IEEE Control Systems MAGAZINE

APRIL 2017 VOLUME 37 NUMBER 2

Tribute to Prof. Rudolf Kalman

High-Assurance Control

Control Systems Society
Advancing Control Science and Technology

IEEE

IEEE control systems MAGAZINE

April 2017 Volume 37 Number 2

WWW.IEEECSS.ORG/PUBLICATIONS/CSM

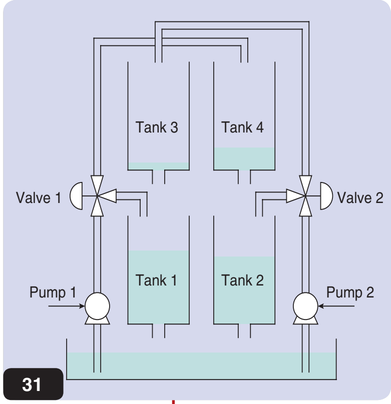
FEATURES

DEPARTMENTS

Cover credit: Highlighting the high-assurance control issues for cyberphysical systems (courtesy Nicola Bezzo). Inset: Prof. Rudolf Kalman (photo courtesy of the National Academy of Engineering, United States).

Digital Object Identifier 10.1109/MCS.2016.2643481

» DEPARTMENTS



31

153

IEEE PERIODICALS MAGAZINES DEPARTMENT
445 Hoes Lane, Piscataway,
NJ 08854 USA

Senior Managing Editor
Geraldine Krolin-Taylor

Senior Art Director
Janet Dudar

Associate Art Directors
Gail A. Schnitzer, Mark Morrissey

Production Coordinator
Theresa L. Smith

Advertising Production Manager
Felicia Spagnoli

Production Director
Peter M. Tuohy

Director, Business Development — Media & Advertising
Mark David

Editorial Director
Dawn M. Melley

Staff Director Publishing Operations
Fran Zappulla

IEEE prohibits discrimination, harassment, and bullying. For more information, visit http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html.

MISSION STATEMENT AND SCOPE: As the official means of communication for the IEEE Control Systems Society, *IEEE Control Systems Magazine* publishes interesting, useful, and informative material on all aspects of control system technology for the benefit of control educators, practitioners, and researchers. With this mission statement in mind, *IEEE Control Systems Magazine* encourages submissions, both feature articles and columns, on all aspects of control system technology.

SUBMISSION OF MANUSCRIPTS: A feature article typically provides an in-depth treatment of either an application of control technology, a tutorial on some area of control theory, or an innovation in control education.

IEEE Control Systems Magazine publishes a variety of columns. "Applications of Control" columns are industrially oriented summaries of innovations in control technology. "Focus on Education" typically describes some aspect of education such as novel control experiments. "Lecture Notes" can be theoretical in nature as long as they have clear tutorial value and intent. See recent issues for examples of these and other types of columns. Authors are encouraged to contact the editor-in-chief about the suitability of potential columns.

A detailed Author's Guide, a sample formatted manuscript, and LATEX template can be found at http://www.ieeecss.org/publications/csm/submissions. The specifications in this Guide should be followed by all submissions.

All manuscripts should be submitted electronically to the *IEEE Control Systems Magazine* website, https://css.paperplaza.net/conferences/scripts/start.pl, with inquiries on appropriateness of content emailed to jhow@mit.edu.

SPECIAL ISSUES: *IEEE Control Systems Magazine* encourages proposals for special issues. Proposers are encouraged to contact the editor-in-chief to discuss potential topics.

BOOKS AND CONFERENCES: Submit information about recently published books to the associate editor for book reviews. Submit information about past and future conferences to the corresponding editor for conferences.

ADVERTISING: *IEEE Control Systems Magazine* accepts advertising for educational products, books, software, conferences, employment, and control-related technology. For information about advertising, contact Mark David, m.david@ieee.org, +1 732 465 6473.

IEEE CONTROL SYSTEMS MAGAZINE—(ISSN 1066-033X) (ISMAD7) is published bimonthly by The Institute of Electrical and Electronics Engineers, Inc. Headquarters: 3 Park Avenue, 17th Floor, New York, NY 10016-5997, U.S.A. +1 212 419 7900. Responsibility for the contents rests upon the authors and not upon the IEEE, the Society, or its members. The magazine is a membership benefit of the IEEE Control Systems Society, and subscriptions are US$4.00 per member per year (included in Society fee). Replacement copies for members are available for US$20.00 (one copy only). Nonmembers can purchase individual copies for US$103.00. Nonmember subscription prices are available on request. Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limits of the U.S. Copyright law for private use of patrons: 1) those post-1977 articles that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01970, U.S.A.; and 2) pre-1978 articles without fee. For other copying, reprint, or republication permission, write to: Copyrights and Permissions Department, IEEE Service Center, 445 Hoes Lane, Piscataway NJ 08854, U.S.A. Copyright © 2017 by The Institute of Electrical and Electronics Engineers, Inc. All rights reserved. Periodicals postage paid at New York, NY and at additional mailing offices. Postmaster: Send address changes to *IEEE Control Systems Magazine*, IEEE, 445 Hoes Lane, Piscataway, NJ 08854 U.S.A. Canadian GST #125634188 Printed in U.S.A

High-Assurance Control

This edition of *IEEE Control System Magazine* (*CSM*) includes several articles focused on high-assurance control systems and a collection of tributes to Prof. Rudolf Kalman, who passed away on July 2, 2016. Darren Cofer arranged the collection of features from recent research on the High-Assurance Cyber Military Systems (HACMS) program. DARPA initiated the HACMS research program to create technology for the construction of high-assurance cyberphysical systems (CPSs) [1]. HACMS research is focused on vehicle control systems (both air and ground) because of the inherent complexity, criticality, and significance for the military and

Digital Object Identifier 10.1109/MCS.2016.2643219
Date of publication: 17 March 2017

Contributors

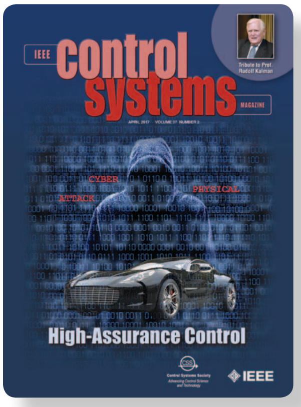
Noortje Groot speaking at a graduation ceremony.

Sam Coogan overlooking Fan Canyon while hiking in Joshua Tree National Park, California.

Anders Lindquist speaking at Shanghai Jiaotong University.

Yutaka Yamamoto

civilian applications. The program is developing new technologies based on formal methods that enable semi-automated code synthesis from executable, composable, formal specifications that are subject to analytic verification. The term “formal methods” refers to the analysis of software (or models of software) to prove its conformance to specifications. The use of analytic techniques for verification is, of course, standard practice in the control community, but it is still relatively new for software engineering. This issue includes three features related to HACMS and an additional article on the use of formal methods in traffic flow networks.



The article “Design and Implementation of Attack-Resilient Cyberphysical Systems,” by Miroslav Pajic, James Weimer, Nicola Bezzo, Oleg Sokolsky, George J. Pappas, and Insup Lee, describes the development of attack-resilient CPSs. The article considers the case of designing a resilient cruise controller for an autonomous ground vehicle, focusing on one component of the system, an attack-resilient state estimator, and its performance guarantees in the presence of attacks. It is shown that the maximal performance loss imposed by a smart attacker, exploiting the difference between the model used for state estimation and the real physical dynamics of the system, is bounded and linear with the size of the noise and modeling errors. Furthermore, it is described how implementation issues such as jitter, latency, and synchronization errors can be mapped to parameters of the state-estimation procedure. This

Calin Belta

Xavier Bombois

Roger Brockett

William R. Cluett

Bart De Schutter

Franz Franchetti

Mike Franusich

Tryphon Georgiou

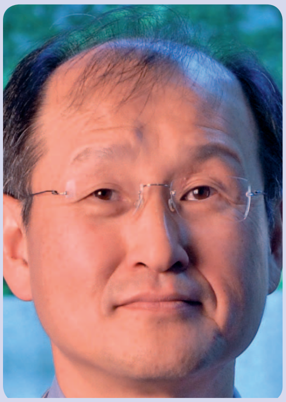
Liangyan Gui

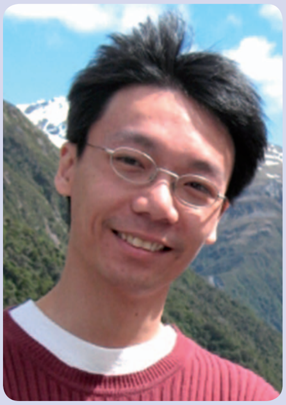
Håkan Hjalmarsson

Thomas Kailath

Soummya Kar

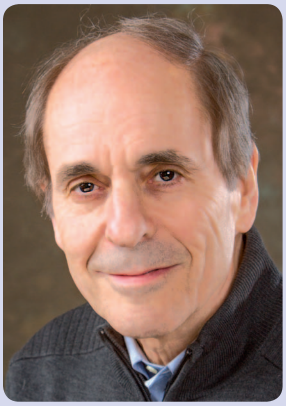
Vladimír Kučera


Insup Lee


Tze Meng Low

Stefan Mitsch

Sanjoy Mitter


A. Stephen Morse

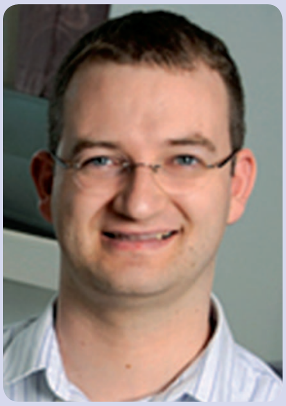
José M.F. Moura

David Padua

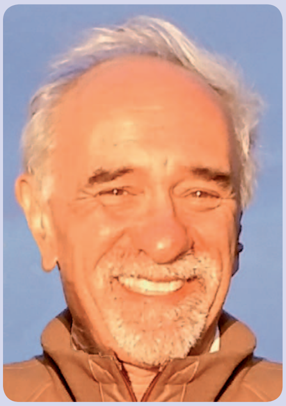
Miroslav Pajic

George J. Pappas

Amarin Phaosawasdi


André Platzer

Oleg Sokolsky


Eduardo Sontag

Allen Tannenbaum

Manuela Veloso

Li Xia

Georges Zaccour

Nicola Bezzo

Jeremy Johnson

Eric Thayer

Murat Arcak near Oppdal, Norway, during a visit to the NTNU Centre for Autonomous Marine Operations and Systems.

Michael Arbib

Sergio Bittanti

Christian A. Larsson on a hike to Torvedalen in Voss, Norway.

Geographic South Pole
Roald Amundsen
December 14, 1911
"So we arrived and were able to plant our flag at the geographical South Pole."
Robert F. Scott
January 17, 1912
"The Pole. Yes, but under very different circumstances from those expected."
elevat n 9,301 feet

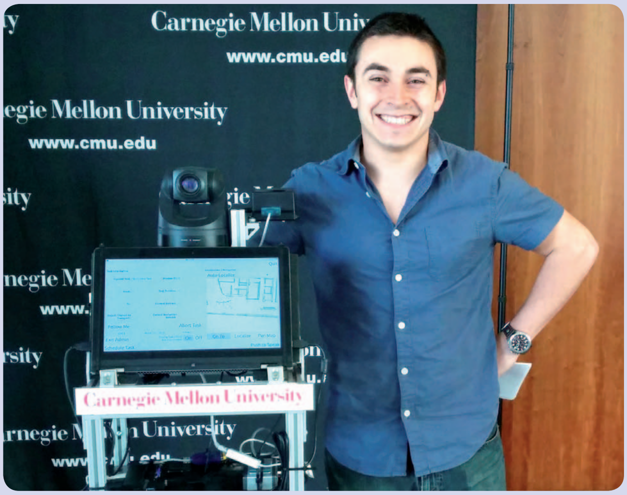
Pramod P. Khargonekar

Bayu Jayawardhana (right) sailing in a Frisian regatta.

Fumio Hamano visiting the Asakusa Shrine in Tokyo, Japan.

Ricardo Sanfelice at Inspiration Point, Santa Ynez Mountains, Santa Barbara, California (photo courtesy of Andrew Teel).

Bo Wahlberg at 3000 m in Sölden, Austria.

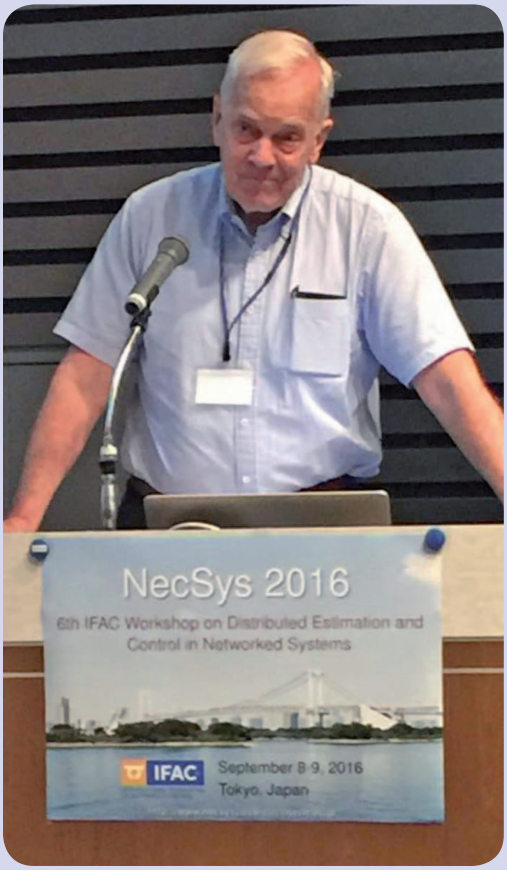


Juan Pablo Mendoza

Alberto Isidori opening the 17th IFAC World Congress.

Malcolm C. Smith holding an "inerter."

Mariette Annergren with a proportional-integral-derivative controller.


NecSys 2016
6th IFAC Workshop on Distributed Estimation and Control in Networked Systems
IFAC
September 8-9, 2016
Tokyo, Japan

Brian Anderson delivering the keynote lecture at NecSys 2016, Tokyo.

Penn Research in Embedded Computing and Integrated Systems Engineering

James Weimer

In "Historical Perspectives," Yutaka Yamamoto organized a tribute to Rudolf Kalman, which includes numerous remembrances of his research, life, and influence by former students and colleagues.

enables the mapping of control performance requirements to real-time specifications imposed on the underlying platform. The article also shows how to construct an assurance case for the system that covers both a mathematical model of the state estimator and its physical environment as well as a software implementation of the controller. While the models considered are specific to the control system and its intended deployment platform, the modeling, robustness analysis, and assumptions encountered in the case study are typical of many other CPS control problems.

The feature "High-Assurance SPIRAL," by Franz Franchetti, Tze Meng Low, Stefan Mitsch, Juan Pablo Mendoza, Liangyan Gui, Amarin Phaosawasdi, David Padua, Soummya Kar, José M.F. Moura, Mike Franusich, Jeremy Johnson, André Platzer, and Manuela Veloso, presents techniques that provide end-to-end guarantees for robot and car control. The article makes the point that CPSs, ranging from critical infrastructure, such as power plants, to modern, semi-autonomous vehicles, typically use software to control physical processes. As such, CPSs generally have many different computational components that execute separate software codes to implement various control algorithms. Collectively, these components, and the code they run, yield the behaviors and capabilities that modern society has come to expect and rely on. However, there are typically many intricate interactions between these components, and analyzing the millions of lines of code to ensure that the system will perform as desired is often very challenging. The article presents an approach that addresses this complexity in three ways. First, the desired behavior of the system and assumptions about the environment are described formally and proven, over all valid executions, to perform correctly based on the formalized assumptions. Second, a high-performance monitor code that checks that the environment complies with stated assumptions, and a proof that its implementation is a faithful representation of the mathematical specifications are automatically synthesized to reduce human error. Third, side-channel information, such as statistical noises, are fused with traditional sensor inputs such as a global positioning system, based on fundamental analytical redundancy, to establish that the inputs to the system do not contradict the known physics of the system.

The final HACMS feature, "Adversarial Testing to Increase the Overall Security of Embedded Systems," by Eric Thayer, describes methods used by the HACMS Red Team to evaluate the cybersecurity of the control systems developed by other researchers in the program. Additional information on HACMS results includes the comprehensive verification of an operating system microkernel [2], a domain-specific language for the synthesis of cybersecure control laws, mode logic, encrypted communications, and device drivers [3] and tools for compositional reasoning about system safety and security properties [4].

The article "Formal Methods for Control of Traffic Flow," by Samuel Coogan, Murat Arcak, and Calin Belta, investigates techniques for synthesizing correct-by-design controllers for dynamical systems. The approach first obtains a finite-state abstraction and then applies a game-based algorithm for synthesizing a control strategy to satisfy a linear temporal-logic specification. The article also reviews vehicular traffic-flow models to characterize a general model amenable to formal control synthesis by overapproximating the set of states that are one-step reachable under the traffic flow dynamics. These results are demonstrated on a case study that leads to a discussion of open problems and avenues for future research.

The last feature, "Hierarchical Game Theory for System-Optimal Control" by Noortje Groot, Georges Zaccour, and Bart De Schutter, is associated with the special issue on game theory in control that ran in the February 2017 *CSM* issue. This feature discusses the potential of adopting Stackelberg games in the context of both pricing and traffic control engineering applications. In particular, the article highlights how Stackelberg game theory can help solve pricing and traffic control problems in ways that differ from traditional methods.

In the "Applications of Control" column, the article "Application-Oriented Input Design in System Identification," by Mariette Annergren, Christian Larsson, Håkan Hjamarsson, Xavier Bombois, and Bo Wahlberg, presents a framework for application-oriented input design in system identification. The main idea of the framework is to note that the choice of the input signal used in the identification experiment greatly affects the model obtained. Thus, by designing the input signal, the operator is also implicitly designing the model so the intended application for the model should be taken into account in the input design as well. The concepts and capabilities of the framework proposed by authors are illustrated in several analytical, simulated, and experimental examples.

"On the Lighter Side" takes a look at model options at the dynamical systems dealership.

In "Historical Perspectives," Yutaka Yamamoto organized a tribute to Rudolf Kalman (an obituary ran in the February 2017 issue of the magazine [5]), which includes numerous remembrances of his research, life, and influence by former students and colleagues. Short tributes are included from Vladimír Kucera, Anders Lindquist, A.S. Morse, Brian D.O. Anderson, Eduardo D. Sontag, Sanjoy Mitter, Tryphon Georgiou, Allen Tannenbaum, Alberto Isidori, Roger Brockett, Michael A. Arbib, Pramod P. Khargonekar, Sergio Bittanti, Malcolm C. Smith, Fumio Hamano, and Thomas Kailath.

"From the Editor" presents "Letters of Reference," which discusses a recent study of the gender differences in recommendation letters for postdoctoral fellowships in geosciences and provides some guidance on how to write "excellent" recommendation letters. In the "President's Message," Edwin K.P. Chong talks about "The Control Problem," which recommends that the IEEE Control Systems Society (CSS) community, as control theorists and engineers, take a closer look at the artificial intelligence *control problem*. "CSS News" discusses the opening of the *Robotarium* by Magnus Egerstedt. "People in Control" has interviews with Katsuhisa Furuta, the former president and senior counselor of Tokyo Denki University; Kingsley Fregene, the group leader for Robotics and Intelligent Systems at Lockheed Martin Advanced Technology Laboratories; and Sebastián Dormido, a professor at the Universidad Nacional de Educación a Distancia and program chair for the IEEE 23rd Mediterranean Conference on Control and Automation.

"Member Activities" presents excerpts from the report to the IEEE CSS Board of Governors (BOG) from Vice President, Member Activities, Sandra Hirche. "Publication Activities" presents excerpts from the report to the CSS BOG from Vice President, Publication Activities, Fabrizio Dabbene. "Technical Activities" presents excerpts from the report to the CSS BOG from Vice President, Technical Activities, Kirsten Morris; a report from the Technical Committee on Hybrid Systems by Ricardo Sanfelice; and a report from the Technical Committee on Systems Biology by Bayu Jayawardhana.

"Conference Reports" has a report by Ding Liu, Christos G. Cassandras, Alessandro Giua, and Zhiwu Li on the 13th International Workshop on Discrete Event Systems held May 30–June 1, 2016, in Xi'an, China; a summary by Yanlong Zhao and Ying Qu of the 35th Chinese Control Conference held July 27–29, 2016, in Chengdu, China; a report by R. Sánchez-Peña and M. Sznaier on the 10th Multiconference on Systems and Control held in Buenos Aires, Argentina, September 19–22, 2016; and a discussion by Vicenç Puig, Christophe Aubrun, Dominique Sauter, and Horst Schulte on the Third International Conference on Control and Fault-Tolerant Systems held September 6–9, 2016, in Barcelona, Spain.

Among the regular columns, "25 Years Ago" revisits an article that was originally presented at the 1991 American Control Conference, "Reinforcement Learning Is Direct Adaptive Optimal Control" by Richard S. Sutton, Andrew G. Barto, and Ronald J. Williams. "Conference Calendar" lists upcoming conferences sponsored or cosponsored by the CSS. "Book Announcements" provides summaries of books recently published in the control field. "Book Reviews" provides discussions by William R. Cluett on the book *Principles of System Identification: Theory and Practice*, authored by Arun K. Tangirala, and by Li Xia on *Iterative Learning Control: An Optimization Paradigm*, authored by David H. Owens. "On the Lighter Side" takes a look at model options at the dynamical systems dealership.

I would like to thank the following members of the *CSM* editorial board for their significant efforts in helping to get the tribute to Rudolf Kalman finished on such short notice:

- » Yildiray Yildiz
- » Jeremy VanAntwerp
- » Sean Humbert
- » Antonella Ferrara
- » Warren Dixon
- » Daniel Quevedo,
- » Daniel Davison
- » Behcet Acikmese
- » Marco Pavone.

REFERENCES

[1] K. Fisher, "Using formal methods to enable more secure vehicles: DARPA's HACMS program," in *Proc. 19th ACM SIGPLAN Int. Conf. Functional Programming*, Gothenburg, Sweden, 2014, p. 1.

[2] G. Klein, J. Andronick, K. Elphinstone, T. Murray, T. Sewell, R. Kolanski, and G. Heiser, "Comprehensive formal verification of an OS microkernel," *ACM Trans. Comput. Syst.*, vol. 32, pp. 2:1–2:70, Feb. 2014.

[3] P. C. Hickey, L. Pike, T. Elliott, J. Bielman, and J. Launchbury, "Building embedded systems with embedded DSLs (Experience Report)," in *Proc. Int. Conf. Functional Programming*, ACM, 2014. Available: http://www.cs.indiana.edu/~lepike/pub_pages/icfp14.html

[4] M. W. Whalen, D. Cofer, and A. Gacek, "Requirements and architectures for secure vehicles," *IEEE Softw.*, vol. 33, no. 4, pp. 22–25, 2016.

[5] A. Antoulas, T. T. Georgiou, P. P. Khargonekar, A. B. Özgüler, E. D. Sontag, and Y. Yamamoto, "Prof. Rudolf Emil Kalman [Obituary]," *IEEE Control Syst. Mag.*, vol. 37, no. 1, pp. 151–152, 2017.

Jonathan P. How