

**SPECIAL ISSUE**

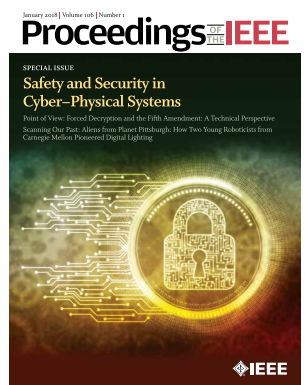
**SAFE AND SECURE CYBER-PHYSICAL SYSTEMS**

*Edited by M. Wolf and D. Serpanos*

- 9 Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems**  
*By M. Wolf and D. Serpanos*  
**|INVITED PAPER|** This paper identifies key issues in the safety and security of CPSs and Internet-of-Things (IoT) systems as well as design-time and runtime approaches to handle safety and security.
- 21 System-on-Chip Platform Security Assurance: Architecture and Validation**  
*By S. Ray, E. Peeters, M. M. Tehranipoor, and S. Bhunia*  
**|INVITED PAPER|** This paper surveys the security of VLSI systems-on-chip, identifies potential concerns, and proposes new approaches.
- 38 Wireless Communication and Security Issues for Cyber-Physical Systems and the Internet-of-Things**  
*By A. Burg, A. Chattopadhyay, and K.-Y. Lam*  
**|INVITED PAPER|** This paper looks at wireless communication used for CPS and IoT; the authors identify gaps between the vulnerabilities posed by cyber-physical and IoT applications and the security measures provided by wireless standards.
- 61 HoneyBot: A Honeypot for Robotic Systems**  
*By C. Irvine, D. Formby, S. Litchfield, and R. Beyah*  
**|INVITED PAPER|** This paper describes a novel honeypot for robotic systems. Honeypots are internet computers that are set up as lures for attackers.
- 71 Parameter-Invariant Monitor Design for Cyber-Physical Systems**  
*By J. Weimer, R. Ivanov, S. Chen, A. Roederer, O. Sokolsky, and I. Lee*  
**|INVITED PAPER|** This paper describes techniques for online monitoring of CPSs that are robust in the face of sparse data and system variability.
- 93 SURE: A Modeling and Simulation Integration Platform for Evaluation of Secure and Resilient Cyber-Physical Systems**  
*By X. Koutsoukos, G. Karsai, A. Laszka, H. Neema, B. Potteiger, P. Volgyesi, Y. Vorobeychik, and J. Sztipanovits*  
**|INVITED PAPER|** This paper describes a modeling and simulation environment that can be used to evaluate attacker-defender behavior.
- 113 A Framework for Attack-Resilient Industrial Control Systems: Attack Detection and Controller Reconfiguration**  
*By K. Paridari, N. O'Mahony, A. El-Din Mady, R. Chabukswar, M. Boubekeur, and H. Sandberg*  
**|INVITED PAPER|** This paper describes an industrial control systems policy that uses estimations to provide resiliency against attacks.
- 129 ARMET: Behavior-Based Secure and Resilient Industrial Control Systems**  
*By M. T. Khan, D. Serpanos, and H. Shrobe*  
**|INVITED PAPER|** This paper describes a reliable/secure-by-design methodology for industrial control systems and complementary online monitoring approach.

**DEPARTMENTS**

- 3 POINT OF VIEW**  
**Forced Decryption and the Fifth Amendment: A Technical Perspective**  
*By S. B. Wicker*
- 7 SCANNING THE ISSUE**  
**Safe and Secure Cyber-Physical Systems**  
*By M. Wolf and D. Serpanos*
- 201 SCANNING OUR PAST**  
**Aliens From Planet Pittsburgh: How Two Young Roboticians From Carnegie Mellon Pioneered Digital Lighting**  
*By B. Johnstone*
- 209 FUTURE SPECIAL ISSUE/SPECIAL SECTIONS**



**On the Cover:** Our cover image aptly represents the topic of cyber-security which is the key theme of this month's issue.

[Continued on page 2 ▶]

SPECIAL ISSUE: Safe and Secure Cyber-Physical Systems

**144 Improving the Safety and Security of Wide-Area Cyber-Physical Systems Through a Resource-Aware, Service-Oriented Development Methodology**

By *M. U. Tariq, J. Florence, and M. Wolf*

**INVITED PAPER** This paper describes a service-oriented architecture for CPSs that preserves the quality-of-service (QoS) requirements of real-time control.

**160 Privacy and Integrity Considerations in Hyperconnected Autonomous Vehicles**

By *S. Karnouskos and F. Kerschbaum*

**INVITED PAPER** This paper examines the privacy and data integrity issues in the operation of fleets of cooperating, autonomous vehicles.

**171 Semantics-Preserving Cosynthesis of Cyber-Physical Systems**

By *D. Roy, L. Zhang, W. Chang, S. K. Mitter, and S. Chakraborty*

**INVITED PAPER** While control theory provides methods for designing provably correct controllers, there is a lack of available techniques to ensure that high-level controller models are transformed into implementations while preserving model-level semantics and safety properties. This paper reviews recent efforts to address this issue using cyber-physical system (CPS)-oriented controller/platform cosynthesis techniques.

**Proceedings** OF THE **IEEE**

On the Web

[proceedingsoftheieee.ieee.org](http://proceedingsoftheieee.ieee.org)

Find the following information on our website.

- About the Proceedings
- Recent and Upcoming Issues
- Featured and Popular Articles
- Instructions for Guest Editors and Authors
- Editorial Leadership
- Webinar Series
- Subscription Information



On the Web

[www.ieee.org](http://www.ieee.org)

**MEMBERSHIP**

Check out the many features available through the IEEE Membership Portal.

**PUBLICATIONS**

Find IEEE articles by using the search features of IEEE Xplore

**SERVICES**

The IEEE offers many services to Members, as well as other groups.

**STANDARDS**

The IEEE is the leader in the development of many industry standards.

**CONFERENCES**

Search for the ideal IEEE Conference, on the subject of your choice

**CAREERS/JOBS**

Find your next job through this IEEE service.