A REVIEW STUDY ON CYBER-PHYSICAL SYSTEMS AND THEIR CONCEPT

Viren Babulal Shah
Research Scholar
Department of Commerce and Management
Sunrise University, Rajasthan.
getviren@gmail.com

Dr. Rajpal Singh
Research Guide
Department of Commerce and Management
Sunrise University, Rajasthan.

Abstract

Cyber-physical systems are intricate systems that naturally integrate and work closely with 3C (control, communication, and computing) technologies. The development of CPS is subject to the theory and technology of current network systems and physical systems, which presents significant hurdles. This essay initially discusses the idea and characteristics of CPS before analyzing the state of CPS research at the moment. After that, the system model, information processing technology, and software design facets of CPS development are covered. Finally, it evaluates the major challenges and significant studies in creating CPS.

INTRODUCTION

THE development of computer and information technology has seen a number of turning points. In the 1960s and 1970s, mainframe computers first emerged. Internet and desktop computers equipped to handle both personal and commercial business were developed in the 1980s and 1990s. Pervasive computing, which allows users to execute calculations at any time or location, first debuted about 2000. All of these incidents have had a significant impact on the growth of the information society. Many professionals from a wide range of disciplines are now closely monitoring the creation of a new engineering system called cyber-physical systems (CPS). CPS are interdisciplinary systems that combine computer, communication, and control technologies to provide feedback control on widely dispersed embedded computing systems. They include the translation and integration of conventional embedded systems with current network systems. CPS may provide real-time, secure, dependable, and dynamic cooperation with physical systems represented by embedded systems via integration. The real-time capabilities and accuracy of the data acquired are ensured by physical system data collection modules, which collect data using distributed field devices in the CPS system. In accordance with service requests, they transfer data to the information processing layer where it is processed using information processing technologies such data uncertainty management, statistical signal processing, data security processing, and feedback control to accomplish assigned tasks. Applications for CPS are many and include distributed energy systems, industrial control, aerospace and aviation control, and digital medical devices and systems that use automated acquisition and control technologies. Additionally, CPS has enormous economic potential and will ultimately fundamentally alter how current engineering physical systems operate.

This article begins by outlining the idea and characteristics of cyber-physical systems. Then it examines the state of CPS research today as well as the difficulties in developing a CPS system model and important technologies. The potential for CPS studies and applications is the last section.

CONCEPT AND CHARACTERISTICS

Concept

Computer scientists and network professionals must work closely with experts in a variety of fields, including automation and control, civil engineering, mechanical engineering, and biology, as CPS is an emerging research area that involves the overlapping and integration of multiple fields of science and engineering. As a result, the current definitions of CPS are mostly provided by various academics from their respective views.

Cyber-physical systems, according to E. A. Lee, are those that combine computation with physical operation by using embedded computers and networks to monitor and manage the latter. Through feedback loops, physical processes influence calculations, and vice versa. Academician J. F. He describes CPS as scalable, believable, and controllable networked physical equipment systems that deeply integrate computing, communication, and control on the basis of perception of the environment. To increase or expand the functionality of networks and physical systems and to monitor or control a physical entity in a safe, dependable, efficient, and real-time manner, in-depth integrations and real-time interactions are made possible through the feedback loop of mutual effects between computing processes and physical processes.

Fig. 1 depicts the service-oriented architecture of CPS.

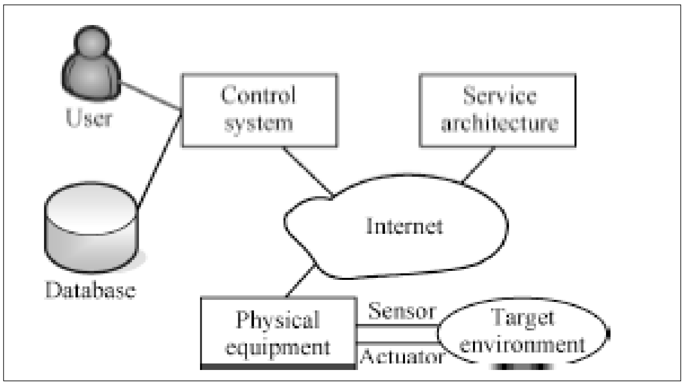

Fig. 1. Service-oriented architecture of CPS.

Some researchers believe CPS is a network physical engineering system that computes to monitor and control physical systems. DARPA defines physical network systems as software- and electromechanical-based systems. All defense systems and subsystems—aircraft, spacecraft, naval vessels, land vehicles, etc.—are CPS. CPS includes integrated circuits, MEMS, and NEMS.

WSN, IOT, and CPS vary. WSN merely detects the signal, not the object. Data collection, processing, integration, and routing serve a range of applications and emphasis information perception. IOT is a new type of network that connects Internet information sensing devices like wireless sensors and radio frequency identification (RFID) through wireless networks and Internet technology to achieve information perception, transmission, and processing. CPS is a controlled, believable, and scalable network physical equipment system that thoroughly combines IOT information gathering, processing, communication, and control. Deep integration and real-time interaction between computation and physical processes expand or extend new functions to detect or operate a physical object safely, reliably, and efficiently. CPS can sense and control the physical environment, unlike the Internet of Things. Its equipment computing requirements greatly beyond IOT and WSN.

CPS are network-physical systems that function together. They may achieve real-time sensing, dynamic control, and information services for big engineering systems by organically integrating and deeply collaborating compute, communications, and control (3C) technologies. CPS also refers to distributed heterogeneous systems having network and physical systems with various functionalities, subsystems with distinct structures and functions, and different geographic scopes. Coordinating subsystems requires wired or wireless connectivity. Fig. 2 shows CPS integration.

Characteristics

CPS communicate with physical systems via networks. The final system of CPS is usually a classic centralized tightly linked embedded computer system with many intelligent wireless sensing nets. CPS has these traits:

CPS's Most Important Field: Physical System It includes hardware design, energy management, hardware size, connection encapsulation, and system testing. This field's engineers and scientists comprehend mechanics, electronics, biology, and chemistry, sensors, and signal processing. Every physical system has unique network features, including maximum multi-level network coverage, complex temporal and geographical scale to satisfy task time requirements, and high automation.

Information system permits engineering professionals to transfer data from physical system engineering into software system rules and models, forming CPS. The biggest issue for these specialists is balancing real-time systems, network systems, file systems, hierarchical storage systems, memory management, modular software design, current design, and formal verification.

CPS is the Product of Integration of Heterogeneous Systems: Heterogeneous distributed systems with significant information system and physical system integration and interaction must handle time synchronization and component geographical dispersion.

CPS needs security, real-time capabilities, and predictability: Due to the open nature of network and physical systems and network transmission delays, CPS must be able to combat invasion, manipulation, counterfeiting, and other hostile activities. CPS must address credibility, security, efficacy, real-time, dynamic, and predictability. Credibility means authenticating information gathering sources or control instruction senders, and security means encrypting and decrypting information and protecting privacy. Validity requires both processing accuracy and information or instruction set validity to prevent CPS processing uncertainties and noise from affecting system processing accuracy. Task processing requires immediate delivery of information or instructions. Dynamic rearrangement and reconfiguration update rules and provide instructions based on job demands and environmental changes to decrease bias and perform activities according to specified rules.

Predictability means that CPS resource allocation technique may allocate resources to many competing real-time activities at any moment and in any scenario to meet the real-time demands of each task.

TECHNICAL RESEARCHES

Scientific CPS requires a unique system design pattern with hierarchical systems, components and subsystems, service quality theory, agreements, modeling language, and tools to evaluate, integrate, and simulate components. Computation should handle feedback control of event-driven real-time systems appropriate for asynchronous dynamic event processing on diverse time scales. CPS investigates a young world. Since CPS integrates disparate systems without a global model, professionals in numerous domains conduct CPS research from their own field's perspective. CPS researchers focus on system architecture, information processing, and software design.

Researches on Architecture of CPS

Modeling describes the goal system before completion. Based on current physical, network, and computer systems, CPS models must be changed and combined for research and development. Abstraction and modeling of communication, computation, and physical dynamics at multiple timescales are also needed to assist CPS development. Our CPS system structure model has three layers: user, information, and physical. The CPS's physical system gathers, transmits, and executes control signals via embedded systems, sensor networks, smart chips, etc. The information system layer transmits and processes the CPS's basic physical system data. In a human-computer interaction environment, the user layer manages data query, strategy, and safety protection. Frequent CPS operations should assure this. CPS is closed-loop. Fig. 3 shows CPS architecture.

Sensor Networks: For the capture of real-time data, use a range of sensors and real-time embedded systems. Perform further procedures, such as data encryption and data integration, on the gathered data via the collecting nodes. Maintain the confidentiality, integrity, and non-repudiation of data transfer. Utilize energy management to lower network energy usage. Real-time processing should use technologies for data security in real-time.

Next Generation Network Systems: Utilize anti-hacking and defensive technologies to fend off various network assaults. To guarantee the security of data transfer, use a high-performance encryption technique and CA authentication mechanism. By improving current routing methods, you may achieve quick data exchange. In a "best effort" to offer real-time network transmission services for the system, modify the current network system structure.

Data Center: Next-generation network systems store sensor data in data centers. If data passes authentication and integrity checks, data center stores it; otherwise, it notifies control center. Then the control center sends actuator control signals to alert sensor network nodes to gather data again. Data center maintains database and responds quickly to control center queries. Regular emergency treatments avoid database breakdown.

Control Center: CPS's control center matters most. After identity authentication, it sends query commands to data center from user inquiries. It categorizes query results according to control strategies, reports back to the user whether they match criteria, and locates the node using node positioning technology and delivers control instructions to actuators for processing. Users may dynamically change control center configuration policies. Use data mining and uncertainty processing to anticipate and evaluate CPS behavior. Fault diagnosis and processing of network and node failures. Real-time control technology ensures CPS processing.

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

System User: Web servers, hosts, and devices are system users. It handles CPS communication, control center inquiry instructions, and feedback data. Control center executes user definitions and altered control strategies.

This model considers real-time capabilities, security, and system performance to satisfy future CPS needs. CPS runs under closed-loop control. Some researchers researched CPS system architecture with diverse themes and applications.

Complex real-time network and physical components make up the advanced power grid. Each item may work fine alone, but when coupled, interference may create problems like frequency domain Nyquist rate violation. Y. Sun et al. suggested using RT-PROMELA to develop a model that can represent frequency interference and utilize real-time interference of real time-sensor protocol for information through negotiation (RT-SPIN) detection to assess CPS component correctness. It addressed collaborative processing's many clock variables due to components' asynchronous and non-real-time interaction. M. D. Ilic et al. created a CPS energy system dynamic model with distributed sensing and control and discussed information exchange between components and developing interactive protocols between embedded system control terminal and network system.

He coordinated model and future energy system control. Data mining and sensors enhanced complicated power system operation. Energy research is rigid.

Actuator networks have control nodes and actuators. The control center instructs actuator units to affect the physical environment through control nodes. Discussed an off-line and online scheduling approach for multiple actuators controlled by a controller (single CPU) that balances time delay and control performance to address collaborative design of feedback control and scheduling. CPS's data was disregarded. Reference studies CPS architecture and proposes an event-driven real-time job scheduling system using sensor nodes periodic work model and actuator event-triggered task model. System efficiency requires experimental verification.

Researches on Information Processing of CPS

The gathering, transmission, and processing of perceptual data, the feedback of control information, as well as the physical system's reaction to orders, are all examples of information processing.

Data Processing:

Data Acquisition Technology Research: CPS has several information detecting devices, including RFID, sensors, global positioning systems, laser scanners, and more, that can be networked to the Internet. Network protocols integrate field equipment-management layers smoothly. Thus, CPS data processing needs fast, accurate physical system data collection.

CPS uses low- or high-precision sensor perception data. Sensor nodes and sink-nodes in sensor network subsystems can sense physical world information users want, such as traffic information in intelligent transportation, soil temperature and humidity in environmental detection, and patient blood pressure and blood sugar in intelligent medication. The gathering center delivers perceived data to the data center for decision-making. Thacker et al. developed the distributed technique to rapidly collect CPS sensor data. Priority media access control (MAC) protocol transfers sensor data approximated by function interpolation geographical coordinates. In a large CPS, the algorithm may acquire valid data if some sensor nodes fail. Real-time CPS data processing was overlooked. C. Qi et al. created a real-time data gathering instrument system employing the HMS30C7202 CPU and CAN connectivity. He linked it with CPS to construct an Internet-based information service system using distributed monitoring and control devices as network nodes. He used field bus and the Internet to build a real-time, efficient network control system for industrial control system decentralization, networking, and intellectualization. The embedded system structure is broken and CPS real-time data collecting is referenced, however network data security is not addressed by this technology.

Researches on CPS System Security

The Internet cannot fulfill future CPS security and privacy needs. Traditional Internet security technology rarely considers the security of physical system in CPS (such as randomly distributed sensor network, ubiquitous wireless network, etc.), so existing network monitoring and defense technologies are facing CPS with more complex structure, and we need a CPS security framework combining control and information. Our nation lacks systematic study on issues such information sensitivity and privacy protection, transaction security, information system security, security certification and audit, trust mechanism, etc. Cyber-physical systems will become vital national infrastructure and riskier. To collect more information, manage end users, and assemble nodes in an open and linked network may indefinitely compound faults or malevolent conduct and damage CPS, necessitating CPS security research.

Security Architecture: CPS security must include network-physical environment feedback, distributed management and control, uncertainty, real-time demand, and geographic dispersion. While creating CPS, C. Neuman wrote about modeling, sensor, actuator, system architecture, and application security. He did not give development tools for his more extensive design approach of integrating security into the system's core due to operating system, network, and middleware technology restrictions. N. Adam wrote about CPS security issues like the lack of mature verification and validation technology, mechanisms to meet real-time, reliability, and security requirements, lack of awareness of CPS risks, no irrelevant safety performance indicators, and insufficient knowledge of CPS size and complexity. He proposed creating a security strategy and providing frameworks with safe interfaces to secure handcrafted system dynamic behaviors. A new technology allows network self-configuration, self-healing, and feedback. Cyber-physical systems use computing and physics. Information flow between physical systems defines CPS. H. Tang evaluated his safe information flow model utilizing power system flexible AC transmission technology. The approach has been evaluated for information flow security and information security assessment. It could develop CPS security. However, it only addresses certain security flaws.

Security Control: Y. Tan et al. highlighted CPS safety control, message integrity, availability, and confidentiality problems. He divided CPS into physical systems and control and explored misleading and Dos attacks in information flow between them. He examined the limitations of active defense and passive response mechanisms in CPS information security and automatic control theory in CPS safety control, such as the problem of traditional filters predicting network status with uncertain packet loss. He used game theory to examine intrusion detection models and build novel active/passive algorithms for system infiltration.

Reference explained passivity using control theory, demonstrated elastic system control under malicious assaults, and offered ways to simplify and enhance analysis.

Attack Defense: R. A. Thacker et al. analyzed CPS system security threats and their effects, compared CPS to traditional IT security, and established security mechanisms for CPS, including prevention, detection, recovery, and dynamic guard against attacks, but did not specify methods. T. L. Crenshaw et al. created a component-based programmable multi-node attack system and UPBOT test platform for CPS security threat and defense testing. Physical scope restricts software to local testing and does not solve real-time capabilities.

CPS security research utilizes key management and integrity verification. Current research cannot match CPS's real-time capabilities, reliability, and safety requirements due to its uniqueness, hence further study is required.

CHALLENGES

CPS progress is most hindered by a unified theoretical framework of network and physical resources. Computer science and control theory differ technically and culturally in most computer and physical systems. Design presupposes a range. Computer scientists and engineers cannot interpret physical system needs like stability, performance, and power consumption. Control and signal theory simplifies computers as exact digital instruments, neglecting fundamental computing principles such the time difference rising due to cache-caused software error rate, energy management, and complexity. Wireless CPS communication channels are low-energy, shared, and fast. Future CPS standards must address measurement noise, collection inaccuracy, environmental effect, and unified framework calculation mistakes. To reduce design complexity while keeping the essence of the abstracted issue, CPS models must be straightforward to abstract. Shannon, infinite horizon linear time-invariant, resilient control, and general equilibrium theories apply. CPS design has scale, robustness, performance matching, and other difficulties. System theory changes must integrate physical system theories like control systems, signal processing, and computer system theories like complexity, scheduling, and computing to address protocols. Computers must coordinate space and time. Thus, embedded computer communication networks manage physical process and collaborate interference. Bottom-up computer development provides real-time system abstraction. It involves replacing the cache with the scratchpad memory buffer, developing temporal semantic described programming languages, choosing appropriate concurrency models for static analysis, developing concurrent and real-time software components, providing new technical means for networks to provide highly precise time synchronization, etc. Top-down modeling substitutes the programming language to express system behavior and is rich in semantic space to describe the dynamic timing of the physical world. Both techniques are immature.

Scale and Efficiency Large-scale integrated physical modular network systems may provide high-quality event detection, monitoring, control, and real-time prediction using densely positioned sensors [94]. The application generally focuses about sensor readings' calculation and target location functions. Energy restricts embedded computers. Energy conservation requires energy management. Information processing size and efficiency must be addressed. Information processing efficiency studies should calculate at the lowest cost of energy, communication links, energy storage, and processor resources to slow or eliminate energy consumption from digital sensor reading and processing or embedded computer nodes. We may collaborate on distributed sensor data processing algorithms and resource management methods for distributed network computing systems to reduce resource demand and usage.

Robustness: Device and wireless connection failures and unanticipated security attacks risk system robustness and security.

APPLICATIONS

Modern economy demands integrating cyber and physical worlds, expanding computer technology to all human activities, and integrating physical world-information systems.

The rapid proliferation of the Internet is expected to connect a variety of gadgets to evaluate information swiftly and govern the physical environment. Ubiquitous computing captured and processed data anywhere, anytime. Internet of things (IOT) stresses the connectivity and information exchange of all types of products utilizing sensing equipment like RFID and 802.15.4 to expand the original people-people interaction Internet into a content-content connection network. IOT uses omnipresent computers and networks. CPS includes IOT since it controls and perceives.

CPS are used in aerospace, highly credible medical devices and systems, manufacturing, traffic control, environmental control, critical infrastructure control (electricity, irrigation networks, communication systems), industrial production data collection automation, automated process control, energy consumption and regeneration, the next generation power grid, future defense systems, distribution, and more. As science and engineering advance, cyber-physical systems are expected to improve in areas like interventions (collision avoidance), precision (robotic surgery and nano-scale manufacturing), data mining (data classification, evaluation, predicted aggregation, etc.), dangerous or inaccessible operating environments (search and rescue, firefighting, and deep-sea exploration), coordination (air trajector), and US and EU CPS research is extensive. Since 2006, the NSF has supported CPS seminars with other government agencies.

CONCLUSION

CPS will impact and develop computer science and other areas across social and economic sectors. CPS progress is additionally hampered by processing, communications, and control theory and technology. Breakthrough in CPS essential technology will allow our country to lead the world in CPS development and create our own benchmark for national social and economic growth.

REFERENCES

1. *Z. Song, Y. Q. Chen, C. R. Sastry, and N. C. Tas, Optimal Observa- tion for Cyber-Physical Systems: A Fisher-Information-Matrix-Based Approach. London: Springer-Verlag, 2009.*
2. *R. Rajkumar, "A cyber-physical future," Proc. IEEEE, vol. 100, no. Special Centennial Issue, pp. 1309−1312, May 2012.*
3. *C. Tricaud and Y. Q. Chen, "Optimal mobile actuator/sensor network motion strategy for parameter estimation in a class of cyber physical systems," in Proc. 2009 American Control Conf., St. Louis, MO, 2009, pp. 367−372.*
4. *E. A. Lee, "Computing foundations and practice for cyber-physical systems: a preliminary report," Tech. Rep. UCB/EECS-2007-72, Uni- versity of California, Berkeley, May 2007.*
5. *J. F. He, "Cyber-physical systems," Commun. China Comput. Feder., vol. 6, no. 1, pp. 25−29, 2010.*
6. *G. R. Gonzalez, M. M. Organero, and C. D. Kloos, "Early infrastructure of an internet of things in spaces for learning," in Proc. 8th IEEE Int. Conf. Advanced Learning Technologies, Santander, Cantabria, 2008, pp. 381−383.*
7. *Y. Sun, B. McMillin, X. Q. Liu, and D. Cape, "Verifying nonin- terference in a cyber-physical system*

the advanced electric power grid," in Proc. 7th Int. Conf. Quality Software, Portland, OR, 2007, pp. 363−369.

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

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

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

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

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

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

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

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

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

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

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

19. *C. Qi and Y. He, "Design of data collection system based on CPS,"*

20. *Comput. Syst. Appl., vol. 19, no. 6, pp. 5−8, Jul. 2010.*

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

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

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

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

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

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

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

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

29. *W. Jiang, W. H. Guo, and N. Sang, "Periodic real-time message scheduling for confidentiality-aware*

cyber-physical system in wireless networks," in Proc. 5th Int. Conf. Frontier of Computer Science and Technology, Changchun, China, 2010, pp. 355−360.

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

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

32. U. Kremer, "Cyber-physical systems: a case for soft real-time", Ac- cessed on: May 1, 2013. [Online].

Available: http://www.research.rutgers.edu/~uli/Sarana/documents/CPS-Uli.pdf

33. H. Al-Omari, F. Wolff, C. Papachristou, and D. McIntyre, "Avoiding delay jitter in cyber-physical systems using one way delay variations model," in Proc. 2009 Int. Conf. Computational Science and Engineering, Vancouver,