

Michael Butler Cliff Jones  
Alexander Romanovsky Elena Troubitsyna (Eds.)

# Rigorous Development of Complex Fault-Tolerant Systems



Springer

# Table of Contents

Train Systems .....	1
<i>Jean-Raymond Abrial</i>	
Formalising Reconciliation in Partitionable Networks with Distributed Services .....	37
<i>Mikael Asplund, Simin Nadjm-Tehrani</i>	
The Fault-Tolerant Insulin Pump Therapy .....	59
<i>Alfredo Capozucca, Nicolas Guelfi, Patrizio Pelliccione</i>	
Reasoning About Exception Flow at the Architectural Level .....	80
<i>Fernando Castor Filho, Patrick Henrique da S. Brito, Cecília Mary F. Rubira</i>	
Are Practitioners Writing Contracts? .....	100
<i>Patrice Chalin</i>	
Determining the Specification of a Control System: An Illustrative Example .....	114
<i>Joey W. Coleman</i>	
Achieving Fault Tolerance by a Formally Validated Interaction Policy ...	133
<i>Alessandro Fantechi, Stefania Gnesi, Laura Semini</i>	
F(I)MEA-Technique of Web Services Analysis and Dependability Ensuring .....	153
<i>Anatolii Gorbenko, Vyacheslav Kharchenko, Olga Tarasyuk, Alexey Furmanov</i>	
On Specification and Verification of Location-Based Fault Tolerant Mobile Systems .....	168
<i>Alexei Iliasov, Victor Khomenko, Maciej Koutny, Alexander Romanovsky</i>	
Formal Development of Mechanisms for Tolerating Transient Faults .....	189
<i>Dubravka Ilić, Elena Troubitsyna, Linas Laibinis, Colin Snook</i>	
Separating Concerns in Requirements Analysis: An Example .....	210
<i>Daniel Jackson, Michael Jackson</i>	

Rigorous Fault Tolerance Using Aspects and Formal Methods ..... 226  
*Shmuel Katz*

Rigorous Development of Fault-Tolerant Agent Systems ..... 241  
*Linus Laibinis, Elena Troubitsyna, Alexei Iliasov, Alexander Romanovsky*

Formal Service-Oriented Development of Fault Tolerant Communicating Systems ..... 261  
*Linus Laibinis, Elena Troubitsyna, Sari Leppänen, Johan Lilius, Qaisar Ahmad Malik*

Programming-Logic Analysis of Fault Tolerance: Expected Performance of Self-stabilisation ..... 288  
*Carroll Morgan, Annabelle K. McIver*

Formal Analysis of the Operational Concept for the Small Aircraft Transportation System ..... 306  
*César Muñoz, Víctor Carreño, Gilles Dowek*

Towards a Method for Rigorous Development of Generic Requirements Patterns ..... 326  
*Colin Snook, Michael Poppleton, Ian Johnson*

Rigorous Design of Fault-Tolerant Transactions for Replicated Database Systems Using Event B ..... 343  
*Divakar Yadav, Michael Butler*

Engineering Reconfigurable Distributed Software Systems: Issues Arising for Pervasive Computing ..... 364  
*Apostolos Zarras, Manel Fredj, Nikolaos Georgantas, Valerie Issarny*

**Position Papers**

Tools for Developing Large Systems (A Proposal) ..... 387  
*Jean-Raymond Abrial*

Why Programming Languages Still Matter ..... 391  
*Peter Amey*

**Author Index** ..... 403