Chapter 2

Cyber-physical systems: basics and fundamentals

Syed Hassan Ahmed[1], Safdar Hussain Bouk[2], Dongkyun Kim[3] and Mahasweta Sarkar[4]

Abstract

In the first decade of the 21st century, the cyber world and the physical world were considered as two different entities. However, in the literature we can easily find that these two entities are closely correlated with each other after integration of sensor and actuators in the cyber systems. Cyber systems became responsive to the physical world by enabling real-time control emanating from conventional embedded systems, thus giving birth to a new research paradigm named the cyber-physical system (CPS). In this chapter, we investigate the major challenges in integrating the cyber world with the physical world and its applications, followed by the basics and fundamentals of CPS. In addition, we discuss the CPS requirements for building its architectures, which should contain several modules supporting the CPS. The motivation of this chapter is to provide an overview of the CPS and the prerequisite knowledge for modeling and simulations.

2.1 Introduction

Computer systems provide a way of working, organizing or performing one or many tasks according to a fixed set of rules, program or plan. In other words, the main objective of computer(s) and the software(s) operating on them is to process information to perform better decisions. Apart from information processing, computing devices have also paved the way forward in various other systems, ranging from

[1]School of Computer Science and Engineering, Kyungpook National University, Daegu, Republic of Korea, e-mail: hassan@knu.ac.kr
[2]School of Computer Science and Engineering, Kyungpook National University, Daegu, Republic of Korea, e-mail: bouk@knu.ac.kr
[3]School of Computer Science and Engineering, Kyungpook National University, Daegu, Republic of Korea, e-mail: dongkyun@knu.ac.kr
[4]Department of Electrical and Computer Engineering, San Diego State University, California, USA, e-mail: msarkar2@mail.sdsu.edu

vehicles, manufacturing plants, cellphones, to home appliances. Following the emergence of computational capability, these systems became more interactive and intelligent. For example, vehicle breaks are applied if the vehicle comes into close proximity of another vehicle or object. Manufacturing plants work continuously without any human intervention and in the event of any fault in the production line, it will pause automatically. Home appliances, such as heating or cooling systems, react according to the home environment, the tenant's preferences and his/her presence in the home. This type of computing system is termed an embedded system and the software designed to run on that system is called embedded software.

An embedded system interacts with the physical process or environment and reacts accordingly. It is designed for dedicated application(s), a specific subsection of an application or product or part of a larger system. Successful applications include aircraft control systems, automotive electronics, home appliances, weapons systems, games, toys and so on. However, most of these embedded systems are closed 'boxes' that do not expose the computing capability to the outside. A simplified version of an embedded system is shown in Figure 2.1. The information about the physical environment is gathered by the system through sensors, either continuously or periodically. Sensed information is provided through the analog-to-digital (A/D) converters. The embedded software residing in the memory processes

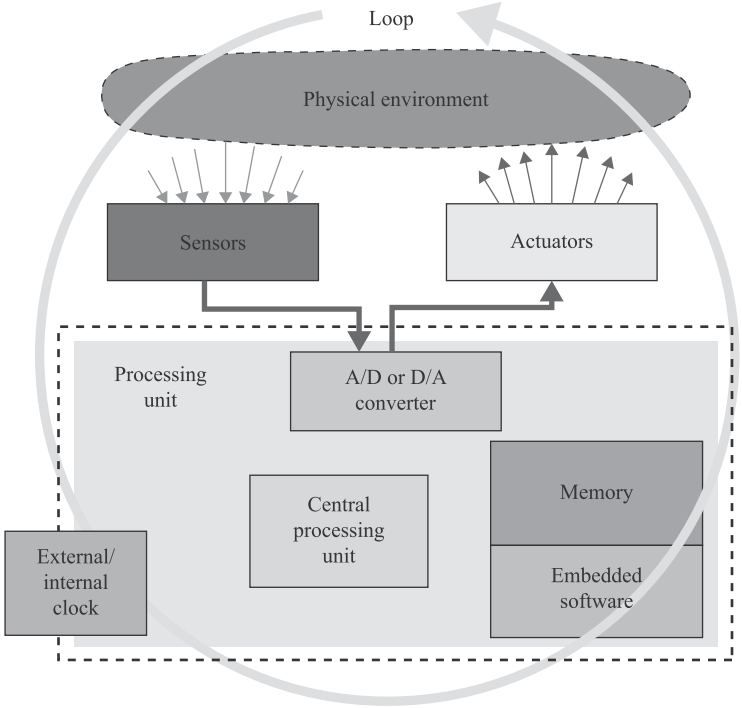

Figure 2.1 Embedded system

this information and sends instructions to the actuator circuit through the A/D converter. The actuators are mainly the electromechanical devices that perform actions to control the properties of the physical environment.

Initially, computing and embedded systems worked as standalone components. For example, embedded systems were largely an industrial problem and they used computing component(s) to enhance the performance or functionality of the system. In this earlier context, embedded software differed from other software only in its resource limitations (small memory, small data word sizes and relatively slow clocks). In this context, the 'embedded software problem' is an optimization problem.

Solutions rely on efficiency; engineers write software at a very low level (in assembly code or C), avoid operating systems with a rich suite of services and use specialized computer architectures such as programmable Digital Signal Processors (DSPs) and network processors that provide hardware support for common operations. These solutions have defined the practice of embedded software design and development for the past 30 years or so. In an analysis that remains as valid today as a couple of decades ago, Rajkumar *et al.* [1] lament the resulting misconceptions that real-time computing 'is equivalent to fast computing' or 'is performance engineering' (most embedded computing is real-time computing). But the resource limitations of 30 years ago are surely not resource limitations today. Indeed, the technical challenges have centered more on predictability and robustness than on efficiency.

The characteristics of an embedded system are outlined as follows.

The embedded system, either as a whole or subsystem, must exhibit the following characteristics:

1. The embedded system must be reactive to the physical environment. This can be achieved by continuously monitoring the environment and later on performing actions within the physical environment via sensors and actuators respectively.
2. The reaction of the system should be within the time constraints, which means that the embedded system must respond to the changes in physical environment within the dedicated time interval. Any late, but correct response from the system is considered as an incorrect response.
3. Along with the restiveness, the system should unveil maximum robustness with minimum resources (cost, energy, minimum code size, etc.).
4. The system should be safe, reliable, secure, extendable and available.

Soon, it was realized that there should be a mechanism so that these standalone systems can interact with each other and, consequently, the communication networks emerged. The communication system enabled all standalone systems to ubiquitously communicate information (such as digital data, text, video, audio) with each other through wires or wirelessly. The research community has intensively explored the networks in past decades due to their wide variety of applications. Enormous improvements have been made in both wired and wireless communication technology that lead us to the new communication paradigms such as ubiquitous and pervasive computing, wireless sensor networks (WSNs), underwater sensor networks (UWSNs) and machine-to-machine (M2M) communication systems. More recently,

embedded systems have dominated the computing market because of their usage trends, i.e. anytime, anywhere information access, wearable devices, intelligent appliances and buildings, the Internet of Things (IoT), etc.

The radical transformation that we envision today solely came from the networking of these devices. Such networking also posed considerable technical challenges. For example, a usual practice in embedded systems is that they rely on bench testing for concurrency and timing properties. This has worked reasonably well, because programs are small, and because software gets encased in a box with no outside connectivity that can alter the behavior. However, the applications that we envision today demand that embedded systems be feature-rich and networked, so bench testing and encasing become inadequate. In a networked environment, it becomes impossible to test the software under all possible conditions. Moreover, general-purpose networking techniques themselves make program behavior much more unpredictable. A major technical challenge is to achieve predictable timing in the face of such openness.

2.1.1 Cyber-physical system

The integration of networked computational devices with physical processes has found the new system paradigm called CPSs, as shown in Figure 2.2. It shows that the communication-enabled embedded systems monitor and control the physical processes and the computerized system is closely and seamlessly integrated with the dynamics of the physical processes. Put simply, the CPS provides connectivity between computer, network, control and physical systems. Therefore, the CPS is not merely a simple control system but a real-time, intelligent, predictive, adaptive, distributed and networked system with little human involvement [2]. As CPSs are

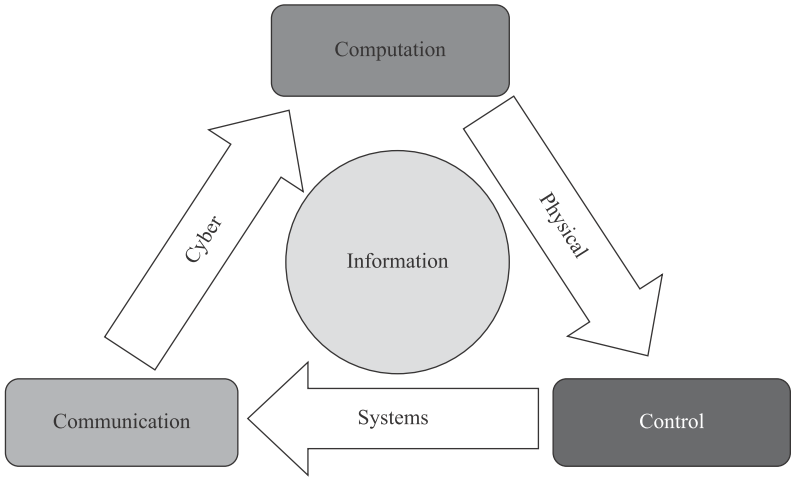

Figure 2.2 A general cyber-physical system

enabling the upcoming new networking model, industry and academic stakeholders are investing in the exploration of this future network.

As stated earlier, CPS seamlessly integrates physical processes with computation and communication and provides the abstractions, design, modeling and analysis techniques for the integrated whole [3]. Therefore, the networking and computation technologies in CPS need to embrace information and the physical dynamics as well. CPS as an integrated whole necessitates new design technologies because CPS merges multiple disciplines, such as computing science, control theories and communication engineering. In addition, software is embedded in devices, the principal mission of which is not computation alone. CPSs range from relatively small systems, such as aircrafts and automobiles, to large systems such a national power grid [4].

Before proceeding further, we need to discuss the behavior of the current networking techniques and the embedded systems. The most widely used networking techniques present today introduce a great deal of timing variability and random behavior. As we know that the embedded systems are real-time and often use specialized networking technologies (such as CAN bus in manufacturing systems and FlexRay in automotive applications), therefore as far as concurrency is concerned, the physical processes are intrinsically concurrent and their interaction with computing requires, at a minimum, concurrent composition of the computing with the physical processes. The current embedded systems must simultaneously react to multiple real-time streams from sensors and control multiple actuators. The interaction mechanism between sensors and actuator hardware is done by the notion of interrupts that lies in the area of the operating system. Unfortunately, the programming languages cannot achieve the concurrency because the interactions with the hardware are exposed to the programmers through abstraction of threads. It is stated in Tang *et al*. [5] that the threads are by nature problematic. The cyber-physical systems that are extensively networked will alleviate the concurrency problem because of their stochastic behavior. Hence, before realizing the future networks and CPS that are envisioned to be concurrent by nature, the following questions must be answered:

- What aspects of those networking technologies should or could be important in large-scale networks?
- Are they compatible with global networking? To be specific, recent advances in time synchronization across networks promise networked platforms that share a common notion of time to a known precision [6].
- How are distributed cyber-physical applications to be developed?
- What are the implications for security measures?
- Can we mitigate security risks created by the possibility of disrupting the shared notion of time?
- Can security techniques effectively exploit a shared notion of time to improve robustness?

Recently, it has been observed that CPS is basically the emergence of wireless networks (such as WSNs) and the IoTs. CPSs have gained much attention from many

vendors, researchers and manufacturers [7]. This emergence of multiple disciplines has accelerated the new series of applications and thus brings new challenges. Following this, in the recent past, some significant achievements have been made in the said emerging domains. Later on, those achievements endorse the expansion of CPS. However, it is also true that instead of a rapid development, we continuously face new challenges and implementation issues. Added to this are security issues, since emerging different domains compromise security, privacy and data integrity.

The main objective of research in the CPS domain is to tightly amalgamate the cyber and physical world in such a way that designing of computing, control and communication becomes possible. It is also true that CPS differs from traditional desktop computers, and similarly from conventional real-time/embedded systems, and therefore WSN; however, they do have some essential properties as listed below [8]:

- CPS expects to provide cyber capabilities to every component in the physical world that is supposed to be a resource constraint. We must understand that the software is a part of every embedded system and physical module, and so is counted as the system resource. But such software brings several challenges as well.
- CPS is an intensely integrated computation with physical processes.
- CPS is usually designed and networked at multiple and extremely wide scales. Therefore, it is considered as networks, which include both wired and wireless domains. Moreover, highly varied system scales and device category needs are supported by CPS.
- In CPS, the different components likely have unequal granularity of time and spatiality. CPSs are strictly constrained by spatiality and real-time capacity.
- Dynamically reorganizing/reconfiguring. CPSs, as very complicated and large-scale systems, must have adaptive capabilities.
- Closed-loop control and high degrees of automation. CPSs favor convenient man–machine interaction, and advanced feedback control technologies widely apply to these systems.
- The CPS operations must be dependable and certified in some cases. On the other hand, reliability and security are also necessary for CPSs because of their extreme scales and complexities.

2.2 CPS concept and requirements

In the literature, the term ‘CPS’ has recently been introduced where it leads toward the development of a modern and new vision for services to society. Those services may extend the dimensions of communications to a breakthrough performance level in the future. For instance, CPS is defined as an integration of physical processes with computation. Here it is worth mentioning that CPS is not about combining physical and cyber characteristics, but it is about their intersection. From the recent literature we can obtain a few definitions of CPS; for example, one complex

CPS definition was made by Shankar Sastry from the University of California, Berkeley, in 2008: 'A cyber-physical system (CPS) integrates computing, communication and storage capabilities with monitoring and/or control of entities in the physical world, and must do so dependably, safely, securely, efficiently and in real-time' [9]. It is quite clear that CPS is definitely not similar to the traditional or existing embedded systems, including real-time systems. More precisely, CPSs differ from the current wireless or wired sensor networks and so-called desktop applications, and they have certain properties that define them as cyber-physical integration, which are as follows:

1. Cyber/communication capabilities in every physical component available.
2. Networked at various multiple and huge scale.
3. Reconfiguring and reorganizing with respect to the dynamics of the environment.
4. The control loops must be close with high degrees of computation and automation.
5. The certified and dependable operations are key elements in some cases.
6. The physical and cyber components are integrated for initially learning and later on adaptation purposes.
7. CPSs are expected to provide high-performance, self-organized, auto-assembly operations.

As for other communication and information systems, CPSs are also distinguished by the following basic properties:

1. Operability/functionality
2. Performance metrics
3. Security and dependability
4. Cost effectiveness

Additional characteristics affecting the overall system security and dependability are not limited to CPS usability, its management and system adaptability. The main expected features of CPS are as follows:

1. CPS will support the input from the physical environment and then feed back to the physical environment in the presence of the secured channels for communication.
2. Furthermore, CPS will guarantee a combined management approach and distributed controlling mechanism.
3. CPS will also meet the real-time communication and performance requirements.
4. Different from current embedded systems, a wide geographical coverage without the physical security components will be supported by CPS.
5. Forthcoming technology, known as system of systems (SoS), will be as a result of CPS.

Due to the higher reliability and predictability standard, the existing embedded systems have always been considered more reliable than other generic computing systems. For example, customers do not expect their TV/other

electronic devices to crash and restart. People have started counting on secure and reliable vehicles, where the use of computer controllers has effectively improved both the reliability and increased efficiency of cars and so on. Indeed, if the improved reliability and predictability function is skipped, the CPS will not be able to perform as expected for various applications such as automotive safety, health care and traffic control. On the other hand, we must remember that the physical world is not completely predictable.

2.3 CPS architectures

To date there is no identified or standard concept of a CPS. However, in general, the CPS is referred to as the combination of the dynamic physical world and the cyber world. In the case of CPS, it makes a distinction between the physical and cyber world and processes the data by computers. Later on, that data effectively changes the physical world. From the literature, we can find some examples, such as He Jifeng who proposed the concepts of Computation, Communication and Control and named this 3C [33]. The main objective was to fuse computation, communications and controlling with 'information' at the center, thus achieving dynamic control, real-time sensing and information services in a large-scale system. CPS is closely related to embedded systems, wireless networks and ad-hoc sensor networks, but has its own characteristics or properties as well. Those properties include the dynamics and complexity of an environment that together bring a big space problem and demand a highly reliable system, i.e. CPS. Since CPS is in its early stages, few researchers have divided CPS into a simple two-tier structure, which inherits the physical part and computing part from the above-mentioned definitions. More specifically, the physical part includes sensors or receivers that sense the physical environment and collect data. Later on, the computing part executes the decision made by itself on behalf of the data collected by the physical part. Here it is worth mentioning that the computing part analyzes and processes the data from the physical part, and then makes a decision. We can collectively refer to it as a feedback control relation of the two parts. On the other hand, Hu *et al*. [10] proposed a three-tier architecture of CPS. This architecture consists of the Environmental Tier that is made up of various physical devices and a target environment with end users having the devices and being a part of their associated physical environment. The second tier, named the Service Tier, is composed of a classic computing environment with several services and cloud computing. Similarly, the Control Tier is designed to receive the monitored data, which are collected via sensors, to make further control decisions. Also, control tiers help the CPS to find the right services by a service-consulting framework and invoke the services on the physical devices (Figure 2.3).

It is expected that the architecture of a CPS will provide homogeneous treatment of the cyber and physical elements together. Likewise, a new architecture for software proves to be a good initiative; however, the concept should be extended to CPS by using new terminologies in vocabulary for physical and cyber-physical elements,

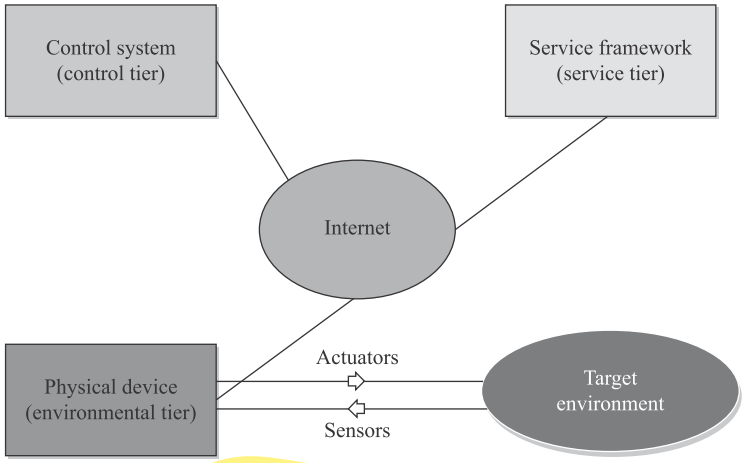

Figure 2.3 Tire-based architecture of cyber-physical systems

which are necessary to analyze the system behavior. To achieve this, one effort has been made in Hoang *et al*. [11], where the authors have proposed a prototype of the CPS concept, in which events or information of the cyber world are highlighted. In addition, also an abstraction of the real physical world ruled by semantic laws is illustrated which is evolving the current architecture of the embedded systems and aligning that abstract to the current CPS technology requirements. More precisely, we list the outcomes of the proposed architecture as follows:

1. The proposed architecture provides the Global Reference Time with the help of the next-generation networks that are expected by all the CPS components.
2. Remember that the events are 'raw data/facts' noted down or collected by a set of sensor nodes and so on. Similarly, some actuator modules or humans make the 'actions'. Here it is worth explaining that system control units or humans through event processing are the providers of information set for a CPS following the proposed architecture.
3. Quantified Confidence – a standard method to calculate the confidence of the events/information at any point in time.
4. The proposed work also enables a CPS control unit to subscribe for specific data and once the provider (i.e. sensors) collects that data it will transfer that data to the subscriber autonomously.
5. Any CPS architecture is expected to support the Semantic Control Laws, such as possessing the event–condition–action form, the precise laws defining the behaviors of a control system which are relative to the environment aligned with the user-defined scenarios or conditions.

Similarly, the paper entitled 'A software architecture for next-generation cyber-physical systems' by West and Parmar in 2006 [34] proposes to develop a CPS on their software architecture, which is in actual fact a collection of specific-application

services or domains. According to the authors, a CPS organizes itself with the more suitable methods of communication and continuously switches to an isolation mode between various services. Additionally, the proposed software architecture also considers the autonomous composition of different services to satisfy the given constraints of an application. Moreover, the proposed architecture also takes into account the underlined limitations of hardware and its heterogeneity in the generation from which the hardware belongs. Furthermore, the verification of a software system for a given application is also valued.

In the past decade, architectural evolution has shifted into systems integration, ensuring that SOA (Service Oriented Architecture) will have a major role to play in many branches of technology. SOA basically enables a rapid, low-cost composition of interoperable and scalable systems based on reusable services exposed by these systems. In Tan *et al*. [12], the authors proposed a simplified middleware CPS architecture, integrating with web services named 'WebMed', through which an interaction with physical devices becomes as easy as invoking a computation service. Emphasizing the basics of service-oriented guidelines, the authors built a loosely coupled infrastructure that exposes the functionality of physical devices to the web for application development. However, Sanislav *et al*. [13] addressed the architecture of a CPS to precisely provide a uniform treatment of cyber and physical elements. The software architecture provides a good starting point, but the concept should be extended to CPS by using a new vocabulary for physical and cyber-physical elements necessary to analyze the system behavior. Tan *et al*. [14] presented representative prototype architecture of the CPS concept. They highlighted the cyber world represented by events/information as an abstraction of the real physical world governed by semantic laws, evolving the typical architecture of the embedded systems and aligned it to current technological requirements. In Wan *et al*. [15], the authors analyzed the features of M2M, WSNs, CPS and IoT, and highlighted the correlations among them. Then, home M2M networks were reviewed. The authors gave a CPS scenario, called human-centric cyber-physical system (HCPS), which takes into account human activities to design and develop the CPS-based social system. This demonstrates how M2M systems with the capabilities of decision-making and autonomous control can be upgraded to CPS and sketches the important research proposals and challenges related to CPS designs.

Recently a new architecture has been designed to meet the basic requirements of future CPS systems and their applications [16]. This is depicted in Figure 2.4, where we have five main modules for CPS architecture. For data collection of the physical world through sensors, the main function of this module works for environmental awareness, which is achieved by preliminary data pre-processing. The data are provided to the data management module (DMM). The Sensing module supports multiple networks. It depends on the nature of networks that are deployed. For example, in a WSN, each sensor node is equipped with a sensing module for real-time sensing. Other network nodes can also operate with a part of this module in different scenarios. In the case of the vehicular cyber-physical system (VCPS), VANETS nodes (i.e. cars) can be equipped with a sensing

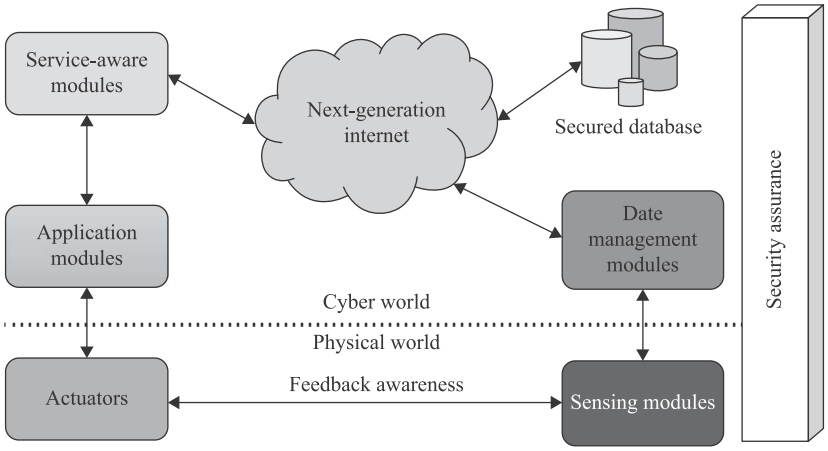

Figure 2.4 Recently proposed architecture of cyber-physical systems

module to sensor data from the physical world. In the case of HCPS, using BAN, sensors attached to patients are equipped with sensing module nodes to enable real-time control.

DMM consists of the computational devices and storage media. This provides heterogeneous data processing such as normalization, noise reduction, data storage and other similar functions. DMM is considered as the bridge between the dynamic environment and services as it is collecting the sensed data from sensors and forwards the data to service-aware modules (SAM) using next-generation internet (NGI).

A common feature of the emerging NGI is the ability for applications to select the path, or paths, that their packets take between the source and destination. This dynamic nature of internet service is required for designing CPSs. Unlike the current internet architecture where routing protocols find a single (the best) path between a source and destination, future internet routing protocols will need to present applications with a choice of paths. To achieve this, research is still ongoing to find quality of service (QoS) routing. While QoS routing provides applications with a path that best meets the application's needs, it does not scale to the size of the current internet, let alone the NGI. IPv6 and exploiting 802.16n and 802.21 are ongoing projects and expected to be included in NGI services trial. On the other hand, the SAM provides the typical functions of the whole system, including decision-making, task analysis, task schedule and so on. After receiving sensed data, this module recognizes and sends data to the services available.

In the Application Module, a number of services are deployed and interact with the NGI. Simultaneously, information is saved in a secure database for QoS support. The database is stored locally and simultaneously on cloud platforms in order to keep data safe. We can use a concept of NoSQL for saving data [17].

Although the NoSQL systems have a variety of different features, there are some common ones. First, many NoSQL systems manage data that is distributed across multiple sites. This saved data over the cloud system can be accessed from anywhere followed by authenticated access.

Actuators and the Sensing Modules are two different electronic devices which interact with the physical environment [18]; the actuator may be a physical device, a car, a lamp or a watering pump. It receives the commands from the Application Module, and executes. The security assurance part is inherently important in a whole system, from the access security, data security to device security. We divide CPS security into different requirements in different scenarios. For example, in terms of military applications, the confidentiality feature is more important, but in the smart home system or HCPS, the real-time requirements are more emphasized. Security of CPS can be divided into the following three phases: awareness security, which is to ensure the security and accuracy of the information collected from the physical environment; transport security, which is to prevent the data from being destroyed during the transmission processes; physical security, such as safety procedures in servers or workstations. Feedback Awareness is one of the advanced level services to minimize the data processing by communication between sensor and actuator for executing required actions directly.

So far, we have seen that CPS presents a set of advantages and advancements in the field of wireless communications and so on. It is also expected that CPS is a collection or combination of a secured and efficient systems. Those systems enable individual entities to work together in order to form various complex systems with a new set of applications and capabilities. As previously mentioned, cyber-physical technology may be applied in a wide range of domains, offering numerous opportunities such as critical infrastructure control, providing security and efficient transportation systems, alternative energy, environmental control, tele-presence, medical devices and integrated systems, telemedicine, assisted living, social networking and gaming, manufacturing, agriculture. Similarly, we have critical infrastructure, and assets that are essential for the functioning of a society and the economy for any region. Those assets include but are not limited to the facilities for water supply (storage, treatment, transport and distribution, waste water), generating or producing electricity, transmission and distribution of gas and its production, the supply of various oil products and the oil itself, and last but not the least telecommunication. With this economic impact in mind, Wan *et al*. [35] proposed some requirements of CPS that the authors believed every CPS should meet according to the business sectors in which they would be used. For example, we can consider CPS enabling intelligent automotive, environment monitoring/protection, aviation and defense, critical infrastructure, healthcare (see Table 2.1 later). In addition, the physical platforms and support for CPS must satisfy five essential capabilities: (a) computing, (b) communication, (c) precise control, (d) remote cooperation and (e) autonomy. Different from traditional embedded systems, CPSs interact directly with the physical world where they detect environmental changes; therefore, adaptation of system behavior must be considered as one of the key challenges in the design of CPS.

Table 2.1 CPS applications and requirements

Applications	CPS requirements
Vehicular CPS	Due to the complex algorithms for traffic control, for example the best route calculation in given traffic situations, the automotive industry requires more computing power for enabling CPS.
Environmental CPS	For monitoring the environment in a wide geographical area such as mountains, rivers and forests, the CPS system must avoid human physical intervention for prolonged durations, thus guaranteeing low energy consumption. For such a scenario, enabling low-powered ad-hoc networks to collect time-sensitive data using a precise and secured CPS is still an ongoing research issue.
Air CPS	An aviation and defense CPS requires highly secured and precise controlling with low power computing. Therefore, the designing and developing of security protocols is an ongoing research issue.
Smart grid CPS	Water resource management and energy control are the key requirements of smart grid CPSs. Furthermore, application software methodologies are still missing from the literature to guarantee QoS in current software.
Health CPS	Health care and medical equipment demand a complete new series of synthesis, analysis and hypothesis. In addition, emerging technologies are still needed for medical or health CPSs. Therefore, we are still lacking the design and development of such applications for inter-operable algorithms.

2.4 CPS applications

CPS can be used in a wide range of applications, including intelligent transportation, precision agriculture, health CPS, water and mine monitoring, aerospace and so on. Figure 2.5 illustrates the range of possible forthcoming applications to be supported by CPS.

2.4.1 CPS for vehicular environments

The rapid increase in the number of the vehicles on the roads brings several challenges, for example an increased volume of air pollution, traffic congestion, safety issues. Therefore, much effort is required to improve the driver's experience and road safety. It is expected that in the near future, roads will be significantly aided by the next-generation intelligent vehicle with the support of an Intelligent Transportation System (ITS), inter-vehicle sensing and advanced computing. Those technologies will be widely used in order to provide protected air traffic, a secured railway traveling experience and automatic car control for safety throughput.

Similarly, other applications for CPS include the VCPS, which is not a new concept. For instance, VCPS may refer to a wide range of transportation management systems that are highly integrated and should be highly accurate, real-time and efficient. Due to modern computing technologies such as electronic circuits,

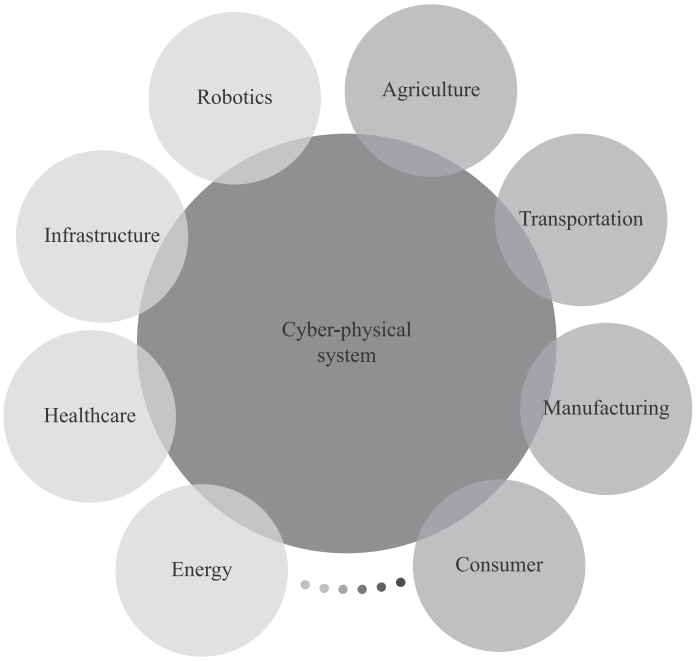

Figure 2.5 Applications of cyber-physical systems

sensors, computers and wireless networks, traditional transport modules are becoming more intelligent and effective. For that reason, the NAHSC (the National Automated Highway System Consortium) is studying and developing an independent high-speed system known as AHS (Automated Highway System), whose aim is to achieve more intelligent and secure traffic. Furthermore, one of the many American National Science Foundation (NSF) projects is CarTel, originally developed by MIT [19]. The main objective of the CarTel project is to combine sensing and mobile computing via wireless networking. To achieve this, data-intensive algorithms are under construction to be evaluated on servers located in the cloud to address challenges such as the VCPS. Moreover, the CarTel project supports applications designed for easy data collection, data processing, delivery, data analyzing and its visualization from sensors located on/in vehicle units. To date, the main contributions of the CarTel project include wireless traffic mitigation, monitoring the road surface and hazard detection to avoid accidents, vehicular ad-hoc networking and so on.

2.4.2 CPS for agriculture

During the first decade of the 21st century, a lot of attention has been given to the agricultural domain in order to improve crop reproduction and quality. In addition, human input has reduced and currently numerous experimental studies are

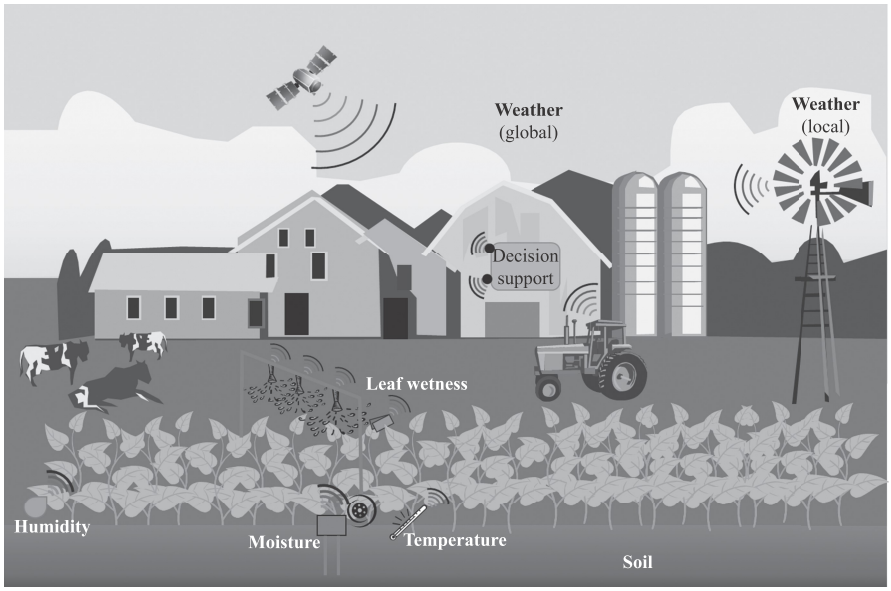

Figure 2.6 Agricultural CPS

illustrating the benefits of using WSNs in the agriculture sector. However, great accuracy in agriculture is demanded in order to meet the global demands of food consumption. As we know, the main goal of achieving accuracy in agriculture is to reduce wastage during the entire agricultural cycle and also to increase crop yield (i.e. from preparation of the crop field through to harvesting). In order to achieve this, we continuously evaluate the field crop with respect to macro- and micro-level weather and climate information. Also, we need to consider the effect of natural components in the soil, the fundamental geographic of farmland and so on, throughout the crop production cycle. See Figure 2.6 for a possible scenario of agricultural CPS.

One of the many efforts to bring CPS into the agriculture sector was undertaken by the University of Nebraska–Lincoln. Agnelo R. Silva and Mehmet C. Vuran, under the project entitled 'Underground Wireless Sensor Network', developed a novel CPS, where the integration of center pivot systems with wireless underground sensor networks was deployed and the main objective was to make a CPS for an accurate agriculture monitoring system [20]. This system was proposed by the Cyber-Physical Networking Lab where the wireless underground sensor networks (WUSNs) consisted of wirelessly connected underground sensor nodes. These nodes were capable of subsoil communications. Moreover, the experimental results illustrated that the concept of the CPS is possible and can be utilized to make a highly reliable agricultural CPS. This combination of CPS and precision agriculture is one of the typical applications of CPS, with good prospects.

2.4.3 CPS for health and medical sciences

Through embracing the potential of embedded network and software connectivity, a rapid transformation is under way in the medical industry. In the near future, distributed systems will control and monitor the multiple aspects of a patient's physiology; hence, the standalone systems designed, certified and used independently for different purposes for the treatment of patients will be replaced. The modern medical device systems, which combine embedded software controlled devices, networking capabilities and complex physical dynamics revealed by patient bodies, can be classified as a distinct class of CPSs termed medical cyber-physical systems (MCPSs).

MCPSs face numerous developmental challenges due to their increased size and complexity relative to conventional medical systems. However, new developments in design, verification, composition and validation techniques can address the challenges faced by MCPSs. These developments provide new opportunities for research into embedded systems, CPS and specifically MCPSs. In the case of MCPSs, new protocols need to be approved for their use in the treatment of patients. Furthermore, the conventional approval method used by the US Food and Drug Administration (FDA) – a process-based regulatory regime for the approval of medical devices – is not feasible as it is too lengthy and expensive for the increased complexity of MCPSs. Possible solutions to ease this process are presented here. In this chapter, we describe some of the research directions that we are taking toward addressing some of the challenges involved in building MCPSs. The ultimate goal is to develop foundations and techniques for building safe and effective MCPSs.

Overall, we advocate a systematic analysis and design of MCPS for handling its inherent complexity. Consequently, MCPS design is largely affected by model-based design techniques. These models should include the devices, the communication between them, and the relationship between these and the patients and caregivers. These models help the developers to build systems confidently, by accessing the system properties earlier in the development process prior to manufacturing. At the modeling level the analysis of system effectiveness and safety is further complemented by using generative implementing techniques, preserving the properties of the model in the implementation stage. The basis of evidence-based regulatory approval is formed through the results of model analysis and the guarantees of the generation process. MCPSs are safety-critical, interconnected, intelligent systems of medical devices. Conventional clinical scenarios are depicted as closed-loop systems controlled through the caregivers, with sensing achieved through medical devices and actuators and the plants being the patients. The introduction of MCPSs gives additional computational procedures to the caregivers, thus aiding in the controlling of the plant.

In Figure 2.7, a conceptual overview of the MCPS is shown. Two large groups of devices that are used in MCPSs can be categorized on the basis of their primary functions: monitoring devices, which provide the patient's physiologic state information, such as the oxygen-level monitors, heart rate and sensors; and delivery

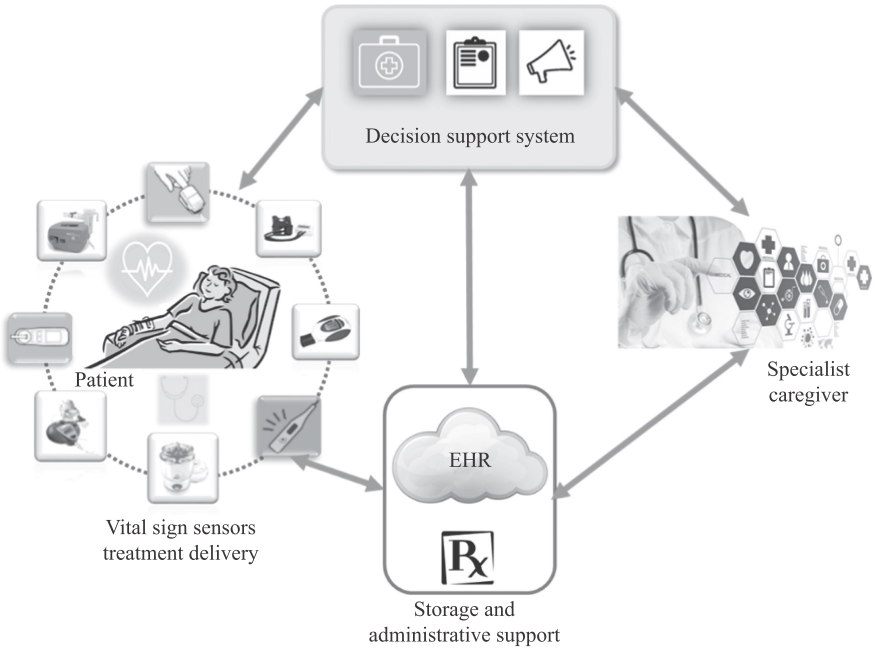

Figure 2.7 CPS for medical overview

devices, which target changing the patient's physiologic state through therapy, such as ventilators and infusion pumps. In MCPSs, the decision support or administrative support entities are directly fed the data collected through the monitoring devices, each of which serves a complementary and different purpose.

When we look at a medical set-up in a hospital, we come across different administrative units, including electronic health records (EHRs) and various pharmacies. The main objective of any medical care unit is to manage patients' health and treatment information which is collected periodically. Assuming the access of those medical units to provide the very best outcome from personalized information, they do have the potential to provide better combined treatment actuation based on a more comprehensive view of the particular patient's health, such as considering potential drug interactions or by considering the long-term progress of a patient's physiological limit. In such cases, those medical units can assist in fulfilling the demand for the continuous care of any specific patient. The periodic data collection and its management is important for today's health challenges and issues such as dealing with the older population and the rapid rise in the number of people with chronic symptoms such as diabetes and asthma. Therefore, decision-making entities can process the collected data and can generate alarms for various situations that may require medical attention. Such alarms are essential to let clinicians know when the patient's state has deteriorated and what information is relevant to treat them properly. Thus, we can say that it is a present-day necessity to

develop a smart alarm system that will go beyond current state-of-the-art time-based methodologies and provide more accurate and targeted alarms, along with related information. Medical caregivers can then analyze the information provided and use it properly to deliver a clear message to devices to initiate any necessary treatment immediately. In this way, we bring the caregiver into the controlled loop around the patient. Alternatively, decision-making entities can utilize a smart controller that analyzes the received data from the monitoring modules and can estimate the state of the patient's condition, and it is expected that it may start the treatment autonomously. Those treatments may include drug infusion by releasing commands to drug delivery smart devices, thereby closing the controlled loop. However, building such MCPSs brings a significant number of challenges and issues which have to be addressed. These include the following:

- Software plays a vital and essential role in designing medical devices. Many functions traditionally implemented in hardware, including safety interlocks, are now being implemented in software. Thus, high-confidence software development is absolutely essential to ensure the safety and effectiveness of medical CPS.
- Since medical devices should include communication interfaces, it is also essential to ensure that integrated medical devices are effectively safe, secure, and can ultimately be certified.
- The patient information exchanged while the device is interoperating may not only ensure a better understanding of the general health conditions of the patient but can also enable early detection of infirmities. As a result, the generation of effective and smart alarms is imperative in case of emergency situations. One must remember the complexity of the human body and thus the huge variations of physiological parameters over the number of patients in one medical unit; therefore, developing such computational intelligence is not an easy task.
- Computing intelligence should be a property of MCPS. Going forward, that property can be used for increasing the authority of the system by enabling actuation of therapies based on the patient's current health status. Therefore, closing the controlled loop in this manner must be done safely and effectively.
- MCPS collects very critical medical data and also aims to manage that data. Therefore, any unauthorized access or tampering with this information can have severe consequences for the patient's health and can breach or break privacy laws, resulting in attempted abuse, discrimination and physical harm. Preserving the security of MCPS is therefore crucial and would be a compulsory prerequisite.
- The demonstration of dependability and cost-effectiveness for medical device software is the backbone of complex and safety-critical MCPSs. Certification of such medical devices provides a way of achieving this goal. Verification is therefore an essential requirement for the eventual viability of MCPS devices and is, therefore, an important challenge to be addressed.

Similarly, health CPSs (HCPSs) will soon replace traditional health devices which work independently, and will become part of our lives in the future.

Currently, along with sensors and other networks, various health devices work together to detect patients' physical condition in real time, especially for critical patients, such as patients with heart disease. These tasks are achieved by using body area network (BAN) technology. There are also portable terminal devices on the market which are carried by the patient and which can detect the patient's condition at any time and send timely warnings or predictions. Furthermore, the merging of health equipment and real-time data delivery would be much more advantageous for patients. To this end Lee and Sokolsky [21] reviewed the issues regarding the development of a highly trustworthy health CPS system. Their study suggested that HCPS would depend on software for new function development, and the need for network connections together with the continuous monitoring of patients, plus further research into the future development of health CPS. For such health devices, we are presented with interoperability challenges as well. Similarly, Kim *et al*. [22] proposed a generic framework named the network-aware supervisory systems (NASS), whose main purpose would be to integrate health devices into such a clinical interoperability system that uses real networks. It provides a development environment, in which health-device supervisory logic can be developed based on the assumptions of an ideal, robust network. In view of the complexity of these health applications, features such as higher security, real time and reduced network delay will need to be considered in the design of health CPSs.

2.4.4 CPS for smart grid

The development and value of smart applications are bound up in the interactions between people, their businesses and general entities. Wireless networks need to operate by their own rules over an infrastructure to ensure that these interactions occur. One example is the electricity grid infrastructure, which is connected to limited interactive entities. Nowadays, consumers' energy requirements are met through a few central power stations, following the typical centralized approach. However, due to the development of renewable energy resources, in the future we can expect users to also produce energy – hence the term 'prosumers'. Thus consumers can interchange the consumer/producer roles. Karim and Phoba [23] propose the concept of a smart grid to provide a next-generation electricity network boasting advanced reactiveness, configurability and self-management. This is achieved through a complex infrastructure, SoS, taking care of a number of characteristics [24] such as geographical distribution, independent operational and managerial elements, interdisciplinary nature, highly heterogeneous networked systems as well as their behavior and evolutionary development. This technology is expected to be the key part of the worldwide ecosystem of interacting entities, thus innovating the future of cross-industry services. An efficient management and energy utilization requirement is the key driving force of these efforts, such as to obtain granularity in the monitoring and management in the utilization of both local and global available resources (see Figure 2.8).

CPSs [25] describe the combination of computer and physical properties; it is found in multiple domains, particularly the electricity grid. Networked embedded

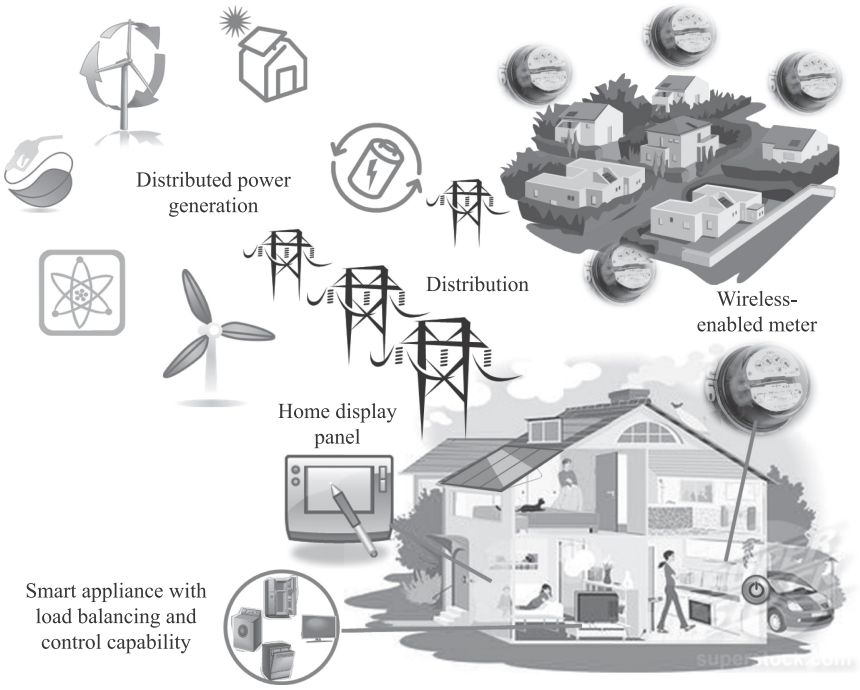

Figure 2.8 CPS smart home applications

devices that offer real-time information exchange between the real world and the virtual world have, over the past decade, reached such an advanced stage that these can no longer be distinguished. With the increase in computation and communication capabilities and the decrease in size, these devices provide control and monitoring of real-world processes to an exceptional scale. CPS is relied upon by modern businesses in the synchronization of their real-world status on backend systems and processes. At its core, the combination of the physical and virtual world helps gather useful information about physical objects seamlessly which in turn is used in various applications throughout the objects' whole life span. Information collection, such as the objects' and goods' source, geographic location, mobility, usage history, physical properties and context, can help business owners create and improve current intracompany and intercompany business processes. This direct information from the real-world scenarios of the objects can be used to enhance decision-making algorithms, leading to more accurate business processes. The need to evolve embedded and ubiquitous computing technologies, by decreasing costs and increasing capabilities, has led businesses to gain access to the network and network edge, i.e. the CPS, which in turn has simplified a number of limitations faced by centralized approaches. The impact of CPS on current business is evident from industry predictions and visions for the future. The network industry, especially mobile and the all-pervasive CPS, has high stakes in, and expectations from, this

technology. According to Hakan Djuphammar, VP of systems architecture at Ericsson, '[In 10 years' time], everything will be connected. We're talking about 50 billion connections, all devices will have connectivity...'. Hans Vestberg, President and CEO of Ericsson, who stated that 50 billion devices would be connected to the web by 2020, further endorsed this belief. Furthermore, the late John Woodget, Intel's global director of the Telecom sector, made a more moderate prediction, forecasting approximately 20 billion connected devices by 2020 [26]. Marie Hattar, VP of marketing at Cisco's network systems solutions group, specifically targeting smart grid networks, estimated that these networks would be '100 or 1000 times larger than the Internet' [27]. Vishal Sikka, CTO of SAP, expressed similar views that 'the next billion SAP users will be smart meters' [28].

One example of smart grid CPS is smart meters in homes and the installation cost of this system is estimated at $4.8 billion according to ABI Research [29]. According to another study by Pike Research, by 2020 the energy management systems market will be worth an estimated $6.8 billion per year. This includes lighting controls, WSNs, cooling and heating management in buildings, and it is estimated that a total investment of $67.6 billion will have been generated between 2010 and 2020 [30]. Also, currently (2015) an estimated $4.3 billion will have been spent on the installation, management and maintenance service for smart grids [31].

According to an estimation by the Canada Electronics Research Network, the smart home WSN market will rise from $470 million in 2007 to $2.8 billion in 2018 [32]. The massive shipping market and WSN-based home monitoring services provided by AT&T and SK Telecom have made the smart home (Figure 2.8) a reality. Another breakthrough is the latest CPS-enabled smartphones and tablets which promise powerful communication and computation along with various on-board sensors. As per Gartner's report [36], worldwide shipment of devices will reach 2.5 billion units in 2015 and will exceed 2.228 billion in 2017. These estimations further enhance the fact that the CPS-dominated era has begun. Currently, a number of research and deployment projects are under way worldwide in the field of smart grids and their CPS nature.

2.4.5 Overview

Table 2.1 gives a tabulated overview and summary of the major applications and requirements of CPS as discussed in the preceding subsections.

2.5 Future aspects of CPS

For CPS, research areas are distributed across isolated sub-domains, including communications and networks, mathematical modeling, systems theory, software engineering, wireless networks (i.e. sensor and ad-hoc networks) and computer science. Therefore, designing and developing digital systems is achieved by using various models, formalisms and tools. Those systems illustrate a set of features, and on the other hand can skip a complete system. More often, any formalism depicts

either physical processes, or cybernetic processes, but does not utilize both at the same time, as per the requirements of the CPS domain.

Globally, research into CPSs has been driven in various directions, such as the description of a general architecture or a generic classification of the CPS designing principles for varying domains of the applications. Research has also included modeling of the CPS, where the dependability of CPS must be guaranteed, and finally the implementation of a CPS for critical infrastructure control and so on. In this section, we therefore enlist the future research challenges of the CPS domain which is still at an early stage.

Architectures and abstractions: In order to let any CPS communicate, control, compute and integrate between physical and cyber properties, we need to develop an innovative approach and define abstracts to formulate new architectures. Those architectures may allow the fusion and integration of a set of various heterogeneous systems with different properties that composed the CPS in an integrated, robust and efficient manner.

Network control and distributed computations: Here we refer to developing new frameworks, methods, algorithms and Software Development Kits (SDKs) related to event-driven and time-dependent calculations (computing). Moreover, we also lack software tools, various time-delay tolerance, malfunctions, runtime configuration and rapid decision support for distributed systems such as CPS. Therefore, we should take into account the satisfactory interaction of the physical environment with highly reliable and secure but varying components, which later on take decisions on runtime autonomously.

Validation and verification: Any CPS system expects to be composed of such hardware and software modules that should outperform their current stage and must achieve a high level of re-configurability, dependability and certification when it is required. Hereafter, new algorithms, models, tools and methods are expected in order to validate the software components. In addition, an entire system from its early design stage leads us toward the research directions to be addressed by the scientific and research community. Also, those research challenges in the CPS field were highlighted by the CPS Steering Group in their report [37] and are described in detail below:

1. The redesigning of abstract layers is required where those layers must include some physical concepts including energy and time. Those changes will relatively allow the fusion of computations/calculations together with the physical properties and physical system dynamics which are currently causing uncertainties in the implementation of CPS.
2. Semantic foundations need to be developed for heterogeneous models of CPS. Also, various modeling languages are also required in order to describe the numerous associated logics of physics.
3. Understanding and composing of a new heterogeneous system that tolerates the large amount of data. In addition, a networked system that fulfills a set of essential physical characteristics and has the ability to deliver the desired CPS functionalities in a more reliable fashion.

4. The development of a technology for achieving the predictability in partially compositional properties.
5. The modeling of a predictable and precise technology to be considered as a base foundation for integrating various systems in the future.
6. Proposing a new infrastructure for swift design and automation of CPS.
7. The design of a new series of flexible architectures, enabling CPS, ensuring the development of the nationwide and global effective systems.
8. From the existing but unreliable modules, developing the architectures and modeling tools for a reliable and resilient CPS that must be able to withstand malicious attack from either the physical or cyber world. Furthermore, the newly designed architectures may leverage an open system and other technologies with fluctuating design time while increasing the confidence interval of the CPS.

2.6 Conclusion

This chapter has provided a concept of CPSs together with their applications and current research progress in this area. The basics and fundamentals of CPS are then explained. In addition, the characteristics of CPS, such as real time, scalability and reliability, are introduced and which present a number of challenges in CPS design and implementation. There are numerous possible applications yet to be highlighted; however, this chapter also provides a technical overview of forthcoming applications such as smart grid, vehicular environments and agriculture. Along with that, we also highlight several research issues and architectures, including one explicit CPS architecture which was recently introduced in 2013, verifying the basic requirements for modeling and simulations of CPS environments. In short, 'dynamic communications' will be the future of networks and CPS is thus providing the necessary upcoming technologies.

Acknowledgments

The authors of this chapter would like to thank the editors and the editing staff of this book for giving them the opportunity to contribute to this forthcoming book.

References

[1] R. Rajkumar, I. Lee, L. Sha and J. Stankovic. Cyber-physical systems: the next computing revolution. In *Proceedings of the 47th ACM Design Automation Conference*, pp. 731–736, 2010.

[2] P. Tabuada, S. Y. Caliskan, M. Rungger and R. Majumdar. Towards robustness of cyber-physical systems. In *IEEE Transactions on Automatic Control*, 59(12): 3151–3156, December 2014.

[3] M.Broy. Challenges in modeling cyber-physical systems. In *Proceedings of the 12th ACM International Conference on Information Processing in Sensor Networks*, pp. 5–6, 2013.

[4] A. Mahmood, A. Ismail, Z. Zaman, H. Fakhar, Z. Najam, M. S. Hasan and S. H. Ahmed. A comparative study of wireless power transmission techniques. *Journal of Basic and Applied Scientific Research (JBASR)*, 4(1): 321–326, 2014.

[5] L.-A. Tang, X. Yu, S. Kim, Q. Gu, J. Han, A. Leung and T. La Porta. Trustworthiness analysis of sensor data in cyber-physical systems. *Journal of Computer and System Sciences*, 79(3): 383–401, 2013.

[6] S.-S. Lim, E.-J. Im, N. Dutt, K.-W. Lee, I. Shin, C.-G. Lee and I. Lee. A reliable, safe, and secure run-time platform for cyber physical systems. In *Proceedings of the 6th IEEE International Conference on Service-Oriented Computing and Applications (SOCA)*, pp. 268–274, 2013.

[7] M. P. E. Heimdahl, L. Duan, A. Murugesan and S. Rayadurgam. Modeling and requirements on the physical side of cyber-physical systems. In *Proceedings of the 2nd IEEE International Workshop on the Twin Peaks of Requirements and Architecture (Twin Peaks)*, pp. 1–7, 2013.

[8] J.-S. Choi, T. McCarthy, M. Yadav, M. Kim, C. Talcott and E. Gressier-Soudan. Application patterns for cyber-physical systems. In *Proceedings of the 1st IEEE International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA)*, pp. 52–59, 2013.

[9] A. A. Cardenas, S. Amin and S. Sastry. Secure control: Towards survivable cyber-physical systems. In *Proceedings of the 28th International Conference on Distributed Computing Systems (ICDCS '08)*, pp. 495–500, 17–20 June 2008.

[10] L. Hu, N. Xie, Z. Kuang and K. Zhao. Review of cyber-physical system architecture. In *Proceedings of the 15th IEEE International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing Workshops (ISORCW)*, pp. 25–30, 2012.

[11] D. D. Hoang, H.-Y. Paik and C.-K. Kim. Service-oriented middleware architectures for cyber-physical systems. *International Journal of Computer Science and Network Security*, 12(1): 79–87, 2012.

[12] Y. Tan, S. Goddard and L. C. Perez. A prototype architecture for cyber-physical systems. *ACM Signed Review*, 5(1): 26, 2008.

[13] T. Sanislav and L. Miclea. Cyber-physical systems – concept, challenges and research areas. *Journal of Control Engineering and Applied Informatics*, 14 (2): 28–33, 2012.

[14] Y. Tan, S. Goddard and L. C. Perez. A prototype architecture for cyber-physical systems. *ACM SIGBED Review*, 5(1): 1–2, 2008.

[15] J. Wan, H. Yan, Q. Liu, K. Zhou, R. Lu and D. Li. Enabling cyber-physical systems with machine-to-machine technologies. *International Journal of Ad Hoc and Ubiquitous Computing*, 9(3/4): 1–9, 2012.

[16] S. Hassan Ahmed, G. Kim and D. Kim. Cyber physical system: Architecture, applications and research challenges. In *Proceedings of IEEE/IFIP Wireless Days (WD)*, Valencia, Spain, pp. 1–5, 13–15 November 2013.

[17] M.Stonebraker. SQL databases v. NoSQL databases. *Communications of the ACM*, 53(4): 10–11, 2010.

[18] A. Rezgui and M. Eltoweissy. Service-oriented sensor-actuator networks [ad hoc and sensor networks]. *IEEE Communications Magazine*, 45(12): 92–100, 2007.

[19] B. Hull, V. Bychkovsky, Y. Zhang, K. Chen and M. Goraczko. CarTel: A distributed mobile sensor computing system. In *Proceedings of the 4th ACM Conference on Embedded Networked Sensor Systems*, Boulder, pp. 125–138, 2006.

[20] M. Zhijun, Z. Chunjiang, W. Xiu, C. Liping and X. Xuzhang. Field multi-source information collection system based on GPS for precision agriculture. *Transaction of the CSAE*, 19(4): 13–18, 2003.

[21] I. Lee and O. Sokolsky. Health cyber physical systems. In *Proceedings of the 47th ACM/IEEE Design Automation Conference*, Anaheim, pp. 13–18, 2010.

[22] C. Kim, M. Sun, S. Mohan, H. Yun, L. Sha and T. F. Abdelzaher. A framework for the safe interoperability of health devices in the presence of network failures. In *Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems*, Stockholm, pp. 149–158, 2010.

[23] M. E. Karim and V. V. Phoha. Cyber-physical systems security. In *Applied Cyber-Physical Systems*, Springer, New York, pp. 75–83, 2014.

[24] W. Ait-Cheik-Bihi, A. Nait-Sidi-Moh, M. Bakhouya, J. Gaber and M. Wack. TransportML platform for collaborative location-based services. *Service Oriented Computing and Applications*, 6(4): 363–378, 2012.

[25] A. Hahn, A. Ashok, S. Sridhar and M. Govindarasu. Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *IEEE Transactions on Smart Grid*, 4(2): 847–855, 2013.

[26] S. Liu, S. Mashayekh, D. Kundur, T.Zourntos and K. Butler-Purry. A framework for modeling cyber-physical switching attacks in smart grid. *IEEE Transactions on Emerging Topics in Computing*, 1(2): 273–285, 2013.

[27] M. J. Stanovich, I. Leonard, K. Sanjeev, M. Steurer, T. P. Roth, S. Jackson and M. Bruce. Development of a smart-grid cyber-physical systems testbed. In *Proceedings of IEEE/PES Innovative Smart Grid Technologies (ISGT)*, pp. 1–6, Washington, DC, USA, 24–27 February 2013.

[28] A. AlMajali, E. Rice, A. Viswanathan, K. Tan and C. Neuman. A systems approach to analysing cyber-physical threats in the smart grid. In *Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 456–461, Vancouver, Canada, 21–24 October 2013.

[29] I. Stojmenovic. Machine-to-machine communications with in-network data aggregation, processing, and actuation for large-scale cyber-physical systems. *IEEE Internet of Things Journal*, 1(2): 122–128, 2014.

[30] A. Anwar and A. Naser Mahmood. Cyber security of smart grid infrastructure. *arXiv preprint arXiv*:1401.3936, 2014.
[31] C. Beasley, G. Kumar Venayagamoorthy and R. Brooks. Cyber security evaluation of synchrophasors in a power system. In *Proceedings of IEEE Power Systems Conference (PSC)*, Clemson University, pp. 1–5, 2014.
[32] A. Nandanwar, M. Preetam Korukonda and L. Behera. A routing scheme for voltage stabilization in cyber physical energy systems. *Advances in Control and Optimization of Dynamical Systems*, 3(1): 812–818, 2014.
[33] H. Jifeng. Cyber-physical systems journal, *China Computer Federation*, 6(1): 25–29, 2010.
[34] R. West and G. Parmer. A software architecture for next-generation cyber-physical systems. In *Proceedings of the NSF Cyber-Physical Systems Workshop*, Austin, Texas, October 2006.
[35] K. Wan, K. L. Man and D. Hughes. Specification, analyzing challenges and approaches for cyber-physical systems (CPS). *Engineering Letters*, 3, 2010.
[36] Gartner.com. Gartner says worldwide device shipments to grow 1.5 per cent, to reach 2.5 billion units in 2015. See: http://www.gartner.com/newsroom/id/3088221 (accessed 20 August 2015).
[37] Cyber-Physical Systems Virtual Organization. Cyber-Physical Systems – Executive Summary. See: http://cps-vo.org/node/204 (accessed 20 August 2015].