## Contents

### Invited Talks

Medical Devices, Electronic Health Records and Assuring Patient Safety: Future Challenges? ................................................................. 3  
*Cor J. Kalkman*

Cyber (In-)security of Industrial Control Systems: A Societal Challenge. . 7  
*Eric Luiijf*

### Flight Systems

Modeling Guidelines and Usage Analysis Towards Applying HiP-HOPS Method to Airborne Electrical Systems ........................................ 19  
*Carolina D. Villela, Humberto H. Sano, and Juliana M. Bezerra*

The Formal Derivation of Mode Logic for Autonomous Satellite Flight Formation ................................................................. 29  
*Anton Tarasyuk, Inna Pereverzeva, Elena Troubitsyna, and Timo Latvala*

### Automotive Embedded Systems

Simulation of Automotive Security Threat Warnings to Analyze Driver Interpretations and Emotional Transitions .................................. 47  
*Robert Altschaffel, Tobias Hoppe, Sven Kuhlmann, and Jana Dittmann*

Improving Dependability of Vision-Based Advanced Driver Assistance Systems Using Navigation Data and Checkpoint Recognition ........ 59  
*Ayhan Mehmed, Sasikumar Punnekkat, Wilfried Steiner, Giacomo Spampinato, and Martin Lettner*

Safely Using the AUTOSAR End-to-End Protection Library .................. 74  
*Thomas Arts and Stefano Tonetta*

A Structured Validation and Verification Method for Automotive Systems Considering the OEM/Supplier Interface .......................... 90  
*Kristian Beckers, Isabelle Côté, Thomas Frese, Denis Hatebur, and Maritta Heisel*
Automotive Software

Model-Based Analysis for Safety Critical Software ........................................... 111
Stefan Gulan, Jens Harnisch, Sven Johr, Roberto Kretschmer,
Stefan Rieger, and Rafael Zalman

Integrated Safety Analysis Using Systems-Theoretic Process Analysis
and Software Model Checking ................................................................. 121
Asim Abdulkhaleq and Stefan Wagner

Back-to-Back Fault Injection Testing in Model-Based Development ............ 135
Peter Folkesson, Fatemeh Ayatolahi, Behrooz Sangchoolie,
Jonny Vinter, Mafijul Islam, and Johan Karlsson

Error Detection

Understanding the Effects of Data Corruption on Application Behavior
Based on Data Characteristics ................................................................. 151
Georgios Stefanakis, Vijay Nagarajan, and Marcelo Cintra

A Multi-layer Anomaly Detector for Dynamic Service-Based Systems ....... 166
Andrea Ceccarelli, Tommaso Zoppi, Massimiliano Itria,
and Andrea Bondavalli

Medical Safety Cases

Safety Case Driven Development for Medical Devices ............................... 183
Alejandra Ruiz, Paulo Barbosa, Yang Medeiros, and Huascar Espinoza

Towards an International Security Case Framework for Networked Medical
Devices ...................................................................................................... 197
Anita Finnegan and Fergal McCaffery

Medical Systems

Systems-Theoretic Safety Assessment of Robotic Telesurgical Systems ....... 213
Homa Alemzadeh, Daniel Chen, Andrew Lewis, Zbigniew Kalbarczyk,
Jaishankar Raman, Nancy Leveson, and Ravishankar Iyer

Towards Assurance for Plug & Play Medical Systems ............................... 228
Andrew L. King, Lu Feng, Sam Procter, Sanjian Chen,
Oleg Sokolsky, John Hatcliff, and Insup Lee

Risk Classification of Data Transfer in Medical Systems ........................... 243
Dagmar Rosenbrand, Rob de Weerd, Lex Bothe,
and Jan Jaap Baalbergen
Requirement Engineering for Functional Alarm System for Interoperable Medical Devices .............................................................. 252

  Krishna K. Venkatasubramanian, Eugene Y. Vasserman, Vasiliki Sfyrla,
  Oleg Sokolsky, and Insup Lee

Architectures and Testing

The Safety Requirements Decomposition Pattern .......................... 269

  Pablo Oliveira Antonino, Mario Trapp, Paulo Barbosa,
  Edmar C. Gurjão, and Jeferson Rosário

Automatic Architecture Hardening Using Safety Patterns ............... 283

  Kevin Delmas, Rêmi Delmas, and Claire Pagetti

Modeling the Impact of Testing on Diverse Programs .................... 297

  Peter Bishop

Safety Cases

A Model for Safety Case Confidence Assessment .......................... 313

  Jérémie Guiôchet, Quynh Anh Do Hoang, and Mohamed Kaaniche

Towards a Formal Basis for Modular Safety Cases ....................... 328

  Ewen Denney and Ganesh Pai

Security Attacks

Quantifying Risks to Data Assets Using Formal Metrics in Embedded System Design ................................................................. 347

  Maria Vasilevskaya and Simin Nadjm-Tehrani

ISA²R: Improving Software Attack and Analysis Resilience via Compiler-Level Software Diversity .................................................. 362

  Rafael Fedler, Sebastian Banescu, and Alexander Pretschner

Cyber Security and Integration

Barriers to the Use of Intrusion Detection Systems in Safety-Critical Applications ................................................................. 375

  Chris W. Johnson

Stochastic Modeling of Safety and Security of the e-Motor, an ASIL-D Device ................................................................. 385

  Peter T. Popov
Organisational, Political and Technical Barriers to the Integration of Safety and Cyber-Security Incident Reporting Systems .......................... 400
  Chris W. Johnson

A Comprehensive Safety, Security, and Serviceability Assessment Method. . . 410
  Georg Macher, Andrea Höller, Harald Sporer, Eric Armengaud,
  and Christian Kreiner

Programming and Compiling

Source-Code-to-Object-Code Traceability Analysis for Avionics Software:
Don’t Trust Your Compiler ................................................................. 427
  Jörg Brauer, Markus Dahlweid, Tobias Pankrath, and Jan Peleska

Automated Generation of Buffer Overflow Quick Fixes Using Symbolic
Execution and SMT ................................................................. 441
  Paul Muntean, Vasantha Kommanapalli, Andreas Ibing,
  and Claudia Eckert

A Software-Based Error Detection Technique for Monitoring the Program
Execution of RTUs in SCADA ..................................................... 457
  Navid Rajabpour and Yasser Sedaghat

Real-World Types and Their Application ........................................ 471
  Jian Xiang, John Knight, and Kevin Sullivan

Author Index ................................................................. 485
Computer Safety, Reliability, and Security
Koornneef, F.; van Gulijk, C. (Eds.)
2015, XXII, 486 p. 141 illus. in color., Softcover
ISBN: 978-3-319-24254-5