

# Contents

## Invited Talks

Medical Devices, Electronic Health Records and Assuring Patient Safety: Future Challenges? . . . . .	3
<i>Cor J. Kalkman</i>	
Cyber (In-)security of Industrial Control Systems: A Societal Challenge. . . . .	7
<i>Eric Luijff</i>	

## Flight Systems

Modeling Guidelines and Usage Analysis Towards Applying HiP-HOPS Method to Airborne Electrical Systems . . . . .	19
<i>Carolina D. Villela, Humberto H. Sano, and Juliana M. Bezerra</i>	
The Formal Derivation of Mode Logic for Autonomous Satellite Flight Formation . . . . .	29
<i>Anton Tarasyuk, Inna Pereverzeva, Elena Troubitsyna, and Timo Latvala</i>	

## Automotive Embedded Systems

Simulation of Automotive Security Threat Warnings to Analyze Driver Interpretations and Emotional Transitions. . . . .	47
<i>Robert Altschaffel, Tobias Hoppe, Sven Kuhlmann, and Jana Dittmann</i>	
Improving Dependability of Vision-Based Advanced Driver Assistance Systems Using Navigation Data and Checkpoint Recognition . . . . .	59
<i>Ayhan Mehmed, Sasikumar Punnekkat, Wilfried Steiner, Giacomo Spampinato, and Martin Lettner</i>	
Safely Using the AUTOSAR End-to-End Protection Library. . . . .	74
<i>Thomas Arts and Stefano Tonetta</i>	
A Structured Validation and Verification Method for Automotive Systems Considering the OEM/Supplier Interface . . . . .	90
<i>Kristian Beckers, Isabelle Côté, Thomas Frese, Denis Hatebur, and Maritta Heisel</i>	

**Automotive Software**

Model-Based Analysis for Safety Critical Software . . . . .	111
<i>Stefan Gulan, Jens Harnisch, Sven Johr, Roberto Kretschmer, Stefan Rieger, and Rafael Zalman</i>	
Integrated Safety Analysis Using Systems-Theoretic Process Analysis and Software Model Checking . . . . .	121
<i>Asim Abdulkhaleq and Stefan Wagner</i>	
Back-to-Back Fault Injection Testing in Model-Based Development . . . . .	135
<i>Peter Folkesson, Fatemeh Ayatollahi, Behrooz Sangchoolie, Jonny Vinter, Mafijul Islam, and Johan Karlsson</i>	

**Error Detection**

Understanding the Effects of Data Corruption on Application Behavior Based on Data Characteristics . . . . .	151
<i>Georgios Stefanakis, Vijay Nagarajan, and Marcelo Cintra</i>	
A Multi-layer Anomaly Detector for Dynamic Service-Based Systems . . . . .	166
<i>Andrea Ceccarelli, Tommaso Zoppi, Massimiliano Itria, and Andrea Bondavalli</i>	

**Medical Safety Cases**

Safety Case Driven Development for Medical Devices. . . . .	183
<i>Alejandra Ruiz, Paulo Barbosa, Yang Medeiros, and Huascar Espinoza</i>	
Towards an International Security Case Framework for Networked Medical Devices . . . . .	197
<i>Anita Finnegan and Fergal McCaffery</i>	

**Medical Systems**

Systems-Theoretic Safety Assessment of Robotic Telesurgical Systems . . . . .	213
<i>Homa Alemzadeh, Daniel Chen, Andrew Lewis, Zbigniew Kalbarczyk, Jaishankar Raman, Nancy Leveson, and Ravishankar Iyer</i>	
Towards Assurance for Plug & Play Medical Systems . . . . .	228
<i>Andrew L. King, Lu Feng, Sam Procter, Sanjian Chen, Oleg Sokolsky, John Hatcliff, and Insup Lee</i>	
Risk Classification of Data Transfer in Medical Systems . . . . .	243
<i>Dagmar Rosenbrand, Rob de Weerd, Lex Bothe, and Jan Jaap Baalbergen</i>	

Requirement Engineering for Functional Alarm System for Interoperable Medical Devices . . . . .	252
<i>Krishna K. Venkatasubramanian, Eugene Y. Vasserman, Vasiliki Sfyrla, Oleg Sokolsky, and Insup Lee</i>	

## Architectures and Testing

The Safety Requirements Decomposition Pattern. . . . .	269
<i>Pablo Oliveira Antonino, Mario Trapp, Paulo Barbosa, Edmar C. Gurjão, and Jeferson Rosário</i>	
Automatic Architecture Hardening Using Safety Patterns . . . . .	283
<i>Kevin Delmas, Rémi Delmas, and Claire Pagetti</i>	
Modeling the Impact of Testing on Diverse Programs . . . . .	297
<i>Peter Bishop</i>	

## Safety Cases

A Model for Safety Case Confidence Assessment . . . . .	313
<i>Jérémie Guiochet, Quynh Anh Do Hoang, and Mohamed Kaaniche</i>	
Towards a Formal Basis for Modular Safety Cases . . . . .	328
<i>Ewen Denney and Ganesh Pai</i>	

## Security Attacks

Quantifying Risks to Data Assets Using Formal Metrics in Embedded System Design . . . . .	347
<i>Maria Vasilevskaya and Simin Nadjm-Tehrani</i>	
ISA <sup>2</sup> R: Improving Software Attack and Analysis Resilience via Compiler-Level Software Diversity . . . . .	362
<i>Rafael Fedler, Sebastian Banescu, and Alexander Pretschner</i>	

## Cyber Security and Integration

Barriers to the Use of Intrusion Detection Systems in Safety-Critical Applications . . . . .	375
<i>Chris W. Johnson</i>	
Stochastic Modeling of Safety and Security of the e-Motor, an ASIL-D Device . . . . .	385
<i>Peter T. Popov</i>	

Organisational, Political and Technical Barriers to the Integration of Safety and Cyber-Security Incident Reporting Systems . . . . .	400
<i>Chris W. Johnson</i>	
A Comprehensive Safety, Security, and Serviceability Assessment Method. . .	410
<i>Georg Macher, Andrea Höller, Harald Sporer, Eric Armengaud, and Christian Kreiner</i>	
<b>Programming and Compiling</b>	
Source-Code-to-Object-Code Traceability Analysis for Avionics Software: Don't Trust Your Compiler . . . . .	427
<i>Jörg Brauer, Markus Dahlweid, Tobias Pankrath, and Jan Peleska</i>	
Automated Generation of Buffer Overflow Quick Fixes Using Symbolic Execution and SMT . . . . .	441
<i>Paul Muntean, Vasantha Kommanapalli, Andreas Ibing, and Claudia Eckert</i>	
A Software-Based Error Detection Technique for Monitoring the Program Execution of RTUs in SCADA. . . . .	457
<i>Navid Rajabpour and Yasser Sedaghat</i>	
Real-World Types and Their Application . . . . .	471
<i>Jian Xiang, John Knight, and Kevin Sullivan</i>	
<b>Author Index</b> . . . . .	485

Computer Safety, Reliability, and Security

34th International Conference, SAFECOMP 2015, Delft,  
The Netherlands, September 23-25, 2015, Proceedings

Koornneef, F.; van Gulijk, C. (Eds.)

2015, XXII, 486 p. 141 illus. in color., Softcover

ISBN: 978-3-319-24254-5