Trustworthy Cyber-Physical Systems Engineering

CHAPMAN & HALL/CRC
COMPUTER and INFORMATION SCIENCE SERIES

Series Editor: Sartaj Sahni

PUBLISHED TITLES

ADVERSARIAL REASONING: COMPUTATIONAL APPROACHES TO READING THE OPPONENT'S MIND
Alexander Kott and William M. McEneaney

COMPUTER-AIDED GRAPHING AND SIMULATION TOOLS FOR AUTOCAD USERS
P. A. Simionescu

DELAUNAY MESH GENERATION
Siu-Wing Cheng, Tamal Krishna Dey, and Jonathan Richard Shewchuk

DISTRIBUTED SENSOR NETWORKS, SECOND EDITION
S. Sitharama Iyengar and Richard R. Brooks

DISTRIBUTED SYSTEMS: AN ALGORITHMIC APPROACH, SECOND EDITION
Sukumar Ghosh

ENERGY-AWARE MEMORY MANAGEMENT FOR EMBEDDED MULTIMEDIA SYSTEMS: A COMPUTER-AIDED DESIGN APPROACH
Florin Balasa and Dhiraj K. Pradhan

ENERGY EFFICIENT HARDWARE-SOFTWARE CO-SYNTHESIS USING RECONFIGURABLE HARDWARE
Jingzhao Ou and Viktor K. Prasanna

FROM ACTION SYSTEMS TO DISTRIBUTED SYSTEMS: THE REFINEMENT APPROACH
Luigia Petre and Emil Sekerinski

FUNDAMENTALS OF NATURAL COMPUTING: BASIC CONCEPTS, ALGORITHMS, AND APPLICATIONS
Leandro Nunes de Castro

HANDBOOK OF ALGORITHMS FOR WIRELESS NETWORKING AND MOBILE COMPUTING
Azzedine Boukerche

HANDBOOK OF APPROXIMATION ALGORITHMS AND METAHEURISTICS
Teofilo F. Gonzalez

HANDBOOK OF BIOINSPIRED ALGORITHMS AND APPLICATIONS
Stephan Olariu and Albert Y. Zomaya

HANDBOOK OF COMPUTATIONAL MOLECULAR BIOLOGY
Srinivas Aluru

HANDBOOK OF DATA STRUCTURES AND APPLICATIONS
Dinesh P. Mehta and Sartaj Sahni

HANDBOOK OF DYNAMIC SYSTEM MODELING
Paul A. Fishwick

HANDBOOK OF ENERGY-AWARE AND GREEN COMPUTING
Ishfaq Ahmad and Sanjay Ranka

Trustworthy Cyber-Physical Systems Engineering

Edited by

Alexander Romanovsky
Newcastle University, UK

Fuyuki Ishikawa
National Institute of Informatics, Tokyo, Japan

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
A CHAPMAN & HALL BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed on acid-free paper
Version Date: 20160719

International Standard Book Number-13: 978-1-4987-4245-0 (Hardback)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Contents

Foreword

For decades the vast majority of computers produced have been embedded processors running software that senses, computes, and actuates as part of a larger system. Over time, increasing numbers of embedded processors have been placed into various systems to improve performance, reduce operating costs, and provide advanced functionality. As this has happened, system interdependencies have increased, as has the ability of these systems to exert an ever greater influence over the physical environment. At some point these complex systems become Cyber-Physical Systems (CPSs), which in general involve multiple computer systems interacting to sense and control things that happen in the real world. While a CPS might sound a lot like just a bigger embedded system, the changes that come with Internet-level scale and the integration of disparate components into aggregated systems of systems are profound.

As a longtime researcher, teacher, and practitioner in the areas of embedded systems and computer dependability, I've witnessed dramatic changes in the cruciality of getting these systems right. Thirty-five years ago I used a computer to control the lights in a building with primitive power-line-carrier remote switches. (And people asked me why I'd ever want to do such a thing.) If the networked lighting system failed back then, the physical wall switches worked just fine. Today, some buildings soft-link networked wall switches to varying sets of networked lighting fixtures, and do real-time control on illumination conditions building-wide based on how much light is coming in through the windows on a minute-to-minute basis. If part of the computing system fails the wall switches might not do anything, because they are just input devices on a computer network, and the surviving parts must make sure enough lights are on to get by until a repair is made. In the future, we might see every lightbulb and thermostat in every house automatically negotiating for a better electricity rate with the national electricity consortium by offering to reduce consumption during peak loads. (This is already starting to happen with smart electric meters.) But if such a deeply interconnected system fails, we could easily have a significant outage. In principle, a software bug in a lightbulb could take down an entire power grid.

In other words, functionality, optimization, interdependencies, and the potential cost of failure are all increasing over time. The scope and capability of CPSs has increased to the point that dependability is no longer a luxury—it has become a necessity. This is true for utilities, building management, chemical processing, transportation, health care, urban infrastructure, agriculture, telecommunications, and just about every other aspect of modern life. Even computing server farms are being pulled into a critical role via cloud-connected CPS services. At this point we're still busy connecting previously isolated embedded systems up to the Internet. Soon enough we'll be dealing with the consequences of creating ad hoc CPS amalgams out of components not originally designed for such purposes, and finding out that "good enough" software wasn't really as good as it needed to be.

Which brings us to the purpose of this book. The chapters in this book address many of the problems that will have to be solved to get from where we are now to where we need to be to attain truly dependable CPS design, deployment, and operations. In other words, its important to make sure we can justifiably trust that these systems will actually work as needed. But, developing a suitable level of trust is difficult because the scope of a modern CPS can be so broad, and the issues that must be addressed so pervasive. Topics in this book cover questions such as

- What does having a trustworthy CPS actually mean for something as pervasive as a global-scale CPS?
- How does CPS trustworthiness map onto existing knowledge, and where do we need to know more?
- How can we mathematically prove timeliness, correctness, and other essential properties for systems that may be adaptive and even self-healing?
- How do we represent, reason about, and ensure the correctness of an inherently discrete system (the computer) that interacts with an inherently continuous system (the real world)?
- How can we better represent the physical reality underlying real-world numeric quantities in the computing system?
- How can we expand the notion of trustworthiness to include system support aspects such as ensuring that a software defect doesn't drain the batteries of a critical component?
- How can we establish, reason about, and ensure trust between CPS components that are designed, installed, maintained, and operated by different organizations, and which may never have really been intended to work together?
- How can we make sure that when we use a new replacement part for an older component, the entire system won't come crashing down around us due to a subtle incompatibility?
- Once we have solutions to these problems, how can we impart that knowledge to future designers?

This is a book primarily about concepts, and as such these chapters emphasize theory, formality, modeling, and rigor. For example, more than a third of the chapters feature discussions of the Event-B approach for modeling and reasoning about CPS functionality.

The authors include a broad and deep sampling of CPS researchers spanning many application areas, with an emphasis on European formal methods-based approaches. The authors met for several days at an NII Shonan meeting, which affords researchers a distraction-free setting structured to permit digging deep into a problem and figuring out what needs to be done to solve it. This book is the follow-up to that retreat.

Getting CPS dependability right is essential to forming a solid foundation for a world that increasingly depends on such systems. This book represents the cutting edge of what we know about rigorous ways to ensure our CPS designs are trustworthy. I recommend it to anyone who wants to get a deep look at concepts that will form a cornerstone for future CPS designs.

Phil Koopman
Pittsburgh, Pennsylvania

Preface

This preface briefly introduces the area of trustworthy Cyber-Physical Systems (TCPS), outlines challenges in developing TCPS, and explains the structure of the book.

TRUSTWORTHY CYBER-PHYSICAL SYSTEMS

Societal and business activities depend more and more on software-intensive systems. Novel systems paradigms have been proposed and actively developed, notably Cyber-Physical Systems (CPS). The envisioned systems expand target entities and processes handled by the systems, stepping more deeply into human activities as well as real-world entities. There are emerging application areas such as automated driving and smart cities, while the existing areas, such as aviation, railways, business process management, and navigation systems, are also evolving by including a richer set of features. Visions for CPS include or extend a number of systems paradigms, such as Systems of Systems, Ubiquitous Computing, the Internet of Things, Smart Cities, and so on. Obviously, the increased involvement with human activities and real-world entities leads to greater demand for trustworthy systems. Here, and in this book, we treat *system trustworthiness* in a broad sense of a system being worthy of confidence or being dependable, so that it delivers service that can be justifiably trusted.

The developers of CPS face unprecedented complexity, caused not only by expanded application features, but also by combined mechanisms for trustworthiness (self-adaptation, resilience, etc.). Considering this growing complexity the construction of trustworthy CPSs and ensuring their trustworthiness is absolutely the key challenge in systems and software engineering.

The only solution that can help tackle this challenge is the development of new engineering methods for trustworthy CPS. One of the difficulties here is development of abstractions and semantic models for effective orchestration of software and physical processes [1]. There is no doubt that foundational theories and various technological components are essential as the building blocks for the new engineering methods. The building blocks for the engineering of trustworthy systems spread across verification algorithms, probabilistic analysis, fault models, self-adaptation mechanisms, and so on. The challenge of complexity requires further elaboration and integration of such blocks into sound engineering methods. Engineering methods define systematic and reliable ways for modeling analyzing, and verifying the system and its trustworthiness while mitigating the complexity. Recently, there have been yet more active efforts in engineering methods for trustworthy systems, on the basis of various approaches. Formal methods are one of the promising approaches that have been actively explored not only by academia but also by industry. Each approach has different, unique features, but essentially relevant to each other, focusing on modeling of the system, modeling of trustworthiness or faults, and their analysis and verification for complex systems, especially CPSs.

It is clear that in order to speed up the development of novel engineering methods for emerging complex CPSs, it is absolutely necessary to promote active discussions on subjects beyond specific applications, engineering approaches, or even paradigms. On October 27–30, 2014 we organized an NII Shonan Meeting on the Science and Practice of Engineering Trustworthy Cyber-Physical Systems. The NII Shonan Meeting, following the well-known Dagstuhl Seminars, is a scheme for meetings to promote discussions by world-leading researchers and practitioners. Our TCPS meeting aimed at providing this opportunity by inviting world-leading researchers working on engineering methods for TCPS. The meeting was attended by 32 participants from Asia, Europe, and North America and helped the participants to exchange ideas and develop a good common understanding of the area of TCPS. It was an extremely successful event that spawned new ideas and new collaborations. Further information about this meeting can be found at the Web site http://shonan.nii.ac.jp/seminar/055/ and in the final report (No. 2014-14 at http://shonan.nii.ac.jp/shonan/report/).

The idea for this book was conceived and discussed during the meeting. The chapters of the book were written by the participants of the seminar, to whom we are really grateful for their participation in the Meeting, for sharing their ideas, and for supporting the idea of the book.

KEY QUESTIONS

During the Meeting we organized several discussion sessions focusing on the following four key questions:

- What are the essential differences between CPS and traditional software systems?
- What are the technical challenges facing TCPS engineering?
- What are the nontechnical challenges facing TCPS engineering?
- What are the gaps between academia and industry (research and practice) in engineering (so far/for future TCPS)?

Most of the participants are top academic researchers on techniques for trustworthiness, such as formal methods, who have active collaborations with industry. There were also participants from industry. Below we include a brief summary of the issues identified.

1. What are the essential differences between CPS and traditional software systems?

   To understand these differences we need to first identify the essential properties of the systems we wish to develop. CPSs consist of collaborating computational elements controlling physical entities, which interact with humans and their environment. The design method should consider their elements differently from those of traditional software-based systems.

The main characteristics of physical systems are their continuous behavior and stochastic nature. This is why the development of CPS requires the involvement of specialists in multiple engineering disciplines. These systems often use close interaction between the plant and the discrete event system, and their complexity can grow due to interaction among multiple CPSs and the need to deal with time.

These are some of the essential features of CPS beyond conventional control systems: context awareness, cognitive computation, and autonomy.

2. What are the technical challenges facing TCPS engineering?

The technical challenges in TCPS engineering derive from the need to deal with system heterogeneity. TCPS engineering needs sound foundations to deal with modeling and analyzing the parts (e.g., continuous and discrete) and their compositions. These systems are often so complex that the humans in the loop may not completely understand them, which calls for special engineering methods to develop systems to assist humans as much as possible and make sure that the systems are always safe.

These systems have to be modeled/reasoned about together with their environments; the difficulties here are in choosing the right level of detail in representing the environment and in ensuring that all relevant elements of the environment are represented.

There is a wide range of CPS starting from social interaction systems and the Internet (Internet of Things) to safety-critical CPS in medicine/surgery.

Typically the general properties of CPSs can only be deduced from the local behaviors of their parts. The execution of these parts might have global effects and typically result in an emergent behavior of the whole. CPS engineering will need to include methods for compositional verification and compositional certification.

It is crucial to guarantee CPS trustworthiness for the guaranteed as well as the nonguaranteed behavior of the system. The safety, security, and reliability risk analysis of CPS require methods that go beyond the traditional hazard analysis techniques.

3. What are the nontechnical challenges facing TCPS engineering?

Perception of technology by the general public is crucial for deploying CPS. The difficulty lies in the problem that public acceptance of technologies depends on more than technical evidence (e.g., proof) of their correctness. It is challenging to communicate arguments, which include stochastic behavior and risks. We need to better understand how people feel about new technologies and also about collecting data to support analysis of trustworthiness.

There have been discussions on the development culture in some companies in which computer science (CS) and mathematics (e.g., formal methods) are not considered so relevant in practice. However, scientific approaches are inevitable to ensure trustworthiness under higher complexity of CPS. There are also obstacles in changing the culture in large companies. We need to understand how to demonstrate advantages of new technologies, and for this we need to clearly demonstrate business cases.

TCPS development requires interdisciplinary approaches that rely on communication between various experts. The CS people are expected to play a larger role by serving as hubs, as well as the ambassadors of new technologies. They will be able to develop rigorous unambiguous foundations for communicating knowledge and decisions across the domain involved.

In the area of certification and assurance important topics are the liability of companies, the use of specification as contract, and the need to develop a standard for standards. One important issue is to understand when and why the life of CPSs end.

The main challenges in education are as follows: CS engineering education does not cover continuous domain, and there is a need to educate the general public about new technologies.

4. What are the gaps between academia and industry (research and practice) in engineering so far/for future TCPS?

There is a cultural gulf between academia and industry, reified by the career requirements of both groups, but there is also a gulf within industry between research and production. There is a gap between different industries as well as between single-product organizations and heterogeneous CPS, where no one industry dominates. Sometimes companies are aware of the advantages of engagement but encounter difficulties in implementing it.

The goals are different as well. There is an academic need for academic excellence and an industrial need for commercial success. Academics are mainly into science; industry is into engineering. To add to this, there is inflexibility in both, academics and industry; for example, industries keep academics at a distance.

The successes achieved so far include government support for smaller joint projects (as in the EU), large EU projects (e.g., the development of software for avionics has successfully mixed academics and industry in long-term projects and large investment has been key), moving PhDs from industry to academia and vice versa.

The ways forward are as follows. Relevant government policies should be developed, and the governments should be lobbied for support. Unfortunately, information and communication technology and CPS are not given the attention afforded to, for example, high energy physics. In addition we need to lobby academia to promote the value of industrial engagement (the detail here is not trivial!) and industry to show the cost implications of academic engagement. Cross-fertilization between academic disciplines and between academia and industry should be encouraged. There should be a greater academic presence on standards committees. Lastly, industry should be more involved in the teaching of CPS.

OBJECTIVES AND STRUCTURE OF THIS BOOK

It will require joint effort by researchers working in a number of disciplines related to systems engineering in general to ensure that the CPSs that we are using now and will be using in the future are trustworthy. The traditional software-centric approaches are not applicable in this domain. In CPS, the physical part, the environment, the humans, and a variety of other systems are interacting with the increasingly cyber realm traditionally handled by computer scientists and software engineers.

There are already several excellent books that have been published on CPS (e.g., [2–4]). The aim of this book is to give practitioners and researchers a comprehensive introduction to the area of TCPS engineering.

The book covers various topics related to engineering of modern/future TCPS, including modeling, verification, rigorous design, simulation, requirements engineering, dependability, resilience, safety, architectural design, codesign/cosimulation, validation, modeling of constraint resources, safety cases, service-level agreement, and run-time resource optimization/allocation.

The book largely draws on the 4-day Shonan meeting that helped the contributors to analyze the challenges in developing trustworthy CPS, to identify important issues in developing engineering methods for CPS, and to develop a common understanding of the area and its challenges.

The individual chapters are written by teams led by the participants in the Shonan meeting. Joint participation in the meeting allowed the contributors to develop a good common understanding of the domain and of the challenges faced by the developers of TCPS.

The book has wider than usual technical coverage addressing various issues contributing to trustworthiness complemented by the contributions on TCSP roadmapping, taxonomy, and standardization, as well as on the experience in deploying advanced systems engineering methods in industry. Bringing all these topics together is unique and extremely important for the domain.

The book features contributions from the leading researchers in Japan, Canada, the USA, and Europe. The European partners have been and are being involved in a number of major FP7 and Horizon 2020 projects on CPS engineering.

The book consists of 16 chapters. The chapters are self-contained and provide discussions from various points of view; thus the readers can read the chapters independently according to their interests.

Chapters 1 through 3 discuss definitions, visions, and challenges of TCPS. This provides a good starting point to review concepts and difficulties in CPS and trustworthiness of CPS. Different viewpoints are provided, such as comparisons between embedded systems and systems of systems, as well as views of CPS as a type system.

Chapters 4 through 7 present specific approaches to ensuring trustworthiness, namely, proof and refinement. Mathematical proofs make it easier to rigorously ensure the trustworthiness of the target system. Refinement adds a further power onto proofs as an effective way of mitigating complexity through incremental or gradual formal development. The core challenges reside in how to model and verify self-* (adaptive, healing, etc.) and resilient systems.

Chapters 8 through 10 focus on engineering methods for dealing with hybrid aspects, that is, both continuous and discrete aspects. This is one of the key unique challenges in CPS, which requires the developers to go beyond the classical realm of computer science and software engineering.

Chapters 11 and 12 exemplify advances in developing the foundational techniques. Two studies are presented that envision strong support for modeling of domain-specific structures and verification of power consumption.

Chapters 13 through 15 present approaches based on agreements and assurance. Both of these concepts focus on properties that define trustworthiness of the target system and are often discussed beyond organizational boundaries. Different agreements and assurance techniques are presented in the chapters: monitoring and enforcement by the system as well as careful analysis and discussion by the involved engineers.

This book ends with Chapter 16, which discusses transfer of these advanced techniques to a wide range of engineers in the industry. This discussion is based on an intensive, long experience of industry education through industry–academia collaboration.

REFERENCES

1. E. A. Lee. Cyber physical systems: Design challenges. *The 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC 2008)*, Orlando, FL, pp. 363–369, 2008.
2. M. Klein, R. Rajkumar, and D. de Niz. *Cyber-Physical Systems (SEI Series in Software Engineering)*. Addison-Wesley Professional, Boston, MA, 2016.
3. F. Hu. *Cyber-Physical Systems: Integrated Computing and Engineering Design*. CRC Press, Boca Raton, FL, 2010.
4. P. Marwedel. *Embedded System Design: Embedded Systems Foundations of Cyber-Physical Systems*. Springer, Berlin Heidelberg, 2010.

Acknowledgments

The editors would like to thank the committee of the Shonan Meeting at NII (National Institute of Informatics, Tokyo, Japan) for supporting the TCPS meeting that led to the idea for this book. We thank the attendees of the TCPS meeting for their active and interesting discussions during the meeting as well as their contributions to this book. We are grateful to the book contributors for their help in reviewing the chapters. Our thanks to Stefan Hallerstede, Carolyn Talcott, Thai Son Hoang, and Kenji Tei, who kindly reviewed several book chapters. Last but not least, we thank the staff of CRC Press and Randi Cohen who gave us the opportunity and support for publication of this book.

Editors

Alexander Romanovsky is a professor at the Centre for Software Reliability and the leader of the Secure and Resilient Systems Group at the School of Computing Science, Newcastle University, UK. He earned his PhD from St. Petersburg State Technical University (Russia) in 1987. He joined Newcastle University in 1996 and since then has been working on various EU and UK systems dependability projects. One of these was a major EC FP7 Integrated Project on Industrial Deployment of System Engineering Methods Providing High Dependability and Productivity (DEPLOY), which he led in 2008–2012. Professor Romanovsky is an editorial board member of the Elsevier Journal of Systems Architecture and a visiting professor at the National Institute of Informatics (NII, Tokyo, Japan). He has more than 350 publications on various aspects of dependability. His research interests include resilience engineering, fault tolerance, safety verification, fault modeling, exception handling, system structuring, and formal engineering methods. Professor Romanovsky has been successfully working with industrial partners in the railway, automotive, aerospace, and business information domains.

Fuyuki Ishikawa is an associate professor at the National Institute of Informatics (NII) in Tokyo, Japan. He earned a Bachelor of Science degree in 2002 and a Masters degree in information science and technology in 2004, both from the University of Tokyo. He earned a PhD degree in information science and technology from the University of Tokyo in 2007. He is also a visiting associate professor at the University of Electro-Communications in Japan. His research interests include service-oriented computing and software engineering. He has served as the leader of six funded projects and published more than 100 papers.

Contributors

Yamine Aït-Ameur
Université de Toulouse
IRIT-INPT
Toulouse, France

Manamiary Bruno Andriamiarina
Lorraine Research Laboratory in Computer Science and its Applications
Université de Lorraine
Nancy, France

Guillaume Babin
Université de Toulouse
IRIT-INPT
Toulouse, France

Szilárd Bozóki
Department of Measurement and Information Systems
Budapest University of Technology and Economics
Budapest, Hungary

Ben Breimer
McMaster Centre for Software Certification
McMaster University
Hamilton, Ontario, Canada

John Fitzgerald
School of Computing Science
Newcastle University
Newcastle upon Tyne, United Kingdom

László Gönczy
Department of Measurement and Information Systems
Budapest University of Technology and Economics
Budapest, Hungary

Alexei Iliasov
School of Computing Science
Newcastle University
Newcastle upon Tyne, United Kingdom

Claire Ingram
School of Computing Science
Newcastle University
Newcastle upon Tyne, United Kingdom

Fuyuki Ishikawa
Digital Content and Media Sciences Research Division
National Institute of Informatics
Tokyo, Japan

Paul Joannou
McMaster Centre for Software Certification
McMaster University
Hamilton, Ontario, Canada

John Knight
Department of Computer Science
University of Virginia
Charlottesville, Virginia

Imre Kocsis
Department of Measurement and Information Systems
Budapest University of Technology and Economics
Budapest, Hungary

Linas Laibinis
Department of Information Technologies
Åbo Akademi University
Turku, Finland

Peter Gorm Larsen
Department of Engineering
Aarhus University
Aarhus, Denmark

Mark Lawford
McMaster Centre for Software Certification
McMaster University
Hamilton, Ontario, Canada

Thierry Lecomte
ClearSy
France

Thomas S. E. Maibaum
McMaster Centre for Software Certification
McMaster University
Hamilton, Ontario, Canada

István Majzik
Department of Measurement and Information Systems
Budapest University of Technology and Economics
Budapest, Hungary

Tom McCutcheon
Defence Science and Technology Laboratory
United Kingdom

Dominique Méry
Lorraine Research Laboratory in Computer Science and its Applications
Université de Lorraine
Nancy, France

Shin Nakajima
National Institute of Informatics
Tokyo, Japan

Marc Pantel
Université de Toulouse
IRIT-INPT
Toulouse, France

András Pataricza
Department of Measurement and Information Systems
Budapest University of Technology and Economics
Budapest, Hungary

Inna Pereverzeva
Department of Information Technologies
Åbo Akademi University
Turku, Finland

Alexander Romanovsky
School of Computing Science
Newcastle University
Newcastle upon Tyne,
United Kingdom

Ágnes Salánki
Department of Measurement and Information Systems
Budapest University of Technology and Economics
Budapest, Hungary

Neeraj Kumar Singh
Université de Toulouse
IRIT-INPT
Toulouse, France

Kevin Sullivan
Department of Computer Science
University of Virginia
Charlottesville, Virginia

Yoshinori Tanabe
School of Literature
Tsurumi University
Kanagawa, Japan

Elena Troubitsyna
Department of Information Technologies
Åbo Akademi University
Turku, Finland

Sasan Vakili
McMaster Centre for Software Certification
McMaster University
Hamilton, Ontario, Canada

Alan Wassyng
McMaster Centre for Software Certification
McMaster University
Hamilton, Ontario, Canada

Jim Woodcock
Department of Computer Science
University of York
York, United Kingdom

Jian Xiang
Department of Computer Science
University of Virginia
Charlottesville, Virginia

Nobukazu Yoshioka
Information Systems Architecture Science Research Division
National Institute of Informatics
Tokyo, Japan