Preface

To accompany the 33rd edition of SAFECOMP, and the overarching FLORENCE 2014, the one-week scientific event on the development of safe, secure, dependable, and performing systems, we selected workshops covering different partially overlapping application areas and different phases of the lifecycle of such safety-critical systems. We decided to give various domain experts a common meeting place at SAFECOMP in the format of domain-specific workshops. The joining aspects are always safety and security. Bringing these experts together at one place and collecting their articles in one volume fosters collaboration and exchange of ideas.

For SAFECOMP 2014, we accepted 6 domain-specific, high-quality workshops, each with well-known chairs and an International Program Committee:

– 3rd Workshop on Architecting Safety in Collaborative Mobile Systems (ASCoMS 2014) (Chairs Renato Librino and Martin Törngren)
– Workshop on DEvelopment, VeriFIcation and VAlidation of cRiTical Systems (DEVVARTS 2014) (Chairs Francesco Brancati, Nuno Laranjeiro, and Ábel Hegediüs)
– 1st International Workshop on the Integration of Safety and Security Engineering (ISSE 2014) (Chairs Laurent Rioux and John Favaro)
– Workshop on Reliability and Security Aspects for Critical Infrastructure Protection (ReSA4CI 2014) (Chairs: Silvia Bonomi and Ilaria Matteucci)

Altogether 92 researchers from 21 countries reviewed the following 42 articles. Summarizing, we have to say that the correspondence and organization of these 6 workshops for SAFECOMP took a lot of time. But when looking at the program now, we are very proud of it and wish to thank all workshop chairs, their Program Committee members and all the people involved in the organization. You did a fantastic job.

We hope readers and attendees share our opinion that this will be a great extension to SAFECOMP 2014.

July 2014

Andrea Bondavalli
Andrea Ceccarelli
Frank Ortmeier
Organization

EWICS TC7 Chair
Francesca Saglietti University of Erlangen-Nuremberg, Germany

General Chair
Andrea Bondavalli University of Florence, Italy

Program Co-chairs
Andrea Bondavalli University of Florence, Italy
Felicita Di Giandomenico ISTI-CNR, Italy

Workshop and Tutorial Chair
Frank Ortmeier Otto -v.-Guericke-University, Germany

Industry-liaison Chair
Michael Paulitsch AIRBUS Group, Germany

Finance Chair
Ettore Ricciardi ISTI-CNR, Italy

Publication Chair
Andrea Ceccarelli University of Florence, Italy

Publicity Chair
Francesco Flammini Ansaldo STS, Italy
Local Organizing Chair

Paolo Lollini  
University of Florence, Italy

ASCoMS Program Committee

- Luis Almeida  
  FEUP, Portugal
- Abele Andreas  
  Bosch, Germany
- Fredrik Asplund  
  KTH, Sweden
- António Casimiro  
  FCUL, Portugal
- Karl Goeschka  
  TUWIEN, Austria
- Teruo Higashino  
  Osaka University, Japan
- Per Johannessen  
  Volvo AB, Sweden
- Rolf Johansson  
  SP, Sweden
- Jörg Kaiser  
  OVGU, Germany
- Vana Kalogeraki  
  Athens University of Economics and Business, Greece
- Marc-Olivier Killijian  
  Laas, France
- Renato Librino  
  4S s.r.l, Italy
- Henrik Lönn  
  Volvo AB, Sweden
- Mattias Nyberg  
  Scania and KTH, Sweden
- Elad Michael Schiller  
  Chalmers University of Technology, Sweden
- Erwin Schoitsch  
  AIT, Austria
- Martin Törngren  
  KTH, Sweden

DECSoS Program Committee

- Bettina Buth  
  HAW Hamburg, Germany
- Francesco Flammini  
  Ansaldo STS Italy, University “Federico II” of Naples, Italy
- Denis Hatebur  
  Universität Duisburg-Essen, Germany
- Floor Koornneef  
  TU Delft, The Netherlands
- Michael Lipaczweski  
  Otto-von-Guericke-Universitaet, Germany
- Dejan Nickovic  
  AIT Austrian Institute of Technology, Austria
- Frank Ortmeier  
  Otto-von-Guericke-Universitaet, Germany
- Thomas Pfeiffenberger  
  Salzburg Research Forschungsgesellschaft m.b.H, Austria
- Francesca Saglietti  
  University of Erlangen-Nuremberg, Germany
- Christoph Schmitz  
  Zühlke Engineering AG, Switzerland
- Erwin Schoitsch  
  AIT Austrian Institute of Technology, Austria
- Rolf Schumacher  
  Ingenieurbüro, Germany
- Amund Skavhaug  
  NTNU, Norway
- Mark-Alexander Sujan  
  University of Warwick, UK
- Meine van der Meulen  
  DNV, Norway
DEVVARTS Program Committee

Andrea Ceccarelli
Alessandro Cimatti
Barbara Gallina
Michaela Huhn
Hardi Hungar
Melinda Kocsis-Magyar
Rui Lopes
Henrique Madeira
Istvan Majzik
Roberto Natella
Francesco Rossi
Stefano Russo
Marco Vieira

Università di Firenze, Italy
Bruno Kessler Foundation, Italy
Mälardalen University, Sweden
Technische Universität Clausthal, Germany
German Aerospace Center - Braunschweig, Germany
PROLAN zrt, Hungary
Airbus Defence and Space, UK
University of Coimbra, Portugal
Budapest University of Technology and Economics, Hungary
University of Naples Federico II, Italy
ResilTech s.r.l., Italy
University of Naples Federico II, Italy
University of Coimbra, Portugal

ISSE Program Committee

Pasi Ahonen
Julien Brunel
Adele-Louise Carter
Barbara Czerny
Gjalt de Jong
Rami Debouk
Huascar Espinoza
Anthony Faucogney
Donald Firesmith
Jarkko Holappa
Flemming Nielsen
Stephane Paul
Michael Paulitsch
Giovanni Sartori
Erwin Schoitsch
Michal Sojka
Lorenzo Strigini
Robert Stroud
Timo Wiander

VTT, Finland
Onera, France
KITEWAY, UK
Chrysler Group LLC, USA
Melexis, Belgium
General Motors, USA
Tecnalia, Spain
ALL4TEC, France
SEI, USA
NIXU, Finland
DTU, Denmark
Thales, France
Airbus Group, Germany
Yogitech, Italy
AIT, Austria
Czech Technical University, Czech Republic
City University, UK
Adelard, UK
Stuk, Finland

ReSA4CI Program Committee

Valentina Bonfiglio
Silvia Bonomi

University of Florence, Italy
University of Rome La Sapienza, Italy
Felicita Di Giandomenico  
Maria Gradinariu  
Potop-Butucaru  
Karama Kanoun  
Ilaria Matteucci  
Alexia Milani  
Simin Nadjm-Tehrani  
Federica Paci  
Marta Patino Martinez  
Marinella Petrocchi  
Sara Tucci Piergiovanni  

ISTI-CNR, Italy
UPMC Paris 6, France
LAAS, France
IIT-CNR, Italy
University of Bordeaux, France
Linköping University, Sweden
University of Trento, Italy
Technical University of Madrid, Spain
IIT-CNR, Italy
CEA, France

**SASSUR Program Committee**

Michael Armbruster  
Ronald Blanrue  
Markus Borg  
Marc Born  
Daniela Cancila  
Ibrahim Habli  
Tudor Ionescu  
Sunil Nair  
Paolo Panaroni  
Ansgar Radermacher  
Laurent Rioux  
Mehrdad Sabetzadeh  
Kenji Taguchi  
Martin Wassmuth  
Gereon Weiß  
Ji Wu  

Siemens, Germany
EADS/Eurocopter, France
Lund University, Sweden
ikv++, Germany
CEA, France
University of York, UK
TTTech, Austria
Simula Research Laboratory, Norway
Intecs, Italy
CEA, France
Thales Research and Technology, France
University of Luxemburg, Luxemburg
AIST, Japan
EADS, Germany
Fraunhofer, Germany
Beihang University, China
Sponsors

Scientific Sponsors

EWICS TC7

Università degli Studi di Firenze

Consiglio Nazionale delle Ricerche (CNR) - Istituto di Scienza e Tecnologie dell’Informazione (ISTI) “A. Faedo”

Industrial Sponsors

ResilTech

Prolan Process Control Co.
Technical Co-sponsors

Associazione Italiana Esperti in Infrastrutture Critiche (AIIC)

Austrian Institute of Technology

European Network of Clubs for Reliability and Safety of Software

European Research Consortium for Informatics and Mathematics (ERCIM)

Gesellschaft für Informatik e. V

International Federation for Information Processing

Oesterreichische Computer Gesellschaft-Austrian Computer Society
# Table of Contents

**Architecting Safety in Collaborative Mobile Systems (ASCoMS’14)**

3rd Workshop on Architecting Safety in Collaborative Mobile Systems (ASCoMS) ................................................................. 1  
*Renato Librino and Martin Törngren*

Intelligent Transport Systems - The Role of a Safety Loop for Holistic Safety Management .............................................................. 3  
*Kenneth Östberg, Martin Törngren, Fredrik Asplund, and Magnus Bengtsson*

Safety Verification of Multiple Autonomous Systems by Formal Approach ...................................................................................... 11  
*Kozo Okano and Toshifusa Sekizawa*

Checking Verification Compliance of Technical Safety Requirements on the AUTOSAR Platform Using Annotated Semi-formal Executable Models ....................................................................................................................... 19  
*Martin Skoglund, Hans Svensson, Henrik Eriksson, Thomas Arts, Rolf Johansson, and Alex Gerdes*

Evaluation of Safety Rules in a Safety Kernel-Based Architecture .......... 27  
*Eric Vial and António Casimiro*

Driving with Confidence: Local Dynamic Maps That Provide LoS for the Gulliver Test-Bed ................................................................. 36  
*Christian Berger, Oscar Morales, Thomas Petig, and Elad Michael Schiller*

Sensor- and Environment Dependent Performance Adaptation for Maintaining Safety Requirements ....................................................... 46  
*Tino Brade, Georg Jäger, Sebastian Zug, and Jörg Kaiser*

Collaborative Development of Safety-Critical Automotive Systems: Exchange, Views and Metrics ....................................................... 55  
*Johan Ekberg, Urban Ingelsson, Henrik Lönn, Magnus Skoog, and Jan Söderberg*

Towards Energy Efficient, High-Speed Communication in WSNs .......... 63  
*Attila Nagy and Olaf Landsiedel*

Comparing Adaptive TDMA against a Clock Synchronization Approach .............................................................................................. 71  
*Luis Almeida, Frederico Santos, and Luis Oliveira*
**Table of Contents**

**ERCIM/EWICS/ARTEMIS Workshop on Dependable Embedded and Cyberphysical Systems and Systems-of-Systems (DECSoS’14)**


*Erwin Schoitsch and Amund Skavhaug*

True Error or False Alarm? Refining Astrée’s Abstract Interpretation Results by Embedded Tester’s Automatic Model-Based Testing ........ 84

*Sayali Salvi, Daniel Kästner, Tom Bienmüller, and Christian Ferdinand*

Proving Compliance of Implementation Models to Safety Specifications .......................................................... 97

*Markus Oertel, Omar Kacimi, and Eckard Böde*

MTBF Inconsistency Analysis on Inferred Product Breakdown Structures .................................................. 108

*Christian Ellen, Martin Bösch, and Thomas Peikenkamp*

Critical Systems Verification in MetaMORP(h)OSY .................. 119

*Rocco Aversa, Beniamino Di Martino, and Francesco Moscato*

Report on the Railway Use-Case of the Crystal Project: Objectives and Progress ........................................... 130

*Alexandre Ginisty, Frédérique Vallée, Elie Soubiran, and Vidal-delmas Tchapet-Nya*

Contract-Based Analysis for Verification of Communication-Based Train Control (CBTC) System .......................... 137

*Marco Carloni, Orlando Ferrante, Alberto Ferrari, Gianpaolo Massaroli, Antonio Orazzo, Ida Petrone, and Luigi Velardi*

An Interoperable Testing Environment for ERTMS/ETCS Control Systems .................................................. 147

*Gregorio Barberio, Beniamino Di Martino, Nicola Mazzocca, Luigi Velardi, Aniello Amato, Renato De Guglielmo, Ugo Gentile, Stefano Marrone, Roberto Nardone, Adriano Peron, and Valeria Vittorini*

Modelling Resilient Systems-of-Systems in Event-B .................. 157

*Linas Laibinis, Inna Pereverzeva, and Elena Troubitsyna*
Towards Assured Dynamic Configuration of Safety-Critical Embedded Systems ........................................................ 167
Nermin Kajtazovic, Christopher Preschern, Andrea Höller, and Christian Kreiner

Towards Trust Assurance and Certification in Cyber-Physical Systems ........................................................ 180
Daniel Schneider, Eric Armengaud, and Erwin Schoitsch

DEvelopment, Verification and VAlidation of cRiTical Systems (DEVVARTS’14)

Introduction to the Safecomp 2014 Workshop: DEvelopment, Verification and VAlidation of cRiTical Systems (DEVVARTS’14) ........................................ 192
Francesco Brancati, Nuno Laranjeiro, and Ábel Hegedüs

Verification of Fault-Tolerant System Architectures Using Model Checking ........................................................ 195
Jussi Lahtinen

Verification of a Real-Time Safety-Critical Protocol Using a Modelling Language with Formal Data and Behaviour Semantics ........................................ 207
Tamás Tóth, András Vörös, and István Majzik

Visualization of Model-Implemented Fault Injection Experiments ........................................................ 219
Daniel Skarin, Jonny Vinter, and Rickard Svenningsson

Cost-Effective Testing for Critical Off-the-Shelf Services ........................................................ 231
Fabio Duchi, Nuno Antunes, Andrea Ceccarelli, Giuseppe Vella, Francesco Rossi, and Andrea Bondavalli

On Security Countermeasures Ranking through Threat Analysis ........................................................ 243
Nicola Nostro, Ilaria Matteucci, Andrea Ceccarelli, Felicita Di Giandomenico, Fabio Martinelli, and Andrea Bondavalli

Enabling Cross-Domain Reuse of Tool Qualification Certification Artefacts ........................................................ 255
Barbara Gallina, Shaghayegh Kashiyarandi, Karlheinz Zugsbratl, and Arjan Geven

Integration of Safety and Security Engineering (ISSE’14)

1st International Workshop on the Integration of Safety and Security Engineering (ISSE’14) ........................................ 267
Laurent Rioux and John Favaro
From Safety Models to Security Models: Preliminary Lessons Learnt

_**Pierre Bieber and Julien Brunel**_  

FMVEA for Safety and Security Analysis of Intelligent and Cooperative Vehicles

_**Christoph Schmittner, Zhendong Ma, and Paul Smith**_  

Uniform Approach of Risk Communication in Distributed IT Environments Combining Safety and Security Aspects

_**Jana Fruth and Edgar Nett**_  

---

## Reliability and Security Aspects for Critical Infrastructure Protection (ReSA4CI’14)

Introduction to the Safecomp 2014 Workshop: Reliability and Security Aspects for Critical Infrastructure Protection (ReSA4CI 2014)

_**Silvia Bonomi and Ilaria Matteucci**_  

Modeling and Evaluation of Maintenance Procedures for Gas Distribution Networks with Time-Dependent Parameters

_**Laura Carnevali, Marco Paolieri, Fabio Tarani, Enrico Vicario, and Kumiko Tadano**_  

Quantification of the Impact of Cyber Attack in Critical Infrastructures

_**Oleksandr Netkachov, Peter Popov, and Kizito Salako**_  

Probabilistic Inference in the Physical Simulation of Interdependent Critical Infrastructure Systems

_**Paolo Franchin and Luigi Laura**_  

Energy-Based Detection of Multi-layer Flooding Attacks on Wireless Sensor Network

_**Cesario Di Sarno and Alessia Garofalo**_  

Towards a Non-intrusive Recognition of Anomalous System Behavior in Data Centers

_**Roberto Baldoni, Adriano Cerocchi, Claudio Ciccotelli, Alessandro Donno, Federico Lombardi, and Luca Montanari**_  

Toward Resilience Assessment in Business Process Architectures

_**Richard M. Zahoransky, Thomas Koslowski, and Rafael Accorsi**_  

---

## Next Generation of System Assurance Approaches for Safety-Critical Systems (SASSUR’14)

Introduction to SASSUR 2014

_**Alejandra Ruiz, Tim Kelly, and Jose Luis de la Vara**_
Assuring Avionics – Updating the Approach for the 21st Century ...... 375
  Tom Ferrell and Uma Ferrell

Rethinking of Strategy for Safety Argument Development .............. 384
  Linling Sun, Nuno Silva, and Tim Kelly

Towards a Cross-Domain Software Safety Assurance Process for
Embedded Systems.......................................................... 396
  Marc Zeller, Kai Höfig, and Martin Rothfelder

A Software Safety Verification Method Based on System-Theoretic
Process Analysis .............................................................. 401
  Asim Abdulkhaleq and Stefan Wagner

Quantifying Uncertainty in Safety Cases Using Evidential Reasoning ... 413
  Sunil Nair, Neil Walkinshaw, and Tim Kelly

Metamodel Comparison and Model Comparison for Safety Assurance ... 419
  Yaping Luo, Luc Engelen, and Mark van den Brand

Does Visualization Speed Up the Safety Analysis Process? ............ 431
  Ragaad AlTarawneh, Max Steiner, Davide Taibi,
  Shah Rukh Humayoun, and Peter Liggesmeyer

Agile Change Impact Analysis of Safety Critical Software ............ 444
  Tor Stålthane, Geir Kjetil Hanssen, Thor Myklebust, and
  Børge Haugset

Author Index ..................................................................... 455