

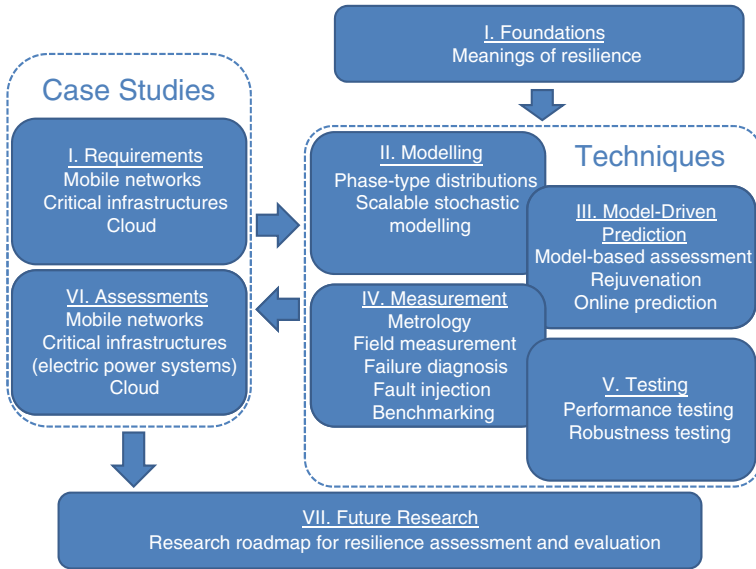
# Preface

This Springer Verlag book is a natural consequence of the workshop on Resilience Assessment and Evaluation organized in the seminar series of Schloss Dagstuhl in July 2010. As such, the book got its inspiration from the high quality and serene professional facilities at the Leibniz Centre for Informatics and the relaxing and inspiring Saarland country side near the Dagstuhl castle. For one week, about 25 scientists and engineers in resilience assessment and evaluation came together at Dagstuhl and discussed the latest trends in the field, in highly informal manner. You can find information about the original seminar by googling for ‘Dagstuhl seminar10292’.

The aim of the book is to provide an extensive overview of past, current, and future trends in resilience assessment and evaluation. Most participants at the seminar have contributed to this book, discussing case studies, general concepts, and their latest research. This book also leverages another effort that ran for the 2 years preceding the seminar, namely the EU FP7 sponsored coordination action AMBER: Assessing, Measuring and Benchmarking Resilience. AMBER aimed at providing a research agenda for the EU in resilience assessment and evaluation. Several chapters in this book are extensions of earlier versions that were made available publicly in the form of deliverables in the AMBER project.

We perceived the need for a book that targets engineers in dependable computer systems as well as academics and their PhD and MSc students. Modern-day computer systems integrate increasingly many components and systems, with growing demands from users and increasingly diverse failure and attack modes from which the system requires to be protected. This holds in varying degrees for our home and entertainment networks, for increasingly integrated enterprise systems, for safety critical computers in planes and plants, and for the critical infrastructure that serves us water, energy, communication, and other basic elements of our daily lives.

Our society would want us to be able to assess the resilience of these computer systems: what types of accidental failures and malicious attacks are these systems subject to, and how do they deal with the failures and attacks? Can we quantify and measure the resulting resilience for a system in a meaningful way, and if we can



**Fig. 1** How to use this book

quantify it, can we already predict it at design time, before we deploy and run the systems? These are the main questions researchers and engineers in resilience assessment try to answer, trying to invent and improve methods, techniques, and tools to answer these questions.

**The process in creating this book.** At the Dagstuhl workshop the participants created an outline table of contents for the book, subdivided into main parts and individual chapters. An open call for contributions was then launched and sent to the resilience community through widespread e-mails. The editors of this book selected the chapters that they considered the best fit with the purpose of this book and invited the authors to submit their proposed paper for peer review. Two rounds of peer review were used to assure the quality of the contributions. The result, we believe, is a set of high-quality papers that cover the most important aspects of resilience assessment and evaluation.

**How to use this book?** The accompanying diagram in Fig. 1 sketches the structure of this book, and should help the student and general reader in making use of this book. The book is divided in seven parts, I–VII.

Each part provides a natural grouping of related topics, such as challenges in Part I and Testing in Part V. Moreover, the parts can be grouped further as given in Fig. 1. The core of the book is a set of 12 chapters on Techniques, as depicted in the box on the upper right-hand side. These have been organized into four blocks, which we will comment on in some more detail.

The techniques are both motivated and demonstrated two times by three chapters on Case Studies for a number of areas highly relevant in modern times. The case studies are grouped together on the left-hand side of Fig 1. For each case study

(mobile, critical infrastructure, and cloud) there is a chapter on resilience assessment challenges in Part I as well as a chapter on assessment results in Part VI.

Each of the chapters is stand-alone, that is, a reader will be able to learn from each individual chapter without having to consult any of the other chapters. As a consequence, the reader can consult chapters in somewhat arbitrary order. This makes the book particularly suitable for seminar series or group reading discussions. With respect to the case studies, it would be natural to read the challenges and results in tandem, although to appreciate how results have been derived, a deeper study of the techniques discussed in the other part is recommended for those wanting to penetrate deeper into the material. The arrows back and forth between Case Studies and Techniques illustrate that chapters from both parts can be read in various orders depending on the specific needs and background of the reader.

The set of techniques and case studies then culminates in the chapter on Future Research, which presents a version of the research roadmap delivered by the AMBER EU coordination action. The material discussed in the research roadmap chapter is immediately accessible to the experienced resilience engineer. However, for a general audience, the diagram shows a directed arrow pointing from Case Studies to the Future Research box. We believe that for more novice readers the discussion on future research is especially useful once the reader has gained some appreciation for the challenges and advances discussed in the chapters on techniques and case studies.

Resilience Assessment and Evaluation of Computing  
Systems

Wolter, K.; Avritzer, A.; Vieira, M.; van Moorsel, A. (Eds.)

2012, XVIII, 490 p., Hardcover

ISBN: 978-3-642-29031-2