0018-9162/17/$33.00 © 2017 IEEE

CYBER-PHYSICAL SYSTEMS

Stefano Zanero, Politecnico di Milano

Our society increasingly relies on the successful marriage of digital and physical systems to perform advanced automation and control tasks. Engineering these cyber-physical systems to ensure their efficiency, security, and dependability is a research area of tremendous importance.

In many real-world systems, computational and physical resources are strictly interconnected: embedded computers and communication networks govern physical actuators that operate in the outside world and receive inputs from sensors, creating a smart control loop capable of adaptation, autonomy, and improved efficiency. Such systems are commonly and broadly defined as cyber-physical systems (CPSs).[1]

Common examples of CPSs include industrial control systems (now particularly interesting in light of the so-called Industry 4.0 developments, which are in essence a tight integration of information systems, company data, and computerized production systems), computerized vehicle and aircraft controls, wireless sensor networks, smart grids, and almost all devices typically encompassed by the Internet of Things.[2] Many medical devices, particularly implantable ones such as pacemakers, are also becoming CPSs.[3,4] Such systems are often key components of modern critical infrastructure, and thus are essential to our society's economic viability and social stability. For these reasons, the security, safety, and reliability of CPSs are critically important research areas.

Unique CPS challenges arise when we combine the computational framework (which is, by definition, discrete and adherent to rigid specifications) with a continuous physical system (which is often neither easily modeled nor completely understood). Adaptability and survivability are thus key elements of many CPSs.

Another challenge in working with CPSs is that they must be autonomous, as many are increasingly designed to function without a human in the control loop. Self-driving cars—highly complex CPSs with an array of sensors and actuators that possess external connectivity to the road infrastructure and often the Internet—are a key example of this and a very hot research area.[5]

These complex autonomous systems, which interact digitally and physically, will evolve to become a cloud-like, transparent infrastructure supporting our daily activities. Designing these systems' desired behaviors will be as important as being able to analyze the emerging properties and potentially surprising results of their interactions.

As a final challenge, most CPSs are constrained by environmental and operational limitations such as low computational power, battery life considerations, communication ranges, and bandwidth.

The combination of the keen interest in and explosive deployment of CPSs, along with the inherent challenges in designing, implementing, and operating them securely and safely, make CPSs an interesting, timely, and very challenging research area to which we dedicate this special issue of *Computer*.

IN THIS ISSUE

In "Using Information-Flow Methods to Analyze the Security of Cyber-Physical Systems," Gerry Howser and Bruce McMillin approach the unique

ABOUT THE AUTHOR

STEFANO ZANERO is an associate professor in the Department of Electronics, Information, and Bioengineering at Politecnico di Milano. His research interests include cybersecurity, computer virology, and the security of cyber-physical systems. Zanero received a PhD in computer engineering from Politecnico di Milano. He is a Senior Member of IEEE and ACM, a Fellow of the Information Systems Security Association (ISSA), and a member of the Board of Governors of the IEEE Computer Society and the international board of directors of the ISSA. Contact him at stefano.zanero@polimi.it.

confidentiality- and integrity-related vulnerabilities posed by CPSs using the methodology of information-flow security. They present ways to solve the issues posed by the combination of discrete "cyber" elements and continuous "physical" elements, integrating their respective information flows in a unified security model.

In "A Cloud-Integrated, Multilayered, Agent-Based Cyber-Physical System Architecture," Teodora Sanislav, Sherali Zeadally, and George Dan Mois attempt to tackle well-known CPS complexity and architectural challenges. They observe that problems related to the interoperability of heterogeneous components, distributed computation, and efficient management of large data collections have already been studied in the realms of intelligent-agent technologies and cloud computing. Thus, they propose incorporating lessons learned from these fields into a reference architecture, which they then evaluate in a case study of a cloud-based CPS for monitoring environmental parameters.

Finally, in "The (Not) Far-Away Path to Smart Cyber-Physical Systems: An Information-Centric Framework," Cesare Alippi and Manuel Roveri analyze the case of pervasive CPSs, which consist of a high number of low-cost sensors, and propose INformation-Centric Adaptive Systems (INCAS), a framework that supports intelligent energy management, adaptation, and fault detection and diagnosis at sensor and actuator levels. They also approximate the computing functionalities in such systems. Currently, such characteristics are studied in a fragmented manner, but a comprehensive understanding is in order to ensure that smart CPSs are resilient to change.

The articles in this theme issue provide insight into some of the deep, intriguing research questions surrounding the design, implementation, and operation of CPSs, and we hope you find them interesting. Many aspects remain open for investigation. For instance, how do we ensure the availability of back-end services that are needed to keep IoT devices up and running? What are the underlying economics? How can we ensure that the necessary security updates can be written and deployed in a timely manner? How do we model and properly design for interactions among a high number of heterogeneous devices?

As the adoption of CPSs increasingly offers tremendous potential advantages, the engineering challenges we face are breathtaking.

REFERENCES

1. E.A. Lee, "Cyber Physical Systems: Design Challenges," *Proc. 11th IEEE Int'l Symp. On Object and Component-Oriented Real-Time Distributed Computing* (ISORC 08), 2008, pp. 363–369.
2. "IEEE Smart Grid Initiative," IEEE; smartgrid.ieee.org.
3. M. Rushanan et al., "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks," *Proc. 2014 IEEE Symp. Security and Privacy* (S&P 14), 2014, pp. 524–539.
4. S. Zanero and E. Evenchick, "Up Close and Personal: Cybersecurity in Medical IoT Devices," *Proc. 38th IEEE Int'l Conf. Eng. Medicine Biology Soc.* (EMBS 16), 2016.
5. E. Guizzo, "How Google's Self-Driving Car Works," *IEEE Spectrum*, 18 Oct. 2011; spectrum.ieee.org/automaton/robotics/artificial-intelligence/how-google-self-driving-car-works.