Design Techniques and Applications of Cyberphysical Systems: A Survey

Siddhartha Kumar Khaitan, *Senior Member, IEEE*, and James D. McCalley, *Fellow, IEEE*

***Abstract*—Cyberphysical systems (CPSs) are new class of engineered systems that offer close interaction between cyber and physical components. The field of CPS has been identified as a key area of research, and CPSs are expected to play a major role in the design and development of future systems. In this paper, we survey recent advancements made in the development and applications of CPSs. We classify the existing research work based on their characteristics and identify the future challenges. We also discuss the examples of prototypes of CPSs. The aim of this survey is to enable researchers and system designers to get insights into the working and applications of CPSs and motivate them to propose novel solutions for making wide-scale adoption of CPS a tangible reality.**

***Index Terms*—Application, challenges, classification, cyberphysical systems (CPSs), design, development, review, security, survey, system of system.**

I. Introduction

SEVERAL modern computing systems feature a combination of cyber and physical systems, which are independently developed. However, the recent trends of increased performance demands and complex usage patterns have changed the dynamics and interactions of cyber and physical components in a significant manner. These changes fundamentally necessitate new design approaches where cyber and physical components are integrated at all levels [1]. This need has led to advancements in the research field of cyberphysical systems (CPSs). CPSs are defined as the systems that offer integrations of computation, networking, and physical processes [2]–[5] or, in other words, as the systems *where physical and software components are deeply intertwined, each operating on different spatial and temporal scales, exhibiting multiple and distinct behavioral modalities, and interacting with each other in a myriad of ways that change with context* [6].

Some of the defining characteristics of CPS include the following: 1) cyber capability in every physical component; 2) high degree of automation; 3) networking at multiple scales; 4) integration at multiple temporal and spatial scales; and 5) reorganizing/reconfiguring dynamics [7]. An example of CPS is seen in modern power grid. In such a system, wind farm and solar farm constitute the physical resources, and data are collected from the sensors of these resources, which constitute the cyber part of the system. Often, a communication channel is involved to transmit data that are used to monitor and control the physical resources. On the cyber side, computations are carried out with the objective of maximizing utilization of renewable sources, and a suitable decision is taken, based on which the physical resources are further controlled. Another example is the body sensor network, which is a network of medical devices that can sense, actuate, and communicate with each other through a wireless network. An aircraft can be also seen as a CPS whose smart sensors and networking system enable it to monitor its operation while coordinating with ground stations. Thus, CPSs range from miniscule such as pacemakers to large scale such as power grid.

Due to the close interaction between cyber and physical worlds, several challenges exist in the design of CPSs. To enable seamless integration, the events in the physical world need to be reflected in the cyber world, and the decision taken by the cyber world needs to be communicated to the physical world. Both these actions need to be accurately performed and in a timely manner. Thus, CPSs need to coordinate between heterogeneous systems, which consist of computing devices and distributed sensors and actuators. The sensors and actuators provide an interface between the physical and cyber worlds, and to adapt to the time-varying physical and cyber context, effective policies are required. Thus, the study and design of CPSs are extremely important.

In this paper, we survey several recent works in the field of CPSs. We classify the developmental efforts based on their characteristics and identify the future challenges in the development of CPSs. We discuss applications of CPSs, along with the examples of existing CPS prototypes. Since it is not possible to cover all the aspects of CPSs in a paper of this length, we review few works from different aspects of CPS and focus on their key ideas. We also discuss how different real-world systems are modeled as CPSs. This survey aims to help system developers in gaining insights into the frontiers of CPSs and encourage them to propose further design innovations to continuously push these frontiers forward.

The rest of this paper is organized as follows. Section II presents an overview of the advancements in CPS and presents a classification of the works based on the areas. In Sections III–V, we review some research works from these areas. Section VI identifies future challenges in the design of CPSs. Finally, Section VII concludes this paper.

II. Overview and Classification

Modern CPSs vary in their characteristics, applications, and levels of operations. To address these diverse requirements, several researchers have proposed different methods and design

Manuscript received December 19, 2012; revised May 17, 2013 and April 28, 2014; accepted May 3, 2014.

The authors are with the Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011 USA (e-mail: skhaitan@iastate.edu; jdm@iastate.edu).

Digital Object Identifier 10.1109/JSYST.2014.2322503

TABLE I
CLASSIFICATION OF CPSs

Classification	References
Design	
Architecture and Modeling	[8–78]
Simulator/Simulation	[79–87]
Tools/Programming Framework	[88–90]
Verification	[59, 91–97]
Aspects/Issues	
Security	[56, 87, 98–129]
Resiliency	[130–138]
Reliability	[139–147]
QoS	[148–153]
Real-time requirements	[64, 154–158]
Applications	
Vehicular systems and transportation	[45, 54, 84, 159–168]
Medical and health-care systems	[95, 114, 169–181]
Smart homes and buildings	[182–195]
Social network and gaming	[41, 196–202]
Scheduling	[57, 164, 203–207]
Power/Thermal management	[208–215]
Cloud computing and data centers	[216–223]
Power Grid or Power Systems	[76, 101, 122, 129, 131, 138, 224–235]
Networking systems	[125, 153, 177, 190, 236–247]
Surveillance	[248–250]
Industrial process control	[251]
Aerospace and air-traffic management	[252–256]
Search engines	[257]
Environmental monitoring	[258]
Civil Engineering	[185, 259]
Video processing	[162, 260]
Water-distribution	[81]
Robotics	[261]
Challenges and Roadmap	[3, 16, 170, 172, 262–268]

architecture. Here, we broadly classify these works into different categories, based on whether they deal with the design and development of CPSs or address specific issues of CPSs or discuss application of CPSs in specific domains. This classification is shown in Table I, which also shows the overall scope of this paper. Some of these works can be classified under multiple categories; however, for the sake of convenience, we classify them only in one category. In the following sections, we discuss some of these systems in more detail.

III. DESIGN OF CPSs

A CPS is a "system of systems" where complex and heterogeneous systems interact in a continuous manner, and proper regulation of it necessitates careful codesign of the overall architecture of CPSs. To address this need, researchers have proposed several modeling techniques, semantics, and programming tools for design of CPSs.

A. Architecture and Modeling of CPSs

Models provide useful abstractions of the physical reality with formal properties such as determinism. High-fidelity models are very valuable in building confidence in the physical realization of the systems. The challenges in CPS modeling arise due to the heterogeneous nature, concurrence of different physical processes, and real-time requirements. Different levels and types of abstractions are required for physical and computational components and their interactions. These abstractions differ due to the underlying physics, granularity, and details required. These stringent modeling requirements of CPSs with heterogeneous components and their interactions make the current modeling approaches, frameworks, and architectures inadequate.

In recent years, a number of modeling approaches and tools for CPSs have emerged to address the natural heterogeneity in CPS and to model application-domain-specific concepts and requirements. Researchers have used metamodeling and metaprogramming techniques; different formal semantics approaches such as denotational, axiomatic, operational, or a hybrid of these; different models to represent CPSs, such as multiagent semantic models, event-based semantic models, and actor-oriented design approach [78]; and different models of computation, such as continuous time [269], finite state machines [270], discrete events [271], and process networks [272]. These approaches together lay a theoretical foundation for representing and describing CPSs and their different aspects such as concurrence and communication. The heterogeneous nature of most CPS applications necessitates the use of heterogeneous mixtures of models of computation. In the same vein, the hybrid systems approach involves integration of continuous physical dynamics expressed with ordinary differential equations with the discrete behaviors expressed using finite automata [273]. We now briefly discuss some of the research works in CPS design.

1) Models and Frameworks: Yue *et al.* [51] proposed a modeling technique for CPSs. Their method uses the adaptive discrete event model, which incorporates the discrete event calculus (DEC). Use of DEC enables handling events of the environment while avoiding inconsistencies in the specification of the domain rules. Furthermore, to improve the adaptability of CPS application, the authors introduced abnormal reasoning set, which enables the CPS to handle unanticipated events. The authors demonstrated the usefulness of their modeling approach by object motion tracking CPS.

Tan *et al.* [11] presented an architecture for CPS, based on the temporal and spatial properties of events. The authors represented an event as a function of attribute-based, spatial, and temporal event conditions. Furthermore, using the logical operators, different types of event conditions are combined to capture composite events, which enable capturing complex relationships of CPSs. Thus, their framework allows conducting formal spatial and temporal analysis of the CPSs.

Jensen *et al.* [42] presented a model-based design methodology for CPSs. They decomposed the model-based design into ten steps and proposed an iterative design methodology. They demonstrated the effectiveness of their design approach with the example of a tunneling ball device [42], which requires close interaction of real-time embedded computing and hardware motion with high-precision sensing and actuation.

Lee [71] discussed two complementary approaches for design of CPSs. The first approach, which is called "cyberizing the physical," refers to wrapping software abstractions around physical subsystems. The second approach, which is called "physicalizing the cyber," refers to endowing software and networking components with abstractions, which are suitable for physical subsystems. As the complexity of CPSs increases, the challenges of modeling the interaction of cyber and physical systems also increase, and hence, using these approaches helps in bridging their differences for achieving more realistic modeling.

Jha *et al.* [56] discussed an approach to model a CPS with multimodal dynamics. Such a system operates in different modes, where the dynamics of each mode is well known. To ensure safety, it is important to properly switch between different modes. The authors proposed a method to synthesize the switching logic for a given intramode dynamics. The human designer can assist the synthesis process by providing initial approximations of the switching guards.

Ehyaei *et al.* [73] discussed the problem of aggregating the sensor readings in a CPS. These readings are obtained from a large number of sensors that are densely located and communicate over single broadcast domain (i.e., at any time, at most one sensor can communicate). The authors proposed an efficient method for data acquisition based on interpolation of all readings. Their method also models the dynamics of the physical system, which enables it to perform data acquisition at a time that is independent of the number of nodes.

2) Metaarchitecture and Metaprogramming: While there are several architectural and programming languages to model the properties of individual cyber or physical components in a CPS, there is a need for formal methods to specify and verify properties of heterogenous components involved in the system. Here, we summarize works that address this need.

Hang *et al.* [64] proposed techniques for enabling algorithmic synthesis of cyberphysical architectural models with real-time constraints. They utilized a metaarchitectural specification language for allowing the designers to specify the desired properties of the architectural model without requiring them to specify how to achieve them. Furthermore, they also developed an integer linear programming modulo theories solver along with a scheduling theory solver and deployed it to synthesize cyberphysical architectural models with hard real-time constraints. This system has applications in large-scale industrial designs.

Rajhans *et al.* [44] presented a metaarchitectural design methodology for facilitating design and evaluation of alternative architectures for CPSs, using Acme architectural description language [274], which extends existing architectural specification languages such as Unified Modeling Language (UML), Systems Modeling Language (SysML), and Abstract Architecture Description Language (AADL) by allowing modeling of components using formal methods such as finite state processes, labeled transition systems, and hybrid automata, using which behavior of components and systems can be formally specified and verified. Their approach allows the use of plugins to perform behavior analysis. Their work enables a unified framework for modeling both physical and cyber elements in a CPS architectural style.

Dabholkar *et al.* [40] presented an approach to systematically specialize general-purpose middleware to meet the demands of CPSs used in different domains. Their approach builds on the principles of feature-oriented software development, which employs an algebraic structure of existing middleware. By raising the level of abstraction to the level of features the middleware offers instead of focusing on source-code-level details, their approach specializes the general-purpose middleware to the needs of domain-specific CPS. Their approach uses origami matrices to model combination or sets of features provided by the components in the system, which is more expressive than binary decision matrices. This also avoids the excessive cost of development, maintenance, and testing of domain-specific CPS and promotes code reuse.

3) Semantics: Bujorianu *et al.* [61] presented a framework of a reference model for multiagent CPSs and a formal logic for expressing safety properties in CPSs. In their framework, the agents have continuous physical mobility and evolve in an uncertain physical environment, which closely models the real world. Their framework models both the human control and the automated control, thus making the model user centric.

Talcott [16] developed an event-based semantics for CPSs. She classified different events according to their characteristics, e.g., punctual versus durative and single versus stream. The author noted that using event-based semantics provides a natural way to specify components of open systems in terms of interfaces and observable behavior. Furthermore, it also provides a foundation for design, monitoring, and implementation of CPSs. Bujorianu *et al.* [77] proposed a formal approach called Hibertean formal method to provide a denotational semantics for CPSs. They combined denotational semantics with an algebraic model for physical processes to model physical causality and observability.

4) Codesign: Goswami *et al.* [57] discussed an architecture for addressing the design considerations to facilitate the interaction between control applications that run on spatially distributed processing units. By codesigning the control and communication architecture, they designed control applications and decided the communication schedule, which can work under flexible communication delay constraints.

Miller *et al.* [28] presented a codesign framework for cyberphysical device development where real devices or prototypes are connected to real-time models that simulate the interacting environment. Their framework supports hardware/software codesign to enable models of varying speed and accuracy to be implemented within an embedded processor. Using their approach, an application-specific platform for testing CPS can be automatically generated.

Zhang *et al.* [203] discussed the task scheduling problem for CPSs whose behaviors are regulated by feedback control laws. By codesigning the control law and the task scheduling algorithm, their method achieves predictable performance and power dissipation for the system where multiple inverted pendulums are controlled by a single processor.

B. Simulation of CPS

The dynamics of CPS evolve very fast, and hence, design of CPS requires handling the complexities posed by temporal variations and designing situation-specific control actions [185], [242]. Singh *et al.* [85] addressed the problem of situation-based control in cyberphysical environments using situation calculus. Their approach enables effectively handling temporal events and creating appropriate response actions.

Zhu *et al.* [86] proposed a technique for translating the analytical dynamics of a physical system into running simulation codes. The authors used a subset of the mathematics, which is used for analytical modeling as a domain-specific language for building simulation codes. The authors discussed the syntax of the core analytical modeling language, which provides constructs for modeling both simple and complex features of the physical system. The authors also discussed the steps for mapping this language to the executable code.

C. Tools and Programming Frameworks for CPSs

A number of tools and frameworks have been developed to ease correct implementations and deployments of CPS tools. One approach is synthesis: the tool converts some form of a specification of a CPS into an implementation. Martin and Egerstedt [90] discussed system tools for translating high-level CPS specification to actual execution and implementation on physical devices. To remove the gap between the high-level specification and the actual implementation, the authors formulated the specifications for CPSs in terms of motion description languages. This reduces the complexity of implementation and allows breaking the control tasks into smaller motion primitives, which can be easily interpreted by the system. Roy *et al.* [89] introduced a CPS design tool named PESSOA. PESSOA is used for synthesizing controllers for CPSs. It accepts a CPS represented in the form of a set of differential equations and automata and outputs a controller for the system that enforces the given specification up to an abstraction parameter.

Another area is to automate the deployment of CPS programs. Hnat *et al.* [88] presented a macroprogramming framework, which is called MacroLab, for programming CPS. Using MacroLab, a user writes a single program for the entire CPS, and then, the program is decomposed into a set of microprograms, which are loaded into each node. MacroLab decomposes a macroprogram in the way that is suitable for a particular deployment (i.e., hardware topology and network). It allows easy manipulation of data from sensors and actuators and has small overhead for implementation.

D. Model Checking and Verification of CPSs

A few works relate to formal methods to assert the correctness of CPS design and guarantee relevant properties. Bhave *et al.* [23] proposed a method for defining and evaluating consistency between architectural views derived from different heterogeneous models and the base architecture. They formulated the problem of consistency checking as typed graph matching problem between the connectivity graphs of the different architectural view and the base architecture of the system. Another important dimension of correctness is whether the system as a whole works correctly given that individual components at some level of granularity do. Sun *et al.* [92] used model checking to verify the correctness of composition in a power grid CPS while assuming that the individual components work correctly. Using a decomposition approach, the system is logically divided into smaller modules, which can be efficiently checked.

McMillin and Akella [96] verified confidentiality properties in CPSs. Due to the nature of CPSs, an observation about physical information flow may permit an observer to infer about possibly sensitive cyber actions. As an example, the operation of a wind turbine depends on its physical size, velocity of wind, etc., which are observable; and these properties may reveal about the cyber features of the system. To address these issues, the authors presented a methodology for information flow verification.

TABLE II
WORKS ON SECURITY, RESILIENCY, AND RELIABILITY

Threat Detection	[98, 102, 108, 116, 118, 120]
Threat Prevention	[98, 101, 104, 110]
Modeling of attack/fault/adversary	[87, 101, 106, 108, 111, 116, 121, 122, 127, 143]
Trust management	[100, 107, 109, 112, 115, 123, 124]
Assessing vulnerable component	[128, 129]

IV. ASPECTS/ISSUES OF CPSs

Several researchers present methods for addressing specific issues in CPSs, such as quality of service (QoS), security, and resiliency. Table II presents an overview of works on security, resiliency, and reliability. Note that we assume that a threat can be posed due to natural, incidental, or intentional factors. We now review some of these works.

A. Security-Related Aspects

A number of security-related aspects such as intrusion detection and prevention, privacy, anonymity, and so on need to be handled in CPSs [100]. Handling these aspects is specially challenging in the context of CPSs. For example, a multipronged attack may exploit the weaknesses of the separate components of the system, while may not individually pose a serious threat, but when combined together, may have catastrophic consequences. An example of this is the attack on a sewage treatment system in Australia, which caused thousands of liters of raw sewage to be released into local rivers and parks [275].

The problem of defining secure control and the challenges in securing CPSs are further outlined in a position paper by Cardenas *et al.* [113]. They also outlined the manner in which the developments from the fields of information security, sensor network security, and control theory can be utilized to ensure survivability of CPSs. Cardenas *et al.* [98] further discussed the possible threats and their consequences. Compared with traditional IT security, security in CPS poses challenges, since installing new software patches is not straightforward due to the time-critical and heterogeneous nature of operation of CPSs. Hence, based on the unique properties of CPSs, they proposed methods for detection, prevention, recovery, and resilience of attacks.

A number of works exist to detect and prevent intrusions and cyber attacks. As with classical attacks, there are signature-based schemes and anomaly-detection-based schemes, which are often complementary to each other. Xu *et al.* [115] discussed an efficient signature-based scheme for mobile wireless CPSs. They also tested their scheme against different types of attacks, such as black-hole attack and rushing attack, and found that their scheme is able to guard against these attacks.

Zimmer *et al.* [103] discussed a method for time-based intrusion detection in CPSs. Their work may be classified as an anomaly detection work. They utilized the timing information from static worst case execution time analysis. Using this, microtimings are determined for different parts of application code. Breach in security involves execution of unauthorized code, which can be detected by checking the bounds of these application codes.

Another fundamental approach to prevent attacks is to minimize the vulnerabilities that may lead to attacks. Mohajerani *et al.* [128] presented a method to detect the vulnerability of power systems against the cyber attacks. Their method works in iterations. It first finds the most vulnerable substation inside the grid and then finds the most critical asset inside that substation. Afterward, based on computation of risk of each asset, a security agent is placed on the most vulnerable positions. Ten *et al.* [118] proposed a framework to systematically evaluate the vulnerabilities of both physical and cyber systems of the power grid control centers. They integrated CPS attack/defense modeling with system simulation capability to quantify the potential impact of an attack.

There also exist a few works using formal modeling and methods to guarantee and verify security. Zhu and Basar [126] proposed a theoretical framework to address the security in CPSs. Their framework takes into account the interaction between cyber and physical components to design a cross-layer security model that connects the cyber security with the physical layer control system. In other words, security mitigation strategies are designed from the perspective of both controller design and cyber security defense strategies. Another work with similar ends is that of Burmester *et al.* [111], who also presented a framework for modeling the security of cyber and physical aspects of CPSs in a unified way. To depict the behavior of adversary, they considered a threat model. Furthermore, they also defined the security policies, which specify the cyber-physical features that need to be protected. Pasqualetti *et al.* [116] presented a framework to detect and identify both cyber and physical attacks in power grids. Their approach hinges on geometric control theory to allow identification of network components malfunction or false measurements caused by an omniscient adversary.

A few works take advantage of the CPS environments to make these systems more secure. Barsocchi *et al.* [107] discussed a method to generate secret keys in smart homes. In CPSs, the unpredictable and erratic nature of physical environments presents a rich source of randomness. By leveraging it, the secret key generation algorithm can be made smarter and can be used to make secure wireless sensor communication.

Another important challenge is how to securely meet the requirements of safety and real-time operation. As an example, in a car design, the doors of the car can be designed to automatically unlock if the car was involved in an accident and rolled over. This, however, also makes it easy for the intruders to open the car door without using the keys, by merely applying pressure. Sun *et al.* [102] discussed a method to detect the conflict between security and safety in CPSs. They proposed the use of extensible global language to specify the system and mechanisms to specify domain requirements, using which the conflict between different requirements can be easily detected.

B. Resiliency- and Reliability-Related Aspects

CPSs are typically expected to be available 24/7, providing correct behavior and surviving even under stressful conditions (such as natural disasters and severe weather in case of power grids).

Since several CPSs have 24/7 availability requirement, upgrading them or correcting their faults is very challenging. Xiao *et al.* [133] proposed adding a new layer, which is called "coordination layer," to CPSs. Through this, fault-tolerant schemes can be managed. Moreover, at the time of faults, coordination between critical services can be achieved.

Some works present algorithms and techniques for enhancing resilience of CPSs toward different kinds of failures. Woo *et al.* [130] presented a design methodology to make CPSs resilient toward hardware and software failures. Their approach uses principles from software engineering and feedback control laws to define a protocol for designing resilient CPSs. Using sensors and actuators, the failures in the system components can be detected, and the suitable decision can be taken. To efficiently read data obtained from many sensors, Andersson *et al.* [134] presented a scalable distributed algorithm for CPSs to transmit and receive an approximation of sensor data, instead of complete sensor data. Zhu *et al.* [138] presented a theoretical framework for control design in CPSs where the policy made at cyber level affects the design of control system at physical level and the control policy affects the decisions made at cyber level. Using this framework, resilient control of the cyber system can be connected with the robust control of the physical system.

Given the importance of power transmission in power grid CPSs, some efforts, such as vital infrastructure, networks, information and control system management (VIKING) [131], propose methods for secure and resilient power transmission and distribution system. In VIKING, the cyber part is the IT system, and the physical part is the power transmission and distribution system. For ensuring security, the authors in [131] proposed models and techniques for understanding vulnerabilities of control systems and their impact on the electric power transmission and distribution system. They also devised solutions to mitigate these vulnerabilities.

Tang *et al.* [141] conducted trustworthiness analysis of sensor networks in CPSs. Their method helps in filtering out noise from the input to CPS and find out trustworthy alarms. Their method estimates the locations of objects causing alarms, forms an object-alarm graph, and makes inferences about the trustworthiness of the system. For this purpose, they assign trustworthiness scores to different events to avoid false alarms and measure the confidence in an alarm.

C. QoS-Related Issues

Balasubramanian *et al.* [149] presented a method for QoS provisioning in cyberphysical networking systems. They proposed the use of a middleware for providing a layer that isolates the application developers from complexities of lower level programming and QoS mechanisms.

Xia *et al.* [148] discussed network design to ensure QoS in CPS. The authors showed that, using a feedback-based design in CPS, wireless sensor/actuator networks can achieve resource self-management and provide network QoS guarantees in CPS. Xia *et al.* [153] discussed network reliability issues in the design of wireless sensor and actuator networks (WSANs). In these networks, several QoS challenges, such as resource constraints, platform heterogeneity, and dynamic network topology, make it difficult to fulfill the requirements of real-time and reliable cyberphysical control. They also discussed the methods to address the problem of unreliability and packet loss in WSANs.

D. *Real-Time Requirements*

CPSs are required to handle both aperiodic and periodic events, and several of these events have hard or soft real-time requirements. For handling these events, Zhang *et al.* [156] discussed the use of configurable component middleware services for admission control and load balancing, which supports the diverse requirements of CPSs. Using the word ‘task’ to refer to a collection of ‘jobs,’ the middleware offers flexibility to dynamically choose from different load balancing strategies such as load balancing per task or load balancing per job and from different admission control policies such as admission control per task or admission control per job.

Study of challenges in the design of time-sensitive CPSs and proposing methods to ensure timeliness are the focus of some research works. Kang and Son [154] presented an approach for information services in CPSs, while ensuring timeliness and security. They integrated network-enabled real-time embedded databases with wireless sensors. The wireless sensors transmit data to the database in the vicinity, and by communicating with each other, these databases collectively detect important real-world events. To meet deadlines of real-time data services, the authors used feedback control.

Huang *et al.* [157] presented a case study to evaluate challenges in the design of cyberphysical instrument for real-time hybrid structural testing. As an example, the performance of a newly designed vibration suppression system (e.g., for earthquake or hurricane mitigation) cannot be easily validated at full scale prior to its implementation (e.g., on a large bridge), since this requires destructive testing and large cost. As a step toward addressing this challenge, the authors proposed a reusable middleware architecture within which both cyber and physical components can be flexibly integrated. Using this framework enables getting insights into real-time hybrid structural testing such as tolerance toward violations of small numbers of timing constraints and the effects of interactions between cyber and physical components on the overall system behavior.

V. Applications of CPSs

Due to their unique features, CPS design approach has been used in many domains. In what follows, we summarize a few of these applications.

TABLE III
Works on Vehicular Systems and Transportation

Data fusion in distributed CPS	[159, 163, 165]
Public transport	[160–163, 166]
Design of cyber-physical vehicles	[45, 54, 162]
Electrical vehicle charging	[164, 167]
Road monitoring	[168]

A. *Vehicular Systems and Transportation*

Modern vehicles are CPSs, which provide enhanced displays, information, and entertainment and manage the motion and energy consumption of the automotive. As shown in Table III, CPS functionality has been used in several aspects of vehicular systems.

Bhatia *et al.* [54] discussed the AUTomotive Open System ARchitecture (AUTOSAR), which provides cyber infrastructure in modern automotive platforms. Development of an automotive system involves system requirements specification, system analysis, and implementation. Of this, AUTOSAR handles the system requirements specification. AUTOSAR has different modules, which perform software component and operating system specification and provide a communication model.

Wagh *et al.* [159] discussed a method for human-centric data fusion in vehicular CPSs. They presented a design architecture that takes human factors into account while employing safety applications to assist human drivers. They proposed a data fusion algorithm to fuse multiple messages and maximize the total utility of the messages. Their approach helps in avoiding potential negative influences of cyber applications on driver such as information overload, confusion, and distraction.

For facilitating the testing of intelligent automotive models, Jha and Sukthankar [84] proposed the use of machine learning methods to learn stochastic models of human–vehicle interaction. By utilizing the existing psychological theories of human behavior, the accuracy of automotive models can be improved. The authors suggested using a combination of statistical and randomized methods for verifying automotive CPSs. As an example, for a given set of obstacles, humans do not typically function as an optimal route planner. Instead, by basing the path prediction model on egocentric features that are known to affect human steering preferences, improved prediction is obtained.

Loos *et al.* [161] presented formal verification of a distributed car control system for enhancing road safety. In this system, each car optimizes its navigation planning locally, whereas different cars coordinate their actions in a distributed way in order to minimize (avoid) collisions. For this purpose, the physical aspects of car movement are controlled using cyber technologies such as local and remote sensor data. The authors developed a formal proof system to verify that the control model satisfies its important safety objective and guarantees collision avoidance for an arbitrary number of cars driving on a street.

Smaldone *et al.* [162] presented a method to enhance the safety of bicycle drivers. Their method adds video processing and computation capabilities to the bicycle to continuously monitor the environment behind the biker. Using this, the rear-approaching vehicles can be detected, and prior to their approach, the driver can be informed for ensuring his/her safety.

TABLE IV
WORKS ON MEDICAL AND HEALTH CARE SYSTEMS

Implantable/life-support medical devices	[95, 114, 171, 173, 178, 180]
Robot-assisted operation	[174]
Development of medical application platform	[181]

Ahmadi *et al.* [45] presented a hierarchical modeling methodology for designing open CPSs. Their approach combines estimation techniques with data mining techniques to fully capture complex system behavior at different levels of abstraction. They demonstrated their approach with the example of green transportation, where the goal is to reduce vehicular fuel consumption and carbon footprint. In their method, the "system" modeled is the collection of cars that travel on different roads under different traffic conditions. The software, which performs routing optimizations, uses physical models of cars, streets, and traffic conditions to enable energy savings. They have shown that using their modeling techniques leads to significant improvement in the accuracy of fuel consumption predictions.

Yan *et al.* [49] discussed a system performance optimization model for unmanned vehicle CPS with wireless sensor network (WSN) navigation. The vehicle primarily receives signals from WSN for conducting its movements. For improving positioning accuracy, it is important to have fast communication and response of the vehicle. To address this issue, their model uses the particle swarm optimization algorithm.

Lau *et al.* [163] discussed the architecture of a system meant for facilitating public transportation. The system, named ContriSenseCloud, works on client–server model, where data are contributed and queried by the public masses. This creates interactive participatory sensor network, which allows users to collect, analyze, and share local knowledge. Based on this, the commuters can be helped to plan their bus journey based on information distilled from user-contributed data. ContriSenseCloud also allows third party developers to access anonymized user-contributed data as a web service.

B. Medical and Health Care Systems

Table IV summarizes the works on cyberphysical health care systems. Clearly, CPS functionality is very crucial in the development of medical systems.

Among medical CPSs, Medical Device Plug-and-Play (MD PnP) Interoperability initiative [169] is an example, where the aim is to provide a framework for safe interconnectivity of medical devices. Apart from developing interoperability standards, MD PnP initiative aggregates and shows clinical scenarios where interoperability can be helpful in presenting improvements over the existing practice.

Lim *et al.* [195] discussed the design of a CPS for providing health care services to people with disabilities and frail elderly people. The interactive CPS observes the motion and activities of daily living of the users. Based on this, the CPS provides the services to the user at the desired location. These services include reminding the user of crucial and important activities such as taking medicine and assistance in shopping.

TABLE V
WORKS ON SMART HOMES/BUILDINGS

Electronic equipment and HVAC control	[191–193]
Healthcare in smart homes	[186, 195]
Energy/power management in smart homes	[182, 188, 189, 194]

Huang *et al.* [178] discussed the design of a CPS for neurally controlled artificial legs. To allow the user to control the artificial leg as if it were the natural limb, it is imperative that there exists seamless integration of human neuromuscular system and computer system. However, the challenge lies in the fact that the signals recorded from leg muscles during dynamic movements are highly nonstationary. As a step toward addressing this challenge, the authors used a neural–machine interface that senses neural signals from leg amputees and, based on these, makes accurate decisions for prostheses control.

Banerjee *et al.* [177] presented a model-based engineering approach to perform design and analysis of body area networks (BANs). BANs are networks of medical devices that are implanted within or worn on the human body. The authors proposed an abstract model of CPS, which enables capturing the undesirable side effects of the medical devices (cyber) on the human body (physical). Furthermore, they also developed an analysis tool to allow specification of BANs using AADL. Their approach facilitates early stage analytical evaluation of the model to test safety and sustainability of BANs.

C. Smart Homes and Buildings

Table V provides an overview of the use of CPS in smart homes. We now discuss a few of these works.

Li *et al.* [186] discussed a smart community architecture, which is modeled as a CPS with cooperating objects, namely, networked homes. In smart homes, the sensors and actuators are configured such that they can be remotely controlled through the Internet. Through this, the activities of the users can be monitored. Smart community takes the concept of smart homes further by using networking among a group of smart homes. The individual homes are modeled as multifunctional sensors, and whenever necessary, automatic or human-controlled physical feedback is given to improve community safety, health care quality, and home security. The authors also discussed the communication and networking in the smart community.

Xia and Ma [187] modeled a smart community as convergence of social world, cyber world, and physical world. It consists of humans and smart physical entities that interact with each other. They also discussed the technical challenges in the development of a smart community, which involve ubiquitous sensing, autonomous networking, collaborative reasoning, and community management.

Kleissl and Agarwal [182] modeled modern buildings as CPSs and examined the possibility of joint optimization of energy use by its occupants and IT equipment. Their work aims at designing zero net energy buildings, i.e., buildings with zero net annual energy consumption. The authors viewed the information and communication infrastructure of the building as energy consumer and energy/operations optimizers. They studied the energy consumption of different buildings and

TABLE VI
WORKS ON SOCIAL NETWORK AND GAMING

Integrating physical inputs	[196, 199, 200]
Single-player/one-to-one	[198–200]
Multi-player/social-network	[197, 198, 201, 202]

explored the opportunity of saving electrical energy by various means such as renewable energy sources (RESs) and efficient lighting and computing.

Savvides *et al.* [189] discussed the application of CPSs in smart buildings to provide rapid access to information and autonomous interaction with the grid. The cyberphysical capabilities enable the buildings to participate in the utility markets.

D. Social Network and Gaming

As shown in Table VI, the integration of CPS functionality into social networks and entertainment can make a revolutionary impact. For example, CPS video games enhance the video games of cyber world with more physical inputs, such as those from inertial sensors. This can improve users' participation and provide better experience of realism.

Miluzzo *et al.* [197] discussed the design and implementation of "CenceMe," which enables sharing of information obtained using mobile sensors over social networks. CenceMe senses the activities of an individual user in different environments. This information can be shared using social networking portals such as Facebook. The authors conducted a user survey to assess the usefulness of CenceMe. This survey revealed that CenceMe stimulates curiosity among users and aids people in social networking. Furthermore, although there are concerns of privacy, but by allowing the user to control their privacy settings, wide-scale adoption of CenceMe can be achieved.

Wu *et al.* [200] discussed an example of CPS network where the users can practice traditional Chinese Tai-Chi over the Internet. The users wear multiple sensors on their body, and the data obtained from these sensors are shared in real time.

Wu *et al.* [202] discussed the study of distributed gaming in 3-D tele-immersive (3DTI) environments. The authors presented a conceptual framework for modeling nontechnical influences for user experience in 3DTI environments. Their study reveals how metrics such as delay and visual quality of the game, along with nontechnical factors such as age and social interaction, affect the quality of experience of game players in the cyberphysical gaming environment.

Wu *et al.* [199] discussed an example of CPS video game, which uses multiple game screens to broaden players' views and provides more realistic interaction experiences. To play this game, a user wears multiple inertial sensor nodes, which sense the orientation and motion of the user. This information is fed to the game controller, which takes suitable action.

Li and Negi [164] discussed the scheduling problem in cyberphysical network systems. Such systems find applications in wireless ad hoc networks and the coordinated electric vehicle (EV) charging in power grids. The authors solved the problem of distributed EV charging scheduling using a combination of Lyapunov optimization and Markov chain Monte Carlo sampling techniques.

TABLE VII
WORKS ON POWER AND THERMAL MANAGEMENT

Minimizing electricity cost	[219, 222]
Workload placement	[219–221]
Cyber-physical interaction based thermal/power management	[208, 217, 218]

E. Power and Thermal Management

In recent years, power consumption of all computing systems ranging from embedded systems to data centers has greatly increased [276], [277]. This trend has motivated researchers to leverage CPS principles for power and thermal management, as shown in Table VII.

A number of works propose power management approaches for multiprocessor systems on chip (MPSoCs) or 3-D multicore processors or Intel's single-chip cloud computer (SCC). For example, Puschini *et al.* [215] proposed a technique to improve performance and energy efficiency in energy- and latency-constrained MPSoCs. Their technique uses game theory to find the best frequency values for the processing elements (PEs). They modeled the PEs as players and the energy/latency optimization as the local objective function that depends on the global state of PEs. They provided different algorithms to either minimize latency or energy in a distributed manner. In contrast, the power management approach proposed for MPSoCs by Bogdan *et al.* [209] accounts for both PEs and routers. In an MPSoC, communication takes place via the network on chip, and multiple voltage and frequency islands (VFIs) exist, for which voltage and frequency (VnF) can be individually controlled. They proposed an online control approach to determine the optimal operating frequencies for both PEs and routers that belong to separate VFIs. Their technique leverages the workload variation to save energy, while aiming to meet the performance constraints subject to fractal state equations [209].

CPS approach to temperature management of 3-D multicore processor can provide real-time fine-grained control, as shown by Qian *et al.* [208]. Their technique models the heat consumption of the 3-D chip using a thermal model and uses this model to estimate future power consumption of the chip. Furthermore, their technique senses the temperature of the processor chip and adjusts the fluidic flow rate to always maintain the system temperature.

The different characteristics of the workloads running on computing systems provide scope for saving energy while maintaining performance, as shown by David *et al.* [210]. They demonstrated their approach for Intel's SCC using an image processing algorithm. The algorithm reduces the VnF for light workloads for saving energy, while maintaining high VnF for heavy workloads to improve performance. The algorithm running on a parent core first identifies the image regions that have significant information content and then sends only those regions to the remaining (children) core to reduce the computation and communication overhead.

F. Data Centers

A data center includes online applications and services for ensuring computation and communication and physical components for ensuring correct functioning; thus, a data center

TABLE VIII
WORKS ON POWER SYSTEMS

Sustainability	[227, 233]
Modeling	[8, 74, 76]
Security related aspects	[118, 128, 129, 234, 235]

can be modeled as a CPS. The complex interaction of cyber and physical components in a large-scale data center necessitate using the principles of CPS design for addressing the issues in data center management. Parolini *et al.* [216] presented a strategy for data centers to maximize the benefits from the provided quality of computational services, while keeping the energy costs for computation and cooling minimal. They modeled the data center in terms of interacting cyber and physical systems, where cyber component refers to the computational network representing the distribution and flow of computational tasks, and physical network refers to the thermal network characterizing the distribution of thermal energy.

In data centers, cyber and physical systems have close interactions, for example, work-scheduling algorithms can have marked influence on temperature distribution. Li *et al.* [218] proposed a thermal forecasting model to predict the temperatures near the servers in a data center based on continuous streams of temperature and airflow measurements. The modeling integrates physical laws and sensor observations in the data center. Their method uses the data obtained from the sensor to learn the parameters of a data center's CPS. Rao *et al.* [222] presented techniques for managing data center power consumption by exploiting server on/off and dynamic voltage and frequency scaling.

G. Electric Power Grid and Energy Systems

Table VIII presents a classification of CPS research works in the area of electric power and energy systems. The research focus areas include improving the sustainability of energy system by better resource utilization and management, modeling of complex interactions between electric grids (physical), and monitoring (cyber) infrastructure and security of the power system against cyber threats. Security-related aspects can be further classified into detection, prevention, mitigation, and restoration. Currently, most of the cyber security research in power system deals with vulnerability/attack detection and prevention. Please refer to Table II for few other works related to security in electric power grid.

An approach for improving the sustainability of the energy system using CPS theory has been provided in [227]. In this paper, an integrated electricity and transportation infrastructure for promoting the use of RESs had been discussed. They modeled the energy system as a cyberphysical energy system, where RESs, gridable vehicles (GVs), and thermal power plants constitute physical resources. An onboard system in a GV acts as a cyber resource, which communicates with utility and vehicle owner's preferences, etc., for proper function. The authors studied the effectiveness of RESs and GVs for a sustainable cyberphysical energy system. They also suggested techniques for maximizing utilization of distributed RESs to reduce emission and cost of operation.

An example for better resource utilization using CPS approach has been discussed in [74]. This work presents a dynamic model of battery to describe the variations in the capacity of a battery under time-varying discharge current. In CPSs, the current drawn from the batteries is decided by the control laws and online scheduling algorithms, according to the state of the plant and the processor. For this reason, the life of a battery cannot be determined at the design stage. Hence, using the battery model provided in [74], the optimal discharge profile for a square wave current can be determined.

An approach for modeling cyberphysical energy systems has been proposed in [8]. This approach is based on representing all physical components as modules interconnected by means of an electric network. Each component is modeled as a cyberphysical module, which is characterized by both physical and cyber input–output signals, internal dynamics, local sensing, and actuation. Based on this, the modular components are integrated according to the network constraints.

The major challenges with the CPS modeling for power system are developing common terminologies and semantics for describing the interactions between cyber and physical components, interoperability of various components developed in different engineering domains, and development of standards for integrated modeling of cyber and physical systems.

The white paper on CPS security for smart grid [278] identifies a set of cyber security challenges at various levels, such as information-level security, infrastructure-level security, and application-level security. In this white paper, the research issues in modeling, detection and prevention algorithms, trust management, and attack attributions have been outlined.

Power system application-level cyber security has been discussed in [235]. This work addresses the issue of power system security by taking into account the coupling between power control applications and cyber systems. In an electric grid, cyber vulnerabilities may occur due to improper privileges and access controls, weak firewall rules, cryptographic issues, lack of input validation, and so on. After identifying these, the physical impact of attack on power applications can be determined using transient and steady-state simulations. Based on this, the risk mitigation steps can be determined.

Infrastructure-level security in wide-area monitoring systems using a flocking-theory-based model for communication routing strategies has been proposed in [76]. For the case of denial-of-service attacks on communications infrastructure, their model helps in developing effective routing strategies to promote the transient stabilization of faulted power systems. Hong *et al.* [234] proposed an integrated anomaly detection approach for cyberphysical power system, which contains network-based and host-based anomaly detection systems for the substations and simultaneous anomaly detection for multiple substations. The host-based anomaly detection considers temporal anomalies in the substation facilities, and the network-based anomaly detection considers malicious behaviors of substation automation based on the network messages.

Information-level security issues at the control center for malicious data attacks have been studied in [129]. A graph theoretic approach has been used to identify the smallest set of vulnerable meters in a power system, which, when attacked, lead to network unobservability. They studied both adversarial schemes and countermeasures at the control center for malicious data attacks.

H. Networking Systems

In several CPSs, camera-equipped portable devices are used to capture, send, and receive real-time videos for CPS; however, it also requires them to have ubiquitous broadband network access. Xing *et al.* [239] presented a network architecture for supporting video communication between third-generation (3G) phones and Internet hosts in CPSs. The architecture proposed by them is useful for supporting several CPSs that require video-based information collection and sharing.

Xue *et al.* [244] presented a technique to minimize network-wide energy consumption for real-time applications in wireless CPSs. Their technique jointly considers the execution modes of processors and the radio sleep scheduling of wireless nodes to explore the opportunity of energy saving, while always meeting the timing and precedence constraint.

I. Surveillance

Ma *et al.* [250] discussed the design of a cyberphysical alarm system. This alarm establishes connection using the Internet through general packet radio service/code division multiple access/3G. Using the existing mobile communication network, the alarm achieves mutual communication control among terminal equipment and users. The alarm uses terminal equipment, which detects the physical world. This information is communicated to the user. In turn, the user can control and manage the physical world using the communication system of the alarm.

VI. Future Challenges and Promises

Despite the advances made in CPSs, several prominent challenges remain, which, when addressed, will enable making wide-scale adoption of CPSs a reality.

Modeling and Design: The design of CPSs is more challenging than either ‘purely’ physical or cyber systems. This is because, for example, for a purely computing (cyber) system, hardware description language or programming language is sufficient to implement desired behavior. However, for CPSs, the expected behavior of computational components needs to be specified in terms of their action on the physical environment. Thus, a unifying framework is required for modeling them, which allows easy interfacing and consistency. In addition, real-world data sets are required for testing and validating the proposed research ideas. Furthermore, the programming languages must allow inherent integration of time-based computation with event-based computation, which will enable effectively modeling asynchronous dynamics taking place at different temporal and spatial scales [5].

Since real world is concurrent, CPSs also need to be concurrent, and this aspect should be reflected right at the modeling and architectural stages. It is widely acknowledged that the mechanisms for interaction with sensor and actuator hardware are not fully represented by existing programming languages [266]. Future CPSs need to use suitable abstractions, which allow intuitive modeling of real world.

Future work needs to propose novel methods for verifying and validating both hardware and software components and the entire system, to ensure high degree of dependability and reconfigurability [268]. We envision the use of high-performance computing and sophisticated algorithms to carry out simulation, model checking, and verification of large-scale CPSs.

CPS Aspects: It is further necessary to work on the functionality, performance, security, reliability, scalability, and such other properties to enhance CPSs. With increasing integration of cyber capabilities, many systems (e.g., smart homes) are operated in new ways that were never intended when the systems were designed and built. To enable seamless integration, novel design methodologies need to be developed, which promote minimal disruption of existing system operation, while providing a rich extension of functionalities of CPSs. For example, in power systems, we expect integration of smart meters capable of two-way communication and some local memory and computations. This will allow interactive relationships to emerge between the supplier and the consumers. One of the grand challenges for CPS is to create an extensible infrastructure that will support the widest possible variety and number of sensor inputs and actuator outputs, while also providing easy access to a large number of potential users.

In computing systems, small execution time merely translates to better performance; however, in CPSs, this may be critically related to its correctness. For example, in vehicular, aerospace, and surveillance, high performance is extremely important to ensure low delay and high user satisfaction. In fact, in several CPSs, maintaining timeliness is important to avoid disastrous consequences. Fulfilling the demands of time-sensitive CPS applications will require highly efficient tools and abstractions for domain-specific analysis and synthesis tasks.

The mutual coordination and interdependence among cyber and physical components come at the price of increased vulnerability to failures and attacks. In several mission-critical CPSs, such as elderly health care systems, medical systems, networking systems, and smart power grids, security and reliability are of prime importance. Hence, future CPSs must ensure highly secure and reliable operation. Researchers need to develop self-healing architectures to enable security-state monitoring with real-time remediation. In addition, security performance metrics need to be developed to assess the security of the systems.

In several scenarios, the physical objects are not static (e.g., vehicular and air-traffic management systems), which introduces additional concerns in implementation of CPSs due to motion speed and synchronization of devices. Real-world CPSs operate at very large scale such as smart transportation system of a city. Thus, the challenges of mobility are expected to be much more significant.

CPSs such as power systems are large-sized distributed and networked systems. These CPSs must be adaptive, resilient to failures of individual components, and able to maintain an overall situation awareness that emerges from partial distributed knowledge. In such systems, achieving overall goals with local asynchronous actions presents a major challenge.

CPSs are being deployed in a much wider range of applications than ever before, and to facilitate this, a great deal of research progress is required in both theoretical foundations and application tools. In addition, using networking technologies, information collected from a wide variety of smart devices such as sensor-rich smartphones can be meaningfully utilized to further fuel the development of CPSs. Similarly, in power grid, integration of alternate energy sources will require significant changes to traditional planning and operating techniques to ensure reliability.

Applications: Specific opportunities are also present in individual CPS domains. Energy efficiency is directly related to the cost effectiveness of CPSs. In several applications, such as smart buildings and homes, data centers, and processor systems, power optimization is of vital importance. In power systems, as the demand for electricity increases, matching generation to demand will become increasingly challenging since overgeneration of power for peak demand is expensive and contributes to greenhouse gas emissions. Hence, energy efficiency is expected to be a key design constraint in future CPSs. Power systems are further seeing a change toward distributed generation (small generation facilities such as solar panels distributed throughout grid), and the integration of innovative systems such as demand-response and phasor-measurement units presents further optimization opportunities through the grid.

Smart homes would need to optimize resource usage without sacrificing human comfort. Automation of many of the currently manual tasks through integration of centralized computer controls with physical sensors and actuators will be the key. Similar developments are needed in civil engineering and environmental monitoring: how to perform the tasks of monitoring without disturbing the environment and to enable self-healing of the environment and the civil engineering systems.

VII. Conclusion

CPSs offer coordination between computational and physical resources, and thus, they are expected to play a major role in the design and development of next-generation smart grid, airplanes, space vehicles, and smart homes. In this paper, we have reviewed several research works in the design and applications of CPSs. We have discussed several cyberphysical application tools and prototypes developed in different areas. We have also identified future challenges that need to be addressed before CPSs can be widely used. We believe that the advancements made in the development of CPSs will greatly enhance their effectiveness in many important applications.

Acknowledgment

The authors would like to thank the anonymous reviewers for their constructive comments.

References

[1] H. Giese, B. Rumpe, B. Schätz, and J. Sztipanovits, "Science and engineering of cyber-physical systems (Dagstuhl Seminar 11441)," *Dagstuhl Rep.*, vol. 1, no. 11, pp. 1–22, 2012.

[2] M. Conti *et al.*, "Looking ahead in pervasive computing: Challenges and opportunities in the era of cyber-physical convergence," *Pervasive Mobile Comput.*, vol. 8, no. 1, pp. 2–21, Feb. 2012.

[3] L. Sha, S. Gopalakrishnan, X. Liu, and Q. Wang, "Cyber-physical systems: A new frontier," in *Machine Learning in Cyber Trust*. New York, NY, USA: Springer-Verlag, 2009, pp. 3–13.

[4] I. Horváth and B. Gerritsen, "Cyber-physical systems: Concepts, technologies and implementation principles," in *Proc. TMCE Symp.*, 2012, pp. 19–36.

[5] E. Lee, "Computing needs time," *Commun. ACM*, vol. 52, no. 5, pp. 70–79, May 2009.

[6] National Science Foundation (NSF), Cyber Physical Systems NSF10515, Arlington, VA, USA, 2013. [Online]. Available: http://www.nsf.gov/pubs/2010/nsf10515/nsf10515.htm

[7] L. Miclea and T. Sanislav, "About dependability in cyber-physical systems," in *Proc. EWDTS*, 2011, pp. 17–21.

[8] M. Ilic, X. Le, U. A. Khan, and J. M. F. Moura, "Modeling future cyber-physical energy systems," in *Proc. IEEE PES-GM–Convers. Del. Elect. Energy 21st Century*, 2008, pp. 1–9.

[9] M. Ilic, X. Le, U. A. Khan, and J. M. F. Moura, "Modeling of future cyber-physical energy systems for distributed sensing and control," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 40, no. 4, pp. 825–838, Jul. 2010.

[10] P. Zhao, M. G. Simoes, and S. Suryanarayanan, "A conceptual scheme for cyber-physical systems based energy management in building structures," in *Proc. IEEE/IAS Int. Conf. INDUSCON*, 2010, pp. 1–6.

[11] Y. Tan, M. Vuran, and S. Goddard, "Spatio-temporal event model for cyber-physical systems," in *Proc. IEEE ICDCS Workshops*, 2009, pp. 44–50.

[12] J. Lin, S. Sedigh, and A. Miller, "Modeling cyber-physical systems with semantic agents," in *Proc. IEEE COMPSACW*, 2010, pp. 13–18.

[13] Y. Tan *et al.*, "A concept lattice-based event model for cyber-physical systems," in *Proc. ACM/IEEE ICCPS*, 2010, pp. 50–60.

[14] P. Derler, E. A. Lee, and A. S. Vincentelli, "Modeling cyber-physical systems," *Proc. IEEE*, vol. 100, no. 1, pp. 13–28, Jan. 2012.

[15] J. Kim and D. Mosse, "Generic framework for design, modeling and simulation of cyber physical systems," *ACM SIGBED Rev.*, vol. 5, no. 1, pp. 1–2, Jan. 2008.

[16] C. Talcott, "Cyber-physical systems and events," in *Software-Intensive Systems and New Computing Paradigms*. Berlin, Germany: Springer-Verlag, 2008, pp. 101–115.

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

[18] J. Huang, F. Bastani, I.-L. Yen, and J.-J. Jeng, "Toward a smart cyber-physical space: A context-sensitive resource-explicit service model," in *Proc. IEEE COMPSAC*, 2009, vol. 2, pp. 122–127.

[19] J. Lin *et al.*, "A semantic agent framework for cyber-physical systems," in *Semantic Agent Systems*. Berlin, Germany: Springer-Verlag, 2011, pp. 189–213.

[20] J. Sztipanovits *et al.*, "Toward a science of cyber-physical system integration," *Proc. IEEE*, vol. 100, no. 1, pp. 29–44, Jan. 2012.

[21] J. Eidson, E. A. Lee, S. Matic, S. A. Seshia, and J. Zou, "A time-centric model for cyber-physical applications," in *Proc. ACES-MB*, 2010, pp. 21–35.

[22] R. West and G. Parmer, "A software architecture for next-generation cyber-physical systems," presented at the Position Paper NSF Cyber-Physical Systems Workshop, Austin, TX, USA, 2006.

[23] A. Bhave, B. Krogh, D. Garlan, and B. Schmerl, "View consistency in architectures for cyber-physical systems," in *Proc. IEEE/ACM ICCPS*, 2011, pp. 151–160.

[24] H. Abbas, G. Fainekos, S. Sankaranarayanan, and F. Ivančić, "Probabilistic temporal logic falsification of cyber-physical systems," *ACM Trans. Embedded Comput. Syst.*, vol. 12, no. 2, p. 95, May 2013.

[25] L. Ma, J. Yao, M. Xu, T. Yuan, and M. Shao, "Net-in-Net: Interaction modeling for smart community cyber-physical system," in *Proc. UIC/ATC*, 2010, pp. 250–255.

[26] M. Kim, M.-O. Stehr, and C. Talcott, "A distributed logic for networked cyber-physical systems," in *Fundamentals of Software Engineering*. Berlin, Germany: Springer-Verlag, 2012, pp. 190–205.

[27] F. Fouquet *et al.*, "A dynamic component model for cyber physical systems," in *Proc. ACM SIGSOFT Symp. Compon. Based Softw. Eng.*, 2012, pp. 135–144.

[28] B. Miller, F. Vahid, and T. Givargis, "Application-specific codesign platform generation for digital mockups in cyber-physical systems," in *Proc. ESLsyn*, 2011, pp. 1–6.

[29] Y. Tan, S. Goddard, and L. Perez, "A prototype architecture for cyber-physical systems," *ACM SIGBED Rev.*, vol. 5, no. 1, pp. 1–2, Jan. 2008.

[30] M. Gavrilescu, G. Magureanu, D. Pescaru, and A. Doboli, "Accurate modeling of physical time in asynchronous embedded sensing networks," in *Proc. SISY*, 2010, pp. 477–482.

[31] A. Sangiovanni-Vincentelli, W. Damm, and R. Passerone, "Taming Dr. Frankenstein: Contract-based design for cyber-physical systems," *Eur. J. Control*, vol. 18, no. 3, pp. 217–238, 2012.

[32] M. Sveda and R. Vrba, "A cyber-physical system design approach," in *Proc. ICONS*, 2011, pp. 12–18.

[33] G. Magureanu, G. Gavrilescu, D. Pescaru, and A. Doboli, "Towards UML modeling of cyber-physical systems: A case study for gas distribution," in *Proc. SISY*, 2010, pp. 471–476.

[34] L. Zhang and J. He, "A formal framework for aspect-oriented specification of cyber physical systems," in *Convergence and Hybrid Information Technology*. Berlin, Germany: Springer-Verlag, 2011, pp. 391–398.

[35] Y. Liu, "Toward a unified object model for cyber-physical systems," in *Proc. Workshop Softw. Eng. Sensor Netw. Appl.*, 2011, pp. 65–66.

[36] T. Paul, J. W. Kimball, M. Zawodniok, T. P. Roth, and B. McMillin, "Invariants as a unified knowledge model for cyber-physical systems," in *Proc. IEEE SOCA*, 2011, pp. 1–8.

[37] N. Saeedloei, "Logic programming foundations of cyber-physical systems," in *Proc. Tech. Commun. 26th Int. Conf. Logic Programm.*, 2010, vol. 7, pp. 289–293.

[38] A. Benveniste, "Loosely time-triggered architectures for cyber-physical systems," in *Proc. Conf. Des., Autom. Test Europe*, 2010, pp. 3–8.

[39] L. Sha and J. Meseguer, "Design of complex cyber physical systems with formalized architectural patterns," in *Software-Intensive Systems and New Computing Paradigms*. Berlin, Germany: Springer-Verlag, 2008, pp. 92–100.

[40] A. Dabholkar and A. Gokhale, "An approach to middleware specialization for cyber physical systems," in *Proc. ICDCS Workshops*, 2009, pp. 73–79.

[41] H. Zhuge, "Semantic linking through spaces for cyber-physical-socio intelligence: A methodology," *Artif. Intell.*, vol. 175, no. 5/6, pp. 988–1019, Apr. 2011.

[42] J. Jensen, D. H. Chang, and E. A. Lee, "A model-based design methodology for cyber-physical systems," in *Proc. IWCMC*, 2011, pp. 1666–1671.

[43] L. Kong, D. Jiang, and M.-Y. Wu, "Optimizing the spatio-temporal distribution of cyber-physical systems for environment abstraction," in *Proc. IEEE ICDCS*, 2010, pp. 179–188.

[44] A. Rajhans *et al.*, "An architectural approach to the design and analysis of cyber-physical systems," *Electron. Commun. EASST*, vol. 21, 2009.

[45] H. Ahmadi, T. Abdelzaher, J. Han, N. Pham, and R. K. Ganti, "The sparse regression cube: A reliable modeling technique for open cyber-physical systems," in *Proc. IEEE/ACM ICCPS*, 2011, pp. 87–96.

[46] M. Kim *et al.*, "A semantic framework for reconfiguration of instrumented cyber physical spaces," presented at the Workshop Event-Based Semantics, CPS Week, St. Louis, MO, USA, 2008.

[47] K. Fujinami, T. Yamabe, and T. Nakajima, "Take me with you!: A case study of context-aware application integrating cyber and physical spaces," in *Proc. ACM Symp. Appl. Comput.*, 2004, pp. 1607–1614.

[48] J. Sztipanovits, "Model integration and cyber physical systems: A semantics perspective," in *Proc. Int. Conf. Formal Methods*, 2011, p. 1.

[49] H. Yan, J. F. Wan, and H. Suo, "Adaptive resource management for cyber-physical systems," *Appl. Mech. Mater.*, vol. 157/158, pp. 747–751, Feb. 2012.

[50] A. Bhave, B. Krogh, D. Garlan, and B. Schmerl, "Multi-domain modeling of cyber-physical systems using architectural views," in *Proc. AVICPS*, San Diego, CA, USA, 2010, p. 43.

[51] K. Yue, L. Wang, S. Ren, X. Mao, and X. Li, "An adaptive discrete event model for cyber-physical system," in *Proc. Anal. Virtual Integr. Cyber-Phys. Syst. Workshop*, 2010, pp. 9–15.

[52] D. D. Hoang, H.-Y. Paik, and C.-K. Kim, "Service-oriented middleware architectures for cyber-physical systems," *Int. J. Comput. Sci. Netw. Security*, vol. 12, no. 1, pp. 79–87, Jan. 2012.

[53] A. Rowe and R. Rajkumar, "A model-based design approach for wireless sensor-actuator networks," in *Proc. AVICPS*, 2010, pp. 1–8.

[54] G. Bhatia, K. Lakshmanan, and R. Rajkumar, "An end-to-end integration framework for automotive cyber-physical systems using sysweaver," in *Proc. AVICPS*, 2010, p. 23.

[55] R. Balani *et al.*, "Programming support for distributed optimization and control in cyber-physical systems," in *Proc. IEEE/ACM ICCPS*, 2011, pp. 109–118.

[56] S. Jha, S. Gulwani, S. A. Seshia, and A. Tiwari, "Synthesizing switching logic for safety and dwell-time requirements," in *Proc. IEEE/ACM ICCPS*, 2010, pp. 22–31.

[57] D. Goswami, R. Schneider, and S. Chakraborty, "Co-design of cyber-physical systems via controllers with flexible delay constraints," in *Proc. ASPDAC*, 2011, pp. 225–230.

[58] D. Cofer *et al.*, "Complexity-reducing design patterns for cyber-physical systems," Air Force Res. Lab., Wright-Patterson Air Force Base, OH, USA, Tech. Rep. AFRL-RZ-WP-TR-2011-2098, 2011.

[59] N. Saeedloei, "Modeling and verification of real-time and cyber-physical systems," Ph.D. dissertation, Univ. Texas Dallas, Richardson, TX, USA, 2011.

[60] P. Anders, "Cybrid principles: Guidelines for merging physical and cyber spaces," *Int. J. Architectural Comput.*, vol. 3, no. 3, pp. 391–406, Nov. 2005.

[61] M. Bujorianu, M. Bujorianu, and H. Barringer, "A formal framework for user-centric control of multi-agent cyber-physical systems," in *Computational Logic in Multi-Agent Systems*. Berlin, Germany: Springer-Verlag, 2009.

[62] K. Willcox, D. Allaire, J. Deyst, C. He, and G. Sondecker, "Stochastic process decision methods for complex-cyber-physical systems," Defense Tech. Inf. Center (DTIC), Fort Belvoir, VA, USA, Tech. Rep., 2011.

[63] A. LaViers, M. Egerstedt, Y. Chen, and C. Belta, "Automatic generation of balletic motions," in *Proc. IEEE/ACM ICCPS*, 2011, pp. 13–21.

[64] C. Hang, P. Manolios, and V. Papavasileiou, "Synthesizing cyber-physical architectural models with real-time constraints," in *Computer Aided Verification*. Berlin, Germany: Springer-Verlag, 2011, pp. 441–456.

[65] S. Park, J. Park, and Y. Jeong, "An efficient dynamic integration middleware for cyber-physical systems in mobile environments," *Mobile Netw. Appl.*, vol. 18, no. 1, pp. 110–115, Feb. 2013.

[66] D. Broman, E. Lee, S. Tripakis, and M. Törngren, "Viewpoints, formalisms, languages, and tools for cyber-physical systems," in *Proc. 6th Int. Workshop Multi-Paradigm Modeling*, 2012, pp. 49–54.

[67] I. Calvo *et al.*, "Towards an infrastructure model for composing and reconfiguring cyber-physical systems," in *Ubiquitous Computing and Ambient Intelligence*. Berlin, Germany: Springer-Verlag, 2012, pp. 282–289.

[68] A. Noguero, I. Calvo, and L. Almeida, "A time-triggered middleware architecture for ubiquitous cyber physical system applications," in *Ubiquitous Computing and Ambient Intelligence*. Berlin, Germany: Springer-Verlag, 2012, pp. 73–80.

[69] S. Owre, I. Saha, and N. Shankar, "Automatic dimensional analysis of cyber-physical systems," in *FM 2012: Formal Methods*, vol. 7436, D. Giannakopoulou and D. Méry, Eds. Berlin, Germany: Springer-Verlag, 2012, ser. Lecture Notes in Computer Science, pp. 356–371.

[70] L. Tang *et al.*, "Multidimensional sensor data analysis in cyber-physical system: An atypical cube approach," *Int. J. Distrib. Sensor Netw.*, vol. 2012, pp. 724846-1–724846-19, 2012.

[71] E. Lee, "CPS foundations," in *Proc. DAC*, 2010, pp. 737–742.

[72] K. Wan, D. Hughes, K. Man, and T. Krilavicius, "Composition challenges and approaches for cyber physical systems," in *Proc. IEEE Int. Conf. NESEA*, 2010, pp. 1–7.

[73] A. Ehyaei, E. Tovar, N. Pereira, and B. Andersson, "Scalable data acquisition for densely instrumented cyber-physical systems," in *Proc. IEEE/ACM ICCPS*, 2011, pp. 174–183.

[74] F. Zhang, Z. Shi, and W. Wolf, "A dynamic battery model for co-design in cyber-physical systems," in *Proc. IEEE Int. Conf. Distrib. Comput. Syst. Workshops*, 2009, pp. 51–56.

[75] P. Bogdan and R. Marculescu, "Towards a science of cyber-physical systems design," in *Proc. IEEE/ACM ICCPS*, 2011, pp. 99–108.

[76] J. Wei and D. Kundur, "A flocking-based model for DoS-resilient communication routing in smart grid," in *Proc. IEEE GLOBECOM*, 2012, pp. 3519–3524.

[77] M. C. Bujorianu and H. Barringer, "An integrated specification logic for cyber-physical systems," in *Proc. IEEE Int. Conf. Eng. Complex Comput. Syst.*, 2009, pp. 291–300.

[78] E. A. Lee, S. Neuendorffer, and W. J. Wirthlin, "Actor-oriented design of embedded hardware and software systems," *J. Circuits, Syst., Comput.*, vol. 12, no. 3, pp. 231–260, 2003.

[79] S. Phatak, D. J. McCune, and G. Saikalis, "Cyber physical system: A virtual CPU based mechatronic simulation," in *Proc. IFAC Mechatron. Syst.*, 2010, pp. 405–410.

[80] G. Quan, "An integrated simulation environment for cyber-physical system co-simulation," presented at the National Workshop High-Confidence Automotive Cyber-Physical Systems, Troy, MI, USA, 2008.

[81] J. Lin, S. Sedigh, and A. Miller, "Integrated cyber-physical simulation of intelligent water distribution networks," in *Matlab/Book2*, E. P. Leite, Ed. Rijeka, Croatia: Intech, 2011.

[82] D. Henriksson and H. Elmqvist, "Cyber-physical systems modeling and simulation with Modelica," in *Proc. 8th Int. Modelica Conf.*, 2011, pp. 502–509.

[83] M. Gavrilescu, G. Magureanu, D. Pescaru, and A. Doboli, "A simulation framework for PSoC based cyber physical systems," in *Proc. ICCC-CONTI*, 2010, pp. 137–142.

[84] S. Jha and G. Sukthankar, "Modeling and verifying intelligent automotive cyber-physical systems," in *Proc. NIST/NSF/USCAR Workshop Develop. Dependable Secure Autom. Cyber-Phys. Syst. Compon.*, Troy, MI, USA, 2011.

[85] V. Singh and R. Jain, "Situation based control for cyber-physical environments," in *Proc. Mil. Commun. Conf.*, 2009, pp. 1–7.

[86] Y. Zhu *et al.*, "Mathematical equations as executable models of mechanical systems," in *Proc. IEEE/ACM ICCPS*, 2010, pp. 1–11.

[87] W. Yan *et al.*, "Integrated simulation and emulation platform for cyber-physical system security experimentation," in *Proc. ACM HiCoNS*, 2012, pp. 81–88.

[88] T. Hnat, T. I. Sookoor, P. Hooimeijer, W. Weimer, and K. Whitehouse, "MacroLab: A vector-based macroprogramming framework for cyber-physical systems," in *Proc. ACM Conf. Embedded Netw. Sensor Syst.*, 2008, pp. 225–238.

[89] P. Roy, P. Tabuada, and R. Majumdar, "Pessoa 2.0: A controller synthesis tool for cyber-physical systems," in *Proc. Int. Conf. Hybrid Syst., Comput. Control*, 2011, pp. 315–316.

[90] P. Martin and M. Egerstedt, "Hybrid systems tools for compiling controllers for cyber-physical systems," *Discr. Event Dyn. Syst.*, vol. 22, no. 1, pp. 101–119, Mar. 2012.

[91] R. Thacker, K. R. Jones, C. J. Myers, and H. Zheng, "Automatic abstraction for verification of cyber-physical systems," in *Proc. IEEE/ACM ICCPS*, 2010, pp. 12–21.

[92] Y. Sun, B. McMillin, X. F. Liu, and D. Cape, "Verifying noninterference in a cyber-physical system the advanced electric power grid," in *Proc. QSIC*, 2007, pp. 363–369.

[93] P. Kumar *et al.*, "A hybrid approach to cyber-physical systems verification," in *Proc. ACM/EDAC/IEEE DAC*, 2012, pp. 688–696.

[94] P. Manolios and V. Papavasileiou, "Virtual integration of cyber-physical systems by verification," in *Proc. AVICPS*, 2010, p. 65.

[95] M. Pajic, Z. Jhing, I. Lee, O. Sokolsky, and R. Mangharam, "From verification to implementation: A model translation tool and a pacemaker case study," in *Proc. RTAS*, 2012, pp. 173–184.

[96] B. McMillin and R. Akella, "Verification of information flow properties in cyber-physical systems," in *Proc. Workshop FDSCPS*, 2011, p. 37.

[97] S. Bak, K. Manamcheri, S. Mitra, and M. Caccamo, "Sandboxing controllers for cyber-physical systems," in *Proc. IEEE/ACM ICCPS*, 2011, pp. 3–12.

[98] A. Cardenas *et al.*, "Challenges for securing cyber physical systems," presented at the Workshop Future Directions Cyber-physical Systems Security, Newark, NJ, USA, 2009.

[99] 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. IEEE COMPSACW*, 2010, pp. 158–163.

[100] M. Anand *et al.*, "Security challenges in next generation cyber physical systems," in *Proc. Beyond SCADA, Netw. Embedded Control Cyber Phys. Syst.*, 2006, pp. 347–356.

[101] Y. Mo *et al.*, "Cyber-physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[102] M. Sun, S. Mohan, L. Sha, and C. Gunter, "Addressing safety and security contradictions in cyber-physical systems," in *Proc. CPSSW*, 2009, pp. 1–5.

[103] C. Zimmer, B. Bhat, F. Mueller, and S. Mohan, "Time-based intrusion detection in cyber-physical systems," in *Proc. IEEE/ACM ICCPS*, 2010, pp. 109–118, ACM.

[104] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "Ensuring safety, security, and sustainability of mission-critical cyber-physical systems," *Proc. IEEE*, vol. 100, no. 1, pp. 283–299, Jan. 2012.

[105] N. Gaddam *et al.*, "Securing physical processes against cyber attacks in cyber-physical systems," in *Proc. Nat. Workshop Res. High-Confidence Transp. Cyber-Phys. Systems, Autom., Aviation Rail*, 2008, pp. 1–3.

[106] B. Genge and C. Siaterlis, "Developing cyber-physical experimental capabilities for the security analysis of the future smart grid," in *Proc. IEEE PES ISGT Europe*, 2011, pp. 1–7.

[107] P. Barsocchi, S. Chessa, I. Martinovic, and G. Oligeri, "A cyber-physical approach to secret key generation in smart environments," *J. Ambient Intell. Hum. Comput.*, vol. 4, no. 1, pp. 1–16, Feb. 2011.

[108] L. Tang *et al.*, "Intrumine: Mining intruders in untrustworthy data of cyber-physical systems," in *Proc. SDM*, 2012, pp. 600–611.

[109] B. Qureshi, G. Min, and D. Kouvatsos, "M-Trust: A trust management scheme for mobile P2P networks," in *Proc. IEEE/IFIP Int. Conf. Embedded Ubiquitous Comput.*, 2010, pp. 476–483.

[110] R. Chow, E. Uzun, A. A. Cárdenas, Z. Song, and S. Lee, "Enhancing cyber-physical security through data patterns," in *Proc. FDSCPS*, 2011, pp. 25–30.

[111] M. Burmester, E. Magkos, and V. Chrissikopoulos, "Modeling security in cyber-physical systems," *Int. J. Critical Infrastr. Protection*, vol. 5, no. 3/4, pp. 118–126, Dec. 2012.

[112] O. Al Ibrahim and S. Nair, "Cyber-physical security using system-level PUFs," in *Proc. IWCMC*, 2011, pp. 1672–1676.

[113] A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. ICDCS*, 2008, pp. 495–500.

[114] D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel, "Security and privacy for implantable medical devices," *IEEE Pervasive Comput.*, vol. 7, no. 1, pp. 30–39, Jan.–Mar. 2008.

[115] Z. Xu *et al.*, "A certificateless signature scheme for mobile wireless cyber-physical systems," in *Proc. ICDCS*, 2008, pp. 489–494.

[116] F. Pasqualetti, F. Dörfler, and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," in *Proc. CDC-ECC*, 2011, pp. 2195–2201.

[117] H. Tang and B. M. McMillin, "Security property violation in CPS through timing," in *Proc. ICDCS*, 2008, pp. 519–524.

[118] C. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. Power Syst.*, vol. 23, no. 4, pp. 1836–1846, Nov. 2008.

[119] B. Genge, I. N. Fovino, C. Siaterlis, and M. Masera, "Analyzing cyber-physical attacks on networked industrial control systems," in *Critical Infrastructure Protection V*. Berlin, Germany: Springer-Verlag, 2011, pp. 167–183.

[120] Y. Chen, J.-S. Shin, and S.-T. Cheng, "A cyber-physical integrated security framework with fuzzy logic assessment for cultural heritages," in *Proc. IEEE Int. Conf. Systems, Man, Cybern.*, 2011, pp. 1843–1847.

[121] C. Neuman and K. Tan, "Mediating cyber and physical threat propagation in secure smart grid architectures," in *Proc. IEEE SmartGridComm*, 2011, pp. 238–243.

[122] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "On malicious data attacks on power system state estimation," in *Proc. UPEC*, 2010, pp. 1–6.

[123] M. Kirkpatrick, E. Bertino, and F. Sheldon, "Restricted authentication and encryption for cyber-physical systems," in *Proc. DHS CPS Workshop Restricted Authentication Encrypt. Cyber Phys. Syst.*, 2009, pp. 1–4.

[124] H. Zhao and X. Li, "VectorTrust: Trust vector aggregation scheme for trust management in peer-to-peer networks," in *Proc. Int. Conf. Comput. Commun. Netw.*, 2009, pp. 1–6.

[125] S. Bhattacharya, A. Khanafer, and T. Basar, "Resource allocation problems in networked cyber physical systems in adversarial scenarios," in *Proc. Workshop FDSCPS*, 2011, p. 18.

[126] Q. Zhu and T. Basar, "Towards a unifying security framework for cyber-physical systems," in *Proc. Workshop Found. Dependable Secure Cyber-Phys. Syst.*, 2011, pp. 47–50.

[127] B. Genge, C. Siaterlis, I. N. Fovino, and M. Masera, "A cyber-physical experimentation environment for the security analysis of networked industrial control systems," *Comput. Elect. Eng.*, vol. 38, no. 5, pp. 1146–1161, Sep. 2012.

[128] Z. Mohajerani *et al.*, "Cyber-related risk assessment and critical asset identification within the power grid," in *Proc. IEEE PES Transmiss. Distrib. Conf. Expo.*, 2010, pp. 1–4.

[129] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[130] H. Woo *et al.*, "Design and development methodology for resilient cyber-physical systems," in *Proc. ICDCS*, 2008, pp. 525–528.

[131] A. Giani, S. Sastry, K. Johansson, and H. Sandberg, "The VIKING project: An initiative on resilient control of power networks," in *Proc. Int. Symp. Resilient Control Syst.*, 2009, pp. 31–35.

[132] N. Kottenstette, G. Karsai, and J. Sztipanovits, "A passivity-based framework for resilient cyber physical systems," in *Proc. ISRCS*, 2009, pp. 43–50.

[133] K. Xiao, S. Ren, and K. Kwiat, "Retrofitting cyber physical systems for survivability through external coordination," in *Proc. Hawaii Int. Conf. Syst. Sci.*, 2008, pp. 465–465.

[134] 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. Int. Workshop Intell. Sol. Embedded Syst.*, 2008, pp. 1–10.

[135] N. Rao, D. Yau, and C. Ma, "On robustness of cyber-physical network infrastructure," in *Proc. Workshop Des., Modeling Eval. Cyber Phys. Syst.*, Istanbul, Turkey, 2011.

[136] B. Bonakdarpour, Y. Lin, and S. Kulkarni, "Automated addition of fault recovery to cyber-physical component-based models," in *Proc. Int. Conf. EMSOFT*, 2011, pp. 127–136, IEEE.

[137] F. Abad, M. Caccamo, and B. Robbins, "A fault resilient architecture for distributed cyber-physical systems," in *Proc. IEEE Int. Conf. Embedded RTCSA*, 2012, pp. 222–231.

[138] Q. Zhu and T. Basar, "Robust and resilient control design for cyber-physical systems with an application to power systems," in *Proc. IEEE CDC-ECC*, 2011, pp. 4066–4071.

[139] S. Abdelwahed, N. Kandasamy, and A. Gokhale, "High confidence software for cyber-physical systems," in *Proc. Workshop Autom. Serv. Qual., Int. Conf. ASE*, 2007, pp. 1–3.

[140] C. Singh and A. Sprintson, "Reliability assurance of cyber-physical power systems," in *Proc. IEEE PES GM*, 2010, pp. 1–6.

[141] L. Tang *et al.*, "Tru-alarm: Trustworthiness analysis of sensor networks in cyber-physical systems," in *Proc. IEEE ICDM*, 2010, pp. 1079–1084.

[142] K. Wan and V. Alagar, "Dependable context-sensitive services in cyber physical systems," in *Proc. IEEE TrustCom*, 2011, pp. 687–694.

[143] A. Faza, S. Sedigh, and B. McMillin, "Integrated cyber-physical fault injection for reliability analysis of the smart grid," in *Computer Safety, Reliability, and Security*. Berlin, Germany: Springer-Verlag, 2010, pp. 277–290.

[144] H. Ahmadi and T. Abdelzaher, "An adaptive-reliability cyber-physical transport protocol for spatio-temporal data," in *Proc. 30th IEEE RTSS*, 2009, pp. 238–247.

[145] T. 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. IEEE Int. Real-Time Syst. Symp.*, 2007, pp. 400–412.

[146] R. Akella and B. McMillin, "Model-checking BNDC properties in cyber-physical systems," in *Proc. IEEE Int. Comput. Softw. Appl. Conf.*, 2009, vol. 1, pp. 660–663.

[147] P. Wang, Y. Xiang, and S. Zhang, "A novel reliability assurance method for cyberphysical system components substitution," *Int. J. Distrib. Sensor Netw.*, vol. 2012, pp. 242654-1–242654-11, 2012.

[148] F. Xia, L. Ma, J. Dong, and Y. Sun, "Network QoS management in cyber-physical systems," in *Proc. ICESS Symp.*, 2008, pp. 302–307.

[149] J. Balasubramanian *et al.*, A Model-Driven QoS Provisioning Engine for Cyber Physical Systems, 2010.

[150] F. Xia, W. Zhao, Y. Sun, and Y.-C. Tian, "Fuzzy logic control based QoS management in wireless sensor/actuator networks," *Sensors*, vol. 7, no. 12, pp. 3179–3191, Dec. 2007.

[151] S. Mittal, Z. Zhang, and Y. Cao, "CASHIER: A cache energy saving technique for QoS systems," *Proc. IEEE VLSID*, pp. 43–48, 2013.

[152] S. Gupta, S. Mittal, and S. Dasgupta, "Guaranteed QoS with MIMO systems for scalable low motion video streaming over scarce resource wireless channels," in *Proc. Int. Conf. Inf. Process.*, 2008, pp. 452–456, IK International Pvt Ltd.

[153] F. Xia, X. Kong, and Z. Xu, "Cyber-physical control over wireless sensor and actuator networks with packet loss," in *Wireless Networking Based Control*. New York, NY, USA: Springer-Verlag, 2010, pp. 85–102.

[154] K. Kang and S. Son, "Real-time data services for cyber physical systems," in *Proc. ICDCS*, 2008, pp. 483–488.

[155] K. Lin and M. Panahi, "A real-time service-oriented framework to support sustainable cyber-physical systems," in *Proc. IEEE INDIN*, 2010, pp. 15–21.

[156] Y. Zhang, C. Gill, and C. Lu, "Reconfigurable real-time middleware for distributed cyber-physical systems with aperiodic events," in *Proc. 28th ICDCS*, 2008, pp. 581–588.

[157] H. Huang *et al.*, "Cyber-physical systems for real-time hybrid structural testing: A case study," in *Proc. ACM/IEEE Int. Conf. Cyber-Phys. Syst.*, 2010, pp. 69–78.

[158] W. Kang, K. Kapitanova, and S. H. Son, "RDDS: A real-time data distribution service for cyber-physical systems," *IEEE Trans. Ind. Informat.*, vol. 8, no. 2, pp. 393–405, May 2012.

[159] A. Wagh, J. Wan, C. Qiao, and C. Wu, "Human centric data fusion in vehicular cyber-physical systems," in *Proc. IEEE INFOCOM WKSHPS*, 2011, pp. 684–689.

[160] J. Yuan, Y. Zheng, X. Xie, and G. Sun, "Driving with knowledge from the physical world," in *Proc. ACM SIGKDD Int. Conf. Mining*, 2011, pp. 316–324.

[161] S. Loos, A. Platzer, and L. Nistor, "Adaptive cruise control: Hybrid, distributed, and now formally verified," in *Proc. FM*, 2011, pp. 42–56.

[162] S. Smaldone, C. Tonde, V. K. Ananthanarayanan, A. Elgammal, and L. Iftode, "The cyber-physical bike: A step towards safer green transportation," in *Proc. Workshop Mobile Comput. Syst. Appl.*, 2011, pp. 56–61.

[163] J. Lau, C. Tham, and T. Luo, "Participatory cyber physical system in public transport application," in *Proc. IEEE Int. Conf. UCC*, 2011, pp. 355–360.

[164] Q. Li and R. Negi, "Distributed scheduling in cyber-physical systems: The case of coordinated electric vehicle charging," in *Proc. IEEE GC Wkshps*, 2011, pp. 1183–1187, IEEE.

[165] C. Tricaud and Y. Chen, "Optimal trajectories of mobile remote sensors for parameter estimation in distributed cyber-physical systems," in *Proc. ACC*, 2010, pp. 3211–3216.

[166] J. Singh and O. Hussain, "Cyber-physical systems as an enabler for next generation applications," in *Proc. Int. Conf. NBiS*, 2012, pp. 417–422.

[167] Y. Ge, Y. Dong, and H. Zhao, "A cyber-physical energy system architecture for electric vehicles charging application," in *Proc. QSIC*, 2012, pp. 246–250.

[168] B. Syed, A. Pal, K. Srinivasarengan, and P. Balamuralidhar, "A smart transport application of cyber-physical systems: Road surface monitoring with mobile devices," in *Proc. ICST*, 2012, pp. 8–12.

[169] J. Goldman, R. A. Schrenker, J. L. Jackson, and S. F. Whitehead, "Plug-and-play in the operating room of the future," *Biomed Instrum Technol.*, vol. 39, no. 3, pp. 194–199, May/Jun. 2005.

[170] I. Lee and O. Sokolsky, "Medical cyber physical systems," in *Proc. ACM/IEEE DAC*, 2010, pp. 743–748.

[171] A. Cheng, "Cyber-physical medical and medication systems," in *Proc. ICDCS*, 2008, pp. 529–532.

[172] I. Lee *et al.*, "Challenges and research directions in medical cyber-physical systems," *Proc. IEEE*, vol. 100, no. 1, pp. 75–90, Jan. 2012.

[173] Z. Jiang, M. Pajic, and R. Mangharam, "Cyber-physical modeling of implantable cardiac medical devices," *Proc. IEEE*, vol. 100, no. 1, pp. 122–137, Jan. 2012.

[174] E. Yeniaras, J. Lamaury, Z. Deng, and N. V. Tsekos, "Towards a new cyber-physical system for MRI-guided and robot-assisted cardiac procedures," in *Proc. IEEE ITAB*, 2010, pp. 1–5.

[175] 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 *ISSRE*, 2009, pp. 51–60.

[176] K. Wan, K. L. Man, and D. Hughes, "Specification, analyzing challenges and approaches for Cyber-Physical Systems (CPS)," *Eng. Lett.*, vol. 18, no. 3, pp. 308–316, Sep. 2010.

[177] A. Banerjee, S. Kandula, T. Mukherjee, and S. K. S. Gupta, "BAND-AiDe: A tool for cyber-physical oriented analysis and design of body area networks and devices," *ACM Trans. Embedded Comput. Syst.*, vol. 11, no. S2, p. 49, Aug. 2012.

[178] H. Huang *et al.*, "Integrating neuromuscular and cyber systems for neural control of artificial legs," in *Proc. ACM/IEEE ICCPS*, 2010, pp. 129–138.

[179] K. Venkatasubramanian, S. Nabar, S. K. S. Gupta, and R. Poovendran, *Cyber Physical Security Solutions for Pervasive Health Monitoring Systems*. Hershey, PA, USA: IGI Global, 2011.

[180] P. Bogdan, S. Jain, K. Goyal, and R. Marculescu, "Implantable pacemakers control and optimization via fractional calculus approaches: A cyber-physical systems perspective," in *Proc. IEEE/ACM ICCPS*, 2012, pp. 23–32.

[181] J. Hatcliff *et al.*, "Rationale and architecture principles for medical application platforms," in *Proc. IEEE/ACM ICCPS*, 2012, pp. 3–12.

[182] J. Kleissl and Y. Agarwal, "Cyber-physical energy systems: Focus on smart buildings," in *Proc. ACM/IEEE DAC*, 2010, pp. 749–754.

[183] C. Lai, Y.-W. Ma, S.-Y. Chang, H.-C. Chao, and Y.-M. Huang, "OSGi-based services architecture for Cyber-Physical Home Control Systems," *Comput. Commun.*, vol. 34, no. 2, pp. 184–191, Feb. 2011.

[184] C. Anumba, A. Akanmu, and J. Messner, "Towards a cyber-physical systems approach to construction," in *Proc. Construct. Res. Congr.*, 2010, pp. 528–538.

[185] G. Hackmann, W. Guo, G. Yan, C. Lu, and S. Dyke, "Cyber-physical codesign of distributed structural health monitoring with wireless sensor networks," in *Proc. ACM/IEEE ICCPS*, 2010, pp. 119–128.

[186] X. Li, X. Liang, X. Shen, J. Chen, and X. Lin, "Smart community: An Internet of things application," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 68–75, Nov. 2011.

[187] F. Xia and J. Ma, "Building smart communities with cyber-physical systems," in *Proc. Int. Symp. Digit. Footprints Social Community Intell.*, 2011, pp. 1–6.

[188] W. Wu, M. K. Aziz, H. Huang, H. Yu, and H. B. Gooi, "A real-time cyber-physical energy management system for smart houses," in *Proc. ISGT IEEE PES*, 2011, pp. 1–8.

[189] A. Savvides *et al.*, "Cyber-physical systems for next generation intelligent buildings," in *Proc. WiP Session ICCPS*, 2011, pp. 35–38.

[190] S. Park, T. Do, Y. Jeong, and S. Kim, "A dynamic control middleware for cyber physical systems on an IPv6-based global network," *Int. J. Commun. Syst.*, vol. 26, no. 6, pp. 690–704, Jun. 2013.

[191] W. Shein, Y. Tan, and A. Lim, "PID controller for temperature control with multiple actuators in cyber-physical home system," in *Proc. 15th Int. Conf. NBiS*, 2012, pp. 423–428.

[192] Z. Bai and X. Huang, "Design and implementation of a cyber physical system for building smart living spaces," *Int. J. Distrib. Sensor Netw.*, vol. 2012, pp. 764186-1–764186-9, 2012.

[193] Z. Wang *et al.*, "Networked loads in the distribution grid," in *Proc. APSIPA ASC*, 2012, pp. 1–7.

[194] M. Simoes and S. Bhattarai, "Improving energy efficiency of cyber physical systems using multi-agent based control," in *Proc. IEEE IAS Annu. Meet.*, 2012, pp. 1–7.

[195] S. Lim, L. Chung, O. Han, and J. Kim, "An interactive cyber-physical system (CPS) for people with disability and frail elderly people," in *Proc. 5th Int. Conf. Ubiquitous Inf. Manage. Commun.*, 2011, p. 113.

[196] F. Wu, F. I Chu, and Y.-C. Tseng, "Cyber-physical handshake," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 4, pp. 472–473, Aug. 2011.

[197] E. Miluzzo *et al.*, "Sensing meets mobile social networks: The design, implementation and evaluation of the CenceMe application," in *Proc. ACM Conf. Embedded Netw. Sensor Syst.*, 2008, pp. 337–350.

[198] M. Chiu *et al.*, "Playful bottle: A mobile social persuasion system to motivate healthy water intake," in *Proc. Int. Conf. Ubiquitous Comput.*, 2009, pp. 185–194.

[199] C. Wu, Y.-T. Chang, and Y.-C. Tseng, "Multi-screen cyber-physical video game: An integration with body-area inertial sensor networks," in *Proc. IEEE PERCOM Workshops*, 2010, pp. 832–834.

[200] F. Wu, C.-S. Huang, and Y.-C. Tseng, "My Tai-Chi book: A virtual–physical social network platform," in *Proc. ACM/IEEE Int. Conf. Inf. Process. Sensor Netw.*, 2010, pp. 428–429.

[201] X. Yu, A. Pan, L.-A. Tang, Z. Li, and J. Han, "Geo-friends recommendation in GPS-based cyber-physical social network," in *Proc. ASONAM*, 2011, pp. 361–368.

[202] W. Wu *et al.*, "I'm the Jedi!—A case study of user experience in 3D tele-immersive gaming," in *Proc. IEEE ISM*, 2010, pp. 220–227.

[203] F. Zhang, K. Szwaykowska, W. Wolf, and V. Mooney, "Task scheduling for control oriented requirements for cyber-physical systems," in *Proc. Real-Time Syst. Symp.*, 2008, pp. 47–56.

[204] Q. Tang, S. Gupta, and G. Varsamopoulos, "A unified methodology for scheduling in distributed cyber-physical systems," *ACM Trans. Embedded Comput. Syst.*, vol. 11, no. S2, p. 57, Aug. 2012.

[205] T. Tidwell, R. Glaubius, C. D. Gill, and W. D. Smart, "Optimizing expected time utility in cyber-physical systems schedulers," in *Proc. IEEE RTSS*, 2010, pp. 193–201.

[206] J. Kim, K.-S. We, and C.-G. Lee, "HW Resource Componentizing for Addressing the Mega-complexity of Cyber-physical Systems," in *Proc. IEEE RTCSA*, 2011, vol. 2, pp. 61–66.

[207] M. Shafique, L. Bauer, W. Ahmed, and J. Henkel, "Minority-game-based resource allocation for run-time reconfigurable multi-core processors," in *Proc. DATE*, 2011, pp. 1–6.

[208] H. Qian, X. Huang, H. Yu, and C. H. Chang, "Cyber-physical thermal management of 3D multi-core cache-processor system with microfluidic cooling," *J. Low Power Electron.*, vol. 7, no. 1, pp. 110–121, Feb. 2011.

[209] P. Bogdan, R. Marculescu, S. Jain, and R. T. Gavila, "An optimal control approach to power management for multi-voltage and frequency islands multiprocessor platforms under highly variable workloads," in *Proc. IEEE/ACM Int. Symp. NoCS*, 2012, pp. 35–42.

[210] R. David, P. Bogdan, and R. Marculescu, "Dynamic power management for multicores: Case study using the Intel SCC," in *Proc. IEEE/IFIP Int. Conf. VLSI-SoC*, 2012, pp. 147–152.

[211] P. Bogdan and R. Marculescu, "Non-stationary traffic analysis and its implications on multicore platform design," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 30, no. 4, pp. 508–519, Apr. 2011.

[212] J.-Y. Ou and Y.-S. Chen, "QoS optimization for thermal-aware cyber-physical systems," in *Proc. ACM Symp. Res. Appl. Comput.*, 2011, pp. 13–19.

[213] A. Barthels *et al.*, "A model for sequence based power management in cyber physical systems," in *Proc. Inf. Commun. Technol. Fight Against Global Warming*, 2011, pp. 87–101.

[214] P. Bogdan and R. Marculescu, "Statistical physics approaches for network-on-chip traffic characterization," in *Proc. IEEE/ACM Int. Conf. Hardw./Softw. Codesign Syst. Synthesis*, 2009, pp. 461–470.

[215] D. Puschini, F. Clermidy, P. Benoit, G. Sassatelli, and L. Torres, "Dynamic and distributed frequency assignment for energy and latency constrained MP-SoC," in *Proc. DATE*, 2009, pp. 1564–1567.

[216] L. Parolini, N. Tolia, B. Sinopoli, and B. H. Krogh, "A cyber-physical systems approach to energy management in data centers," in *Proc. ACM/IEEE ICCPS*, 2010, pp. 168–177.

[217] L. Parolini, B. Sinopoli, B. H. Krogh, and Z. Wang, "A cyber-physical systems approach to data center modeling and control for energy efficiency," *Proc. IEEE*, vol. 100, no. 1, pp. 254–268, Jan. 2012.

[218] L. Li *et al.*, "Thermocast: A cyber-physical forecasting model for data centers," in *Proc. KDD*, 2011, vol. 11, pp. 1370–1378.

[219] L. Rao, X. Liu, M. Ilic, and J. Liu, "MEC-IDC: Joint load balancing and power control for distributed Internet Data Centers," in *Proc. ACM/IEEE ICCPS*, 2010, pp. 188–197.

[220] A. Banerjee, T. Mukherjee, G. Varsamopoulos, and S. K. S. Gupta, "Cooling-aware and thermal-aware workload placement for green HPC data centers," in *Proc. Green Comput. Conf.*, 2010, pp. 245–256.

[221] H. Chen, P. Xiong, A. Gavrilovska, K. Schwan, and C. Xu, "A cyber-physical integrated system for application performance and energy management in data centers," in *Proc. IGCC*, 2012, pp. 1–10.

[222] L. Rao, X. Liu, L. Xie, and W. Liu, "Minimizing electricity cost: Optimization of distributed Internet data centers in a multi-electricity-market environment," in *Proc. IEEE INFOCOM*, 2010, pp. 1–9.

[223] S. Craciunas *et al.*, "Information-acquisition-as-a-service for cyber-physical cloud computing," in *Proc. USENIX Conf. Hot Topics Cloud Comput.*, 2010, p. 14.

[224] S. Karnouskos, "Cyber-physical systems in the SmartGrid," in *Proc. IEEE INDIN*, 2011, pp. 20–23.

[225] Y. Susuki *et al.*, "A hybrid system approach to the analysis and design of power grid dynamic performance," *Proc. IEEE*, vol. 100, no. 1, pp. 225–239, Jan. 2012.

[226] O. Yagan, D. Qian, J. Zhang, and D. Cochran, "On allocating interconnecting links against cascading failures in cyber-physical networks," in *Proc. IEEE INFOCOM WKSHPS*, 2011, pp. 930–935.

[227] A. Saber and G. K. Venayagamoorthy, "Efficient utilization of renewable energy sources by gridable vehicles in cyber-physical energy systems," *IEEE Syst. J.*, vol. 4, no. 3, pp. 285–294, Sep. 2010.

[228] C. Macana, N. Quijano, and E. Mojica-Nava, "A survey on cyber physical energy systems and their applications on smart grids," in *Proc. ISGT*, 2011, pp. 1–7.

[229] N. Hadjsaid, C. Tranchita, B. Rozel, M. Viziteu, and R. Caire, "Modeling cyber and physical interdependencies—Application in ICT and power grids," in *Proc. IEEE/PES PSCE*, 2009, pp. 1–6.

[230] J. Zhao, F. Wen, Y. Xue, X. Li, and Z. Dong, "Cyber physical power systems: Architecture, implementation techniques and challenges," *Dianli Xitong Zidonghua/Autom. Elect. Power Syst.*, vol. 34, no. 16, pp. 1–7, Aug. 2010.

[231] I. Akkaya, Y. Liu, and I. Gorton, "Modeling and analysis of middleware design for streaming power grid applications," in *Proc. Int. Middleware Conf. Ind. Track 13th ACM/IFIP/USENIX*, 2012, p. 1.

[232] C. Ramos, Z. Vale, and L. Faria, "Cyber-physical intelligence in the context of power systems," in *Future Generation Information Technology*. Berlin, Germany: Springer-Verlag, 2011, pp. 19–29.

[233] G. Dondossola *et al.*, "Critical Utility Infrastructural Resilience," arXiv preprint arXiv:1211.5736, 2012.

[234] J. Hong, C.-C. Liu, and M. Govindarasu, "Integrated anomaly detection for cyber security of the substations," *IEEE Trans. Smart Grid*, 2014. [Online]. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6786500&pageNumber%3D126738

[235] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[236] M. Li and W. Zhao, "Visiting power laws in cyber-physical networking systems," *Math. Prob. Eng.*, vol. 2012, pp. 302786-1–302786-13, 2011.

[237] M. Kim, M.-O. Stehr, J. Kim, and S. Ha, "An application framework for loosely coupled networked cyber-physical systems," in *Proc. IEEE/IFIP Int. Conf. EUC*, 2010, pp. 144–153.

[238] R. Ganti, Y.-E. Tsai, and T. F. Abdelzaher, "Senseworld: Towards cyber-physical social networks," in *Proc. IPSN*, 2008, pp. 563–564.

[239] G. Xing *et al.*, "Toward ubiquitous video-based cyber-physical systems," in *Proc. IEEE SMC*, 2008, pp. 48–53.

[240] J. Cao and H. Li, "Energy-efficient structuralized clustering for sensor-based cyber physical systems," in *Proc. UIC-ATC*, 2009, pp. 234–239.

[241] H. Li, L. Lai, and H. V. Poor, "Multicast routing for decentralized control of cyber physical systems with an application in smart grid," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1097–1107, Jul. 2012.

[242] H. Ahmadi, T. F. Abdelzaher, and I. Gupta, "Congestion control for spatio-temporal data in cyber-physical systems," in *Proc. IEEE/ACM ICCPS*, 2010, pp. 89–98.

[243] F. Wu, Y.-F. Kao, and Y.-C. Tseng, "From wireless sensor networks towards cyber physical systems," *Pervasive Mobile Comput.*, vol. 7, no. 4, pp. 397–413, Aug. 2011.

[244] C. Xue, G. Xing, Z. Yuan, Z. Shao, and E. Sha, "Joint sleep scheduling and mode assignment in wireless cyber-physical systems," in *Proc. IEEE ICDCS Workshops*, 2009, pp. 1–6.

[245] O. Yagan, D. Qian, J. Zhang, and D. Cochran, "Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures, and robustness," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1708–1720, Sep. 2012.

[246] Z. Song, C. Sastry, N. Tas, and Y. Chen, "Feasibility analysis on optimal sensor selection in cyber-physical systems," in *Proc. ACC*, 2009, pp. 5368–5373.

[247] F. Xia, Y.-C. Tian, Y. Li, and Y. Sung, "Wireless sensor/actuator network design for mobile control applications," *Sensors*, vol. 7, no. 10, pp. 2157–2173, Oct. 2007.

[248] N. Ozay, U. Topcu, R. M. Murray, and T. Wongpiromsarn, "Distributed synthesis of control protocols for smart camera networks," in *Proc. IEEE/ACM ICCPS*, 2011, pp. 45–54.

[249] J. Chen, R. Tan, G. Xing, X. Wang, and X. Fu, "Fidelity-aware utilization control for cyber-physical surveillance systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1739–1751, Sep. 2012.

[250] L. Ma *et al.*, "A high-confidence cyber-physical alarm system: Design and implementation," in *Proc. IEEE/ACM Int. Conf. Green Comput. Commun. Int. Conf. Cyber, Phys. Social Comput.*, 2010, pp. 516–520.

[251] Y. Wang, M. C. Vuran, and S. Goddard, "Cyber-physical systems in industrial process control," *ACM SIGBED Rev.*, vol. 5, no. 1, pp. 1–2, Jan. 2008.

[252] W. Zhang, M. Kamgarpour, D. Sun, and C. J. Tomlin, "A hierarchical flight planning framework for air traffic management," *Proc. IEEE*, vol. 100, no. 1, pp. 179–194, Jan. 2012.

[253] S. Lintelman, K. Sampigethaya, M. Li, R. Poovendran, and R. V. Robinson, "High assurance aerospace CPS & implications for the automotive industry," in *Proc. Nat. Workshop High Confidence Autom. CPS*, 2008, pp. 1–3.

[254] N. Mahadevan, A. Dubey, and G. Karsai, "Application of software health management techniques," in *Proc. Int. Symp. Softw. Eng. Adapt. Self-Managing Syst.*, 2011, pp. 1–10.

[255] A. Noor, "Intelligent adaptive cyber-physical ecosystem for aerospace engineering education, training, and accelerated workforce development," *J. Aerosp. Eng.*, vol. 24, no. 4, pp. 403–408, Oct. 2011.

[256] T. Johnson and S. Mitra, "Parametrized verification of distributed cyber-physical systems: An aircraft landing protocol case study," in *Proc. IEEE/ACM ICCPS*, 2012, pp. 161–170.

[257] L. Shou *et al.*, "What-you-retrieve-is-what-you-see: A preliminary cyber-physical search engine," in *Proc. ACM SIGIR Conf. Res. Develop. Inf. Retrieval*, 2011, pp. 1273–1274.

[258] H. Lim, M. Iqbal, M. Wang, and Y. Xiao, "The national weather sensor grid: A large-scale cyber-sensor infrastructure for environmental monitoring," *Int. J. Sensor Netw.*, vol. 7, no. 1/2, pp. 19–36, Feb. 2010.

[259] T. Tidwell *et al.*, "Towards configurable real-time hybrid structural testing: A cyber-physical system approach," in *Proc. IEEE ISORC*, 2009, pp. 37–44.

[260] M. Lindberg and K. Arzen, "Feedback control of cyber-physical systems with multi resource dependencies and model uncertainties," in *Proc. IEEE RTSS*, 2010, pp. 85–94.

[261] W. Meng, Q. Liu, W. Xu, and Z. Zhou, "A cyber-physical system for public environment perception and emergency handling," in *Proc. IEEE Int. Conf. HPCC*, 2011, pp. 734–738.

[262] T. Morris *et al.*, "Engineering future cyber-physical energy systems: Challenges, research needs, and roadmap," in *Proc. NAPS*, 2009, pp. 1–6.

[263] J. White *et al.*, "R&D challenges and solutions for mobile cyber-physical applications and supporting Internet services," *J. Internet Serv. Appl.*, vol. 1, no. 1, pp. 45–56, May 2010.

[264] R. von Hanxleden, E. A. Lee, C. Motika, and H. Fuhrmann, "Multi-view modeling and pragmatics in 2020—Position paper on designing complex cyber-physical systems," in *Proc. Int. Monterey Workshop Develop., Oper. Manage. Large-Scale Complex IT Syst.*, 2012, pp. 209–223.

[265] R. Poovendran, "Cyber-physical systems: Close encounters between two parallel worlds [point of view]," *Proc. IEEE*, vol. 98, no. 8, pp. 1363–1366, Aug. 2010.

[266] E. Lee, "Cyber physical systems: Design challenges," in *Proc. IEEE ISORC*, 2008, pp. 363–369.

[267] K.-D. Kim and P. Kumar, "Cyber-physical systems: A perspective at the centennial," *Proc. IEEE*, vol. 100, no. 13, pp. 1287–1308, May 2012.

[268] R. Baheti and H. Gill, "Cyber-physical systems," *Impact Control Technol.*, pp. 161–166, Mar. 2011.

[269] E. A. Lee and H. Zheng, "Operational semantics of hybrid systems," in *Hybrid Systems: Computation and Control*. Berlin, Germany: Springer-Verlag, 2005, pp. 25–53.

[270] E. A. Lee, "Finite state machines and modal models in Ptolemy II," Defense Technical Information Center (DTIC), Fort Belvoir, VA, USA, Tech. Rep., 2009.

[271] E. A. Lee, "Modeling concurrent real-time processes using discrete events," *Ann. Softw. Eng.*, vol. 7, no. 1–4, pp. 25–45, Oct. 1999.

[272] E. A. Lee and T. M. Parks, "Dataflow process networks," *Proc. IEEE*, vol. 83, no. 5, pp. 773–801, May 1995.

[273] O. Maler, Z. Manna, and A. Pnueli, "From timed to hybrid systems," in *Proc. Real-Time, Theory Pract.*, 1992, pp. 447–484.

[274] D. Garlan *et al.*, "Acme: Architectural description of component-based systems," in *Foundations of Component-Based Systems*, vol. 68. New York, NY, USA: Cambridge Univ. Press, 2000, pp. 47–68.

[275] J. Slay and M. Miller, "Lessons learned from the Maroochy water breach," in *Critical Infrastructure Protection*. New York, NY, USA: Springer-Verlag, 2007, pp. 73–82.

[276] S. Mittal, "A survey of architectural techniques for DRAM power management," *Int. J. High Perform. Syst. Architecture*, vol. 4, no. 2, pp. 110–119, Dec. 2012.

[277] S. Mittal and Z. Zhang, "EnCache: Improving cache energy efficiency using a software-controlled profiling cache," in *Proc. IEEE EIT*, Indianapolis, IN, USA, May 2012.

[278] M. Govindarasu, A. Hann, and P. Sauer, "Cyber-physical systems security for smart grid," Power Syst. Eng. Res. Center (PSERC), Tempe, AZ, USA, Tech. Rep., Feb. 2012, PSERC Publications.

Siddhartha Kumar Khaitan (SM'14) received the Ph.D. degree from Iowa State University, Ames, IA, USA, in 2008.

He is currently a Research Assistant Professor with the Department of Electrical and Computer Engineering, Iowa State University. He has authored or coauthored several international journal and conference papers and two edited books. His research interests are in cyberphysical system modeling and simulation, energy storage, renewable energy modeling and integration, infrastructure systems planning and investment, and high-performance computing application in power and energy systems.

Prof. Khaitan was a recipient of a research excellence award during his Ph.D. studies and a university gold medal during his undergraduate studies.

James D. McCalley (F'04) received the B.S., M.S., and Ph.D. degrees from Georgia Institute of Technology, Atlanta, GA, USA, in 1982, 1986, and 1992, respectively, all in electrical engineering.

From 1985 to 1990, he was a Transmission Planning Engineer with Pacific Gas and Electric Company, San Francisco, CA, USA. He is currently a Harpole Professor of electrical and computer engineering with Iowa State University, Ames, IA, USA. His research interests are cyberphysical system, power system security, power system dynamics, wind energy, and long-term investment planning for energy and transportation systems at the national level.

Prof. McCalley is a Registered Professional Engineer in California.