




## Preface

This volume contains the proceedings of the First Workshop on Certification of Safety-Critical Software Controlled Systems (SafeCert'08). The workshop was held in Budapest, Hungary, on April 20, 2008, as a satellite event to the European

[View metadata, citation and similar papers at core.ac.uk](#)

brought to you by  CORE

provided by Elsevier - Publisher Connector

and feasible methods for the development and certification of software controlled high assurance systems. Related events like the Dagstuhl Seminar on *Tools for the model-based development of certifiable, dependable systems* (2007) and a number of recent national workshops (e.g. at the German Software Engineering conference (Munich, 2008)) show the rising interest in the topic.

Software is still an increasing factor in the embedded domain, and in particular in the control of systems with advanced safety or security requirements. In many domains like transportation, power generation, medical technology, manufacturing and space exploration, statutory obligations traditionally require a formalized certification for the development and operation of technical systems. But with progress in mechatronics and worldwide information systems, certification becomes a relevant issue also in areas like automotive or mobile systems and financial software applications. Specific norms and standards (IEC 61508, CENELEC) recommend processes and techniques for the software components of dependable systems to assure that they meet the technical standards and all efforts have been made to reduce the risks. Formal methods are part of these recommendations, in particular for the higher safety integrity levels. However, experience shows that certifiable development of high-assurance software needs a lot more than pure application of formal techniques and tools that are founded on a formal semantics and support in parts automated code generation, verification or testing. Certification authorities require that evidence is provided for the correctness of code generation and formal analysis results. Open issues in research and industrial practice are a sound risk assessment, the propagation of safety related requirements and proof obligations through development phases, modularization of certification, the qualification of design and analysis tools or alternatively, the construction of proofs that can be checked independently. To summarize, the major question to be addressed in the workshop is how to embed formal methods and tools in a seamless design process which covers

several development phases and which includes an efficient construction of a safety case for the product. Some first answers to these questions are given by the papers of this volume.

The program committee of SafeCert'08 consisted of

- Jens Braband, Siemens AG, Germany
- Fabrice Derepas, CEA, France
- Holger Giese, Hasso Plattner Institute, University of Potsdam, Germany
- Javier Goikoetxea, CAF, Spain
- Mats Heimdahl, University of Minnesota, USA
- Michaela Huhn, Technische Universität Braunschweig, Germany (Co-Chair)
- Hardi Hungar, OFFIS, Germany (Co-Chair)
- Yassine Lakhnech, Verimag, University of Grenoble 1, France
- Stephan Merz, INRIA & LORIA, Nancy, France
- Iulian Ober, IRIT, University of Toulouse, France
- Andras Pataricza, Budapest University of Technology and Economics, Hungary
- Bernhard Schätz, Technische Universität München, Germany

The papers were refereed by the program committee and by several outside referees, whose help is gratefully acknowledged. The invited speaker at the conference was

- Constance Heitmeyer, Naval Research Laboratory, USA

Constance Heitmeyer's lecture "Applying Formal Methods in Software Certification" is included in the CD version of these proceedings.

These proceedings will be published as volume in the series *Electronic Notes in Theoretical Computer Science (ENTCS)*. We are grateful to ENTCS for their continuing support, in particular to Mike Mislove, Managing Editor of the ENTCS series.

For the first time, SafeCert has been organized as satellite event to ETAPS. We are very grateful to the ETAPS organizers, especially to Timahér Levendovszky and Dániel Varró, for taking care of all the local organization and for accommodating our special requests.

*Michaela Huhn  
Hardi Hungar*