Contents

1 Introduction **1**
1.1 What Are Formal Methods? 1
1.2 Formal Methods and Mathematics 2
1.3 What Good Are Formal Methods? 2
1.4 The Myth of Control 4
1.5 Hyperprogramming 5
1.6 Recommendations 6

2 Formal Methods of Software Development: Painted into the Corner of High-Integrity Computing? **11**
2.1 The Dominant Rationale for Formal Methods 12
2.2 Some Pragmatic Objections to Formal Methods 13
2.3 Dissolving Resistance to Formal Methods? 15
2.4 A Brief Sketch of Formal Methods in High-Integrity Computing 16
2.5 The Projects 16
2.6 The Formal Methods Community in High-Integrity Computing 18
2.6.1 The Clients 18
2.6.2 The Developers 18
2.7 The Information Networks 19
2.8 Does the Use of Formal Methods Within High-Integrity Computing Perpetuate its "Myths"? 19

3 The Social Negotiation of Proof: An Analysis and a Further Prediction **23**
3.1 Background 23
3.2 VIPER 24
3.3 Disputing "Proof" 25
3.4 Formal Proof and Rigorous Argument 27
3.5 A Further Prediction 28
3.6 Conclusion 29

4 On Constructing Large Software Systems **32**
4.1 Introduction 32
4.2 People 32
4.3 Frames 33
4.4 Sets 35
4.5 Programs 36
4.6 Proof 38
4.7 Tools 38
4.8 Conclusion 39
4.9 Acknowledgments 40

5 Composition of Descriptions: A Progress Report **41**
5.1 Introduction 41

Bibliografische Informationen
http://d-nb.info/931584388

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

5.2 Why Compose Descriptions ? 41
5.3 What is Described? 43
5.4 What is a Description? 45
5.5 What is Composition? 47
5.6 Description Reuse 48
5.7 Conclusion 48

6 Integrating Methods in Practice 51
6.1 Introduction 51
6.2 Development and Development Methods 52
6.3 Aspects of Specification 54
6.4 Aspects of Design 56
6.4.1 Detail and Structure 56
6.4.2 Reification and Algorithm Design 58
6.4.3 Summary 58
6.5 Implications for Research and Development 59

7 Formal Methods and Product Documentation 60
7.1 Introduction 60
7.2 The Fully Formalised Software Product 60
7.3 The Elements of Product Documentation 60
7.4 Product Documentation and the Product Range 65
7.5 Product Documentation and Product Development 65
7.6 Product Documentation and Customers 66
7.7 Developing from a Fully Formalised Base 67
7.8 New Requirements 67
7.9 Errors Detected Before Release 68
7.10 Errors Detected After Release 68
7.11 How to Get There 68
7.12 Summary 69
7.13 Acknowledgments 69

8 Software Quality: A Modelling and Measurement View 71
8.1 Software Quality Needs 71
8.2 Modelling Software Experiences 72
8.3 Model Evolution 75
8.4 An Organization for Packaging Experience Models for Reuse 78
8.5 Conclusions 79

9 Modelling Working Group Summary 81
9.1 Description 81
9.2 Discussion Topics 81
9.3 Discussion 82
9.3.1 Why and to What End Formal Methods? 83
9.3.2 What is a Formal Method? 83
9.4 How Does Mathematical Modelling Help to Increase our Understanding of Digital Systems? 84

9.4.1 What Are the Limits of Mathematical Modelling? 84
9.5 What is Required to Validate that a Mathematical Model Describes a Digital System Accurately? 85
9.5.1 What Insights do Other Fields of Engineering Provide? 85
9.5.2 What Can we Do by 1995 with the Mathematical Modelling Capabilities we Have Now? 85
9.5.3 What Is our Target for the Year 2000? 86
9.5.4 Formal Methods and Safety Standards 86
9.6 Conclusions 86

10 Quality Assurance Working Group 88
10.1 Group Description 88
10.2 Quality Assurance vs. Quality Control 89
10.3 What Is a Formal Method? 89
10.4 Integration of Formal Methods and Quality Control 90
10.5 A Plan to Integrate Formal Methods into QC/QA 90
10.5.1 Phase 1 90
10.5.2 Phase 2 91
10.5.3 Phase 3 91
10.5.4 Phase 4 91

11 Design Methods Working Group 92
11.1 Description 92
11.2 The Context of Formal Methods 92
11.3 The Role of Proof in Assurance 93
11.4 Analytical Capabilities of Formal Methods 94
11.5 Foundational Capabilities of Formal Methods 95
11.6 The Role of Formal Methods with Respect to the Software Development Process 96
11.7 Formal Methods During Development and Implementation 97
11.8 Education 98
11.9 Tools 98

12 Conclusions 100

A Survey of Formal Methods Tools 101

B Survey of Formal Methods Applications 176

C Acronyms and Trademarks 190

List of Contributors 193