

# **Studies in Systems, Decision and Control**

Volume 255

## **Series Editor**

Janusz Kacprzyk, Systems Research Institute, Polish Academy of Sciences,  
Warsaw, Poland

The series “Studies in Systems, Decision and Control” (SSDC) covers both new developments and advances, as well as the state of the art, in the various areas of broadly perceived systems, decision making and control—quickly, up to date and with a high quality. The intent is to cover the theory, applications, and perspectives on the state of the art and future developments relevant to systems, decision making, control, complex processes and related areas, as embedded in the fields of engineering, computer science, physics, economics, social and life sciences, as well as the paradigms and methodologies behind them. The series contains monographs, textbooks, lecture notes and edited volumes in systems, decision making and control spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

\*\* Indexing: The books of this series are submitted to ISI, SCOPUS, DBLP, Ulrichs, MathSciNet, Current Mathematical Publications, Mathematical Reviews, Zentralblatt Math: MetaPress and Springerlink.

More information about this series at <http://www.springer.com/series/13304>

Emil Prícop · Jaouhar Fattahi · Nitul Dutta ·  
Mariam Ibrahim  
Editors

# Recent Developments on Industrial Control Systems Resilience

 Springer

*Editors*

Emil Pricop  
Control Engineering, Computers  
and Electronics Department  
Petroleum-Gas University of Ploiesti  
Ploiesti, Romania

Jaouhar Fattahi  
Department of Computer Science  
and Software Engineering  
Laval University  
Quebec City, QC, Canada

Nitul Dutta  
Computer Engineering Department  
Marwadi University  
Rajkot, Gujarat, India

Mariam Ibrahim  
Department of Mechatronics Engineering,  
School of Applied Technical Sciences  
German Jordanian University  
Amman, Jordan

ISSN 2198-4182                      ISSN 2198-4190 (electronic)  
Studies in Systems, Decision and Control  
ISBN 978-3-030-31327-2              ISBN 978-3-030-31328-9 (eBook)  
<https://doi.org/10.1007/978-3-030-31328-9>

© Springer Nature Switzerland AG 2020, corrected publication 2021

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

*Dedicated to our beloved families for  
supporting us all along.*

Emil Pricop, Jaouhar Fattahi, Nitul Dutta  
and Mariam Ibrahim

# Preface

Industrial control systems (ICS) have a critical place in the functioning and development of today's world. They are key components of every technical infrastructure around us, ranging from air conditioning in our homes and cars to the big factories, the energy production and distribution, the water distribution systems, and even the nuclear plants. The correct operation of the industrial control systems is essential for the functioning of our society, so they have to be designed to be resilient. This means that the ICS should be able to recover from various process faults and failures and to withstand emerging cyberattacks. These objectives can be achieved only by assuring both safety and security, being it physical or cybernetic. Also, a special interest is presented by predictive and preventive maintenance activities.

The main goal of the book is to collect valuable contributions of renowned researchers in the field of control engineering, Internet of Things, and cybersecurity. Some chapters are based on presentations and discussions that took place at the previous editions of the International Workshop on Systems Safety and Security (IWSSS, <https://www.iwsss.org>). The workshop, initiated in 2013, became a traditional annual scientific event in Romania. IWSSS is now a recognized venue for the exchange of experience and ideas in the field of systems safety, security, and resilience with the scope of stimulating joint work at a regional and international level.

The book comprises research based on theory, subsequent simulation and experimental results, numerous case studies, and practical implementations. Given the detailed discussion in the said context, the book offers profound insights on increasing the resilience of industrial control systems. Both fundamental and advanced topics are discussed, having the theoretical approaches sustained by practical examples.

The structure and chapters of the book are broadly grouped into core topics that address challenges related to safe operations of control systems, risk analysis and assessment, usage of attack graphs to evaluate and increase the resiliency of control systems, preventive maintenance, and malware detection and analysis. The resilience and cybersecurity of sensor networks and the Internet of Things devices, which are now an integral part of the various industrial control systems, are discussed in different chapters of the book.

Another notable contribution of this book is the inclusion of necessary and timely response to malicious attacks or hazardous situations. This topic will certainly help readers to decide the best approaches to handle such unwanted situations.

We believe, the contents of the book is essential readings for system engineers, researchers, and specialists. The topics discussed in the book are challenging and recent and we anticipate the book to represent a useful reference for all the professionals in the field of ICS resilience, safety, and security. Finally, the editors expect that this book will be a supportive auxiliary to undergraduate and graduate students, to academia and researchers trying to address security and safety issues related to the modern implementations of the industrial control systems.

Ploiesti, Romania  
Quebec City, Canada  
Rajkot, India  
Amman, Jordan  
August 2019

Dr. Emil Pricop  
Dr. Jaouhar Fattahi  
Dr. Nitul Dutta  
Dr. Mariam Ibrahim

# Contents

<b>Safety Instrumented Systems Analysis</b> .....	1
Alina-Simona Băieșu	
<b>Risks Assessment of Critical Industrial Control Systems</b> .....	21
Gabriel Rădulescu	
<b>Machine Learning Based Predictive Maintenance of Infrastructure Facilities in the Cryolithozone</b> .....	49
Andrey V. Timofeev and Viktor M. Denisov	
<b>Cybersecurity Threats, Vulnerability and Analysis in Safety Critical Industrial Control System (ICS)</b> .....	75
Xinxin Lou and Asmaa Tellabi	
<b>Automatic Attack Graph Generation for Industrial Controlled Systems</b> .....	99
Mariam Ibrahim, Ahmad Alsheikh and Qays Al-Hindawi	
<b>Determining Resiliency Using Attack Graphs</b> .....	117
Mariam Ibrahim and Ahmad Alsheikh	
<b>Modern Methods for Analyzing Malware Targeting Control Systems</b> .....	135
Nitul Dutta, Kajal Tanchak and Krishna Delvadia	
<b>Multi-stage Cyber-Attacks Detection in the Industrial Control Systems</b> .....	151
Tomáš Bajtoš, Pavol Sokol and Terézia Mézešová	
<b>Using Honeypots for ICS Threats Evaluation</b> .....	175
Nitul Dutta, Nilesh Jadav, Nirali Dutiya and Dhara Joshi	



<b>Intrusion Detection on ICS and SCADA Networks</b> .....	197
Marian Gaiceanu, Marilena Stanculescu, Paul Cristian Andrei, Vasile Solcanu, Theodora Gaiceanu and Horia Andrei	
<b>Security Evaluation of Sensor Networks</b> .....	263
Horia Andrei, Marian Gaiceanu, Marilena Stanculescu, Ioan Marinescu and Paul Cristian Andrei	
<b>Innovative Hardware-Based Cybersecurity Solutions</b> .....	283
Octavian Ionescu, Viorel Dumitru, Emil Pricop and Stefan Pircalabu	
<b>Legal Issues of Deception Systems in the Industrial Control Systems</b> .....	301
Pavol Sokol, Radoslav Benko and Laura Rózenfeldová	
<b>Correction to: Cybersecurity Threats, Vulnerability and Analysis in Safety Critical Industrial Control System (ICS)</b> .....	C1
Xinxin Lou and Asmaa Tellabi	

# Editors and Contributors

## About the Editors

**Emil Pricop** is currently with the Control Engineering, Computers and Electronics Department of the Petroleum-Gas University of Ploiesti, Romania. He holds the position of Senior Lecturer since 2018 and he is teaching Computer Networking, Software Engineering, and Human–Computer Interaction courses. He received his Ph.D. in Systems Engineering from Petroleum-Gas University of Ploiesti by defending in May 2017 the thesis with the title “Research regarding the security of control systems”. His research interest is cybersecurity, focusing especially on industrial control systems security. Dr. Emil Pricop is co-editor of the book *Recent Advances in Systems Safety & Security* (Springer, 2016) and author or co-author of two national (Romanian) patents, five book chapters published in books edited by Springer, and over 30 papers in journals or international conferences. From 2013, Dr. Pricop is the initiator and chairman of International Workshop on Systems Safety and Security—IWSSS, a prestigious scientific event organized annually.

**Jaouhar Fattahi** is currently working with Defence Research and Development Canada (DRDC) at the Valcartier Research Centre as a defence scientist. He is also an adjunct professor with Laval University, Quebec City, Canada. He obtained his Ph.D. on the security of cryptographic protocols from Laval University in October 2015. He completed his postdoctoral fellowship at the Canadian Armed Forces Research Centre in the field of cybersecurity. He has also been a computer engineer since 1995. Dr. Jaouhar Fattahi is the author of *The Theory of Witness-Functions* for verifying security of cryptographic protocols. He now specializes in reverse engineering and machine and deep learning applied to security and cybersecurity. He is an IEEE member.

**Nitul Dutta** is a professor in the Computer Engineering Department, Faculty of Engineering (FoE), Marwadi University, Rajkot, Gujarat, since 2014. He has a total experience of 20 years. He received B.E. degree in Computer Science and

Engineering from Jorhat Engineering College, Assam (1995), and M. Tech. degree in Information Technology from Tezpur University, Assam (2002). He completed Ph.D. (Engineering) degree in the field of Mobile IPv6 at Jadavpur University (2013) and published 15 Journal and 30 conference papers. He has completed two AICTE sponsored research projects of worth Rs. 25 Lakhs (approx.) (Rs. Twenty-Five Lakhs only). His current research interests are wireless communication, mobility management in IPv6-based network, cognitive radio networks, and cybersecurity.

**Mariam Ibrahim** received her Bachelor's degree in Electrical and Computer Engineering from the Hashemite University, Jordan, in 2008, and M.S. in Mechatronics Engineering from Al-Balqa Applied University, Jordan, in 2011, and the Ph.D. in Electrical Engineering from Iowa State University, USA, in 2016. She was a lab supervisor with EE department at the Hashemite University (2008–2011). She joined the German Jordanian University (2011) as an RA, where she got a scholarship to pursue her Ph.D. studies; she is currently an assistant professor at GJU. Her research interests include discrete-event systems, stochastic systems, power systems, communication networks, healthcare systems, together with their control and resiliency analysis, and system model-based verification/attack graph generation using AADL. She is a member of Iowa Section IEEE Control Systems Society Technical Chapter. She serves as a scientific reviewer in the international scientific committee of the International Workshop on Systems Safety and Security—IWSSS since 2017, journal of *IET Cyber-Physical Systems: Theory & Application*, 2018, and *IEEE Network Magazine*, 2018.

## Contributors

**Qays Al-Hindawi** Department of Mechatronics Eng, Faculty of Applied Technical Sciences, German Jordanian University, Amman, Jordan

**Ahmad Alsheikh** Department of Mechatronics Eng, Faculty of Applied Technical Sciences, German Jordanian University, Amman, Jordan

**Horia Andrei** SM-IEEE, Bucharest, Romania;  
 Doctoral School of Engineering Sciences, University Valahia Targoviste,  
 Targoviste, Romania

**Paul Cristian Andrei** Department of Electrical Engineering, University Politehnica Bucharest, Bucharest, Romania

**Alina-Simona Băieșu** Automatic Control, Computers and Electronics Department, Petroleum-Gas University of Ploiesti, Ploiesti, Romania

**Tomáš Bajtoš** Faculty of Science, Institute of Computer Science, Pavol Jozef Šafárik University in Košice, Košice, Slovakia

**Radoslav Benko** Faculty of Law Institute of International Law and European Law, Pavol Jozef Šafárik University in Košice, Košice, Slovakia

**Krishna Delvadia** Chhotubhai Gopalbhai Patel Institute of Technology, Bardoli, Gujarat, India

**Viktor M. Denisov** “Flagman Geo” Ltd., Saint-Petersburg, Russia

**Viorel Dumitru** National Institute of Materials Physics, Magurele, Romania

**Nirali Dutiya** Department of Computer Engineering, Faculty of PG Studies, MEF Group of Institutions (MEFGI), Rajkot, India

**Nitul Dutta** Computer Engineering Department, MEF Group of Institutions, Rajkot, Gujarat, India

**Marian Gaiceanu** Department of Control Systems and Electrical Engineering, Dunarea de Jos University of Galati, Galati, Romania

**Theodora Gaiceanu** Gheorghe Asachi Technical University of Iasi, Iasi, Romania

**Mariam Ibrahim** Department of Mechatronics Eng, Faculty of Applied Technical Sciences, German Jordanian University, Amman, Jordan

**Octavian Ionescu** National Institute for Research and Development in Microtechnologies, IMT Bucharest, Bucharest, Romania

**Nilesh Jadav** Department of Computer Engineering, Faculty of PG Studies, MEF Group of Institutions (MEFGI), Rajkot, India

**Dhara Joshi** Department of Computer Engineering, Faculty of PG Studies, MEF Group of Institutions (MEFGI), Rajkot, India

**Xinxin Lou** Bielefeld University, Bielefeld, Germany

**Ioan Marinescu** Doctoral School of Engineering Sciences, University Valahia Targoviste, Targoviste, Romania

**Terézia Mézešová** Faculty of Science, Institute of Computer Science, Pavol Jozef Šafárik University in Košice, Košice, Slovakia

**Stefan Pircalabu** Cyberswarm Inc., San Mateo, CA, USA

**Emil Pricop** Petroleum-Gas University of Ploiesti, Ploiesti, Romania

**Gabriel Rădulescu** Control Engineering, Computers and Electronics Department, Petroleum-Gas University of Ploiești, Ploiești, Romania

**Laura Rózenfeldová** Faculty of Law, Department of Commercial Law and Business Law, Pavol Jozef Šafárik University in Košice, Košice, Slovakia

**Pavol Sokol** Faculty of Science, Institute of Computer Science, Pavol Jozef Šafárik University in Košice, Košice, Slovakia

**Vasile Solcanu** Dunarea de Jos University of Galati, Galati, Romania

**Marilena Stanculescu** Department of Electrical Engineering, University Politehnica Bucharest, Bucharest, Romania

**Kajal Tanchak** Computer Engineering Department, MEF Group of Institutions, Rajkot, Gujarat, India

**Asmaa Tellabi** University Siegen, Siegen, Germany

**Andrey V. Timofeev** LLP “EqualiZoom”, Astana, Kazakhstan