

Contents

Preface	vii
List of Contributors	xxiii
Part I State-Based Approaches	1
1 Z	3
Jonathan P. BOWEN	
1.1 Overview of the Z notation	3
1.1.1 The process of producing a Z specification	4
1.2 Analysis and specification of case 1	5
1.3 Analysis and specification of case 2	13
1.4 Validation of the specification	16
1.5 The natural language description of the specifications	18
1.6 Conclusion	18
2 SAZ	21
Fiona POLACK	
2.1 Overview of the SAZ method	21
2.2 Analysis and specification of case 1	22
2.2.1 Z specification	24
2.3 Analysis and specification of case 2	28
2.4 Natural language description of the specifications	37
2.4.1 Case 1	37
2.4.2 Case 2	37
2.5 Conclusions	38
3 B	41
Hassan DIAB and Marc FRAPPIER	
3.1 Overview of the B notation	41
3.2 Analysis and specification of case 1	42
3.2.1 Identifying operations	42

3.2.2	Defining the state space	44
3.2.3	Defining the behavior of the invoicing operation	46
3.2.4	The Product1 machine	49
3.3	Analysis and specification of case 2	51
3.3.1	Identifying operations	51
3.3.2	The Product2 machine	51
3.3.3	The Invoicing2 machine	52
3.4	Validation of the specification	54
3.5	The natural language description of the specifications	55
3.5.1	Case 1	55
3.5.2	Case 2	55
3.6	Conclusion	56
4	From UML Diagrams to B Specifications	59
	Régine LALEAU and Amel MAMMAR	
4.1	Overview of the method	59
4.1.1	Summary of the B method	59
4.1.2	Data specification	60
4.1.3	Transaction specification	61
4.2	Specification of case 1	64
4.2.1	The class diagram and its B representation	64
4.2.2	Transaction specification	66
4.3	Specification of case 2	69
4.3.1	Transactions specification	69
4.3.2	The formal specification	72
4.4	Validation	76
4.5	The natural-language description of the specifications	77
4.5.1	Case 1	77
4.5.2	Case 2	77
4.6	Conclusion	77
5	UML+Z: Augmenting UML with Z	81
	Nuno AMÁLIO, Fiona POLACK, and Susan STEPNEY	
5.1	Overview of <i>UML + Z</i>	81
5.2	Analysis and specification of case 1	82
5.2.1	UML class model	82
5.2.2	UML state models	83
5.2.3	The Z model	84
5.2.4	Checking model consistency	88
5.2.5	Validating the model	89
5.3	Analysis and specification of case 2	90
5.3.1	Entries of new orders	90
5.3.2	Cancellation of orders	94

5.3.3	Entries of quantities into stock	96
5.4	Natural language description of the specification	101
5.4.1	Case 1	101
5.4.2	Case 2	101
5.5	Conclusion	101
6	ASM	103
	Egon BÖRGER, Angelo GARGANTINI and Elvinia RICCOBENE	
6.1	Overview of the ASM	103
6.2	Requirements capture and specification of case 1	104
6.2.1	Identifying the agents	104
6.2.2	Identifying the states	105
6.2.3	Identifying static and dynamic parts of the states	105
6.2.4	Identifying the transitions	107
6.2.5	Identifying the initial and final states	111
6.2.6	Exceptions handling and robustness	111
6.2.7	Identifying the desired properties (validation/verification)	112
6.3	Requirements capture and specification of case 2	114
6.4	The natural language description of the specification	118
6.4.1	Case 1	118
6.4.2	Case 2	118
6.5	Conclusion	118
7	TLA⁺	121
	Leslie LAMPORT	
7.1	Overview of TLA ⁺	121
7.1.1	TLA	121
7.1.2	TLA ⁺ versus Z	122
7.2	A specification of case 2	124
7.3	The problematic case 1	131
7.4	Validation of the specification	132
7.5	Satisfying the specification	133
7.6	The natural language description	134
7.7	Conclusion	134
	Part II Event-Based Approaches	137
8	Action Systems	139
	Jane SINCLAIR	
8.1	Overview of action systems	139
8.2	Analysis and specification of case 1	140
8.2.1	Modeling the state of the action system	140
8.2.2	Defining the actions	143

8.2.3	An action system for case 1	146
8.3	Analysis and specification of case 2	147
8.3.1	Modeling the state for case 2	147
8.3.2	Defining the actions	147
8.3.3	An action system for case 2	150
8.4	Verification for action systems	151
8.5	The natural language description of the specification	153
8.5.1	Case 1	153
8.5.2	Case 2	153
8.6	Conclusion	153
9	Event B	157
	Dominique CANSELL and Dominique MÉRY	
9.1	Introduction	157
9.2	Analyzing the text of the case study	158
9.3	Event-based modeling	164
9.4	Modeling the first event B model Case 1	167
9.5	Model refinement	170
9.6	Modeling the second event B model Case 2 by refinement of Case 1	171
9.7	The natural language description of the event B models	175
9.8	Conclusion	175
10	VHDL	179
	Laurence PIERRE	
10.1	Overview of VHDL	179
10.2	Analysis and specification of case 1	181
10.2.1	Identifying data structures	181
10.2.2	Identifying operations	182
10.3	Analysis and specification of case 2	186
10.4	The natural language description of the specification	193
10.4.1	Case 1	193
10.4.2	Case 2	194
10.5	Conclusion	194
11	Estelle	197
	Eric LALLET and Jean-Luc RAFFY	
11.1	Overview of the FDT Estelle	197
11.2	Analysis and specification of case 1	198
11.2.1	Defining the architecture of the specification	198
11.2.2	Defining the behavior	200
11.3	Analysis and specification of case 2	204
11.3.1	Defining the new architecture	204
11.3.2	Defining the behavior	205
11.4	Validating the specification	210

11.5	The natural language description of the specifications	210
11.5.1	Case 1	210
11.5.2	Case 2	210
11.6	JEstelle (Estelle with Java)	212
11.7	Conclusion	212
12	SDL	215
	Pascal POIZAT	
12.1	Overview of SDL	215
12.2	Analysis and specification of case 1	216
12.2.1	System structure	216
12.2.2	Process graphs	219
12.2.3	Sort definitions	221
12.2.4	Comments on the first case study	225
12.3	Analysis and specification of case 2	225
12.3.1	System structure	225
12.3.2	Process graphs	227
12.3.3	Sort definitions	228
12.4	The natural language description of the specifications	230
12.4.1	Case 1	230
12.4.2	Case 2	230
12.5	Conclusion	230
13	E-LOTOS	233
	Kenneth J. TURNER and Mihaela SIGHIREANU	
13.1	Overview of the LOTOS notation and method	233
13.1.1	The LOTOS and E-LOTOS languages	233
13.1.2	Requirements capture in LOTOS	234
13.2	Analysis and specification of case 1	236
13.2.1	Analysis	236
13.2.2	Specification	237
13.3	Analysis and specification of case 2	237
13.3.1	Analysis	238
13.3.2	Specification	242
13.4	Validation and verification of the LOTOS specifications	250
13.4.1	Validation	250
13.4.2	Verification	251
13.5	Natural language description of the specifications	255
13.5.1	Case 1	255
13.5.2	Case 2	255
13.6	Conclusion	255
14	EB³	259
	Frédéric GERVAIS, Marc FRAPPIER and Richard ST-DENIS	

14.1	Introduction	259
14.2	Analysis and specification of case 1	260
14.2.1	Entity types and actions	260
14.2.2	Process expressions	262
14.2.3	Input-output rules	262
14.3	Analysis and specification of case 2	263
14.3.1	Entity types, associations and actions	263
14.3.2	Process expressions	266
14.3.3	Input-output rules	268
14.3.4	Attribute definitions	268
14.4	The natural language description of the specification	271
14.4.1	Case 1	271
14.4.2	Case 2	272
14.5	Conclusion	272

Part III Other Formal Approaches 275

15 CASL 277

Hubert BAUMEISTER and Didier BERT

15.1	Overview of the CASL notation	277
15.2	Analysis and specification of case 1	278
15.3	Analysis and specification of case 2	283
15.4	Architectural specification	289
15.5	The natural language description of the specification	290
15.5.1	Case 1	290
15.5.2	Case 2	290
15.6	Conclusion	291

16 Coq 293

Philippe CHAVIN and Jean-François MONIN

16.1	Introduction to Coq	293
16.2	Analysis of the text	294
16.2.1	Stock and orders	294
16.2.2	Operations	295
16.2.3	Requirements on quantities	296
16.3	A specification for case 1	296
16.3.1	Basic types	296
16.3.2	State and operation	298
16.3.3	Operation “invoice”	298
16.4	A specification for case 2	300
16.4.1	Using general operations over sets	300
16.4.2	Reference-dependent measure systems	302
16.5	Experimenting with the specification	304

16.5.1 Refining	304
16.6 Running an example	306
16.7 Rephrasing the text	307
16.8 Conclusion	308
17 Petri Nets	311
Annie CHOQUET-GENIET and Pascal RICHARD	
17.1 Overview of Petri nets	311
17.2 Analysis and specification of case 1	312
17.2.1 One order with a data/action approach	313
17.2.2 One order with a structural approach	316
17.2.3 Several orders	319
17.3 Analysis and specification of case 2	322
17.3.1 Entry flow in stocks	322
17.3.2 Flows of orders	323
17.4 Validation of the specification	324
17.5 The natural language description of the specifications	326
17.5.1 Case 1	326
17.5.2 Case 2	326
17.6 Conclusion	326
18 Petri Nets with Objects	329
Christophe SIBERTIN-BLANC	
18.1 Introduction	329
18.2 A conceptual framework for the representation of systems	330
18.3 Case 1	332
18.4 The system's interface	332
18.5 The components of the system's structure	333
18.6 The Entities	335
18.7 The Operations	338
18.8 The Actors	339
18.9 The Control Structure	340
18.10 Natural language description of the specifications	345
18.11 Comments about our treatment of the case study	346
Part IV Comparison and Glossary	351
19 A Comparison of the Specification Methods	353
Marc FRAPPIER, Henri HABRIAS and Pascal POIZAT	
19.1 Attributes of specification methods	353
19.1.1 Paradigm	353
19.1.2 Formality	356
19.1.3 Graphical representation	357

xxii Software Specification Methods

19.1.4	Object oriented	357
19.1.5	Concurrency	357
19.1.6	Executability	357
19.1.7	Usage of variables	357
19.1.8	Non-determinism	357
19.1.9	Logic	358
19.1.10	Provability	358
19.1.11	Model checking	358
19.1.12	Event inhibition	358
19.2	A qualitative description of the methods	359

20 Glossary **365**

Henri HABRIAS, Pascal POIZAT and Marc FRAPPIER

Index **411**