

Table of Contents

Session 1

System Analysis

Reliability Analysis of Safety-Related Communication Architectures <i>Oliver Schulz and Jan Peleska</i>	1
A Novel HAZOP Study Approach in the RAMS Analysis of a Therapeutic Robot for Disabled Children <i>Petr Böhm and Thomas Gruber</i>	15
Variability Management of Safety and Reliability Models: An Intermediate Model towards Systematic Reuse of Component Fault Trees <i>Carolina Gómez, Peter Liggesmeyer, and Ariane Sutor</i>	28
QoS Analysis of Weighted Multi-state Probabilistic Networks via Decision Diagrams <i>Roberta Terruggia and Andrea Bobbio</i>	41

Session 2

Safety Cases and Certification

Comparison between IEC 60880 and IEC 61508 for Certification Purposes in the Nuclear Domain <i>Jussi Lahtinen, Mika Johansson, Jukka Ranta, Hannu Harju, and Risto Nevalainen</i>	55
Deriving Safety Cases for Hierarchical Structure in Model-Based Development <i>Nurlida Basir, Ewen Denney, and Bernd Fischer</i>	68
Assurance of Automotive Safety – A Safety Case Approach <i>Robert Palin and Ibrahim Habli</i>	82
How to “Survive” a Safety Case According to ISO 26262 <i>Torsten Dittel and Hans-Jörg Aryus</i>	97

Session 3

Aerospace

Benchmarking Software Requirements Documentation for Space
Application 112
*Paulo C. V  ras, Emilia Villani, Ana Maria Ambr  sio,
Rodrigo P. Pontes, Marco Vieira, and Henrique Madeira*

Verifying Mode Consistency for On-Board Satellite Software 126
*Alexei Iliasov, Elena Troubitsyna, Linas Laibinis,
Alexander Romanovsky, Kimmo Varpaaniemi, Pauli V  is  nen,
Dubravka Ilic, and Timo Latvala*

Computational Concerns in the Integration of Unmanned Airborne
Systems into Controlled Airspace 142
Christopher W. Johnson

Session 4

Error Detection

Residual Error Probability of Embedded CRC by Stochastic
Automata 155
Frank Schiller and Tina Mattes

ANB- and ANBDmem-Encoding: Detecting Hardware Errors in
Software 169
Ute Schiffel, Andr   Schmitt, Martin S   kraut, and Christof Fetzer

Session 5

Validation and Verification

Field Test Methods for a Co-operative Integrated Traffic Management
System 183
Thomas Gruber, Egbert Althammer, and Erwin Schoitsch

100% Coverage for Safety-Critical Software – Efficient Testing by Static
Analysis 196
Daniel K  stner, Reinhold Heckmann, and Christian Ferdinand

MODIFI: A MODel-Implemented Fault Injection Tool 210
*Rickard Svenningsson, Jonny Vinter, Henrik Eriksson, and
Martin T  r  ngren*

Automated Test Coverage Measurement for Reactor Protection System Software Implemented in Function Block Diagram.....	223
<i>Eunkyoung Jee, Suin Kim, Sungdeok Cha, and Insup Lee</i>	

Session 6

Testing

Overcoming Non-determinism in Testing Smart Devices: A Case Study	237
<i>Peter Bishop and Lukasz Cyra</i>	
Software Testing by People with Autism	251
<i>Suzanne Haanappel and Sjaak Brinkkemper</i>	

Session 7

Critical Infrastructure - Smart Grid

Information Flow Analysis of Energy Management in a Smart Grid	263
<i>Ravi Akella and Bruce M. McMillin</i>	
Integrated Cyber-Physical Fault Injection for Reliability Analysis of the Smart Grid	277
<i>Ayman Faza, Sahra Sedigh, and Bruce McMillin</i>	
A Metrics for Measuring the Strength of Inter-dependencies	291
<i>Silvia Ruzzante, Elisa Castorini, Elena Marchei, and Vincenzo Fioriti</i>	

Session 8

Security and Safety

Security Analysis of Open Building Automation Systems.....	303
<i>Wolfgang Granzer and Wolfgang Kastner</i>	
A UML Profile for Requirements Analysis of Dependable Software	317
<i>Denis Hatebur and Maritta Heisel</i>	

Session 9

Safety Engineering (1)

Model-Based Safety Engineering of Interdependent Functions in Automotive Vehicles Using EAST-ADL2	332
<i>Anders Sandberg, DeJiu Chen, Henrik Lönn, Rolf Johansson, Lei Feng, Martin Törngren, Sandra Torchiato, Ramin Tavakoli-Kolagari, and Andreas Abele</i>	

Experiences in Applying Formal Verification in Robotics 347
Dennis Walter, Holger Täubig, and Christoph Lüth

Evolving a Safe System Design Iteratively 361
Alexandre Mota, Joabe Jesus, Adriano Gomes, Felipe Ferri, and Edson Watanabe

An Approach to Using Non Safety-Assured Programmable Components in Modest Integrity Systems 375
Peter Bishop, Kostas Tournas, and Nick Chozos

Session 10

Safety Engineering (2)

Development of High-Integrity Software Product Lines Using Model Transformation 389
Stuart Hutchesson and John McDermid

On the Safety Implications of E-Governance: Assessing the Hazards of Enterprise Information Architectures in Safety-Critical Applications 402
Christopher W. Johnson and Stefan Raue

The Right Degree of Configurability for Safety-Critical Embedded Software in Variable Message Signs 418
Thomas Novak and Christoph Stoegerer

INDEXYS, a Logical Step beyond GENESYS: INDustrial EXploitation of the genesYS cross-domain architecture 431
Andreas Eckel, Paul Milbredt, Zaid Al-Ars, Stefan Schneelee, Bart Vermeulen, György Csertán, Christoph Scheerer, Neeraj Suri, Abdelmajid Khelil, Gerhard Fohler, Roman Obermaisser, and Christian Fidi

Session 11

System Modelling and Fault Tolerance

Integrating System Modelling with Safety Activities 452
Bernhard Kaiser, Vanessa Klaas, Stefan Schulz, Christian Herbst, and Peter Lascych

Aspect-Oriented Implementation of Fault Tolerance: An Assessment of Overhead 466
Ruben Alexandersson, Peter Öhman, and Johan Karlsson

Invited Talks (Keynote Abstracts)

System of Systems Challenges	480
<i>Hermann Kopetz</i>	
Murphy Was an Optimist	481
<i>Kevin R. Driscoll</i>	
Process Control Security: Go Dutch! (United, Shared, Lean and Mean)	483
<i>Eric Luijff</i>	
Author Index	485