

# Contents

## Fault Injection

FISSC: A Fault Injection and Simulation Secure Collection . . . . .	3
<i>Louis Dureuil, Guillaume Petiot, Marie-Laure Potet, Thanh-Ha Le, Aude Crohen, and Philippe de Choudens</i>	

FIDL: A Fault Injection Description Language for Compiler-Based SFI Tools. . . . .	12
<i>Maryam Raiyat Aliabadi and Karthik Pattabiraman</i>	

## Safety Assurance

Using Process Models in System Assurance . . . . .	27
<i>Richard Hawkins, Thomas Richardson, and Tim Kelly</i>	

The Indispensable Role of Rationale in Safety Standards . . . . .	39
<i>John C. Knight and Jonathan Rowanhill</i>	

Composition of Safety Argument Patterns . . . . .	51
<i>Ewen Denney and Ganesh Pai</i>	

## Formal Verification

Formal Analysis of Security Properties on the OPC-UA SCADA Protocol . . .	67
<i>Maxime Puys, Marie-Laure Potet, and Pascal Lafourcade</i>	

A Dedicated Algorithm for Verification of Interlocking Systems . . . . .	76
<i>Quentin Cappart and Pierre Schaus</i>	

Catalogue of System and Software Properties . . . . .	88
<i>Victor Bos, Harold Bruintjes, and Stefano Tonetta</i>	

A High-Assurance, High-Performance Hardware-Based Cross-Domain System . . . . .	102
<i>David Hardin, Konrad Slind, Mark Bortz, James Potts, and Scott Owens</i>	

## Automotive

Using STPA in an ISO 26262 Compliant Process . . . . .	117
<i>Archana Mallya, Vera Pantelic, Morayo Adedjouma, Mark Lawford, and Alan Wassynng</i>	

A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context . . . . .	130
<i>Georg Macher, Eric Armengaud, Eugen Brenner, and Christian Kreiner</i>	

**Anomaly Detection and Resilience**

Context-Awareness to Improve Anomaly Detection in Dynamic Service Oriented Architectures . . . . .	145
<i>Tommaso Zoppi, Andrea Ceccarelli, and Andrea Bondavalli</i>	
Towards Modelling Adaptive Fault Tolerance for Resilient Computing Analysis . . . . .	159
<i>William Excoffon, Jean-Charles Fabre, and Michael Lauer</i>	
Automatic Invariant Selection for Online Anomaly Detection . . . . .	172
<i>Leonardo Aniello, Claudio Ciccotelli, Marcello Cinque, Flavio Frattini, Leonardo Querzoni, and Stefano Russo</i>	

**Cyber Security**

Modelling Cost-Effectiveness of Defenses in Industrial Control Systems . . . .	187
<i>Andrew Fielder, Tingting Li, and Chris Hankin</i>	
Your Industrial Facility and Its IP Address: A First Approach for Cyber-Physical Attack Modeling . . . . .	201
<i>Robert Clausning, Robert Fischer, Jana Dittmann, and Yongjian Ding</i>	
Towards Security-Explicit Formal Modelling of Safety-Critical Systems. . . . .	213
<i>Elena Troubitsyna, Linas Laibinis, Inna Pereverzeva, Tuomas Kuismin, Dubravka Ilic, and Timo Latvala</i>	
A New SVM-Based Fraud Detection Model for AMI . . . . .	226
<i>Marcelo Zanetti, Edgard Jamhour, Marcelo Pellenz, and Manoel Penna</i>	
Exploiting Trust in Deterministic Builds . . . . .	238
<i>Christopher Jämthagen, Patrik Lantz, and Martin Hell</i>	

**Fault Trees**

Advancing Dynamic Fault Tree Analysis - Get Succinct State Spaces Fast and Synthesise Failure Rates . . . . .	253
<i>Matthias Volk, Sebastian Junges, and Joost-Pieter Katoen</i>	
Effective Static and Dynamic Fault Tree Analysis . . . . .	266
<i>Ola Bäckström, Yuliya Butkova, Holger Hermanns, Jan Krčál, and Pavel Krčál</i>	

## Safety Analysis

SAFER-HRC: Safety Analysis Through Formal vERification in Human-Robot Collaboration . . . . .	283
<i>Mehrnoosh Askarpour, Dino Mandrioli, Matteo Rossi, and Federico Vicentini</i>	
Adapting the Orthogonal Defect Classification Taxonomy to the Space Domain . . . . .	296
<i>Nuno Silva and Marco Vieira</i>	
Towards Cloud-Based Enactment of Safety-Related Processes . . . . .	309
<i>Sami Alajrami, Barbara Gallina, Irfan Sljivo, Alexander Romanovsky, and Petter Isberg</i>	
<b>Author Index . . . . .</b>	<b>323</b>

Computer Safety, Reliability, and Security  
35th International Conference, SAFECOMP 2016,  
Trondheim, Norway, September 21-23, 2016,  
Proceedings  
Skavhaug, A.; Guiochet, J.; Bitsch, F. (Eds.)  
2016, XV, 324 p. 105 illus., Softcover  
ISBN: 978-3-319-45476-4