Review on Cyber-physical Systems

Yang Liu, Yu Peng, Bailing Wang, Sirui Yao, and Zihe Liu

***Abstract*—Cyber-physical systems (CPS) are complex systems with organic integration and in-depth collaboration of computation, communications and control (3C) technology. Subject to the theory and technology of existing network systems and physical systems, the development of CPS is facing enormous challenges. This paper first introduces the concept and characteristics of CPS and analyzes the present situation of CPS researches. Then the development of CPS is discussed from perspectives of system model, information processing technology and software design. At last it analyzes the main obstacles and key researches in developing CPS.**

***Index Terms*—Cyber-physical systems (CPS), information processing, software design, system model.**

I. Introduction

THERE has been a number of milestones in the development of computer technology and information technology. Mainframe computers appeared in 1960s-1970s. In 1980s-1990s, Internet and desktop computers able to deal with personal and commercial business were created. Around 2000 appeared pervasive computation to conduct calculation at any time or place. All these events have fundamentally influenced the development of information society. At present, many experts from various fields are paying close attention to the emergence of a new engineering system, cyber-physical systems (CPS). CPS are multidisciplinary systems to conduct feedback control on widely distributed embedded computing systems by the combination of computation, communication and control technologies. They are transformation and integration of the existing network systems and traditional embedded systems. Through integration CPS are able to realize the real-time, safe, reliable and dynamic collaboration with physical systems represented by embedded system. Physical system data acquisition modules collect data by distributed field devices in CPS system and guarantee the real-time capability and accuracy of the collected data. They pass data to the information processing layer according to the demands of services and complete given tasks by information processing technologies such as data uncertainty management, statistical signal processing, data security processing and feedback control. CPS have a wide range of applications, such as digital medical instruments and systems adopting automatic acquisition and control technology, distributed energy systems, aerospace and aircraft control, industrial control and so on [1]−[3]. CPS can also bring huge economic benefits and will eventually bring fundamental change to the function of existing engineering physical systems.

This paper first introduces the concept and characteristics of cyber-physical systems. Then it analyzes the present situation of CPS researches as well as the challenges in CPS system model construction and key technology. The last part is the prospect of CPS researches and applications.

II. Concept and Characteristics

A. Concept

Since CPS is an emerging research area which involves the overlapping and integration of multiple fields of science and engineering, it requires computer scientists and network professionals to collaborate closely with experts in various fields such as automation and control, civil engineering, mechanical engineering and biology. Therefore, the present definitions of CPS are mostly given by different scholars from their own perspectives.

E. A. Lee defines Cyber-physical systems as the integration of calculation and physical process, which involves embedded computer and networks monitoring and controlling the physical processes. Physical processes affect computations by feedback loops and vice versa [4]. Academician J. F. He regards CPS as controllable, credible and scalable networked physical equipment systems; which is in-depth integration of computation, communications and control ability on the basis of environmental perception [5]. Through the feedback loop of mutual effects between computing processes and physical processes, in-depth integrations and real-time interactions are achieved to increase or expand the function of networks and physical systems and to monitor or control a physical entity in a safe, reliable, efficient and real-time way.

The service-oriented architecture of CPS is shown in Fig. 1.

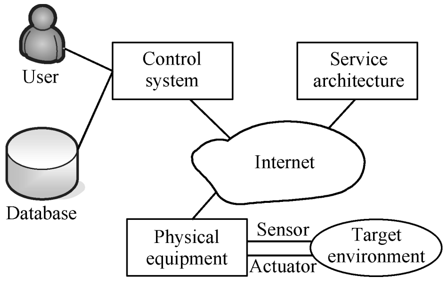


Fig. 1. Service-oriented architecture of CPS.

Some other scholars propose that CPS is a network physical engineering system which monitors and controls the operations

Manuscript received January 23, 2015; accepted October 5, 2015. This work was supported by National Natural Science of China (61170262, 61371177). Recommended by Associate Editor Yilin Mo.

Citation: Y. Liu, Y. Peng, B. L. Wang, S. R. Yao, and Z. H. Liu, "Review on cyber-physical systems," *IEEE/CAA Journal of Automatica Sinica*, vol. 4, no. 1, pp. 27−40, Jan. 2017.

Y. Liu is with the Department of Computer Science and Technology, Harbin Institute of Technology at Weihai, Weihai 264209, China, and also with the Automatic Test and Control Institute, Harbin Institute of Technology, Harbin 150008, China (e-mail: Liuyang322@hit.edu.cn).

Y. Peng is with the Automatic Test and Control Institute, Harbin Institute of Technology, Harbin 150008, China (e-mail: pengyu@hit.edu.cn).

B. L. Wang, S. R. Yao, and Z. H. Liu are with the Department of Computer Science and Technology, Harbin Institute of Technology at Weihai, Weihai 264209, China (e-mail: wbl@hit.edu.cn; lyylwhhit@126.com; lzhwh@hit.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JAS.2017.7510349

of physical system through computation [6]. U.S. Defense Advanced Research Projects Agency (DARPA) believes that the physical network system refers to systems whose functions are largely derived from software and electromechanical systems. In fact, all defense systems (such as aircraft, spacecraft, naval vessels, ground vehicles, etc.) and subsystems in those systems are all CPS. Additionally, integrated circuits, micro-electro-mechanical system (MEMS) and nano-electro mechanical systems (NEMS) also belong to CPS.

However, wireless sensor network (WSN), internet of things (IOT) and CPS are different. Instead of stressing the identification of object, WSN only senses the signal, but not necessarily identifies the specific one from many objects being sensed. It emphasizes the perception of information and provides data support for a variety of specific application through data collection, processing, integration and routing. IOT interconnects Internet information sensing devices like wireless sensor and radio frequency identification (RFID) through wireless network and Internet technology, and it is a new type of network to realize the overall perception, reliable transmission and intelligent processing of information. CPS is a controllable, credible and scalable network physical equipment system which deeply integrates the ability of computing, communication and control on the basis of information acquisition in IOT. Through the feedback loop of the interaction between calculation process and physical process, deep integration and real-time interaction is realized to increase or to extend new function, so that a physical entity can be detected or controlled in a safe, reliable, and efficient way. The Internet of things generally only have the perception, but no or just simple control of the physical world, while CPS not only has the ability of sensing the physical world, but also possesses strong ability to control. Its requirement of computing capability for equipment far exceeded that of IOT and WSN.

To sum up, CPS are systems featuring a tight combination of, and coordination between network systems and physical systems. By organic integration and in-depth collaboration of computation, communications and control (3C) technology, they can realize the real-time sensing, dynamic control and information services of large engineering systems. The term CPS also refers to distributed heterogeneous systems that not only contain network systems and physical systems with different functions, but also the structure and function vary among their subsystems and are distributed in different geographic scopes. Wired or wireless communications are needed for various subsystems to coordinate with each other. System integration of CPS is shown in Fig. 2.

B. Characteristics

CPS interact with physical system through networks, the end system of CPS is normally traditional centralized tightly coupled embedded computing system, which contains a large number of physical systems composed of intelligent wireless sensors net. Therefore, CPS maintains following characteristics:

1) Physical System is the Most Important Field of CPS: It involves physical system design such as hardware design, energy management, hardware size and connectivity encapsulation and system testing. Engineers and scientists in this field have deep understanding of system and environment of mechanics, electronics, biology and chemistry, they master the technical characteristics of sensors, and they know how to process the measurement data by signal processing technology. Every physical system has its network characteristics as well as maximized multi-level network coverage, a variety of complex temporal and spatial scale to meet the time requirements of different tasks and a high degree of automation.

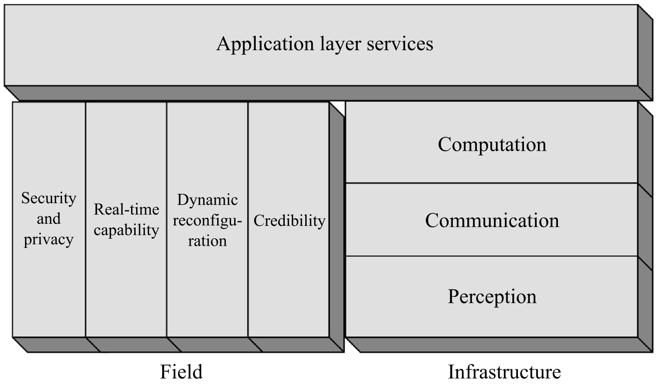


Fig. 2. System integration of CPS.

2) Information System is the Core of CPS: Engineering technicians in the field of information system can transform the information in physical system engineering into the rules and models of software system. For these workers, the most basic task is to reach a balance among factors such as real-time system, network system, file system, hierarchical storage system, memory management, modular software design, concurrent design and formal verification.

3) CPS is the Product of Integration of Heterogeneous Systems: They are heterogeneous distributed systems with deep integration and interaction of information systems and physical systems, which should deal with the problem of time synchronization and space location of different components.

4) CPS has Requirements of Security, Real-time Capability, and Predictability: Due to the characteristic of network system and physical system as being open, there exist problems including invasion, tampering, counterfeiting and other malicious attacks as well as delay in network transmission system, so CPS must be able to deal with the problem of credibility, security, effectiveness, real-time, dynamic and predictability. Credibility means the identity of information collecting sources or control instruction senders must be authenticated, and the receiver must be able to exactly determine the real identity of the sender to prevent counterfeiting; Security refers to the encryption and decryption of sent or received information, while the privacy of information must be protected. Validity means the accuracy of processing as well as the validity and integrity of information or instruction set must be guaranteed to prevent the uncertainties and noise in CPS processing from affecting the system processing accuracy. Real-time capability means collected information or instructions must be transmitted timely to meet the real-time requirements of task processing. Dynamic includes dynamic reorganization and reconfiguration, which is to automatically adjust rules and generate commands based on the task requirements and changes in external environments to eliminate bias and meet task requirements according to preset rules.

Predictability means CPS resource allocation strategy can reasonably allocate resources to multiple competing real-time tasks at any moment and in any case so that the real-time requirements of every real-time task can be satisfied.

III. Technical Researches

Scientific CPS composition must be a new system architecture pattern which is composed of hierarchical systems including components and subsystems, service quality theory, agreements and modeling language and tools that can analyze, integrate and simulate different components. Computation theory should be able to handle feedback control of real-time systems based on event driven which suit the asynchronous dynamic event processing of different time scale. The world CPS researches are just in their beginning. Since CPS is the integration of multidisciplinary heterogeneous systems, without a unified global model, CPS researches are carried out by experts in various areas from the perspective of applications in their own field. At present, CPS researches mainly focus on studies of system architecture, information processing and software design.

A. Researches on Architecture of CPS

Modeling can be considered as the technology to describe the target system before completion. CPS architecture is the base of research and development, and CPS models must be modified and integrated on the basis of existing physical system, network system and computer system structure. Abstraction and modeling of communication, computation and physical dynamics in different scales and sizes of time are also needed to accommodate the development of CPS. We propose a kind of the CPS system structure model which can be divided into three layers: User layer, information system layer and physical system layer. The physical system is composed of a large number of embedded systems, sensor networks, smart chips, etc, taking charge of the collection and transmission of information and the execution of control signals, as it is the foundation of the CPS. Information system layer is mainly responsible for the transmission and processing of the data collected from the physical system, which is the core of the CPS. User layer mainly completes the work such as data query, strategy and safety protection under human-computer interaction environment which should be guaranteed by regular CPS operations. CPS runs in the form of closed loop control. The architecture of CPS is shown in Fig. 3.

The function of each part in Fig. 3 is as follows:

1) Sensor Networks: Use a variety of sensors and real-time embedded systems for real-time data acquisition. Conduct analog-to-digital conversion of collected data and other processes including data encryption and data integration through collection nodes. Protect the security of data transmission (privacy, integrity and non-repudiation). Reduce the network energy consumption by energy management. Apply real-time data protection technology to real-time processing.

2) Next Generation Network Systems: Use anti-hacking and defense technology against a variety of network attacks. Use high-performance encryption algorithm and CA authentication technology to ensure the safety of data transmission. Realize rapid exchange of data transmission by optimizing existing routing algorithms. Change the existing network system structure with the "best effort" to provide real-time network transmission services for the system.

3) Data Center: Sensor network transmits data to data center for storage through next generation network systems. Data center checks the authentication and integrity of received data and stores the data if they pass the inspection otherwise sends a message to control center. Then control center will send control signals to the actuator which would notify the sensor network nodes to collect data again. Data center is also responsible for routine maintenance of the database and quick response to instructions sent by control center such as query. Regular emergency treatments are also needed to prevent database from collapse.

4) Control Center: Control center is the most important part of CPS. It receives the inquiry instructions sent by users and then sends query command to data center after identity authentication. It categorizes the query results according to control strategies, reports back to the user if they meet the requirements, otherwise finds out the location of the node by node positioning technology and sends control instructions to actuators for corresponding processing. Control center configuration policy can be dynamically adjusted according to users' needs. Conduct forecast analysis and performance analysis of CPS behavior through data mining technology and uncertainty processing technology. Detect the network and node failure through fault diagnosis technology and conduct corresponding processing. Ensure the real-time control processing of CPS through real-time control technology.

5) Actuator Networks: Receive control instructions from control center and send control instructions to corresponding nodes.

6) System User: System user includes a variety of WEB servers, individual host and external devices. It is responsible for the communication with CPS, sending inquiry instruction to control center and receiving feedback data. Users can send definitions and revised control strategies to control center to get executed.

In this model, CPS would run under closed-loop control, and the real-time capability, security and system performance are fully considered so that it can preliminarily meet future CPS requirements. Some scholars also conducted researches on the system architecture of CPS with different studied subjects and from different application perspective.

Advanced power grid is a complex real-time system that contains network and physical components. Each part may function well independently, but not when they are combined together because the interference may cause errors, for instance, the violation of Nyquist rate in frequency domain. Y. Sun *et al.* proposed to use RT-PROMELA to build a model that can represent frequency interference and use the real-time interference of real time-sensor protocol for information via negotiation (RT-SPIN) detection to test the accuracy of CPS components. It solved the problem of multiple clock variables in collaboration processing caused by lack of real-time and asynchronous interaction of components [7]. M. D. Ilic *et al.* established a CPS energy system dynamic model with distributed sensing and control, and discussed the process of information exchange between components in this model as well as using the model to develop interactive protocols between embedded system control terminal and network system.

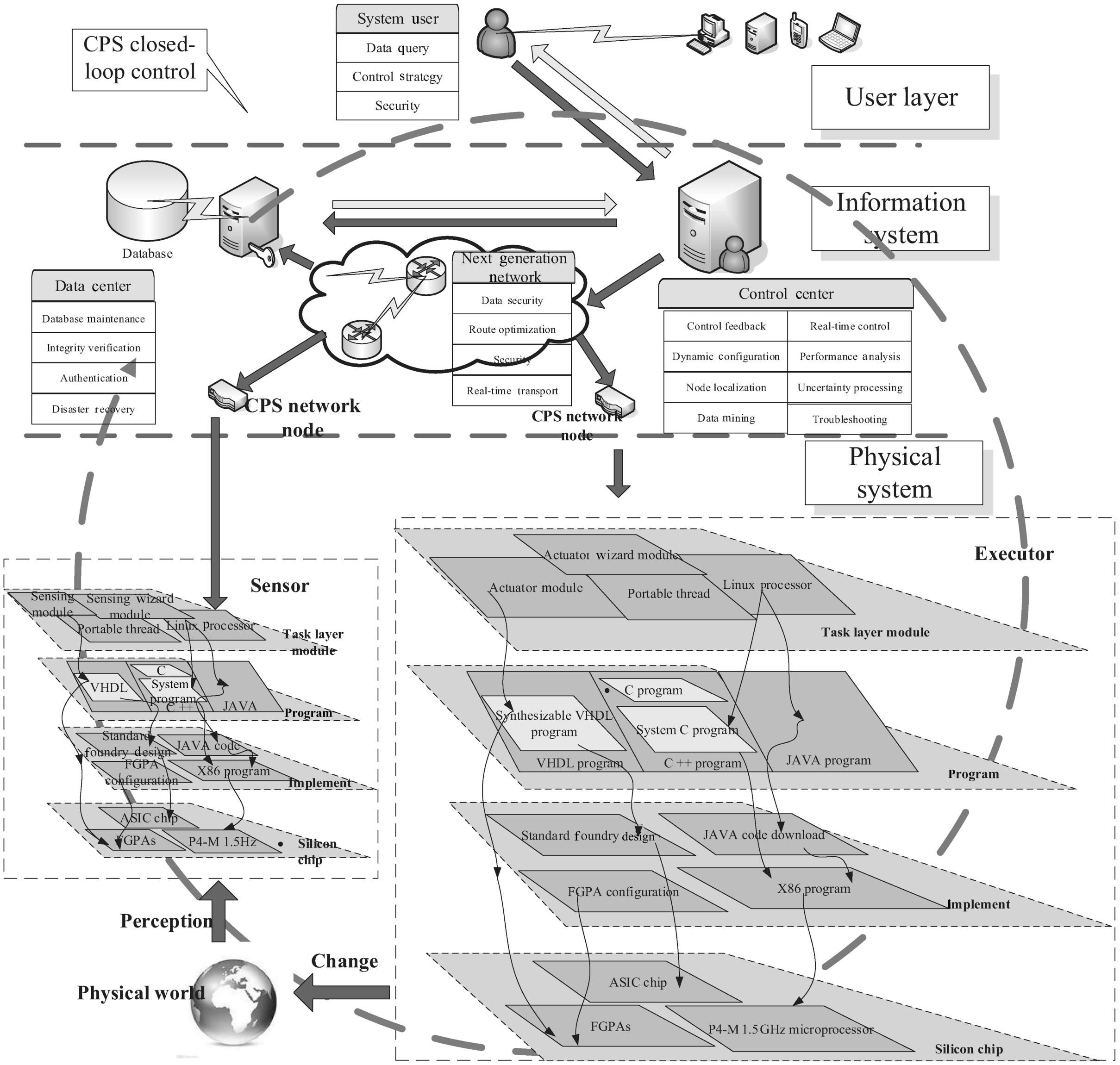


Fig. 3. Architecture of CPS.

He built a coordination framework based on perception of model and future energy system control. He also improved the operation of complex power system using data mining techniques and new sensor technologies [8]. But these studies can only be applied in power systems therefore do not have the versatility.

Actuator network is composed of a plurality of actuator units and control nodes. Control nodes are responsible for receiving the control command from the control center and sending command to one or more specific actuator unit for execution, so that certain physical attributes of the physical world can be adjusted and controlled to change the physical world. To solve the problem of collaborative design of feedback control and scheduling, [9] discussed a method of scheduling when several actuators are controlled by a controller (single processor), which is to achieve a balance between the time delay and the control performance by adopting off-line and online strategy respectively. However, it only considered the physical system part in CPS, namely the control part and ignored the information system part. Reference [10] studies the architecture of CPS and proposed CPS system model adopting event-driven real-time scheduling scheme, which solves the problem of real-time task scheduling through sensor nodes periodic task model and the actuator event-triggered task model. But experimental verification was not provided so it is unable to verify the system running efficiency. Reference [11] proposes to simultaneously process periodic and non-periodic events in CPS oriented real-time middleware, and puts forward the corresponding algorithms of access control and load balancing, but did not analyze the time cost caused by middleware services. The random server concept proposed in [12] performs well in processing event-triggered random tasks and meeting time predictability requirements, but there exists deficiencies in the processing mechanism if there is time overhead or server overload.

CPS has strict requirements on real-time capability and abstraction of physical awareness. Since system components might need synchronous or asynchronous interaction with physical world, a global reference time is fundamental for all CPS components to communicate and work properly. Therefore, global reference time must be considered to ensure real-time performance so that CPS components can properly and orderly conduct behaviors and events. Information and events of physical system are abstraction of system components and the objects abstracted have life cycle. Different system components can distribute different credibility and reliability for different input source according to individual preferences, experiences and knowledge. So the abstraction of same input events may produce completely different output due to different system components. Therefore, CPS must have unified time, trust quantification and communication mechanisms at the system level. Y. Tan *et al*. put forward a CPS architectural prototype from aspects of global reference time, event information-driven, trust quantification, publish/ subscribe plan, control semantics and network technology. In this architectural prototype, advanced control unit adopts the tight coupling sensor and actuator mechanism and conduct precise real-time control at the system level to ensure the validity of control loop [13]. But it did not solve problems such as how to publish scheduling plan and how to define event models and information models in large-scale heterogeneous CPS. T. L. Crenshaw *et al*. designed plants controlled by external association, executive control equipment and domain models to estimate the state of plants and simple reference model which satisfies security requirements [14].

In CPS, it is more difficult to realize real-time predictability, which is to control the next step of controlled physical systems by CPS real-time predictability. In order to enhance the sustainability and predictability of CPS, K. J. Lin *etal*. studied the real-time service-oriented architecture (SOA) and established the real time service oriented architecture enterprise service bus (RT-SOA ESB) model. They use real-time SOA middleware services to establish service accountability mechanism and real-time global resource management service process [15]. Due to limitations of services and known resources, the authors adopted the method of reserving resources and using middleware to monitor the performance of every service in the process in advance to ensure real-time prediction. Pasqualetti *etal.* came up with a model and method of automatically extracting cyber-physical systems using a custom programming language; it can be applied to temperature sensors with fault tolerance [16]. But this model lacks versatility because the abstraction accuracy of the automatic processing is not considered and the scope of application is limited.

Present CPS researches are hugely limited by specific application environment, current development environment and theoretical systems. Most of these system models were established specifically for different local applications, and they have not considered the correlation of various demands and restriction factors in CPS networks. Therefore, without a mature global system model, further researches are still necessary.

B. Researches on Information Processing of CPS

Information processing includes the collection, transmission and processing of perception data, feedback of control information as well as the response of physical system after receiving commands.

1) Data Processing:

a) Researches on Data Acquisition Technology: CPS contains all kinds of information sensing devices, such as radio frequency identification devices (RFID), sensors, global positioning systems, laser scanners, etc, which can be combined with the Internet and form a network. Through network protocols, we can easily realize the seamless connection between the field equipment layer and management layer. Therefore, fast and accurate data acquisition in physical system becomes a key factor in CPS efficient data processing.

Acquisition of perception data plays a key role in CPS; we can choose low-precision sensors or high-precision sensing devices according to specific application requirements [17]. Sensor network subsystems consist of a number of sensor nodes and sink-nodes can sense some information in the physical world which users are interested in, such as traffic information in intelligent transportation, soil temperature and humidity information in environmental detection and the patient's blood pressure and blood sugar information in intelligent medication. After necessary processing, perceived information is integrated in the gathering center and then is sent to data center, to provide important data support for decision. Thacker *et al.* proposed the distributed algorithm to rapidly obtain the data of CPS sensor. The algorithm adopts media access control (MAC) protocol which has priority and transmits the approximate representation of sensor data obtained through spatial coordinates of function interpolation [18]. In CPS containing massive sensor nodes, the algorithm can quickly obtain valid data if part of the nodes failed. But it did not consider real-time processing, which is one of the key factors of CPS data processing. C. Qi *et al.* applied the HMS30C7202 processor and controller area network (CAN) bus technology to the data acquisition of control system to construct real-time data acquisition instrument system. Then he combined it with CPS and formed a corresponding information service system through the Internet, transforming various decentralized monitoring and control equipment into network nodes. Using field bus and the Internet as a link, he constructed a real-time, efficient network control system to meet the requirements of industrial control systems as being decentralized, networked and intellectualized [19]. This system breaks through the framework of traditional embedded system and provides significant reference to the real-time data acquisition of CPS, but it does not solve the problem of how to protect the security of data in network systems.

Present researches on the data acquisition of CPS mainly focus on developing intelligent micro-miniature sensors and data acquisition subsystems according to specific application requirements.

b) Researches on Data Transmission Technology: In CPS, there must be a wireless (or cable) communication system platform with sufficient bandwidth to meet different business needs. Traditional single networks cannot satisfy the complex applications in CPS [19]. Therefore, CPS have integrated transmission networks including ZigBee, Wi-Fi, Bluetooth, UWB (ultra wideband), Ad-hoc networks, Mesh network, mobile cellular communication network and the Internet as well as other new network transmission systems. Generally, a CPS application system is the integration of two or more communication networks. But as the mixture of a variety of networks, integrated network faces problems of network node access, channel switch and business seamless connection.

Self-organization and mobility of Ad-hoc network enable high viability and flexibility, which can be integrated with Internet to greatly extend the application range of the CPS. Reference [20]−[24] studied the gateway discovery and problems of interaction and packet loss in the integration of mobile Ad-hoc nETworks (MANET) and the Internet.

Mobile cellular network has the advantages of having wide coverage and easy management, thus combining it with Ad-hoc network can expand the transmission capacity and coverage of CPS [25]−[27].

Optical fiber access brings huge bandwidth, which can be used to achieve a higher rate of data transmission for CPS. Therefore, optical fiber access is also an important technology of CPS system integration.

The researches of CPS data transmission are focused on putting forward practical converged network data transmission scheme and its strategy according to the demands of specific application.

c) Researches on Safety Control: Current safety control mainly includes password management, identity recognition, etc. Reference [28] summarized the existing CPS security technology and pointed out the main challenges. Reference [29] studied the reliability assurance measures of CPS. Reference [30] presents the general theory of information flow security enhancement mechanism and gives an example to illustrate the idea of the method. In [31], Y. Zhang *et al.* proposed a self-adaptive health monitoring and management system model and defined fault diagnosis quality measures based on the special requirements of fault diagnosis.

Reference [32] proposed a 6-layer security architecture for cyber-physical systems, motivated by the OSI and PRM models. They have addressed the security issues present at each layer and pinpointed a holistic viewpoint for security solutions in CPS. They proposed a game-theoretical model that builds bottom-up from the physical layer and argued that the saddle-point solution to the dynamic game gives rise to a cross layer security policy. They modeled the interaction between an attacker and a defender. $J_i(v_i, g_i) = q_i, f s_i^2(K) + \sum_{i=1}^{K} q_i K s_i^2(K) - v_i^2(K)$. The goal of a defender is to maximize its well-being with minimum control or maintenance effort while an attacker attempts to maximize the damage to the device. Reference [33] studied the message scheduling scheme to improve wireless network application safety in important tasks. The existing real-time data management technology and wireless sensor networks (WSNs) cannot support the real-time capability of CPS and safety data services because of distance. F. Mueller discussed the problems that exist in CPS designing process, such as security, real-time capability and other issues due to real-time limitations of embedded systems. He also gave corresponding solutions from the perspective of verifying the worst-case execution time and preventing and correcting software errors [34].

d) Researches on Real-time Capability: Most CPS are established to support real-time applications, such as real-time observation, real-time monitoring, real-time control and real-time forecasting, to keep updated on the current situation of physical devices and to conduct necessary control and intervention on physical equipment and environments by means of network control. Therefore, CPS data processing must meet real-time requirements to ensure proper results are given within a limited time. Reference [35] emphasizes the importance of CPS security, reliability and real-time capability, and considers the efficient combination of primitive models needed by hardware and software process. Reference [36] points out that real-time capability can hugely influence the design and demand in CPS application systems from soft real-time and hard real-time perspective. In CPS, heterogeneity lead to the main challenges of network in large-scale system design, including time-varying delay, time jitter, data rate limitation, packet loss, etc. To solve these problems, [37] proposes to use a single-path delay variation model to eliminate the influence of delay jitter in CPS. Reference [38] notes passive control mechanism thereby improving reliability. Reference [39] describes a single reference model-aided design CPS architecture, which can limit fault propagation. Reference [40] presents highly configurable and reusable middleware architecture for real-time hybrid test. To solve the real-time capability of networked monitoring of network synchronization, Y. Peng *et al.* proposed to use IEEE1588 to improve the real-time capability of network. He adopted ARM+FPGA architecture to realize the IEEE 1588 standard synchronization system to evaluate the synchronization performance of system and synchronization error can reach 40 ns [41].

Though the model-based software design has an early start, the present development of CPSs progresses at a fast enough rate to provide a competitive challenge.

e) Researches on Reliability: Data reliability is another key factor in CPS data processing. CPS consists of a large number of embedded computing systems with computation function and need to automatically obtain real-time reliable data. S. Andrei *et al.* discussed the automatic optimization problem in designing and realizing highly reliable real-time embedded systems. He also proved, from the perspective of loosely coupled and tightly coupled system specification security assertion theory, that the optimization methods can be applied to large-scale real-time logic processing [42]. K. D. Kang *et al.* came up with a scheme to control and communicate with real-time embedded database through network function; controlled WSNs extract key data associated with the event directly from collected information to enhance the efficiency of perception [43]. But the article did not further discuss the problem of routing validity, event detection and data integration; these factors can directly affect the real-time capability of operations on real-time embedded database in this scheme.

f) Researches on Uncertainty Processing: Practical problems in CPS, such as complex environmental interference in distributed systems, wireless network transmission errors, network node failure, data preprocessing and errors introduced by storage raise problems of noise, outliers, loss of data (or properties), data dispersion, concreteness and randomness and other uncertainties, have become few of the dominant factors that influence the credibility of test information and the reliability of systems. Reference [44] analyzes the problem of non-deterministic testing data that exist in the networked test systems. M. C. Bujorianu *et al.* has established a self-learning uncertainty reasoning model in automotive control system, solving the problems of automatic sensing, rapid response and control of vehicles in multiple scenarios [45]. However, the design of external information acquisition is too ideal. It does not consider the network test environment, especially the uncertainly of information collection and the uncertainty of data in transport layer and network layer under complicated environment. Therefore, the system lacks precision in system processing and cannot guarantee the real-time capability of systems.

g) Researches on the Robustness of the System: For the energy management problem of large-scale data in CPS, [46] proposed to minimize the energy cost by optimizing the task allocation in network nodes. According to the relationship between the transmitted data in CPS network system and the estimation accuracy of corresponding data in physical world, [47] designed new data congestion control strategies, which considered the importance and the space aggregation mechanism of data packet and can effectively reduce the resulting error. In view of QoS, [48] studied the packet loss generated by network congestion, used the noise measurement in Bernoulli and Gilbert-E-lliot packet loss model CPS control system for analogy, and pointed out that if the control parameters have large deviation from actual value, the system estimation of network state will be seriously distorted. Reference [49] analyzed the influence of end-to-end delay on control performance in the collaborative design of control and scheduling, and improved the robustness of the system through end-to-end delay optimization based on resource access analysis, but this method is only suitable for cases of multiple access to the same resource. Reference [50] discussed the fault-tolerant control (FTC) problem and pointed out that increasing the redundancy of sensor and actuator in the design stage can enhance the fault tolerance performance of the network and minimize the adverse effect caused by fault. Reference [51] studied the influence of communication delay in networked control systems on application stability control. Adopting the principle "the biggest information delay is less than the discrete time control sampling period", it discussed the problem of time-varying communication delay in the feedback closed loop.

Above analysis has shown that the data processing of CPS involves the information collection and processing of physical components, information is sent through the network to the data processing center to get processed, and then feedback signals control physical components through the network. Therefore, data processing should have characteristics such as security, real-time capability, reliability and being able to deal with uncertainty. Although the existing researches study the data processing of CPS from different perspectives, the exiting results are still scarce, and there are many facets to be studied. Without overall processing methods, they are unable to meet the basic requirements of large-scale, complex CPS data processing.

2) Problem of Control:

Using the event model to deal with the problem of control plays a key role in the CPS study. But the existing event model is based on individuals, which cannot meet the demands of CPS control. From the view of the traditional control theory, V. K. Singh *et al.* used the formal integration to solve the problem of multi-module and intelligent control in a dynamic environment [52]. It provides a new way for the utilization of CPS event model processing control system. J. L. Ny *et al.* studied the robustness analysis validation in a network control system, and put forward a standard analytic method based on the input and output analysis of the robust control and described its characteristics by integral quadratic constraint [53]. Reference [54] came up with the method of transforming hybrid system into abstract and finite discrete system by using hybrid automata, so that the security and reliability of system can be verified through model checking technology applicable to discrete systems. But if excessive estimation (over approximating) method is adopted in the transformation process, part of the property of the system might be lost. Reference [55] put forward that, for any differential equation model that describes the physical system, when the assumption of specific stability holds true, an approximate equivalent finite state abstraction can be constructed. This theory builds a bridge between differential equation model in the field of control and the finite state machine model in computational domain, but this paper only considers the control algorithms and the design of software, so many other problems still need to be solved for CPS. Reference [56] is shown using several design examples that a holistic cyber-physical design approach is more suitable for such complex design problem. They model $J = \int_0^\infty [u(t)^2 + y(t)^2 y(t)]dt$ where $u(t)$ and $y(t)$ are the system's input and output respectively. There are two main aspects in such design methodology: a) joint control/architecture design or co-design; b) exploiting special properties of control application in the design process. Design examples demonstrate significant improvement in overall design.

From the studies above, it is not difficult to find that the CPS control system are facing huge challenges because of the heterogeneity of CPS physical system and the complexity, coverage and other restrictions of network system. The real-time transmission and response of feedback control are hard to achieve in current network and software system structures, which still need further researches.

C. Researches of CPS Software System

One important problem in CPS is developing a new generation of abstract, strategic and mechanism-enhanced software system, which provides flexible configuration strategy and controls the interaction of the network components and physical components according to relevant constraints.

1) Researches on Software Architecture: Because of the interactivity of CPS internal components and the extensive distribution, particular field, heterogeneity and rich semantic expression of physical system, the existing computer architectures and middleware technology will not be able to meet the needs of the development of the next generation of CPS. So we must develop new software architecture. Based on the characteristics of CPS, C. Gill gave a discussion about the problems of semantic matching and multiple physical system semantic coordination of physical systems in the development of the future operating system and middleware technology. He also provided corresponding solutions [57]. But he did not give the detail of how to do the cutting of specific semantics of special physical systems to ensure the particularity of the physical system, nor did he discuss the coordination of semantic abstraction and the real-time capability. Based on the feature oriented software development model, A. Dabholkar *et al.* puts forward a method for constructing generic middleware in CPS, which is using generic middleware to conduct seamless operations on CPS including adding, cutting and optimizing the basic needs [58]. But this article did not discuss the problems of operating characteristics and processing function in different stages of the software lifecycle.

Along with the continuous growth of the scale and complexity of CPS system, the new generation of CPS contains a large number of network embedded computing devices, and the CPS software engineering based on the network is still relatively immature. The main problem in CPS development is the low efficiency of network transmission and the software operation, which needs further research on the method of software design to improve the efficiency of the development. Woo proposed a method of software design based on the characteristics of the CPS system. It provides the method of realizing software specification, system modeling, testing and code generation, and hence improved the efficiency of software development [59]. This scheme offers brand-new ideas for the method of CPS software design.

2) Researches on Middleware Technology: Middleware can be used to save 50 % time and cost of software development. But due to the limitations of resources, quality of service and requirements of reliable CPS, generic middleware cannot meet the need of CPS application development. A basic principle of modern software technology is software reuse; therefore we can consider transforming the middleware through application-oriented designing approaches. Different distributed cyber-physical systems must process cyclic or non-cyclic event with different needs. The existing real-time processing middleware, such as the real-time processing CORBA middleware can ensure the time limit of distributed system platform, but it still lacks end time management and flexible configuration mechanism while dealing with large-scale CPS events of different cycle or non-cycle. By using generic middleware, P. A. Vicaire *et al.* designed a way to solve the problem of control and load balancing involved in the cycle or non-cycle events processing of distributed CPS [60]. It supports different requirements of periodic and non-periodic CPS events and provides a flexible software platform for distributed CPS constrained by end-to-end time.

There exists a large number of heterogeneous components in CPS, and the interaction between physical components and information components is complicated and dynamic. Therefore one of the main problems CPS is facing with is the detection of the communication efficiency of heterogeneous components. J. Lin *et al.* proposed a configurable and reusable middleware framework for hybrid real-time test, which can detect the problem of communication efficiency of heterogeneous components [61]. This method realized the real-time, dynamic and configurable detection of CPS according to different features of physical systems, providing a new way for the researches and real-time evaluation of middleware. But it does not consider the impact of some factors such as sequential variation on real-time hybrid testing system, which may bring errors in middleware testing.

3) Researches on Scheduling Algorithm: Traditional scheduling strategies cannot meet the requirements of real time CPS which have complex time semantic expression, although a variety of programming languages provide abundant time functions, but how to use these time functions to design scheduling strategy with practical awareness has become an open research problem. T. Tidwell *et al.* designed the scheduling strategy based on time optimization for a non-interrupted, random running CPS, he derived the scheduling strategy from Markov formula which is used to solve the problem of scheduling, thus improved the existing heuristic scheduling strategy [62]. Widely applied CPS which requires effective calculation and physical equipment performance optimization strategy. Aiming at predictable CPS realization and energy consumption, R. R. Rajkumar *et al.* studied the task scheduling of CPS based on feedback control, he put forward a task scheduling algorithm and validated it by examples [63]. This scheduling algorithm has reached a balance among energy consumption, scheduling robustness, etc. The demand model of computer science uses discrete mathematical description while the demand model of control theory is described by the differential equation and the behavior of the system, therefore, discreteness and continuity needs to be combined when establishing models of CPS [64]. CPS involves the problem of time synchronization while the control theory at present is event-driven, which cannot predict what will happen next. Most processing mechanisms of computer system are asynchronous, which just consider how to realize the function in modeling rather than when to implement. Therefore, CPS needs to find ways to integrate the two, otherwise the computing, communication and control capability in physical equipment cannot be realized. Reference [65] discussed in detail the application of hybrid system in CPS. Hybrid system refers to those systems in which continuous variables and discrete events exist at the same time and have mutual influence and interaction. CPS collects the information of physical world (continuous variable) and transmits those information to information world(discrete event), where information is processed and sent back to the physical world. Therefore the hybrid system is a foundation of CPS, but now there is no general model of hybrid system application. Scholars from The University of Paderborn [66] introduced UML state charts into Modelica and extended it into Modelica-statecharts for behavior modeling in continuous domain and discrete event domain, with Modelica's modeling and simulation capability on physical behavior in continuous domain, developers can conduct integrated modeling and simulation of CPS system.

4) Researches on Service Model: CPS are composed of multiple physical systems, completing specific tasks with strict real-time and physical characteristics under the control of software system. More and more embedded computations are applied to physical entities, featuring a certain degree of intellectualization. However, the validity of service combination provided by network and physical systems to complete specific tasks remains a challenge. Traditional service-oriented model and technology combination can no longer meet the needs of CPS. J. Huang *et al.* proposed an innovative physical entity — a service-oriented model to solve this problem. Based on this model, he came up with a two-level combination reasoning method to accelerate the composition reasoning process by the correlation of environmental conditions separation and physical entities; he also provided examples for validation [67].

The research on CPS software technology is still in its infancy, and is without mature software architecture. The existing researches are mostly limited to application of specific environment. The scale of CPS is not considered and also not systematic. Currently, there is no measure associated with calculation error and control theory error, issues such as the design of Church-Turing thesis, the core idea of the algorithm, programming language semantics, and the basic functional expression of uncertainty conversion system should be reconsidered and designed. Therefore, we need to design new programming languages and computation models to meet the requirements of complex, large-scale CPS, and effectively integrate and associate programming languages with semantic models and performance models. It depends on the hardware platform for CPS software to run, so we can add coupling on the basis of control measures to increase the physical network system and integrated plant patterns in the system model, analyze the results of circular software processing, and control the dynamic scheduling system jitter. Meanwhile, programs developed by mainstream programming language can be used, based on their accuracy and time-invariance to operations, to develop and design the "vertical integration" framework of CPS (the modeling, analysis, planning, communications, operating systems, networks, etc.), providing a comprehensive design and implementation of the CPS through integration of a variety of techniques.

On the basis of these, some researchers conduct model based software design for CPSs in the following aspects: event model, physical model, reliability and real-time assurance, etc.

D. Researches on CPS System Security

The existing Internet cannot meet future requirements of CPS for security and privacy protection. Traditional Internet security technology seldom considers the security of physical system in CPS (such as randomly distributed sensor network, ubiquitous wireless network, etc.), so the existing network monitoring measures and defense technologies are facing CPS with more complex structure, and we need to establish a CPS security framework combining control and information. Meanwhile, our country still lacks systematic research of problems such as sensitivity of information and privacy protection, transaction security, information system security, security certification and audit, trust mechanism, etc. Future cyber-physical system will become a critical part of national infrastructure and the risk will be higher. To get more information, control end users and assembling nodes in an open and interconnected network might infinitely magnify the impact of errors or malicious behavior and bring harm to CPS, which necessitate researches on CPS security.

1) Security Architecture: Factors such as the feedback between network and physical environment, distributed management and control, uncertainty, real-time demand and geographic distribution must be considered in CPS security design. C. Neuman addressed in his article about considering modeling security, security of sensors and actuators, system architecture and application security while designing CPS [68]. He also gave the design method of integrating security into the core of system, which is more comprehensive, but he failed to give the corresponding development tools due to the limitation of operation system, network and middleware technology. N. Adam discussed in his article the challenges CPS security is currently facing, including the lack of mature verification and validation technology, lack of mechanisms to meet real-time, reliability and security requirements, lack of awareness of CPS risks, no irrelevant safety performance indicators and insufficient knowledge in size and complexity of CPS. He also gave suggestions such as establishing security policy and creating frameworks with safe interface to enhance the security of homemade system dynamic behaviors [69]. In this article, a new technology is used to enable the network self-configuring and self-healing capabilities and provided appropriate feedback mechanisms. Cyber-physical systems are the integration of computing and physical processes. Flow of information is the main characteristic of CPS which involves multiple heterogeneous physical systems. H. Tang proposed a model for safe processing of information flow and validated it by combining it with the flexible AC transmission systems in power system [70]. Tests have proven that the model can ensure the security of information flow and can be used to analyze the flow of current information security; it provides a reference on security design for future CPS. However, since it only involves part of the security incidents, there are still some security vulnerabilities that are not taken into account.

2) Security Control: Y. Tan *et al.* summarized the safety control problem in CPS, described the message integrity, availability and confidentiality issues related to CPS [71]. He abstracted CPS into two parts, physical systems and control, and studied the deceptive attack and Dos attack in the process of information transfer between these two parts. He analyzed the limitation of existing active defense and passive response mechanism in dealing with the information security of CPS, and problems of automatic control theory in CPS safety control, such as the problem of traditional filter in predicting the status for network with uncertain packet loss. He also elaborated the challenges and directions in CPS safety control research through applying game theory in studying intrusion detection model and designing new active/passive algorithm for intrusion against system. Reference [72] described the concept of passivity based on control theory, realized the elastic control of system under malicious attacks, and came up with some suggestions regarding how to reduce the complexity and improve the accuracy of analysis. Reference [73] safely restrained code execution time by combining static analysis with the worst-case execution time (WCET), while system fault instructions would be provided if the execution time exceeds limit. Reference [74] studied the safety control problem in CPS and analyzed the feasibility of applying methods in the field of information security and control theory to CPS.

3) Attack Defense: R. A. Thacker *et al.* analyzed CPS system security threats and the consequences of attacks, he pointed out the differences between the unique nature of CPS and traditional IT security, and established security mechanisms that are suitable for CPS including prevention, detection, recovery, dynamic guard against attacks [75], but specific methods were not mentioned. T. L. Crenshaw *et al.* put forward a component-based programmable multi-node attack system and established UPBOT test platform which can be effectively used for tests of CPS security threats and defense [76]. However, due to limitations of physical scope, the program applies only to local tests, and did not give a solution to the problem of real-time capability.

Current CPS security researches mainly adopt existing Internet security policies, such as key management technology and integrity verification, etc. However, because of the particularity of CPS, present researches cannot meet the requirements of CPS on real-time capability, reliability and safety, therefore, further and deeper researches are still necessary.

E. Researches on CPS System Testbeds

Reference [77] proposed an idea of complete experimental platform. The whole process can be conducted with simple CPS tools, from the designing of abstract model to the implementation of specific system. According to the environment set and the forming of final experimental products, all this can be achieved through simulation and modeling on the flexible hardware platform of CPS. For the depth calculation-physical fusion in CPS and the application demand of lunar rover system, a typical example of CPS, [78] designed a CPS-based architecture of the lunar rover. In the Rhapsody environment, it builds the static structure diagram and the dynamic behavior diagram of the system, imported the system physical continuous dynamic model established by Simulink into lunar rover unified modeling language (UML) model using the model conversion technology, realized the real-time Simulation and modeling of the fusion of computing entity and physical entity in CPS. Reference [79] used a variety of improved human-computer interaction system and complex system simulation platform, adopted MacroLab as the basis for CPS programming and verification environment and has reached satisfying result of experiment. Reference [80] studied the real-time modeling of direct load control in information physical power system, and put forward a kind of electrical load automatic real-time scheduling technology on the basis of modeling to balance the consumption of power and to optimize the upper bound of power load peak. But the present system testbeds are still in the primary stage, with unperfected comparison and many other problems, which need further research.

IV. Challenges

The main obstacle of developing CPS is the lack of a unified theoretical framework of network and physical resources. Significant differences, both technically and culturally, exist between computer science theory and control theory, which almost extend to all the areas of computer and physical systems. The designing methods of computer systems and physical systems simply assume that the systems established are limited within a certain range [81]. On the one hand, computer scientists and engineers do not know how to transform physical system requirements such as stability, calculation performance and power consumption. On the other hand, control and signal theory largely abstracts computer as precise digital devices [82], this simplification ignores many important aspects of computation principle, for example, the time difference increases because of the software error rate caused by cache, energy management and increasing complexity. This assumption is also applied in communication, the communication channel of most CPS are originally designed to be without lost and delay, they are also assumed to be low-energy, shared and fast switching systems in wireless networks [83]. Future CPS standard must solve problems such as noise in measurement, collection inaccuracy, environmental interference and failures in unified framework calculation process. Therefore, it is crucial in CPS development to establish models easy to abstract so that the complexity of designing can be reduced, and at the same time, maintain the essence of abstracted issue. Theories including Shannon theorem, infinite horizon linear time-invariant, robust control theory and general equilibrium theory are involved. The main problems in current CPS design include scale, robustness, performance matching, etc. The specific challenges include:

1) Pattern Abstraction: Existing programming languages still lack temporal semantics, appropriate concurrency model and hardware abstraction [84]; the temporality of network protocols becomes a key issue; the changes of system theory requires the integration of the physical system theories including control systems, signal processing and the computing system theories including complexity, scheduling, computation [85]. The key point is the synchronized implementation of spatial and temporal theory in the computer systems. Thereby, the collaborative interference and control of the state of physical process are achieved through embedded computer communication networks. Currently, as for the system abstraction, the bottom-up change of computer construction is one of the feasible approaches, which provides accurate real-time capability [86]. It includes replacing the cache with the scratchpad memory buffer [87], developing temporal semantic described programming languages [88], choosing appropriate concurrency models for the static analysis [89], developing concurrent and real-time software components [90], providing new technical means so that networks can offer highly precise time synchronization, etc [91]. Another possibility is a top-down design method based on modeling [92], using models to replace the specific programming language to express the behavior of the system; it is rich in semantic space which can be used to describe the dynamic timing of the physical world [93]. But currently both of these methods are immature yet.

2) Scale and Efficiency: Large-scale, densely deployed sensors can cover a large range of areas, providing high-quality monitoring and control of event detection, and establishing real-time prediction in large-scale integrated physical modules network systems [94]. Normally, the application is not interested in the sensor reading, but the function of sensor reading on the basis of calculation and to further locate the target. However, these embedded computers are limited by energy. To save energy, computation and communication capabilities are limited,and, accordingly, the effectiveness of energy management becomes a key factor. So it is imperative to solve the scale and efficiency of information processing. The studies of information processing efficiency should focus on finding out the methods to perform calculation at least cost of energy, communication links, energy storage and resource of processors, to realize a slow growth of resources consumption, or even do not add energy consumption to digital sensors' reading and processing or embedded computer nodes. We can design distributed algorithms for sensor data to reduce the demand for and the use of resources, and also collaboratively design distributed data processing algorithms for sensors and resource management plans for distributed network computing systems accordingly.

3) Robustness: Security attacks in uncertain environment and errors in physical devices and wireless communications hugely threat the robustness and security of overall system [95].

Reference [96] presents a design methodology for robust cyber-physical systems based on a notion of robustness for CPS termed input-output dynamical stability. It captures two intuitive aims of a robust design: bounded disturbances have bounded consequences and the effect of sporadic disturbances disappears as time progresses. They modeled $o(\xi_t) \leq \max_{t' \in [0;t]}\{1.4 I_d(\xi_t) - 1.4(t - t')\} + \max_{t' \in [0;t]} \frac{1}{\acute{\beta} - 0.8}(\acute{\beta})^{t-t'} \left|\pi_{u_c^d}(V_{\acute{a}})\right| + 0.3$.

This model demonstrates nicely how results enable to separate the design procedure to establish robustness with respect to continuous and discrete disturbances. CPS contains a large number of dynamic environments, so we should establish a prototype model of CPS and a series of effective and consistent measuring standards. It is also necessary to build highly reliable dynamic configuration CPS and organize interoperable aggregation systems to capture the uncertainty, errors, failures and security attacks and to collaboratively detect and manage system interfaces, thereby avoiding cascading failure [97]. Although random hardware failures can be handled by methods such as improved circuit design, redundancy and fault-tolerant processing, the increasing complexity of sub-micron semiconductor devices and multi-core microprocessor brings new challenges [98]. The challenging intermittent errors ranging from milliseconds to several seconds will frequently appear in next generation multi-processor chips. In physical systems, it is feedback control theory which provides basic functions that ensure the robustness and stability of problems such as uncertain environments, sensing and error control. In existing open-loop software systems a small mistake may cascade to the entire system failure, thus close-loop must be adopted in CPS. In order to overcome errors in network and physical systems, it is necessary to establish a reconstructed robust system capable of handling uncertainties at the network level and a topological structure containing uncertainties which is able to flexibly respond to mass uncertain or low-credibility data.

In short, the core issue of CPS researches lies in how to manage the complex dynamic interaction between network systems and physical systems, which involves a series of problems including abstraction of real-time system, system robustness, component service quality and knowledge engineering. The existing technology cannot fully meet the demand of CPS, it still needs quite a long time for further exploration and research on CPS to become practical.

V. Applications

The developments of modern economy require expanding computation technology to the whole human existence and activities, cyber and information the human physical world, and realize the integration and unity of physical world and information system.

The rapid development of the Internet are expected to be used to interconnect a variety of devices so that we can process information rapidly and efficiently and at the same time, correspondingly control the physical world according to the result of processing. As a natural extension of networking computing, ubiquitous computing realized the demands for information acquisition and processing at any time or place and in any way. Internet of things (IOT) emphasizes the interconnection and information exchange of all kinds of items through the sensing equipment attached to them by techniques such as RFID and 802.15.4, so that the original people-people interaction Internet can be transformed into a wider content-content connection network. The core technology of IOT is mainly ubiquitous network and ubiquitous computing. CPS tightly combines the computation space and the physical world together, it covers IOT because it also has the function of control in addition to basic perception function.

CPS have wide and extensive range of application field which mainly include aerospace equipment, highly credible medical devices and systems, manufacturing, traffic control, environmental control, control of critical infrastructure (electricity, irrigation networks, communication systems), industrial production data collection automation, automated process control, energy consumption and regeneration, the next generation power grid , future defense systems, distributed robotics, civil infrastructure, etc. Along with the continuous development and improvement of science and engineering, it is expected to further develop the potential of cyber-physical systems in areas such as interventions (collision avoidance), precision (robotic surgery and nano-scale manufacturing), data mining (data classification, evaluation, predicted aggregation, etc.), dangerous or inaccessible operating environments (search and rescue, firefighting, and deep-sea exploration), coordination (air traffic control, war), efficiency (zero net energy buildings), etc [99].

CPS can also bring great social and economic benefits. Many developed industrial countries, represented by the United States and European Union, have already turned their attention to the research of CPS and provided enormous investment [100]. U. S. National Science Foundation (NSF) has identified CPS as a significant area of research and has sponsored consecutive CPS seminars with other federal agencies since the end of 2006.

U. S. congress required the academy of sciences to assess the U. S. technical competence and to give advice on maintaining and improving. 5 months later, a report based on this research named “Standing on the Storm” came out, and on this basis, The “U. S. Competitiveness Plan” was released in February 2006 and listed CPS as important research project. In July 2007, U. S. President’s Council of Advisors on Science and Technology (PCAST) listed eight key information technologies with CPS ranking the first in its report “Leadership Under Challenge — Information Technology R & D in a Competitive World” [101]. The rest are software, data, data storage and data flow, network, high-end computing, network and information security, human-machine interface and network information technology and social science. EU plans to invest 5.4 billion Euros (over 7 billion U. S. dollars) in Advanced Research & Technology for Embedded Intelligence and Systems (ARTMEIS) and expect to take the world leading position in intelligent electronic systems in 2016. In China, CPS research is fully considered in the “Twelfth Five-Year Plan for Scientific and Technological Research”. The declaration guide of “National High Technology Research and Development Program (863 Program)” listed “system platform for information-physical integration” as key supporting project in the field of information technology.

VI. Conclusion

CPS will cover various aspect of social and economic life, bring wide influence and lead the comprehensive development of computer science as well as other subjects. However, limited by the existing theory and technology of computation, communications and control technology, the development of CPS is also facing big challenges. Breakthrough in CPS key technology will enable our country take the world’s leading position in CPS development so that we can independently set our own standard and to push the national social and economic development.

References

[1] Z. Song, Y. Q. Chen, C. R. Sastry, and N. C. Tas, *Optimal Observation for Cyber-Physical Systems: A Fisher-Information-Matrix-Based Approach*. London: Springer-Verlag, 2009.

[2] R. Rajkumar, "A cyber-physical future," *Proc. IEEEE*, vol. 100, no. Special Centennial Issue, pp. 1309−1312, May 2012.

[3] C. Tricaud and Y. Q. Chen, "Optimal mobile actuator/sensor network motion strategy for parameter estimation in a class of cyber physical systems," in *Proc. 2009 American Control Conf.*, St. Louis, MO, 2009, pp. 367−372.

[4] E. A. Lee, "Computing foundations and practice for cyber-physical systems: a preliminary report," Tech. Rep. UCB/EECS-2007-72, University of California, Berkeley, May 2007.

[5] J. F. He, "Cyber-physical systems," *Commun. China Comput. Feder.*, vol. 6, no. 1, pp. 25−29, 2010.

[6] G. R. Gonzalez, M. M. Organero, and C. D. Kloos, "Early infrastructure of an internet of things in spaces for learning," in *Proc. 8th IEEE Int. Conf. Advanced Learning Technologies*, Santander, Cantabria, 2008, pp. 381−383.

[7] Y. Sun, B. McMillin, X. Q. Liu, and D. Cape, "Verifying noninterference in a cyber-physical system the advanced electric power grid," in *Proc. 7th Int. Conf. Quality Software*, Portland, OR, 2007, pp. 363−369.

[8] M. D. Ilic, L. Xie, U. A. Khan, and J. M. F. Moura, "Modeling of future cyber-physical energy systems for distributed sensing and control," *IEEE Trans. Syst. Man Cybernet. A: Syst. Human.*, vol. 40, no. 4, pp. 825−838, Jul. 2010.

[9] F. M. Zhang, K. Szwaykowska, W. Wolf, and V. Mooney, "Task scheduling for control oriented requirements for cyber-physical systems," in *Proc. 2008 Real-time Systems Symp.*, Barcelona, 2008, pp. 47−56.

[10] P. L. Tan, J. Shu, and Z. H. Wu, "An architecture for cyber-physical systems," *J. Comput. Res. Dev.*, vol. 47, no. Suppl., pp. 312−316, Nov. 2010.

[11] Y. F. Zhang, C. Gill, and C. Y. Lu, "Reconfigurable real-time middleware for distributed cyber-physical systems with aperiodic events," in *Proc. 28th International Conf. Distributed Computing Systems*, Beijing, China, 2008, pp. 581−588.

[12] D. Faggioli, M. Bertogna, and F. Checconi, "Sporadic server revisited," in *Proc. 2010 ACM Symp. Applied Computing*, Sierre, Switzerland, 2010, pp. 340−345.

[13] Y. Tan, S. Goddard, and L. C. Pérez, "A prototype architecture for cyber-physical systems," *ACM SIGBED Rev.*, vol. 5, no. 1, Article No. 26, Jan. 2008.

[14] T. L. Crenshaw, E. Gunter, C. L. Robinson, L. Sha, and P. R. Kumar, "The simplex reference model: limiting fault-propagation due to unreliable components in cyber-physical system architectures," in *Proc. 28th IEEE Int. Real-Time Systems Symp.*, Tucson, AZ, 2007, pp. 400−412.

[15] K. J. Lin and M. Panahi, "A real-time service-oriented framework to support sustainable cyber-physical systems," in *Proc. 8th IEEE Int. Conf. Industrial Informatics*, Osaka, 2010, pp. 15−21.

[16] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Auto. Control*, vol. 58, no. 11, pp. 2715−2729, Nov. 2013.

[17] B. Stasonis, "Introducing the LXI specification — intent & benefits," in *Proc. of International Conference on Distributed Computing Systems (ICDCS)*, Piscataway, 2011, pp. 1−18.

[18] R. A. Thacker, K. R. Jones, C. J. Myers, and H. Zheng, "Automatic abstraction for verification of cyber-physical systems," in *Pro. 1st ACM/IEEE Int. Conf. Cyber-Physical Systems*, Stockholm, Sweden, 2010, pp. 12−21.

[19] C. Qi and Y. He, "Design of data collection system based on CPS," *Comput. Syst. Appl.*, vol. 19, no. 6, pp. 5−8, Jul. 2010.

[20] Y. F. Hu, F. M. Li, and X. H. Liu, "CPS: network system framework and key technologies," *J. Comput. Res. Dev.*, vol. 47, no. Suppl., pp. 304−311, Nov. 2010.

[21] I. D. Chakeres, C. Danilov, T. R. Henderson, and J. P. Macker, "Connecting MANET multicast," in *Proc. IEEE Military Communications Conf.*, Orlando, FL, USA, 2007, pp. 1−7.

[22] C. Y. Wan, C. Y. Li, R. H. Hwang, and Y. S. Chen, "Global connectivity for mobile IPv6-based ad hoc networks," in *Proc. 19th Int. Conf. Advanced Information Networking and Applications*, Taipei, China, 2005, pp. 807−812.

[23] K. Chandran, S. Raghunathan, S. Venkatesan, and R. Prakash, "A feedback based scheme for improving TCP performance in ad-hoc wireless networks," in *Proc. 18th Int. Conf. Distributed Computing System*, Amsterdam, 1998, pp. 472−479.

[24] A. G. Neonakis and R. Tafazolli, "On the relaying capability of next-generation GSM cellular networks," *IEEE Personal Commun.*, vol. 8, no. 1, pp. 40−47, Feb. 2001.

[25] A. N. Zadeh, B. Jabbari, R. Pickhohz, and B. Vojcic, "Self-organizing packet radio ad hoc networks with overlay (SoPRANO)," *IEEE Commun. Mag.*, vol. 40, no. 6, pp. 149−157, Jun. 2012.

[26] W. Hu, C. M. Qiao, S. De, and O. Tonguz, "Integrated cellular and ad hoc relaying systems: iCAR," *IEEE J. Select. Areas Commun.*, vol. 19, no. 10, pp. 2105−2115, Oct. 2001.

[27] B. Andersson, N. Pereira, and E. Tovar, "How a cyber-physical system can efficiently obtain a snapshot of physical information even in the presence of sensor faults," in *Proc. 2008 Int. Workshop on Intelligent Solutions in Embedded Systems*, Regensburg, 2008, pp. 1−10.

[28] A. A. Cárdenas, S. Amin, and S. Sastry, "Secure control: towards survivable cyber-physical systems," in *Proc. 28th Int. Conf. Distributed Computing Systems Workshops*, Beijing, China, 2008, pp. 495−500.

[29] C. Singh and A. Sprintson, "Reliability assurance of cyber-physical power systems," in *Proc. 2010 IEEE Power and Energy Society General Meeting*, Minneapolis, MN, 2010, pp. 1−6.

[30] T. T. Gamage, B. M. McMillin, and T. P. Roth, "Enforcing information flow security properties in cyber-physical systems: a generalized framework based on compensation," in *Proc. 2010 IEEE 34th Annual Computer Software and Applications Conf. Workshops*, Seoul, 2010, pp. 158−163.

[31] Y. Zhang, I. L. Yen, F. B. Bastani, A. T. Tai, and S. Chau, "Optimal adaptive system health monitoring and diagnosis for resource constrained cyber-physical systems," in *Proc. 20th Int. Symp. Software Reliability Engineering*, Mysuru, Karnataka, 2009, pp. 51−60.

[32] Q. Y. Zhu, C. Rieger, and T. Basar, "A hierarchical security architecture for cyber-physical systems," in *Proc. 2011 4th Int. Symp. Resilient Control Systems*, Boise, ID, 2011, pp. 15−20.

[33] W. Jiang, W. H. Guo, and N. Sang, "Periodic real-time message scheduling for confidentiality-aware cyber-physical system in wireless networks," in *Proc. 5th Int. Conf. Frontier of Computer Science and Technology*, Changchun, China, 2010, pp. 355−360.

[34] F. Mueller, "Challenges for cyber-physical systems: security, timing analysis and soft error protection," in *High-Confidence Software Platforms for Cyber-Physical Systems (HCSP-CPS) Workshop*, Alexandria, Virginia, 2006.

[35] E. A. Lee, "Cyber physical systems: design challenges," in *Proc. the 11th IEEE Int. Symp. Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, Orlando, FL, 2008, pp. 363−369.

[36] U. Kremer, "Cyber-physical systems: a case for soft real-time", Accessed on: May 1, 2013. [Online]. Available: http://www.research.rutgers.edu/~uli/Sarana/documents/CPS-Uli.pdf

[37] H. Al-Omari, F. Wolff, C. Papachristou, and D. McIntyre, "Avoiding delay jitter in cyber-physical systems using one way delay variations model," in *Proc. 2009 Int. Conf. Computational Science and Engineering*, Vancouver, BC, 2009, pp. 295−302.

[38] K. Pereira, "Cyber-Physical Systems", Accessed on: Nov. 1, 2013. [Online]. Available: http://www.International.rutgers.edu/

[39] J. H. Shi, J. F. Wan, H. H. Yan, and H. Suo, "A survey of cyber-physical systems," in *Proc. 2011 Int. Conf. IEEE Wireless Communications and Signal Processing (WCSP)*, Nanjing, China, 2011.

[40] T. Tidwell, X. Y. Gao, H. M. Huang, C. Y. Lu, S. Dyke, and C. Gill, "Towards configurable real-time hybrid structural testing: a cyber-physical system approach", in *Proc. IEEE Int. Symp. ObjectComponentService-Oriented Real-Time Distributed Computing*, Tokyo, 2009, pp. 37−44.

[41] Y. Peng, Q. H. Luo, and Z. Q. Liu, "An automatic evaluation system for IEEE1588 synchronization clock unit," in *Proc. 9th Int. Conf. Electronic Measurement & Instruments*, Beijing, China, 2009, pp. 3-408−3-413.

[42] S. Andrei and A. M. K. Cheng, "Optimizing automotive cyber-physical system specifications with multi-event dependencies," in *Proc. 10th Int. Symp. Symbolic and Numeric Algorithms for Scientific Computing*, Timisoara, 2008, pp. 475−479.

[43] K. D. Kang and S. H. Son, "Real-time data services for cyber physical systems," in *Proc. 28th Int. Conf. Distributed Computing Systems Workshops*, Beijing, China, 2008, pp. 483−488.

[44] Y. Peng, Q. H. Luo, and X. Y. Peng, "Analysis of uncertain data processing methods in networking test framework," *Chin. J. Sci. Instr.*, vol. 31, no. 1, pp. 229−240, Jan. 2010.

[45] M. C. Bujorianu, M. L. Bujorianu, and H. Barringer, "A unifying specification logic for cyber-physical systems," in *Proc. 17th Mediterranean Conf. Control and Automation*, Thessaloniki, 2009, pp. 1166−1171.

[46] L. Parolini, N. Tolia, B. Sinopoli, and B. H. Krogh, "A cyber-physical systems approach to energy management in data centers," in *Proc. 1st ACM/IEEE Int. Conf. Cyber-Physical Systems*, Stockholm, Sweden, 2010, pp. 168−177.

[47] H. Ahmadi, T. F. Abdelzaher, and I. Gupta, "Congestion control for spatio-temporal data in cyber-physical systems," in *Proc. 1st ACM/IEEE Int. Conf. Cyber-Physical Systems*, Stockholm, Sweden, 2010, pp. 89−98.

[48] Z. J. Wang and L. L. Xie, "Cyber-physical systems: a survey," *Acta Automat. Sin.*, vol. 37, no. 10, pp. 1157−1166, Oct. 2011.

[49] K. J. Park, M. K. Yoon, K. Kang, and C. G. Lee, "Scheduling and control co-design under end-to-end response time constraints in cyber-physical systems," in *Proc. 2011 IEEE Conf. Computer Communications Workshops*, Shanghai, China, 2011, pp. 762−767.

[50] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and Fault-tolerant Control*. Berlin: Springer-Verlag, 2003.

[51] F. Pasqualetti, F. Dörfler, and F. Bullo, "Cyber-physical attacks in power networks: models, fundamental limitations and monitor design," in *Proc. 2011 50th IEEE Conf. Decision and Control and European Control Conf.*, Orlando, FL, USA, 2011, pp. 2195−2201.

[52] V. K. Singh and R. Jain, "Situation based control for cyber-physical environments," in *Proc. IEEE Military Communications Conf.*, Boston, MA, 2009, pp. 1−7.

[53] J. L. Ny and G. J. Pappas, "Robustness analysis for the certification of digital controller implementations," in *Proc. 1st ACM/IEEE Int. Conf. Cyber-Physical Systems*, Stockholm, Sweden, 2010, pp. 99−108.

[54] S. Bak, A. Greer, and S. Mitra, "Hybrid cyberphysical system verification with simplex using discrete abstractions," in *Proc. 2010 16th IEEE Real-Time and Embedded Technology and Applications Symp.*, Stockholm, 2010, pp. 143−152.

[55] G. Pota, A. Girard, and P. Tabuada, "Approximately bisimilar symbolic models for nonlinear control systems," *Automatica*, vol. 44, no. 10, pp. 2508−2516, Oct. 2008.

[56] D. Goswami, R. Schneider, A. Masrur, M. Lukasiewycz, S. Chakraborty, H. Voit, and A. Annaswamy, "Challenges in automotive cyber-physical systems design," in *Proc. 2012 Int. Conf. Embedded Computer Systems*, Samos, 2012, pp. 346−354.

[57] C. Gill, "Cyber-physical system software for HCMDSS," in *Proc. Joint Workshop on High Confidence Medical Devices, Software, and Systems Medical Device Plug-and-Play Interoperability*, Boston, MA, 2007, pp. 176−177.

[58] A. Dabholkar and A. Gokhale, "An approach to middleware specialization for cyber physical systems," in *Proc. 29th IEEE Int. Conf. Distributed Computing Systems Workshops*, Montreal, QC, 2009, pp. 73−79.

[59] H. Woo, J. L. Yi, J. C. Browne, A. K. Mok, E. Atkins, and F. Xie, "Design and development methodology for resilient cyber-physical systems," in *Proc. 28th Int. Conf. Distributed Computing Systems Workshops*, Beijing, China, 2008, pp. 525−528.

[60] P. A. Vicaire, E. Hoque, Z. H. Xie, and J. A. Stankovic, "Bundle: a group-based programming abstraction for cyber-physical systems," *IEEE Trans. Ind. Inform.*, vol. 8, no. 2, pp. 379−392, May 2012.

[61] J. Lin, S. Sedigh, and A. Miller, "Towards integrated simulation of cyber-physical systems: a case study on intelligent water distribution," in *Proc. 8th IEEE Int. Conf. Dependable, Autonomic and Secure Computing*, Chengdu, China, 2009, pp. 690−695.

[62] T. Tidwell, R. Glaubius, C. D. Gill, and W. D. Smart, "Optimal time utility based scheduling policy design for cyber-physical systems," Washington University, St. Louis, MO, WUCSE-2010-27, 2010.

[63] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: the next computing revolution," in *Proc. 47th Design Automation Conference*, Anaheim, California, 2010, pp. 731−736.

[64] R. F. Li, Y. Xie, R. Li, and L. Li, "Survey of cyber-physical systems," *J. Comp. Res. Dev.*, vol. 49, no. 6, pp. 1149−1161, Jun. 2012.

[65] X. D. Zhang, T. Parisini, and M. M. Polycarpou, "Adaptive fault-tolerant control of nonlinear uncertain systems: an information-based diagnostic approach," *IEEE Trans. Automat. Contr.*, vol. 49, no. 8, pp. 1259−1274, Aug. 2004.

[66] W. Schamai, U. Pohlmann, P. Fritzson, C. J. J. Paredis, P. Helle, and C. Strobel, "Execution of UML state machines using modelica," in *Proc. 3rd Int. Workshop on Equation-Based Object-Oriented Modeling Languages and Tools*, Oslo, Norway, 2010, pp. 1−10.

[67] J. Huang, F. Bastani, I. L. Yen, J. Dong, W. Zhang, F.-J. Wang, and H.-J. Hsu, "Extending service model to build an effective service composition framework for cyber-physical systems," in *Proc. 2009 IEEE Int. Conf. Service-Oriented Computing and Applications (SOCA)*, Taipei, China, 2009.

[68] C. Neuman, "Challenges in security for cyber-physical systems," DHS: S & T workshop on future directions in cyber-physical systems security. Jul. 2009.

[69] N. Adam, "Workshop on future directions in cyber-physical systems security," Report on workshop organized by Department of Homeland Security (DHS), Jan. 2010.

[70] H. Tang, "Security analysis of a cyber-physical system," M.S. thesis, University of Missouri-Rolla, Rolla, 2007.

[71] Y. Tan, M. C. Vuran, and S. Goddard, "Spatio-temporal event model for cyber-physical systems," in *Proc. 29th IEEE Int. Conf. Distributed Computing Systems Workshops*, Montreal, QC, 2009, pp. 44−50.

[72] N. Kottenstette, G. Karsai, and J. Sztipanovits, "A passivity-based framework for resilient cyber physical systems," in *Proc. 2nd Int. Symp. Resilient Control Systems*, Idaho Falls, ID, 2009, pp. 43−50.

[73] C. Zimmer, B. Bhat, F. Mueller, and S. Mohan, "Time-based intrusion detection in cyber-physical systems," in *Proc. 1st ACM/IEEE Int. Conf. Cyber-Physical Systems*, Stockholm, Sweden, 2010, pp. 109−118.

[74] S. Little, D. Walter, K. Jones, and C. Myers, "Analog/mixed-signal circuit verification using models generated from simulation traces," in *Proc. 5th Int. Symp. Automated Technology for Verification and Analysis*, Tokyo, Japan, 2007, pp. 114−128.

[75] R. A. Thacker, C. J. Myers, K. Jones, and S. R. Little, "A new verification method for embedded systems," in *Proc. IEEE Int. Conf. Computer Design*, Lake Tahoe, CA, 2009, pp. 193−200.

[76] T. L. Crenshaw and S. Beyer, "UPBOT: a testbed for cyber-physical systems," in *Proc. 3rd Int. Conf. Cyber Security Experimentation and Test*, Washington, DC, 2010, Article No. 1−8.

[77] S. Kopparty, S. V. Krishnamurthy, M. Faloutsos, and S. K. Tripathi, "Split TCP for mobile ad hoc networks," in *Proc. IEEE Global Telecommunications Conf.*, Taipei, China, 2002, pp. 138−142.

[78] X. Y. Li, Y. Y. Wang, X. S. Zhou, and D. F. Liang, "Approach for cyber-physical system simulation modeling," *J. Syst. Simul.*, vol. 26, no. 3, pp. 631−637, 2014.

[79] T. W. Hnat, T. Sookoor, P. Hooimeijer, W. Weimer, and K. Whitehouse, "MacroLab: a vector-based macroprogramming framework for cyber-physical systems," in *Proc. 6th ACM Conf. Embedded Networked Sensor Systems*, Raleigh, NC, USA, 2008, pp. 225−238.

[80] T. Facchinetti and M. L. D. Vedova, "Real-time modeling for direct load control in cyber-physical power systems," *IEEE Trans. Industr. Inf.*, vol. 7, no. 4, pp. 689−698, Nov. 2011.

[81] M. D. Illic, L. Xie, U. A. Khan, and J. M. F. Moura, "Modeling future cyber-physical energy systems," in *Proc. 2008 IEEE Power & Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century*, Pittsburgh, PA, 2008, pp. 1−9.

[82] G. Karsai and J. Sztipanovits, "Model-integrated development of cyber-physical systems," in *Proc. 6th Int. Workshop on Software Technologies for Embedded and Ubiquitous Systems*, Anacarpi, Capri Island, Italy, 2008, pp. 46−54.

[83] E. A. Lee, "Cyber physical systems: design challenges," in *Proc. 2008 11th IEEE Int. Symp. Object Oriented Real-Time Distributed Computing*, Orlando, FL, 2008, pp. 363−369.

[84] E. Geisberger and M. Broy, *Agenda CPS: Integrierte Forschungsagenda Cyber-Physical Systems*. Berlin: Springer, 2012.

[85] T. Padir, G. S. Fischer, S. Chernova, and M. A. Gennert, "A unified and integrated approach to teaching a two-course sequence in Robotics Engineering," *JRM*, vol. 23, no. 5, pp. 748−758, Oct. 2011.

[86] S. A. Edwards and E. A. Lee, "The case for the precision timed (PRET) machine," in *Proc. 44th ACM/IEEE Design Automation Conf. (DAC)*, San Diego, CA, 2007, pp. 264−265.

[87] O. Avissar, R. Barua, and D. Stewart, "An optimal memory allocation scheme for scratch-pad-based embedded systems," *ACM Trans. Embedded Comput. Syst.*, vol. 1, no. 1, pp. 6−26, Aug. 2002.

[88] T. A. Henzinger, B. Horowitz, and C. M. Kirsch, "Giotto: a time-triggered language for embedded programming," *Proc. IEEE*, vol. 91, no. 1, pp. 84−99, Jan. 2003.

[89] G. Berry, "The effectiveness of synchronous languages for the development of safety-critical systems," Tech. Rep., Esterel Technologies, 2003.

[90] E. A. Lee, S. Neuendorffer, and M. J. Wirthlin, "Actor-oriented design of embedded hardware and software systems," *J. Circuit. Syst. Comput.*, vol. 12, no. 3, pp. 231−260, Jun. 2003.

[91] S. Johannessen, "Time synchronization in a local area network," *IEEE Contr. Syst.*, vol. 24, no. 2, pp. 61−69, Apr. 2004.

[92] O. Tardieu and S. A. Edwards, "Scheduling-independent threads and exceptions in SHIM," in *Proc. 6th ACM & IEEE Int. Conf. Embedded Software*, Seoul, Korea, 2006, pp. 142−151.

[93] Y. Zhao, J. Liu, and E. A. Lee, "A programming model for time-synchronized distributed real-time systems," in *Proc. 13th IEEE Real Time and Embedded Technology and Applications Symp.*, Bellevue, USA, 2007, pp. 259−268.

[94] T. Abdelzaher, "Research challenges in distributed cyber-physical systems," in *Proc. IEEE/IFIP Int. Conf. Embedded and Ubiquitous Computing*, Shanghai, China, 2008, pp. 5.

[95] T. Ahola, P. Korpinen, J. Rakkola, T. Ramo, J. Salminen, and J. Savolainen, "Wearable FPGA based wireless sensor platform," in *Proc. 29th Annual Int. Conf. IEEE Engineering in Medicine and Biology Society*, Lyon, 2007, pp. 2288−2291.

[96] M. Rungger and P. Tabuada, "Abstracting and refining robustness for cyber-physical systems," in *Proc. 17th Int. Conf. Hybrid Systems: Computation and Control*, Berlin, Germany, 2014, pp. 223−232.

[97] K. R. Rohloff and T. Bacşar, "Deterministic and stochastic models for the detection of random constant scanning worms," *ACM Trans. Model. Comput. Simul.*, vol. 18, no. 2, Article No.8, Apr. 2008.

[98] The CPS Steering Group, "Cyber-Physical Systems Executive Summary," Accessed on: Sep. 21, 2010. [Online]. Available: http://iccps2012.cse.wustl.edu/_doc/CPS-Executive-Summary.pdf

[99] W. Wolf, "Cyber-physical systems," *Computer*, vol. 42, no. 3, pp. 88−89, Mar. 2009.

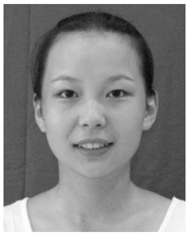
[100] W. Wayne, "The good news and the bad news," Accessed on: Jun. 9, 2010. [Online]. Available: http://www.computer.org/portal/site/computer

[101] President's Council of Advisors on Science and Technology, "Leadership under challenge: information technology R & D in a competitive world. An assessment of the federal networking and information technology R & D program," Accessed on: Aug. 30, 2011. [Online]. Available: http://ostpgov/pdf/nitrd/review.pdf

Yang Liu is an associate professor. His research interests include network information security technology, internet of things security technology, etc. He has participated in many projects of Ministry of National Information and Science Industry, and he has published over 20 academic papers in journals and conferences both in China and abroad. Corresponding author of this paper.

Yu Peng is a professor in the Department of Automatic Test and Control, Harbin Institute of Technology. His research interests include virtual instrumentation and test system, prognostics and health management, reconfigurable computing, cyber-physical system, and digital signal processing.

Bailing Wang is a professor at Harbin Institute of Technology. He received his Ph.D. degree from HIT in 2006. His research interests include information security, network security, and parallel computing.



Sirui Yao received her bachelor degree in computer science and technology from Harbin Institute of Technology in 2015. Her research interests include information security and network security.

Zihe Liu is a undergraduate at Harbin Institute of Technology. Her research interests include information security and network security.