

Contents

Dynamic Fault Trees

- Model-Based Safety Analysis for Vehicle Guidance Systems 3
*Majdi Ghadhab, Sebastian Junges, Joost-Pieter Katoen, Matthias Kuntz,
and Matthias Volk*
- Rare Event Simulation for Dynamic Fault Trees 20
*Enno Ruijters, Daniël Reijbergen, Pieter-Tjerk de Boer,
and Mariëlle Stoelinga*

Safety Case and Argumentation

- Arguing on Software-Level Verification Techniques Appropriateness. 39
Carmen Cârlan, Barbara Gallina, Severin Kacianka, and Ruth Breu
- Confidence Assessment Framework for Safety Arguments 55
Rui Wang, Jérémie Guiochet, and Gilles Motet
- Safety Case Impact Assessment in Automotive Software Systems:
An Improved Model-Based Approach 69
*Sahar Kokaly, Rick Salay, Marsha Chechik, Mark Lawford,
and Tom Maibaum*

Formal Verification

- Modeling Operator Behavior in the Safety Analysis of Collaborative
Robotic Applications 89
*Mehrnoosh Askarpour, Dino Mandrioli, Matteo Rossi,
and Federico Vicentini*
- Development and Verification of a Flight Stack for a High-Altitude
Glider in Ada/SPARK 2014 105
Martin Becker, Emanuel Regnath, and Samarjit Chakraborty
- A Simplex Architecture for Hybrid Systems Using Barrier Certificates 117
*Junxing Yang, Md. Ariful Islam, Abhishek Murthy, Scott A. Smolka,
and Scott D. Stoller*

Autonomous Systems

A Conceptual Safety Supervisor Definition and Evaluation Framework
for Autonomous Systems 135
Patrik Feth, Daniel Schneider, and Rasmus Adler

A Strategy for Assessing Safe Use of Sensors in Autonomous
Road Vehicles 149
*Rolf Johansson, Samieh Alissa, Staffan Bengtsson, Carl Berghem,
Olof Bridal, Anders Cassel, De-Jiu Chen, Martin Gassilewski,
Jonas Nilsson, Anders Sandberg, Stig Ursing, Fredrik Warg,
and Anders Werneman*

Modeling the Safety Architecture of UAS Flight Operations 162
Ewen Denney, Ganesh Pai, and Iain Whiteside

Generic Management of Availability in Fail-Operational
Automotive Systems 179
Philipp Schleiss, Christian Drabek, Gereon Weiss, and Bernhard Bauer

Static Analysis and Testing

Benchmarking Static Code Analyzers 197
Jörg Herter, Daniel Kästner, Christoph Mallon, and Reinhard Wilhelm

Automatic Estimation of Verified Floating-Point Round-Off Errors
via Static Analysis 213
Mariano Moscato, Laura Titolo, Aaron Dutle, and César A. Muñoz

Classification Tree Method with Parameter Shielding. 230
*Takashi Kitamura, Akihisa Yamada, Goro Hatayama, Shinya Sakuragi,
Eun-Hye Choi, and Cyrille Artho*

Safety Analysis and Assessment

ErrorSim: A Tool for Error Propagation Analysis of Simulink Models 245
*Mustafa Saraoğlu, Andrey Morozov, Mehmet Turan Söylemez,
and Klaus Janschek*

Early Safety Assessment of Automotive Systems Using Sabotage
Simulation-Based Fault Injection Framework 255
*Garazi Juez, Estibaliz Amparan, Ray Lattarulo, Alejandra Ruíz,
Joshué Pérez, and Huáscar Espinoza*

Towards a Sensor Failure-Dependent Performance Adaptation
Using the Validity Concept 270
Juliane Höbel, Georg Jäger, Sebastian Zug, and Andreas Wendemuth

SMT-Based Synthesis of Fault-Tolerant Architectures 287
Kevin Delmas, Rémi Delmas, and Claire Pagetti

Safety and Security

A Lightweight Threat Analysis Approach Intertwining Safety
and Security for the Automotive Domain 305
Jürgen Dürrwang, Kristian Beckers, and Reiner Kriesten

A Security Architecture for Railway Signalling. 320
*Christian Schlehuber, Markus Heinrich, Tsvetoslava Vateva-Gurova,
Stefan Katzenbeisser, and Neeraj Suri*

Systematic Pattern Approach for Safety and Security Co-engineering
in the Automotive Domain 329
*Tiago Amorim, Helmut Martin, Zhendong Ma, Christoph Schmittner,
Daniel Schneider, Georg Macher, Bernhard Winkler, Martin Krammer,
and Christian Kreiner*

Author Index 343



<http://www.springer.com/978-3-319-66265-7>

Computer Safety, Reliability, and Security
36th International Conference, SAFECOMP 2017,
Trento, Italy, September 13-15, 2017, Proceedings
Tonetta, S.; Schoitsch, E.; Bitsch, F. (Eds.)
2017, XIX, 344 p. 107 illus., Softcover
ISBN: 978-3-319-66265-7