Preface

This volume contains the proceedings of MARS 2017, the second workshop on *Models for Formal Analysis of Real Systems*, held on April 29, 2017 in Uppala, Sweden, as an affiliated workshop of ETAPS 2017, the *European Joint Conferences on Theory and Practice of Software*.

Logics and techniques for automated reasoning have often been developed with formal analysis and formal verification in mind. To show applicability, toy examples or tiny case studies are typically presented in research papers. Since the theory needs to be developed first, this approach is reasonable.

However, to show that a developed approach actually scales to real systems, large case studies are essential. The development of formal models of real systems usually requires a perfect understanding of informal descriptions of the system - sometimes found in RFCs or other standard documents - which are usually just written in English. Based on the type of system, an adequate specification formalism needs to be chosen, and the informal specification needs to be translated into it. Examples for such formalisms include process and program algebra, Petri nets, variations of automata, as well as timed, stochastic and probabilistic extensions of these formalisms. Abstraction from unimportant details then yields an accurate, formal model of the real system.

The process of developing a detailed and accurate model usually takes a considerable amount of time, often months or years; without even starting a formal analysis. When publishing the results on a formal analysis in a scientific paper, details of the model usually have to be skipped due to lack of space, and often the lessons learnt from modelling are not discussed since they are not the main focus of the paper.

The workshop aims at discussing exactly these unmentioned lessons. Examples are:

- Which formalism is chosen, and why?
- Which abstractions have to be made and why?
- How are important characteristics of the system modelled?
- Were there any complications while modelling the system?
- Which measures were taken to guarantee the accuracy of the model?

The workshop emphasises modelling over verification. In particular, we invited papers that present full models of real systems, which may lay the basis for future comparison and analysis. The workshop thus intends to bring together researchers from different communities that all aim at verifying real systems and are developing formal models for such systems. Areas where large models often occur are within networks, (trustworthy) systems and software verification, from byte code up to programming- and specification languages. An aim of the workshop is to present different modelling approaches and discuss pros and cons for each of them.

The body of this volume contains 11 contributions, which were selected by the Program Committee out of 16 submissions. Each submission was carefully reviewed by at least three members of the programme committee, assisted by outside referees, whose help is gratefully acknowledged.

The papers presented in this volume include formal models for

- **(contemporary) hardware**, in particular a formal model for the interpretation of memory accesses and interrupts;

H. Hermanns, P. Höfner (Eds.): Models for
Formal Analysis of Real Systems (MARS 2017)
EPTCS 244, 2017, pp. i–ii, doi:10.4204/EPTCS.244.0

- **protocols** such as the Better Approach to Mobile Ad hoc Networks (B.A.T.M.A.N.) routing protocol, a fragmentation protocol running on top of the standardised CAN bus, the Stream Control Transmission Protocol (SCTP), and a cluster-tree formation protocol for the IEEE 802.15.4 TSCH MAC operation mode;
- **application software**, including a cryptographic algorithm for message authentication, and AUTOSAR (AUTomotive Open System ARchitecture) components;
- **physical systems** such as robotic cell injection, emergency power supply of a nuclear power plant, and (generic) production cells.

To round off the contributions, this volume also presents a model-derivation framework for software analysis, which itself can be used to generate formal models.

Full specifications of the contributed models are available at `http://mars-workshop.org`—often including executable models—so that their quality can be evaluated. Alternative formal descriptions are encouraged, which should foster the development of improved specification formalisms.

Holger Hermanns
Peter Höfner