Cyber-Physical Systems and Internet-of-Things Week

Submitted by Anonymous on Wed, 09/05/2018 - 1:00pm
Apr 15, 2019 7:00 am - Apr 18, 2019 6:00 pm EDT

CPS Week is the premier event on Cyber-Physical Systems. It brings together four top conferences, HSCC, ICCPS, IPSN, and RTAS, multiple workshops, tutorials, summits, and various exhibitions from both industry and academia. Altogether the CPS Week program covers a multitude of complementary aspects of CPS.

Conferences - 16-18 April 2019

- HSCC - ACM International Conference on Hybrid Systems: Computation and Control
- ICCPS - ACM/IEEE International Conference on Cyber-Physical Systems
- IPSN - ACM/IEEE International Conference on Information Processing in Sensor Networks
- RTAS - IEEE Real-Time and Embedded Technology and Applications Symposium
- IoTDI - ACM/IEEE Conference on Internet of Things Design and Implementation

Workshops - 15 April 2019

6th International Workshop on Applied veRification for Continuous and Hybrid Systems (ARCH19)

This workshop aims at bringing together researchers and practitioners, and to establish a curated set of benchmarks submitted by academia and industry.

Verification of continuous and hybrid systems is increasing in importance due to new cyber-physical systems that are safety- or operation-critical. This workshop addresses verification techniques for continuous and hybrid systems with a special focus on the transfer from theory to practice.

4th Workshop on Monitoring and Testing for Cyber-Physical Systems (MT-CPS 2019)

Cyber-physical systems (CPS) model the integration of computational modules, like decision logic, with physical phenomena in the environment, such as the phenomenon being controlled by the logic. Several CPS applications, such as self-driving cars and other autonomous ground/aerial/underwater vehicles, medical devices, surgical robots, as well as many Internet of Things (IoT) applications, particularly for Industrial IoT or Industry 4.0, are safety-critical, where human lives can be at stake. CPS exhibit complex and unpredictable behaviors, thus making their correctness and robustness analysis a challenging task. Given the gap between the complexity of such systems and the scalability of current formal methods, exhaustive formal verification remains an elusive goal. However, simulation-based lightweight verification techniques, such as monitoring and testing, achieve both rigor and efficiency by enabling the evaluation of systems according to the properties of their exemplar behaviors. The Workshop on Monitoring and Testing of Cyber-Physical Systems (MT-CPS) aims to bring together researchers and practitioners interested in the problems of detecting, testing, measuring, and extracting qualitative and quantitative properties from individual behaviors of CPS.

7th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES2019)

Automation and digitalization have become important topics in the energy sector in recent years, as modern energy systems increasingly rely on communication and information technology to combine smart controls with hardware infrastructure. With the emergence of cyber-physical systems (CPS) as a transdisciplinary field, such modern energy systems can be classified as cyber-physical energy systems (CPES), integrating the related research and development within a broader scope.

An important aspect of the research and development related to CPS is to bridge the gap between the traditional engineering domains and computer science. This is especially true for CPES, where the related engineering domains have in the past come up with proven and reliable methods for designing even large and complex systems. However, existing modeling and simulation tools still struggle to cover all aspects of CPES. Hence, a combination of universal modeling languages and established, domain-specific tools (like grid simulators and telecommunication simulators) is necessary. New methods, tools and algorithms are needed that are compact, computationally inexpensive, potentially self-organizing and intrinsically stable if applied to real energy systems.

2nd Workshop on Benchmarking Cyber-Physical Systems and Internet of Things (CPS-IoTBench)

Over the last decade, research on cyber-physical systems (CPS) and Internet of Things (IoT) has led to smart systems at different scales and environments, from smart homes to smart cities and smart factories. Significant progress has been made through contributions in areas as diverse as control, embedded and real-time systems, wireless communication, and networking. Despite these advances, it is difficult to measure and compare the utility of these results due to a lack of standard evaluation criteria and methodologies. This problem concerns the evaluation against the state of the art in an individual area, the comparability of different integrated designs that span multiple areas (e.g., control and networking), and the applicability of tested scenarios to the present and future real-world CPS and IoT applications and deployments. This state of affairs is alarming as it may significantly hinder further progress in CPS and IoT research.

The 2nd Workshop on Benchmarking Cyber-Physical Systems and Internet of Things (CPS-IoTBench) brings together researchers from the different sub-communities to engage in a lively debate on all facets of rigorously evaluating and comparing CPS and IoT solutions. CPS-IoTBench provides a venue for learning about each other's challenges and evaluation methodologies and for debating future research agendas to jointly define the performance metrics and benchmarking scenarios that matter from an overall system's perspective.

1st Workshop on Next-Generation Operating Systems for Cyber-Physical Systems (NGOSCPS): On Beyond POSIX

The theme of this first edition of the International Workshop on Next-Generation Operating Systems for Cyber-Physical Systems (NGOSCPS) is "On Beyond POSIX." This theme is intended to start a cohesive new conversation across a wide swath of the cyber-physical systems research community about (1) the key limitations of current operating system architectures, abstractions, semantics, models, designs, implementations, and verification and validation methods; and (2) what innovative new research problems, agendas, and overall directions should be pursued towards overcoming those limitations.

Symbolic-Numeric Methods for Reasoning about CPS and IoT (SNR)

The workshop on Symbolic-Numeric methods for Reasoning about CPS and IoT (SNR) focuses on the combination of symbolic and numeric methods for reasoning about Cyber-Physical Systems and the Internet of Things to facilitate model identification, specification, verification, and control synthesis problems for these systems. The synergy between symbolic and numerical approaches is fruitful for two main reasons:

- Symbolic methods that operate on exact and discrete representations of systems, the set of reachable states, the distribution of model parameters or the possible gains for controller parameters.
- Numeric methods that operate on various forms of numerical approximations and continuous transformations of the systems, as developed in the area of continuous dynamical systems and control theory.

Such synergies are already seen in areas such as reachability analysis (symbolic representation of reachable states versus numerical integration), uncertainty reasoning (eg., Rao-Blackwellization), machine learning (eg., learning models through stochastic gradient descent versus symbolic reasoning over the function represented by the network to prove properties) and decision procedures (eg., symbolic SAT solvers versus numerical convex optimization solvers).

Fog Computing and the Internet of Things

When Cyber-Physical Systems (CPS) become interconnected with each other and with the internet, they form the Internet of Things (IoT), forming "the infrastructure of the information society." Fog Computing is a "system-level architecture that distributes resources and services of computing, storage, control and net-working anywhere along the continuum from Cloud to Things" and is about to tremendously impact the IoT. The objective of this workshop is to be a forum for presenting and discussing recent developments and trends in Fog/Edge Computing that represent challenges and opportunities for CPS and IoT researchers and practitioners.

1st Workshop on Design Automation for CPS and IoT (DESTION 2019)

Cyber-Physical Systems (CPS) and Internet-of-Things (IoT) such as autonomous vehicles, industrial robots, and medical devices, promise immense economic and societal benefits. The design and operation of CPS and IoT, however, face tremendous challenges from the fast increase of system scale and complexity, the close interaction with dynamic physical environment and human activities, the adoption of multicore and distributed architectural platforms, and the stringent and diverse requirements on performance, safety, security, fault tolerance, extensibility, energy consumption, etc. Many key processes in current CPS and IoT design practices are ad-hoc (and often manual), and have shown to be incapable of coping with such challenges. It is thus critical to have a new set of design automation methodologies, algorithms and tools for improving CPS and IoT design quality, scalability, reliability and productivity. Most importantly, these methodologies, algorithms and tools will facilitate a bold move from ad hoc CPS and IoT design towards systematic and formal techniques.

ACM/IEEE DESTION provides a premier forum for researchers and engineers from academia, industry, and government to present and discuss pressing challenges, promising solutions, and emerging applications in design automation for CPS and IoT. The conference has a broad scope covering modeling, simulation, synthesis, validation and verification tools and methods for CPS and IoT, and their

4th International Workshop on Social Sensing (SocialSens 2019)

SocialSens 2019 invites researchers and engineers from academia, industry, and government to present recent advances in both theoretical and experimental research on social sensing topics. This effort stems from the observation that social networks can be viewed as new types of "sensors" that carry information on what happens in the physical world. There is therefore much benefit from an exchange of ideas between the relevant communities from physical and social backgrounds, including sensing, data fusion/mining, signal processing, social networks, cognitive modeling, computational social and behavior science, and

IoT/CPS, among other topics. In particular, we are interested in efforts that combine, or point towards combinations, of advanced quantitative modeling with rigorous social and behavioral science theory. Social sensing advances the foundations of data collection and processing that exploits social and physical sources. At present, no forum brings those communities together. SocialSens aims to become one such forum.

2nd International Workshop on Security and Privacy for the Internet-of-Things (IoTSec)

The Internet-of-Things (IoT) has taken off in a big way and finds itself embedded in our daily lives - from smart home applications to process control monitoring in manufacturing systems, wearables to healthcare, public utilities to military applications, to name just a few. The surge in interest in smart cities increases the scope and reach of IoT-style applications in a significant manner. These applications generate huge volumes of data, have access to personal and confidential information, monitor and control critical processes and are often accessed/controlled via public networks such as the Internet. Hence, they are prime targets for malicious entities and have little to no security mechanisms in place. In addition, most users of such devices/systems are not cognizant of the privacy issues - leakage of personal information for instance, or external entities being able to retrace/recreate our activities from public data obtained through the use of IoT devices/services. On the other hand, onerous security and privacy mechanisms may render these systems useless for most consumers. Hence, there is a need to develop innovative techniques to improve protections for such systems. This is particularly challenging since many IoT systems are often limited in terms of computation power, memory, battery life, bandwidth, etc.

Hence, the goal of IoTSec will be to bring together experts in various areas (security, privacy, embedded systems, sensor networks, etc. along with domains experts from medicine, manufacturing systems, mobile devices and so on) to study and develop security and (usable) privacy mechanisms for next generation IoT systems.

2nd Workshop on Cyber-Physical Systems Security and Resilience (CPS-SR)

Cyber-physical systems underpin many of the critical infrastructures that our society depends on. As a consequence, they have very high reliability and availability requirements. Recently, there have been a number of high-profile cyber-attacks to critical infrastructures, which include cyber-physical systems, that have resulted in major disruptions in the physical domain. These threats include a sophisticated cyber-attack component, whose aim is to manipulate the control behaviour of a target system.

To address these threats, a multi-disciplinary approach is necessary that draws on and integrates research findings from cyber security, resilient control, formal methods, human factors, and applied knowledge of the cyber-physical system under attack, for example. The aim of the workshop is to bring together leading researchers in disciplines that are related to ensuring the security and resilience of cyber-physical systems, to discuss hot topics and research directions that will lead to (reusable) solutions that are applicable to numerous forms of cyber-physical system.

4th International Science of Smart City Operations and Platforms Engineering in partnership with Global City Teams Challenge

The problems of 'closing-the-loop' in smart city application areas are compounded due to the spatial and temporal scales of operation, heterogeneity, and complexity of the underlying physical systems, their interaction with socio-economic behaviors, and risks of cybersecurity and privacy. This workshop aims to focus on these problems and the innovative solutions in this area.

1st International Workshop on Smart Manufacturing Modeling and Analysis (SM^{2}N)

Today's manufacturing paradigm is in the midst of a transformation towards smart manufacturing, driven by the generation and analysis of high-volume data coming from interconnected cyber-physical components. This has necessitated an advancement in a number of the tenets of smart manufacturing such as Industrial Internet of Things (IIoT), Artificial Intelligence (AI), anomaly detection, security of industrial plants, novel communication infrastructures, etc. Among the many Smart Manufacturing tenets, a "digital twin" (DT) represents an opportunity to leverage existing and emerging technologies in modeling, simulation and emulation - to improve quality, productivity, and the ability to customize, and reduce energy consumption and waste. While DTs might help address many key performance and effectiveness metrics in manufacturing, however the science needs to be better understood in terms of definitions, capabilities, metrics, technical challenges and potential solutions. There exist some academic and industry efforts that aim to tackle this problem, but more is required. In addition, digital twins are just one way to model theses type of systems; to improve the overall design, efficiency and even security of future manufacturing systems, there is a need for new science that can capture/explain their behavior and new tools for modeling them.

In this workshop, we intend to bring together multidisciplinary researchers and engineers (from academia, industry, as well as standards organizations) from a broad range of fields (manufacturing, control, cyber-security, networking) to provide an overview of the latest advances in the modeling and analysis of smart manufacturing systems. This area (smart manufacturing and especially modeling/analysis) has not received much focus but is an important area, not just from the research perspective but also from societal impact. It includes all the elements of a classic cyber-physical systems domain, in addition to IoT (industrial IoT).

Tutorials - 15 April 2019

- Schedulability analysis of AADL architecture models
- Security of Cyber-Physical Additive Manufacturing System - Challenges and Research Opportunities

Competitions - 15 April 2019

- 4th F1/10 International Autonomous Racing Competition
- Device-Free Localization Competition
- armasuisse aircraft localization competition

Other - 15 April 2019

- IPSN PhD Forum

Important Dates

- Paper Submission: October 17, 2018, AOE (firm)
- Workshops/Tutorials: April 15, 2019
- Conference: April 16-18, 2019

Event Details

Location: Montreal, Canada
URL: http://cpsweek.org

Sync this event to your calendar

CPS-IoT Week 2019 2019 Conference