

# Contents

## Dynamic Fault Trees

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

## Safety Case and Argumentation

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

## Formal Verification

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

## Autonomous Systems

A Conceptual Safety Supervisor Definition and Evaluation Framework for Autonomous Systems . . . . .	135
<i>Patrik Feth, Daniel Schneider, and Rasmus Adler</i>	
A Strategy for Assessing Safe Use of Sensors in Autonomous Road Vehicles . . . . .	149
<i>Rolf Johansson, Samieh Alissa, Staffan Bengtsson, Carl Bergenhem, Olof Bridal, Anders Cassel, De-Jiu Chen, Martin Gassilewski, Jonas Nilsson, Anders Sandberg, Stig Ursing, Fredrik Warg, and Anders Werneman</i>	
Modeling the Safety Architecture of UAS Flight Operations. . . . .	162
<i>Ewen Denney, Ganesh Pai, and Iain Whiteside</i>	
Generic Management of Availability in Fail-Operational Automotive Systems . . . . .	179
<i>Philipp Schleiss, Christian Drabek, Gereon Weiss, and Bernhard Bauer</i>	

## Static Analysis and Testing

Benchmarking Static Code Analyzers . . . . .	197
<i>Jörg Herter, Daniel Kästner, Christoph Mallon, and Reinhard Wilhelm</i>	
Automatic Estimation of Verified Floating-Point Round-Off Errors via Static Analysis . . . . .	213
<i>Mariano Moscato, Laura Titolo, Aaron Dutle, and César A. Muñoz</i>	
Classification Tree Method with Parameter Shielding. . . . .	230
<i>Takashi Kitamura, Akihisa Yamada, Goro Hatayama, Shinya Sakuragi, Eun-Hye Choi, and Cyrille Artho</i>	

## Safety Analysis and Assessment

ErrorSim: A Tool for Error Propagation Analysis of Simulink Models. . . . .	245
<i>Mustafa Saraoğlu, Andrey Morozov, Mehmet Turan Söylemez, and Klaus Janschek</i>	
Early Safety Assessment of Automotive Systems Using Sabotage Simulation-Based Fault Injection Framework . . . . .	255
<i>Garazi Juez, Estibaliz Amparan, Ray Lattarulo, Alejandra Ruíz, Joshué Pérez, and Huáscar Espinoza</i>	
Towards a Sensor Failure-Dependent Performance Adaptation Using the Validity Concept . . . . .	270
<i>Juliane Höbel, Georg Jäger, Sebastian Zug, and Andreas Wendemuth</i>	

SMT-Based Synthesis of Fault-Tolerant Architectures . . . . .	287
<i>Kevin Delmas, Rémi Delmas, and Claire Pagetti</i>	

## Safety and Security

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

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

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

<b>Author Index</b> . . . . .	343
-------------------------------	-----

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