Guest Editorial Special Issue on RRCPS: Reliable and Resilient Cyber-Physical Systems

A CYBER–PHYSICAL system (CPS) consists of physical devices and operations that are closely controlled and monitored by computational processes. This concrete connection involves the real-time actuation of physical devices, real-time sensing of physical quantities, and modeling and control of the overall system. A CPS may be connected to the Internet of Things (IoT) and, if so, should be considered in that context; the IoT is essential to realize a vision of future CPSs, where numerous devices are connected over the Internet, allowing them to collect information about the real world in real time, and share it with other systems and physical devices.

CPSs can provide both improved and new functionalities with efficiency and convenience. However, the increasing use of CPSs and their application to key infrastructure components means that failures (situations in which a system deviates from its expected, externally visible service) can result in disruption, damage, and even loss of life. Avoiding these outcomes is not a trivial problem, because a CPS, which can readily communicate with humans, remote computers, as well as other CPSs, is naturally vulnerable to network failures and malicious interference. Reports of such attacks and public concern about them have increased in recent years.

It is impossible to accurately predict the emergent behaviors of CPSs due to lack of trust—and, therefore, a lack of disclosure—between separate independent constituent systems. Moreover, it is usually too computationally expensive to explore all possible interactions between systems that comprise one CPS. The result of interactions that arise among the systems can be unpredictable, with the physical aspects of some constituents producing side effects on apparently unrelated constituents. Due to the complexity of CPSs, unexpected emergent behavior is prevalent, which creates challenges for the CPS engineer as *safety and dependability are global principles of the CPS*.

Dependable CPSs should be reliable, because their functionality and timing are provably correct (with regard to continuity in correct and timely service). Further, they should be resilient (alternatively called "fault tolerant") and guarantee no catastrophic consequences to the user(s) and the environment, because they are designed to cope with both internal errors and external attack. A resilient CPS will continue to operate normally as long as possible (by means of fault tolerance), and then provide functionality that reduces gracefully and safely if faults increase and cannot be overcome. Note that a fault is the adjudged or hypothesized cause of a failure, but not all faults present in a system necessarily lead to immediate failures. A fault may remain latent while the system transitions through a number of system states before entering a state that is capable of manifesting the fault as a service failure. Fault tolerance is the practice of attempting to detect and correct latent errors before they become effective, or the ability to avoid service failures even if faults are present within the system. In fact, a considerable number of techniques in the area of fault-tolerant CPS design focus on protecting the physical components in the presence of faults.

The design, development, deployment, and maintenance of these dependable CPSs require collaboration among a variety of disciplines, such as software, systems, mechanics, electronics, and system architectures, each with well-established notations, models, and methods. For example, the design of reliable and resilient CPSs (RRCPSs) directly involves aspects, such as real-time control, sensor design, and the IoT, as well as the application of machine learning and data mining to provide more sophisticated and versatile behavior. It should also be noted that a clear link exists between RRCPS and the concept of security. Security violations within a CPS may include external attacks or failures that affect the availability of information and dependability of CPSs.

This special issue, *Reliable and Resilient Cyber–Physical Systems*, covers both the theoretical and practical aspects of platforms on which RRCPS can be built and their applications. The latter include healthcare, power grids, urban infrastructure, manufacturing, automobiles, aircraft, and the construction industry (note that this is not an exclusive list). With 30 submissions from different corners of the world, the response to our call for papers for this special issue was quite satisfactory. During the review process, each paper was assigned to and reviewed by at least three experts in the relevant areas over a rigorous two-round review process. Thanks to the highly efficient administrative support from IEEE INTERNET OF THINGS JOURNAL, we were able to accept seven excellent articles covering various aspects of reliable and resilient CPS design.

In the article "Design Verifiably Correct Model Patterns to Facilitate Modeling Medical Best Practice Guidelines With Statecharts," the authors address safety problems in medical CPSs. In particular, the article addresses the correctness of

Digital Object Identifier 10.1109/JIOT.2019.2926610

computerized medical guidelines represented by statecharts, which describe the operational status of medical devices as states and transitions between the states raised by operational and environmental events (e.g., activate/deactivate device and low oxygen level). Multiple statecharts may execute simultaneously and independently and, thus, a proper synchronization through communication among them is required to avoid reaching unsafe states. Execution orders in statecharts are often required to be configurable so as to incorporate the experience and preference of individual medical practitioners. The authors propose model patterns to support these two-way communications and configurable execution orders in existing statechart modeling mechanisms without jeopardizing the underlying execution semantics. In addition, they present the techniques to transform statechart models into timed automata, and formal verification methods to verify the correctness of the transformation and safety properties. The authors demonstrate how the proposed mechanisms can be applied to a medical practice through a case study using UPPAAL timed automata.

Preserving the security and privacy of mobile healthcare data is one of the most important requirements in healthcare systems. Attribute-based encryption (ABE) offers a promising solution for flexible access control over sensitive personal data. However, naive application of ABE to mobile devices is not a pragmatic choice due to its substantial computation cost. The idea in the article "Trustworthy Delegation Toward Securing Mobile Healthcare Cyber-Physical Systems" is to delegate significant parts of the decryption operations of mobile devices to computationally powerful parties, such as cloud servers, while verifying the computation correctness. This paper demonstrates that the previous commitment or message authentication code (MAC)-based schemes cannot support verifiability in the presence of malicious cloud servers by suggesting two attack scenarios on previous commitment or MAC-based schemes. Then, it proposes a countermeasure for securing resource-limited mobile healthcare systems. Specifically, it introduces a generic tamper-resistant commitment scheme for mobile healthcare CPSs in the cloud environment, which can run on top of any ABE schemes with outsourced decryption capabilities. The experimental results demonstrate that the proposed scheme provides tamper resistance for verifiable outsourced decryption and shows performance similar to that of previous commitment-based schemes. Further, it outperforms the MAC-based scheme.

As an extended adaptation of its preliminary version, which appeared in the Proceedings of the 9th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS'18), the article "Preserving Physical Safety Under Cyber Attacks" introduces a design method for embedded control platforms with formal guarantees on the baseline safety of the physical subsystem when the software is under attack. The main purpose of this article is to enable consecutive evaluations of physical safety conditions within secure execution intervals separated in time such that an attacker with full control will not have enough time to destabilize or crash the physical plant between two consecutive intervals, called the secure execution interval (SEI). The time between consecutive SEIs is dynamically calculated in real time based on the mathematical model of the physical plant and its current state. The key to provide such formal guarantees is to ensure that each SEI takes places before an attacker can cause any physical damage. To establish a trusted execution environment (where the integrity of the executed code can be trusted), the authors utilized two different approaches: 1) restart-based implementation, which adopts full system restarts and software reloads, and 2) trusted execution environment (TEE)-based implementation, which adopts a TEE (such as ARM TrustZone). The proposed restart-based design implementation enables trusted computation in an untrusted environment. It uses platform restarts and common off-the-shelf components, and does not require chip customizations or specific hardware features. Alternative design implementation utilizes TEE to eliminate the restarting overhead while enabling the core safety guarantees to be provided for more challenging physical plants. The authors implemented and tested their approaches against attacks through a prototype implementation for a realistic physical plant and a hardware-in-the-loop simulation.

The article "MC-SDN: Supporting Mixed-Criticality Real-Time Communication Using Software-Defined Networking" is an extension of a preliminary work, which appeared in the Proceedings of 39th IEEE Real-Time Systems Symposium (RTSS'18). The authors propose a novel software-defined networking (SDN)-based networking architecture that supports mixed-criticality real-time flows in the IoT/CPS environment. Although it is promising to apply different scheduling policies according to the system criticality mode to guarantee different real-time requirements of different criticality flows, it is difficult to apply such mode-based scheduling to networking systems, in particular switched Ethernet, due to lack of controllability. To resolve this limitation, the authors try leveraging the flexibility of SDN while addressing a significant challenge: a long and an unpredictable delay in changing the system mode. The paper investigates major delay factors, redesigns the networking system to reduce and bound the delays, and evaluates the system with realistic testbeds, including a 1/10 scale autonomous vehicle. The evaluation results show that the proposed system effectively supports mode-based mixed-criticality scheduling. As the system presents a general architecture, it is applicable to various aspects of dynamic network management subject to real-time constraints.

The article "JMC: Jitter-Based Mixed-Criticality Scheduling for Distributed Real-Time Systems" proposes a novel jitter-based mixed-criticality scheduling framework for more reliable and efficient distributed IoT/CPS systems. Traditional real-time scheduling theories offer strict timing guarantees but suffer from inefficient resource management due to pessimistic analysis based on worst-case scenarios. The paper is the first of its kind to apply the concept of jitter to relax the pessimism on the response-time analysis of real-time flows in distributed systems. The concept accomplishes this by performing efficient resource management based on optimistic estimates and switches to inefficient management based on pessimistic analysis as soon as any optimistic estimate turns out to be inaccurate. To this end, it keeps track of the actual response time of each flow on each node (defined as "jitter") and compares it with an optimistic

response-time estimate (defined as "jitter threshold"). When an optimistic estimate is no longer valid (i.e., the actual response time is greater than the optimistic estimate), it employs a different scheduling strategy to overcome the invalid optimistic estimate. This framework presented in the paper involves an optimal feasibility condition of task schedulability and two effective jitter threshold assignment policies. Simulations show that jitter-based scheduling efficiently supports more low-criticality flows while preserving the strict timing guarantee for high-criticality flows. The key idea of relaxing the pessimism can be applied to other real-time systems.

In the article "A Stealthy Sensor Attack for Uncertain Cyber-Physical Systems," the authors present a study of a sensor attack on a CPS, which can be constructed with limited knowledge of the target system and can maintain stealth until the attack succeeds. The target CPS consists of a physical plant with unstable linear dynamics and a feedback controller. Specifically, the attack mechanism impedes the stabilizing function of the feedback controller by injecting false data to the sensors. The false data are created using the unstable dynamics of the plant. When only the nominal model for the target dynamics is known, the stealthiness is maintained by deploying a mechanism similar to a disturbance observer, which absorbs the effect of the mismatch between the nominal and actual dynamics until the attack succeeds. The success of the attack is defined by the norm of the system state exceeding a threshold. Note that sensor attacks that exploit unstable plant dynamics have been conceived previously. Generation of such attacks requires precise knowledge of the target system for stealthiness; that is, the attack must exactly cancel the effect of instability at the sensor in order to avoid detection. When not exact, the mismatch grows exponentially, leading to the detection of abnormality. The attack presented in this paper absorbs the mismatch using the disturbance observer mechanism, where the degree of absorption is selected such that the detection is delayed until the attack succeeds. Thus, the proposed attack poses a greater level of threat to the CPS compared to its conventional counterparts.

It is of great importance not only in theory, but also in practice, to guarantee resiliency of societal infrastructure from the perspective of CPSs. In particular, a train control system is a representative example of the most critical infrastructure, whose malfunction may result in disasters. In this regard, in the article "Cyber-Physical Vulnerability Analysis of Communication-Based Train Control," the authors analyze the resiliency issue of communication-based train control (CBTC) systems, which are being adopted worldwide as the next-generation *de facto* standard for train control. More specifically, the problem of cyber–physical attacks on a CBTC system is tackled from a realistic viewpoint. First, the authors investigate the cyber–physical vulnerability of a CBTC system and discover that a man-in-the-middle (MITM) attack combined with knowledge on train signaling can cause train collisions. By implementing a realistic CBTC testbed on top of a commercial train control and supervision software, the authors validate the vulnerability with a fault signal-injecting MITM attack based on address resolution protocol (ARP) spoofing. To resolve the issue, they further propose an SDN-based countermeasure to increase the resiliency of the CBTC operation. The empirical study shows that the proposed SDN countermeasure structure can handle the MITM attack based on ARP spoofing in real time and guarantees the reliable operation of the CBTC system.

We express our gratitude to the authors for their excellent contributions to this special issue on Reliable and Resilient Cyber–Physical Systems. We are also grateful to all the reviewers for dedicating their time and effort toward examining these papers, and for their valuable comments and constructive suggestions. Finally, we appreciate the advice and support of the Editor-in-Chief of IEEE INTERNET OF THINGS JOURNAL, Dr. Xuemin (Sherman) Shen, for his help in the publication process. We hope that this special issue will serve as a valuable reference for academicians, scientists, engineers, and practitioners working toward the design and implementation of reliable and resilient CPSs.

ACKNOWLEDGMENT

This special issue was supported by the Next-Generation Information Computing Development Program through the National Research Foundation of Korea funded by the Ministry of Science and ICT under Grant 2017M3C4A7083676.

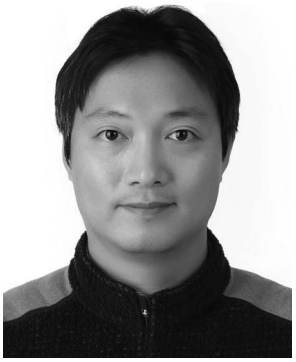
KYUNGTAE KANG
Department of Computer Science and Engineering
Hanyang University
Ansan 15588, South Korea

INSUP LEE
Department of Computer and Information Science
University of Pennsylvania
Philadelphia, PA 19104 USA

KAI LIU
College of Computer Science
Chongqing University
Chongqing 400044, China

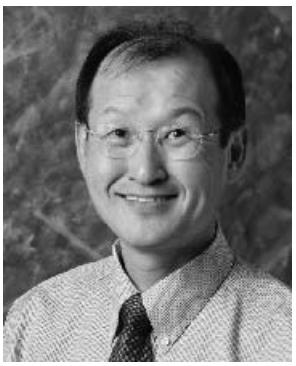
MAN-KI YOON
Department of Computer Science
Yale University
New Haven, CT 06520 USA

KYUNG-JOON PARK
Department of Information and Communication Engineering
Daegu Gyeongbuk Institute of Science and Technology
Daegu 42988, South Korea



Kyungtae Kang (S'08–M'11) received the B.S. degree in computer science and engineering and the M.S. and Ph.D. degrees in electrical engineering and computer science from Seoul National University, Seoul, South Korea, in 1999, 2001, and 2007, respectively.

He is the Founder of Cyber-Physical Systems Laboratory, Hanyang University, Seoul. From 2008 to 2010, he was a Post-Doctoral Research Associate with the University of Illinois at Urbana–Champaign, Urbana, IL, USA. In 2011, he joined the Department of Computer Science and Engineering, Hanyang University, where he is currently a Professor. His current research interests include primarily in systems, including operating systems, mobile systems, distributed systems, and real-time embedded systems. His recent research interest is in the interdisciplinary area of cyber-physical systems. He has published over 120 papers in the above areas, including 27 publications in prestigious IEEE journals, such as *Computer*, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON MOBILE COMPUTING, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON COMPUTERS, the IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE, the IEEE/ACM TRANSACTIONS ON NETWORKING, the IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, the IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, IEEE SYSTEM JOURNAL, and IEEE ACCESS. He also has published papers in prestigious conferences, such as ICDCS, MobiCom, MobiSys, and ICCPS.



Insup Lee (S'80–M'82–F'01) received the B.S. degree (Hons.) in mathematics and the M.S. and Ph.D. degrees in computer science from the University of Wisconsin–Madison, Madison, WI, USA, in 1977, 1978, and 1983, respectively.

He is a Cecilia Fitler Moore Professor of computer and information science and the Director of PRECISE Center, which he co-founded at the University of Pennsylvania, Philadelphia, PA, USA, in 2008, where he also holds a secondary appointment with the Department of Electrical and Systems Engineering. His current research interests include cyber-physical systems, real-time systems, embedded systems, high-confidence medical device systems, formal methods and tools, run-time verification, software certification, and trust management. He has been researching in medical cyber-physical systems and security of cyber-physical systems. The theme of his research activities has been to assure and improve the correctness, safety, and timeliness of life-critical embedded systems.

Prof. Lee was a recipient of the Best Paper Awards in IEEE RTSS 2003, CEAS 2011, IEEE RTSS 2012, ACM/IEEE ICCPS 2014, and IEEE CPSNA 2016, the Best Student Paper Award in IEEE RTAS 2012, the Appreciation Award from the Ministry of Science, IT and Future Planning, South Korea, in 2013, and the IEEE TC-RTS Outstanding Technical Achievement and Leadership Award in 2008. He has served on many program committees, chaired many international conferences and workshops, and served on various steering and advisory committees of technical societies. He has also served on the editorial boards on the several scientific journals, including the *Journal of ACM*, *ACM Transactions on Cyber-Physical Systems*, the IEEE TRANSACTIONS ON COMPUTERS, *Formal Methods in System Design*, and *Real-Time Systems Journal*. He was the Chair of ACM SIGBED from 2015 to 2018 and was the Chair of IEEE TC-RTS from 2003 to 2004. He was a member of Technical Advisory Group of President's Council of Advisors on Science and Technology Networking and Information Technology from 2006 to 2007. He was a member of the National Research Council's Committee on 21st Century Cyber-Physical Systems Education from 2014 to 2015. He is an ACM Fellow.

Kai Liu (S'07–M'12) received the Ph.D. degree in computer science from the City University of Hong Kong, Hong Kong, in 2011.

He is currently an Assistant Professor with the College of Computer Science, Chongqing University, Chongqing, China. From 2011 to 2014, he was a Visiting Scholar with the Computer Science Department, University of Virginia, Charlottesville, VA, USA, and a Post-Doctoral Fellow with Singapore Nanyang Technological University, Singapore, the City University of Hong Kong, Hong Kong, and Hong Kong Baptist University, Hong Kong. His current research interests include Internet of Vehicles, mobile computing, and pervasive computing. He has published over 80 papers, including over 40 publications in prestigious IEEE journals, such as the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, the IEEE TRANSACTIONS ON MOBILE COMPUTING, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE/ACM TRANSACTIONS ON NETWORKING, the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE INTERNET OF THINGS JOURNAL, and the *IEEE Communications Magazine*.

Man-Ki Yoon received the B.S. degree in computer science and engineering from Seoul National University, Seoul, South Korea, in 2009 and the Ph.D. degree in computer science from the University of Illinois at Urbana–Champaign, Urbana, IL, USA, in 2017.

He is an Associate Research Scientist of computer science with Yale University, New Haven, CT, USA. His current research interests include cyber-physical systems, security, real-time embedded systems, and learning-enabled autonomous systems.

Dr. Yoon was a recipient of the Qualcomm Innovation Fellowship in 2013, the Intel Ph.D. Fellowship in 2014, and the Qualcomm Roberto Padovani Scholarship in 2014.

Kyung-Joon Park (M'05) received the B.S. and M.S. degrees in electrical engineering from the School of Electrical Engineering, Seoul National University, Seoul, South Korea, in 1998 and 2000, respectively, and the Ph.D. degree in electrical engineering and computer science from Seoul National University in 2005.

From 2005 to 2006, he was a Senior Engineer with Samsung Electronics, Suwon, South Korea. From 2006 to 2010, he was a Post-Doctoral Research Associate with the Department of Computer Science, University of Illinois at Urbana–Champaign, Champaign, IL, USA. He is currently an Associate Professor with the Department of Information and Communication Engineering, Daegu Gyeongbuk Institute of Science and Technology, Daegu, South Korea. His current research interests include resilient cyber-physical systems and smart production systems.