Guest Editorial
Special Issue on Control of Cyber-Physical Systems

INTRODUCTION

CYBER-PHYSICAL systems are engineered systems whose operations are monitored, coordinated, controlled, and integrated by computing and communication components interacting with the physical environment. Cyber-physical systems transform how we interact with the physical world just like the Internet has transformed how we interact with one another. Advances in this field will have an enormous societal impact and economic benefit in areas such as energy, transportation, manufacturing, health, agriculture and many more.

Recently there has been a rapidly growing scientific and industrial interest in cyber-physical systems worldwide. While many scientific disciplines contribute to cyber-physical systems, the control systems community has been consistently engaged in the development of theories, tools, and practices for the design and operation of these systems. The aim of this special issue is to provide a window into the recent developments of the fundamentals and applications of control of cyber-physical systems.

THE ISSUE AT A GLANCE

The call for papers was very well received and 59 papers were submitted to the special issue. After a rigorous review process, 18 papers were selected for the special issue. In this brief summary, we have clustered the papers into five areas.

A. Abstraction and Verification

Cyber-physical systems are large inter-connected heterogeneous and networked systems with a variety of requirements. To be able to make formal guarantees for such systems despite that their components span multiple domains, it is important to develop mathematical and computational tools that are able to extract and reason about relevant levels of model abstractions. Five of the papers deal with challenges related to such abstraction and verification of cyber-physical systems. The paper by Aydin Gol *et al.* presents an algorithm that constructs a finite bisimulation quotient for switched linear systems. It is shown how the bisimulation quotient can be used for the synthesis of switching control laws and for the verification of specifications given in linear temporal logic. Zamani *et al.* extend symbolic design approaches for nonprobabilistic complex control systems to probabilistic systems modeled as stochastic differential equations. Guarantees are derived in terms of a probabilistic variant of incremental input-to-state stability and explicit bounds on approximate bisimulations. A new notion of robustness of cyber-physical systems is introduced in the paper by Tabuada *et al.* It is shown how to synthesize robust controllers and that efficient algorithms can be used. Tarraf studies discrete-time plants controlled through fixed discrete alphabets. A control design procedure is proposed for such systems with a guaranteed level of approximation. The paper by Rajhans *et al.* proposes an architecture framework for cyber-physical systems that uses structural and semantic mappings to ensure consistency and to enable system-level verification.

B. Cyber-Physical Security

Cyber-physical control systems are vulnerable to adversaries due to the use of open computation and communication platforms. As these systems integrate physical machines and its environment with cyber infrastructure, there are many points for potential attacks, some of which with drastic societal consequences. Conventional computer and information security approaches are in many cases not applicable for cybersecure control. The special issue includes three papers on this topic. The paper by Hendrickx *et al.* studies false data attacks, where scenarios with an adversary tampering with measurements through either the sensor or communication systems are considered. A security index is introduced and it is shown that it can be efficiently computed and used for vulnerability analysis for large systems, as illustrated by benchmark systems for electric power networks. A game-theoretic approach to the estimation of a binary random variable based on sensor measurements that may have been corrupted by a cyber attacker is developed by Vamvoudakis *et al.* Computationally efficient solutions for the construction of the optimal detector are derived. Wormhole attacks are considered in the paper by Lee *et al.* Wormholes allow the adversary to violate the timing constraints of real-time control systems by first creating lowlatency links, which attract network traffic, and then delaying or dropping packets. The impact and the mitigation of such attacks are discussed.

C. Resource-Constrained Embedded and Wireless Control

Cyber-physical systems are in many cases implemented over resource-constrained embedded platforms, which integrate limited computational capacity with wireless networking and control. Two papers deal with the optimal control design for such systems. The paper by Jerez *et al.* extend the use of model predictive control to systems with input, input rate, and soft state constraints arising from embedded implementation. It is shown that reliable operation can be ensured under reduced precision fixed-point arithmetic, through theoretical analysis as well as through real implementation in FPGA's. Demirel *et al.*

Digital Object Identifier 10.1109/TAC.2014.2363896

study wireless control loops with sensor measurements communicated over an unreliable and energy-constrained multihop wireless network. A modular design method is developed that jointly optimize packet forwarding policies and control commands.

D. Event-Based Estimation and Control

Asynchronous sensor and actuator communications are often desirable in cyber-physical control systems. Five of the papers handle event-based estimation and control systems supporting such implementation platforms. The paper by Quevedo *et al.* focuses on the problem of limited communication and computation capabilities. Stochastic stability is shown for a strategy where the sensor only transmits when the state lies outside a target set and control commands are computed and stored in a buffer for potential future use. Trimpe and Raffaello study an event-based state estimation problem where the sensors trigger their transmission to a fusion node only if their associated measurement prediction variance exceeds a certain threshold. The paper by Molin and Hirche proposes distributed self-regulating triggers that adapt their request rate to accommodate a global resource constraint. The problem is formulated as an average-cost Markov decision process with unknown global system parameters to be estimated online. An event-based control scheme with guaranteed quadratic performance for linear systems is developed in the paper by Antunes and Heemels, where ideas from so called rollout algorithms of dynamic programming are used. Tallapragade and Chopra consider a nonlinear state-feedback control problem where distributed sensors communicate asynchronously to a central controller. A design methodology for the sensor triggering condition based only on local information is developed.

E. Applications

There are many applications of cyber-physical systems. Some of the papers above illustrate their results on examples from transportation systems, power networks, smart buildings, process industry, etc. Three papers are devoted explicitly to applications, in particular, camera network tracking, autonomous ground transportation, and air traffic control. In the paper by Tron and Vidal, distributed algorithms that use 2D image measurements for a camera sensor network to estimate 3D poses are developed. The algorithms combine local noisy estimates into a single consistent localization, as illustrated on both synthetic and real data. Kim and Kumar propose an approach based on model predictive control for the development of provably collision-free autonomous ground transportation systems. Based on two vehicle-to-vehicle coordination rules, along with a vehicle-to-infrastructure rule, system-wide safety and liveness of autonomous traffic based on each vehicle's motion planner are established. Finally, the paper by Park *et al.* addresses the design of a secure and fault-tolerant air transportation system in the presence of attempts to disrupt the operation through satellite-based navigation systems. A framework is proposed for the identification of adversaries and malicious aircraft.

ACKNOWLEDGMENT

The guest editors wish to thank all the authors, for their submissions, and the large number of reviewers, who carefully and timely scrutinized and evaluated the many papers submitted.

Karl H. Johansson, *Guest Editor*
ACCESS Linnaeus Center and School of
Electrical Engineering
KTH Royal Institute of Technology
10044 Stockholm, Sweden
kallej@kth.se

George J. Pappas, *Guest Editor*
Department of Electrical and
Systems Engineering
University of Pennsylvania
Philadelphia, PA 10104 USA
pappasg@ee.upenn.edu

Paulo Tabuada, *Guest Editor*
Department of Electrical Engineering
University of California, Los Angeles
Los Angeles, CA 90095 USA
tabuada@ee.ucla.edu

Claire J. Tomlin, *Guest Editor*
Department of Electrical Engineering
and Computer Sciences
University of California, Berkeley
Berkeley, CA 94720 USA
tomlin@eecs.berkeley.edu