in SHM including tarmac temperature, wind sensors, strain gauge, accelerometer, and vibration sensors, etc.

Based on the sensing modality, damage detection and localization techniques have been developed in the civil engineering community. One such method is the Damage Localization Assurance Criterion (DLAC) algorithm, where structural modes are identified using vibration data sensed by each sensor represented in the frequency domain. The resulting mode vector is then correlated with simulated data with hypothetical damages for localization. Though DLAC is an established algorithm, employing it in distributed sensor networks is non-trivial. A significant gap exists between the design considerations in network and system performance – memory footprint, power consumption, latency, computation complexity and scalability, and application requirements in SHM – accuracy and agility.

The paper bridges such a gap by adopting a holistic approach to SHM that integrates a decentralized computing architecture with the DLAC algorithm. The optimal partition between the tasks to be carried out in-network and at a central location is carefully determined and evaluated using a measurement-driven approach using real-world structures and iMote2 sensors. The work gives an excellent example of cross-disciplinary research, which is at the heart of CPS, and demonstrates how domain-specific knowledge can be incorporated in network and system design in addressing practical problems.

The fourth paper, entitled "Real-Time Personal Protective Equipment Monitoring System," proposes a system for personal protective equipment (PPE) monitoring that can be critical in CPS application domains such as the construction industry. The proposed approach can significantly increase the safety of workers in the physical world by adopting appropriate sensors and software technologies in the cyber space.

In the construction industry, even though the use of PPE is critical for the safety of the workers, PPE is usually not worn properly in many cases and the only possible control for PPE is a visual inspection. In the proposed architecture, based on ZigBee and RFID technologies, a microcontroller-based device detects the presence of PPE and reports to a central station so that alerts and historical data can be generated.

In a nutshell, the proposed system introduces a monitoring system that describes the hardware and software components. By using a prototype, the authors also empirically study the limitation of the system in terms of the coverage and power consumption, which are important factors in practice.

The fifth paper, entitled "Implementing Home Energy Management System with UPnP and Mobile Applications," presents a home energy management system (HEMS) in order to realize full automation combining computational and physical systems in a home area by excluding operator-based control and management. In this manner, the overall performance as well as efficiency of the system can be greatly improved.

As an important application domain of CPS, the power grid is undergoing modernization through integrating information and communication technologies with the power system and also installing new electricity system technologies. Distributed control in a certain self-reliant power-service area is a critical means to modernize the power system to be the so-called smart grid. Since the self-reliant area is assumed to perform physical and expert-engineered operations that should be integrated, monitored, and controlled by a computational cyber system, the area is the place where the cyber and physical systems interact together, and home in the smart grid is a salient example.

The proposed system is designed to be built on the universal plug-and-play architecture; it can be accessed remotely over the Internet via mobile applications on smart phones. Based on the architecture, the authors implement the HEMS and construct a testbed that consists of networked personal computers, home appliances, and portable wireless devices. Furthermore, with the testbed, they verify the monitoring and controlling functions of the HEMS. In addition, the authors also perform extensive simulation with the measured data of power consumption and the collected data of power price in order to demonstrate the effectiveness of the proposed HEMS.

5. Conclusion

We expect that CPS will provide a fertile ground for research in the next generation of wireless networking. So far, we have seen the recent efforts and future opportunities in CPS research. In particular, wireless networking plays a key role in the holistic design of CPS.

One of the main challenges in CPS research is to tightly integrate the three research domains, i.e., control, communication, and computation, in order to develop a holistic approach to the design of CPS. In most existing research, among the three research domains, usually only two of them are coupled, namely, control and real-time scheduling co-design for confluence of control and computation, control over networks for integration of communication and control, and sensor and actuator networks for coordination between communication and computation.

In CPS research, it is highly required that the three areas of control, communication, and computation are tightly merged into a unified framework by carefully considering the complex interactions among all the physical and cyber parts in the system. We believe that this special section will be a meaningful step towards this end.

Acknowledgements

This work was supported in part by the Basic Science Research Program through the National Research Foundation (NRF) of Korea funded by the Ministry of Education, Science and Technology (2010-0022076), and in part by the DGIST R&D Program of the Ministry of Education, Science and Technology of Korea (12-BD-0404).

References

[1] M. Conti, S.K. Das, C. Bisdikian, M. Kumar, L.M. Ni, A. Passarella, G. Roussos, G. Troster, G. Tsudik, F. Zambonelli, Looking ahead in pervasive computing: challenges and opportunities in the era of cyber-physical convergence, Pervasive and Mobile Computing 8 (2012) 2–21.
[2] E.A. Lee, Cyber-physical systems – are computing foundations adequate?, in: Proceedings NSF Workshop on Cyber-Physical Systems, Austin, TX, USA.
[3] Leadership Under Challenge:Information Technology R&D in a Competitive World, President's Council of Advisors on Science and Technology, pp. 31–43.
[4] E.A. Lee, Cyber physical systems: design challenges, in: Proceedings of IEEE International Symposium on Object-Oriented Real-Time Distributed Computing (ISORC), Orlando, FL, USA.
[5] L. Sha, S. Gopalakrishnan, X. Liu, Q. Wang, Cyber-physical systems: A new frontier, in: Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, Taichung, Taiwan, 2008.
[6] R.R. Rajkumar, I. Lee, L. Sha, J. Stankovic, Cyber-physical systems: the next computing revolution, in: Proceedings ACM Design Automation Conference, 2010 Anaheim, California, USA, pp. 731–736.
[7] R. Poovendran, Cyber-physical systems: close encounters between two parallel worlds, Proceedings of the IEEE 98 (2010) 1363–1366.
[8] P. Derler, E.A. Lee, A.L. Sangiovanni-Vincentelli, Addressing Modeling Challenges in Cyber-Physical Systems, Technical Report UCB/EECS-2011-17, University of California at Berkeley, 2011.
[9] E.A. Lee, S.A. Seshia, Introduction to embedded systems – a cyber-physical systems approach, LeeSeshia.org, 2011.
[10] R. Baheti, H. Gill, Cyber-Physical Systems, in: T. Samad, A. Annaswamy (Eds.), The Impact of Control Technology, IEEE Control Systems Society, 2011.
[11] K.-D. Kim, P.R. Kumar, Prolog to the section on cyber-physical systems, Proceedings of the IEEE: Centennial Issue 100 (2012) 1285–1286.
[12] K.-D. Kim, P.R. Kumar, Cyber-physical systems: a perspective at the centennial, Proceedings of the IEEE: Centennial Issue 100 (2012) 1287–1308.
[13] R. Rajkumar, A cyber-physical future, Proceedings of the IEEE: Centennial Issue 100 (2012) 1309–1312.
[14] F.-Y. Wang, D. Liu (Eds.), Networked Control Systems, Springer, 2008.
[15] S.K. Mazumder (Ed.), Wireless Networking Based Control, Springer, 2010.
[16] Computer Communications, Special issue: wireless sensor and robot networks: Algorithms and experiments 35 (2012).
[17] S. Samii, P. Eles, Z. Peng, P. Tabuada, A. Cervin, Dynamic scheduling and control-quality optimization of self-triggered control applications, in: Proceedings of the 31st IEEE, Real-Time Systems Symposium (RTSS), 2010.
[18] I. Lee, O. Sokolsky, Medical cyber physical systems, in: Proceedings of Design Automation Conference, 2010.
[19] S.D. Baker, D.H. Hoglund, Medical-grade, mission-critical wireless networks, IEEE Engineering in Medicine and Biology Magazine 27 (2008) 86–95.
[20] IEEE Wireless Communications, Special Topics on Wireless Technologies for e-Healthcare, 2010.
[21] Malignant Spaghetti: A Symposium on Wireless Technologies in Hospital Health Care, 2008.
[22] A. Tiwari, Analysis challenges for automotive CPS, in: Proceedings of National Workshop on High Confidence Automotive Cyber-Physical Systems, 2008.
[23] N. Neogi, Safety and reliability in automotive cyber-physical systems, in: Proc. National Workshop on High Confidence Automotive Cyber-Physical Systems, 2008.
[24] T. Carpenter, Automotive CPS Trust, in: Proceedings of National Workshop on High Confidence Automotive Cyber-Physical Systems, 2008.
[25] S. Lintelman, K. Sampigethaya, M. Li, R. Poovendran, R. Robinson, High assurance aerospace CPS and implications for automotive industry, in: Proceedings National Workshop on High Confidence Automotive Cyber-Physical Systems, 2008.
[26] K. Sampigethaya, R. Poovendran, L. Bushnell, Secure operation, control, and maintenance of future e-enabled airplanes, Proceedings of the IEEE 96 (2008) 1992–12007.
[27] Action webs, 2012. <http://chess.eecs.berkeley.edu/actionwebs/>
[28] A network architecture for localized electrical energy reduction, generation and sharing, 2012. <http://local.cs.berkeley.edu/wiki/index.php/MainPage>
[29] S.R. Azimi, G. Bhatia, R. Rajkumar, P. Mudalige, Vehicular networks for collision avoidance at intersections, in: Proceedings of SAE 2011 World Congress, 2011.
[30] K. Lakshmanan, G. Bhatia, R. Rajkumar, Autosar extensions for predictable task synchronization in multi-core ECUs, in: Proceedings SAE 2011 World Congress, 2011.
[31] J. Kim, G. Bhatia, R. Rajkumar, M. Jochim, An autosar-compliant automotive platform for meeting reliability and timing constraints, in: Proceedings SAE 2011 World Congress, 2011.

[32] Center for energy efficient electronics science, 2012. <http://www.e3s-center.org/>
[33] M. He, S. Murugesanm, J. Zhang, Multiple timescale dispatch and scheduling for stochastic reliability in smart grids with wind generation integration, in: Proc. IEEE INFOCOM, 2011.
[34] Networked sensor swarm of underwater drifters, 2012. <http://maeweb.ucsd.edu/node/98>
[35] Addressing design and human factors challenges in cyber transportation systems, 2012. <http://www.cse.buffalo.edu/CTS/>

Kyung-Joon Park
Department of Information and Communication Engineering, DGIST, Daegu, South Korea
E-mail address: kjp@dgist.ac.kr

Rong Zheng
Department of Computer Science, University of Houston, TX, USA
E-mail address: rzheng@cs.uh.edu

Xue Liu
School of Computer Science, McGill University, Montreal, Canada
E-mail address: xueliu@cs.mcgill.ca

Available online 17 September 2012