Rigorous System Design

Joseph Sifakis

EPFL
Switzerland
Joseph.Sifakis@epfl.ch

now
the essence of knowledge

Boston – Delft
1 Introduction 1
   1.1 About Design 1
   1.2 System Design 4

2 From Programs to Systems —
   Significant Differences 11

3 Achieving Correctness 13
   3.1 Correctness versus Design Productivity 13
   3.2 Trustworthiness Requirements 14
   3.3 Optimization Requirements 15
   3.4 Levels of Criticality 17

4 Existing Approaches and the State of the Art 19
   4.1 System Development Methodologies 19
   4.2 Rigorous Design Techniques 21
   4.3 The Limits of Correctness-by-Checking for Systems 23
   4.4 The Integration Wall — Mixed-Criticality Systems 26

5 Four Principles for Rigorous System Design 31
   5.1 Rigorous System Design 31
   5.2 Separation of Concerns 32
5.3 Component-Based Design 36
5.4 Semantically Coherent Design 40
5.5 Correct-by-Construction Design 44
5.6 Putting Rigorous System Design into Practice in BIP 53

6 A System-Centric Vision for Computing 59
6.1 Linking Computing to Other Disciplines 60
6.2 Rigorous Design versus Controlled Experiments 63
6.3 The Limits of Understanding and Mastering the Cyber-world 64
6.4 The Quest for Mathematically Tractable and Practically Relevant Theory 66

Acknowledgments 69

References 71