

Dines Bjørner

SOFTWARE ENGINEERING

Volume 3

**Domains, Requirements, and
Software Design**

Table of Contents

November 21, 2005

Springer

Berlin Heidelberg New York
Hong Kong London
Milan Paris Tokyo

Preface	vii
General	vii
Brief Guide to Volume 3	vii

Part I OPENING

1 The TripTych Paradigm	3
1.1 Delineations of Software Engineering	3
1.1.1 “Old” Delineations	3
Friedrich L. Bauer, 1968	3
Ian Sommerville, 1980–2000	4
IEEE Std. 610.12–1990	4
David Lorge Parnas	4
Shari Lawrence Pfleeger, 2001	5
Carlo Ghezzi, Mehdi Jazayeri and Dino Mandrioli, 2002	5
Accreditation Board for Engineering and Technology (ABET)	5
Hans van Vliet, 2000	6
1.1.2 Our View: What Is Software Engineering?	6
1.2 The Triptych of Software Engineering	7
1.2.1 On Universes of Discourse and Domains	7
1.2.2 Domain Engineering	9
General	9
What Do We Expect From a Domain Description?	10
What a Domain Description Does Not Describe	10
What a Domain Description Does Describe	10
Domain Phenomena and Concepts	10
Further Expectations From Domain Descriptions	21
Domain Descriptions as Bases for Domain Theories	21
More on Domain Engineering	21
1.2.3 Requirements Engineering	22
The Machine	22
The Machine Environment	22
General	23
Different Kinds of Requirements	23
More on Requirements Engineering	23
1.2.4 Software	24
1.2.5 Software Design	24
Software Architecture and Software Architecture Design	24
Component Structure and Component Design	25
Software Architecture versus Component + Module Structure	25
Modules, Components and Systems	25
Systems, Design and Refinement	27
Components and Modules, Design and Refinement	28
Code Design	29
More on Software Design	29
1.2.6 Discussion	29
1.3 Phases, Stages and Steps of Development	30
Three Terms	30
A Principle of Separation of Concerns”	30
Linear, Cyclic and Parallel Development Activities	30
1.3.1 Phases of Software Development	31
1.3.2 Stages and Steps of Development	31
1.3.3 Domain Development	33

	Stages of Domain Development	33
	Steps of Domain Development	36
1.3.4	Requirements Development	36
	Stages of Requirements Development	36
	Steps of Requirements Development	38
1.3.5	Computing Systems Design	38
	Stages and Steps of Hardware Design	38
	Stages of Software Design	39
	Steps of Software Design	39
1.3.6	Discussion: Phases, Stages and Steps	39
	Iterations of Phases, Stages and Steps	39
	Concurrency of Phases, Stages and Steps	40
1.4	The Triptych Process Model — A First View	41
1.4.1	The Concept of a Process Model	41
1.4.2	The Triptych Process Model	42
1.5	Conclusion to Chapter 1	42
1.5.1	Summary	42
1.5.2	What Will Be Covered Later?	43
1.6	Bibliographical Notes	43
1.7	Exercises	43
1.7.1	On a Series of Software Developments	43
1.7.2	Introductory Remarks	49
1.7.3	The Exercises	49
2	Documents	51
2.1	Documentation Is All!	51
2.2	Kinds of Document Parts	52
2.2.1	General	52
2.2.2	What Is a Description?	52
	Information Versus Description Versus Analysis	52
	Descriptions, Prescriptions and Specifications	54
2.3	Deliverables	54
2.4	Informative Document Parts	55
2.4.1	Name, Place and Date	55
2.4.2	Partners	55
	Clients	56
	Developers	56
2.4.3	Current Situation, Needs, Ideas and Concepts	57
	Current Situation	58
	Needs	58
	Ideas	58
	Concepts and Facilities	59
2.4.4	Scope, Span and Synopsis	60
	Scope	60
	Span	60
	Synopsis	61
2.4.5	Assumptions and Dependencies	62
2.4.6	Implicit/Derivative Goals	63
2.4.7	Standards	63
	Development Standards	63
	Documentation Standards	64
	Standards Versus Recommendations	64
	Specific Standards	64
2.4.8	Contracts and Design Briefs	66

	Contracts	66
	Design Briefs	66
2.4.9	Logbook	67
2.4.10	Discussion of Informative Documentation	67
	General	67
	Methodological Consequences: Principle, Techniques and Tools	68
2.5	Descriptive Document Parts	68
	Generalities	69
	Specifics	69
	Informal and Formal Document Parts	70
2.5.1	Rough Sketches	71
	Pragmatics, Semantics and Syntax of Rough Sketches	71
	Discussion	71
	Methodological Consequences: Principles, Techniques and Tools	72
2.5.2	Terminologies	73
	General	73
	Pragmatics, Semantics and Syntax of Terminologies	73
	Terminologisation — Continued	74
	On Formal Terminologies cum Ontologies	74
	Methodological Consequences: Principles, Techniques and Tools	75
2.5.3	Narratives	76
	Pragmatics, Semantics and Syntax of Narratives	76
	Discussion	78
	Methodological Consequences: Principles, Techniques and Tools	78
2.5.4	Formal Descriptions	79
	Pragmatics, Semantics and Syntax of Formalisations	79
	On Formalisation	79
	Methodological Consequences: Principles, Techniques and Tools	81
2.5.5	Discussion of Descriptive Documentation	82
2.6	Analytic Document Parts	82
	Pragmatics, Semantics and Syntax	82
	Categories of Analytical Document Parts	83
2.6.1	Concept Formation	83
	Pragmatics, Semantics and Syntax	84
2.6.2	Validation	84
2.6.3	Verification, Model Checking, Testing	84
2.6.4	Theory Formation	85
2.6.5	Discussion of Analytic Documentation	85
	General	85
	Methodological Consequences: Principles, Techniques and Tools	85
2.7	Discussion	86
2.7.1	General	86
2.7.2	Summary of Chapter	86
	Methodological Consequences: Principles, Techniques and Tools	87
2.8	Exercises	88
2.8.1	A Preamble	88
2.8.2	The Exercises	88

3	Methods and Methodology	93
3.1	Method	93
3.2	Methodology	94
3.3	Method Constituents	95
3.3.1	Principle	95
3.3.2	Analysis	95
3.3.3	Construction (or Synthesis)	96
3.3.4	Techniques	96
3.3.5	Tools	96
3.4	Development Principles, Techniques and Tools	97
3.4.1	Some Metaprinciples	97
3.4.2	Some Principles, Techniques and Tools	98
	Type Principle, Techniques and Tools	98
	Function Principle, Techniques and Tools	98
	Relation Principle, Techniques and Tools	99
	Algebra Principle, Techniques and Tools	100
	Logic Principle, Techniques and Tools	101
3.5	Discussion	101
3.6	Exercises	102
4	Models and Modelling	103
4.1	Introductory, Context-setting Remarks	103
4.1.1	Models Versus “Possible Worlds”	103
4.1.2	On Models of a Specification	104
4.1.3	Modelling	104
4.1.4	Universes of Discourse	105
4.2	Model Attributes	105
4.2.1	Analogic, Analytic and Iconic Models	105
	Principles and Techniques	106
	Discussion	108
4.2.2	Descriptive and Prescriptive Models	109
	Examples	109
	Principles and Techniques	110
	Discussion	111
4.2.3	Extensional and Intensional Models	111
	Principles and Techniques	112
	Discussion	113
4.3	Roles of Models	113
4.4	The Modelling Principle	114
4.5	Discussion	114
4.6	Exercises	115

Part III DESCRIPTIONS: THEORY AND PRACTICE

5	Phenomena and Concepts	119
5.1	Introduction	119
5.2	Phenomena and Concepts	119
5.2.1	Physically Manifest Phenomena	120
5.2.2	Mentally Conceived Concepts	120
5.2.3	Categories of Phenomena and Concepts	120
5.2.4	Concrete and Abstract Concepts	121
5.2.5	Categories of Descriptions	121
5.2.6	What Is a Description?	122

5.3	Entities	123
5.3.1	Atomic Entities	123
5.3.2	Composite Entities	124
5.3.3	Subentities	124
5.3.4	Values, Mereology and Attributes	124
5.3.5	Entity Mereology	125
5.3.6	Mereologies and Attributes	126
5.3.7	Model-Oriented Mereologies	126
5.3.8	Model-Oriented Attributes — An Aside	126
	Atomic Types and Values	126
	Other Attributes	126
5.3.9	Entity Properties	126
	General	127
	“Thing” Properties	127
5.3.10	Real Examples and Our Type System	127
	Set Compounds	127
	Cartesian Compounds	129
	List Compounds	131
	Map Compounds	132
5.3.11	A Type System	133
5.3.12	Type Constraints	134
5.3.13	Summary: Principles, Techniques and Tools	135
5.4	Functions	136
5.4.1	Function Signatures	137
5.4.2	Function Definition	138
5.4.3	Algorithms	140
5.5	Events and Behaviours	142
5.5.1	States, Actions, Events and Behaviours	142
5.5.2	Synchronisation and Communication	143
5.5.3	Processes	145
5.5.4	Traces	146
5.5.5	Process Definition Languages	146
5.6	Choice On Modelling Phenomena and Concepts	147
5.6.1	Qualitative Characteristics	147
5.6.2	Quantitative Characteristics	147
	Information-Intensive Universe of Discourse	148
	Function-Intensive Universe of Discourse	148
	Event Intensive Universe of Discourse	148
	Process Intensive Universe of Discourse	149
5.6.3	Principles, Techniques and Tools	149
5.7	Discussion	151
5.7.1	Entities, Functions, Events and Behaviours	151
5.7.2	Intensity and Problem Frames	151
5.8	Bibliographical Notes	152
5.9	Exercises	152
5.9.1	A Preamble	152
5.9.2	The Exercises	152
6	On Defining and On Definitions	153
6.1	A Pragmatics of Definitions	155
6.1.1	Phenomena, Artifacts and Concepts	155
6.1.2	What Are Definitions?	156
6.1.3	The Nature of Concepts being Defined	156
6.1.4	Mathematical Definitions	157

6.1.5	Physical World Definitions	157
6.1.6	Formal Definitions	158
6.2	Varieties of Philosophy Definitions	158
6.2.1	Six Varietal Characterisations of Art	159
6.2.2	Discussion	160
6.2.3	A Possible Objection	161
6.3	Preliminary Discussion	161
6.4	A Syntax of Formal Definitions	161
6.4.1	Recognition and Reproduction	163
6.4.2	Uniqueness and Identification	164
6.4.3	Ontological Terms	165
6.5	A Semantics of Formal Definitions	165
6.6	Discussion	166
6.6.1	General	166
6.6.2	Principles, Techniques and Tools	166
6.7	Exercises	167
7	Jackson's Description Principles	171
7.1	Phenomena, Facts and Individuals	171
7.2	Designations	172
7.2.1	Some Observations	173
7.2.2	Formalisation	175
7.2.3	Observer Functions and Identification	176
7.2.4	Mathematical and Computing Entities	177
	Mathematical Entities	177
	Computing Entities	178
	Awareness	178
	Some Guidelines	178
	A "Large" Example	179
	Formal Modelling	181
7.2.5	Discussion: Designations	181
7.3	Explicit Definitions	182
7.3.1	Definitions: "The Narrow Bridge"	182
7.3.2	Definition of Abstract, Intangible Concepts	183
7.3.3	How Much, How Little to Define?	184
7.3.4	Discussion: Definitions	184
7.4	Refutable Assertions	185
7.4.1	Designation and Definition Assertions	185
7.4.2	Analysis	186
7.4.3	"Dangling" Assertions	186
7.4.4	Discussion: Refutable Assertions	187
7.5	Discussion: Description Principles	188
7.6	Bibliographical Notes	188
7.7	Exercises	188
7.7.1	A Preamble	188
7.7.2	The Exercises	188

8	Overview of Domain Engineering	191
8.1	Introduction	191
8.2	A Review of <i>Why Domain Engineering?</i>	192
8.3	Overview of Part and Chapter	192
8.4	Domain Stakeholders and Their Perspectives	193
8.5	Domain Acquisition and Validation	194
8.6	Domain Analysis and Concept Formation	194
8.7	Domain Facets	194
8.8	Auxiliary Stages of Domain Development	195
8.9	The Domain Model Document	195
	8.9.1 A Preview of Things to Come	195
	8.9.2 Contents of a Domain Model Document	196
8.10	Further Structure of This Part	196
8.11	Bibliographical Notes	197
8.12	Exercises	197
9	Domain Stakeholders	199
9.1	Introduction	199
9.2	Stakeholders	199
	9.2.1 General Application Stakeholders	200
	9.2.2 Software Development Stakeholders	200
	Turn-Key Software Development Stakeholders	201
	Commercial Off-the-Shelf SW Development Stakeholders	201
	9.2.3 Purpose of Listing Stakeholders	201
9.3	Stakeholder Perspectives	201
	9.3.1 Perspectives of General Applications	202
	9.3.2 Perspectives of Software Development	206
9.4	Discussion: Stakeholders and Their Perspectives	206
	9.4.1 General	206
	9.4.2 Principles, Techniques and Tools	206
9.5	Exercises	207
	9.5.1 Preamble	207
	9.5.2 Assignments	207
	9.5.3 Postlude	208
10	Domain Attributes	209
10.1	Introduction	209
10.2	Continuity, Discreteness and Chaos	210
	10.2.1 Time	210
	10.2.2 Continuity	210
	10.2.3 Discreteness	212
	On a Notion of State	213
	Methodological Consequences	213
	Hybridicity	214
	Methodological Consequences	218
	10.2.4 Chaos	218
	Methodological Consequences	219
	10.2.5 Discussion	220
10.3	Statics and Dynamics	220
	10.3.1 Static Phenomena and Concepts	221
	Static Attributes	221
	10.3.2 Dynamic Phenomena and Concepts	223
	Inert Phenomena and Concepts	224
	Active Dynamic Attribute	226

	Reactive Dynamics Attribute	237
	Discussion	239
10.4	Tangibility and Intangibility	239
	10.4.1 Humanly Tangible Phenomena.....	239
	10.4.2 Otherwise Physically Tangible Phenomena	242
	10.4.3 Intangible Phenomena	243
	10.4.4 Discussion	243
10.5	One, Two, ..., Dimensionality	244
	10.5.1 Zero Dimensionality	245
	10.5.2 One Dimensionality	245
	10.5.3 Multidimensionality	246
	10.5.4 Discussion	247
10.6	Discussion	247
10.7	Bibliographical Notes	247
10.8	Exercises	248
	10.8.1 A Preamble	248
	10.8.2 The Exercises	248
11	Domain Facets	249
11.1	Introduction	249
	11.1.1 Separation of Concerns	251
	11.1.2 Discussion of the Separation Principle	251
	11.1.3 Structure of Chapter	251
11.2	Domain Facilitators: Business Processes	251
	11.2.1 Business Processes	252
	11.2.2 Overall Principles	255
	11.2.3 Informal and Formal Examples	256
	11.2.4 Discussion	260
	11.2.5 Summary	261
	11.2.6 Reminder	261
11.3	Domain Intrinsic	262
	11.3.1 Overall Principles	262
	11.3.2 Conceptual Versus Actual Intrinsic	266
	11.3.3 Methodological Consequences.....	268
	11.3.4 Discussion	268
	11.3.5 Utter Barebone Intrinsic	268
	11.3.6 Reminder	269
11.4	Domain Support Technologies.....	269
	11.4.1 Overall Principles	269
	11.4.2 Methodological Consequences.....	272
	11.4.3 Discussion	273
	11.4.4 Reminder	273
11.5	Domain Management and Organisation	274
	11.5.1 Overall Principles	274
	11.5.2 A Conceptual Analysis, I	276
	11.5.3 Methodological Consequences, I+II.....	276
	11.5.4 Conceptual Analysis, II	276
	11.5.5 Methodological Consequences, III	278
	11.5.6 Discussion	279
	11.5.7 Reminder	279
11.6	Domain Rules and Regulations.....	280
	11.6.1 Overall Principles	280
	11.6.2 Methodological Consequences.....	281
	11.6.3 Rules and Regulation Languages	283

11.6.4	Principles and Techniques	284
11.6.5	Reminder	284
11.7	Domain Scripts	285
11.7.1	The Description of Scripts	285
	Routine Headers	296
	Example Statements	297
	Example Expressions	297
	Abstract Syntax for Syntactic Types	298
	Semantic Types Abstract Syntax	299
	Semantic Functions	300
11.7.2	Methodological Consequences	305
11.7.3	Reminder + More	305
11.8	Domain Human Behaviour	306
11.8.1	Overall Principles	306
11.8.2	Methodological Consequences	310
11.8.3	Human Behaviour and Knowledge Engineering	312
11.8.4	Discussion	312
11.8.5	Reminder	313
11.9	Other Domain Facets?	313
11.10	Composition of Models	313
11.10.1	Collating Facet Descriptions	314
	General	314
	A Comprehensive Narrative	314
	From Big Lies via Smaller Lies to the Truth	314
11.10.2	Technical Issues	315
11.11	Exercises	315
11.11.1	A Preamble	315
11.11.2	The Exercises	315
12	Domain Acquisition	317
12.1	Introduction	317
12.1.1	Domain Facts	318
12.1.2	Elicitation of Domain Facts	318
12.1.3	Recording Domain Facts	318
12.1.4	Indexing Domain Description Sketches	319
12.2	The Acquisition Process	320
12.2.1	Stakeholder Liaison	321
12.2.2	Elicitation Studies	321
12.2.3	Elicitation Interviews	323
12.2.4	Elicitation Questionnaires	323
	General Guidelines: Questionnaire Structure and Contents	323
	Special Guidelines: Questionnaire Structure and Contents	324
12.2.5	Elicitation Reports	326
12.3	Discussion	326
12.3.1	Concept and Process Review	326
12.3.2	Process Iteration	327
12.3.3	Delineation: Acquisition and Analysis	327
12.3.4	Principles, Techniques and Tools	327
12.4	Exercises	328
12.4.1	A Preamble	328
12.4.2	The Exercises	328

13	Domain Analysis and Concept Formation	329
13.1	Introduction	329
13.2	Concept Formation	329
13.2.1	Simply Abstracted Concepts	330
13.2.2	Breakthrough Abstracted Concepts	331
13.3	Consistencies, Conflicts and Completeness	332
13.3.1	Inconsistencies	333
13.3.2	Conflicts	333
13.3.3	Incompleteness	333
13.3.4	Looseness and Nondeterminism	334
13.4	From Analysis to Synthesis	334
13.5	Discussion	335
13.5.1	General	335
13.5.2	Principles, Techniques and Tools	335
13.6	Bibliographical Notes	336
13.7	Exercises	336
13.7.1	A Preamble	336
13.7.2	The Exercises	337
14	Domain Verification and Validation	339
14.1	Introduction	339
14.2	Domain Verification	340
14.2.1	Informal Reasoning	341
14.2.2	Testing	341
14.2.3	Formal Proofs	341
14.2.4	Model Checking	342
14.3	Domain Validation	342
14.3.1	The Domain Validation Documents	342
14.3.2	The Domain Validation Process	343
14.3.3	Domain Development Iterations	343
14.4	Discussion	344
14.4.1	General	344
14.4.2	Principles, Techniques and Tools	344
14.5	Exercises	344
14.5.1	A Preamble	344
14.5.2	The Exercises	345
15	Towards Domain Theories	347
15.1	Introduction	347
15.2	What Is a Domain Theory?	348
15.3	Example Statements of Domain Theories	348
15.4	Possible Domain Theories	350
15.5	How Do We Establish a Theory?	351
15.6	Purpose of a Domain Theory	352
15.7	Summary Principles, Techniques and Tools	352
15.8	Bibliographical Notes	352
15.9	Exercises	353
15.9.1	A Preamble	353
15.9.2	The Exercises	353

16	The Domain Engineering Process Model	355
16.1	Introduction	355
16.2	Review of Domain Development	355
16.3	Review of Domain Documents	357
16.4	Discussion	358

Part V REQUIREMENTS ENGINEERING

17	Overview of Requirements Engineering	361
17.1	Introduction	364
17.1.1	Further Characterisation of ‘Requirement’	365
17.1.2	The “Machine”	365
17.2	Why Requirements, and for What?	366
17.2.1	Why Requirements?	366
17.2.2	Requirements for What?	366
17.2.3	What Does ‘Implements’ Mean?	366
17.3	Getting Started on Requirements Development	367
17.3.1	Initial Informative Documentation	367
17.3.2	Requirements Eureka	368
	Initial Eureka of Requirements	369
	Ongoing Eureka of Requirements	369
	A Systematic Source of Requirements Eureka	369
	Placement of Initial Requirements Eureka	370
17.3.3	Pragmatic Prescriptive Documentation	370
17.3.4	Planning Requirements Development	371
17.4	On Domains, Requirements and the Machine	371
17.5	Overview: Requirements Engineering Stages	373
17.6	The Requirements Document	374
17.6.1	A Preview of Things to Come	374
17.6.2	Contents of a Requirements Document	374
17.6.3	Comments on Requirements Documents	375
17.7	The Structure of the Rest of the Part	375
17.8	Bibliographical Notes	375
17.9	Exercises	375
17.9.1	A Preamble	375
17.9.2	The Exercises	376
18	Requirements Stakeholders	377
18.1	Introduction	377
18.2	General Application Stakeholders	378
18.3	COTS Software House Stakeholders	378
18.3.1	General	378
18.3.2	“Corporate Knowledge”	379
18.3.3	Classes of Domain-Specific Requirements	379
18.3.4	Generic COTS Software Stakeholder Perspective	379
18.4	Discussion	379
18.4.1	General	379
18.4.2	Principles, Techniques and Tools	380
18.5	Exercises	380
18.5.1	Preamble	380
18.5.2	The Exercises	380

19	Requirements Facets	383
19.1	Introduction	384
19.2	Rough Sketching and Terminology	384
19.2.1	Initial Requirements Modelling	384
19.2.2	Rough-Sketch Requirements	385
	Entities	385
	Functions	387
	Events	388
	Behaviours	388
19.2.3	Requirements Terminology	392
19.2.4	Systematic Narration	397
19.3	Business Process Reengineering Requirements	398
19.3.1	Michael Hammer's Ideas on BPR	398
19.3.2	What Are <i>BPR Requirements</i> ?	399
19.3.3	Overview of BPR Operations	400
19.3.4	BPR and the Requirements Document	400
	Requirements for New Business Processes	400
	Place in Narrative Document	400
	Place in Formalisation Document	401
19.3.5	Intrinsics Review and Replacement	401
19.3.6	Support Technology Review and Replacement	401
19.3.7	Management and Organisation Reengineering	402
19.3.8	Rules and Regulation Reengineering	403
19.3.9	Human Behaviour Reengineering	403
19.3.10	Script Reengineering	404
19.3.11	Discussion: Business Process Reengineering	404
	Who Should Do the Business Process Reengineering?	404
	General	405
19.4	Domain Requirements	405
19.4.1	Domain-to-Requirements Operations	405
19.4.2	Domain Reqs. and the Reqs. Document	406
	Requirements for Functionalities	406
	Place in Narrative Document	406
	Place in Formalisation Document	407
19.4.3	A Domain Example	407
19.4.4	Domain Projection	408
19.4.5	Domain Determination	409
19.4.6	Domain Instantiation	413
19.4.7	Domain Extension	414
19.4.8	Domain Requirements Fitting	415
19.4.9	Discussion: Domain Requirements	417
19.5	Interface Requirements	417
19.5.1	Shared Phenomena and Concept Identification	418
19.5.2	Interface Requirements Facets	418
19.5.3	Interface Reqs. and the Reqs. Document	419
	Requirements for "Input/Output"	419
	Place in Narrative Document	419
	Place in Formalisation Document	420
19.5.4	Shared Data Initialisation	420
19.5.5	Shared Data Refreshment	421
19.5.6	Computational Interface Requirements	422
19.5.7	Man-Machine Dialogue	423
19.5.8	Man-Machine Physiological Interface	423
19.5.9	Machine-Machine Dialogue	431

19.5.10	Discussion: Interface Requirements	432
	Dialogue Prescription Techniques and Tools	432
	General	432
	Special Principles and Techniques	432
19.6	Machine Requirements	433
19.6.1	Machine Requirements Facets	434
19.6.2	Machine Reqs. and the Reqs. Document	434
	Requirements for “The Machine Only”	434
	Place in Narrative and Formalisation Document	434
19.6.3	Performance Requirements	435
19.6.4	Dependability Requirements	437
	Accessibility	439
	Availability	439
	Integrity	440
	Reliability	440
	Safety	440
	Security	440
	Robustness	441
19.6.5	Maintenance Requirements	442
	Adaptive Maintenance	442
	Corrective Maintenance	442
	Perfective Maintenance	443
	Preventive Maintenance	443
	Extensional Maintenance	443
19.6.6	Platform Requirements	444
	Development Platform	444
	Execution Platform	444
	Maintenance Platform	444
	Demonstration Platform	445
	Discussion	445
19.6.7	Documentation Requirements	445
19.6.8	Discussion: Machine Requirements	445
19.7	Full Requirements Facets Document	446
19.8	Discussion: Requirements Facets	446
19.8.1	General	446
19.8.2	Principles, Techniques and Tools	446
19.9	Bibliographical Notes	447
19.10	Exercises	447
19.10.1	A Preamble	447
19.10.2	The Exercises	447
20	Requirements Acquisition	451
20.1	Requirements Acquisition Versus Domain Models	451
20.2	Domain Model-Based Requirements Acquisition	452
20.2.1	Domain Requirements Acquisition, A Preview	452
	Assumptions	452
	Domain Requirements Acquisition, Basic Steps	452
20.2.2	Remaining Requirements Acquisition, A Preview	453
	Assumptions	453
	Machine Requirements Acquisition, Basic Steps	453
	Interface Requirements Acquisition, Basic Steps	453
20.2.3	Further Issues	454
20.3	Overview of Concepts	454
20.3.1	Requirements	455

20.3.2	Elicitation of Requirements	455
20.3.3	Recording Requirements	455
	Requirements Index	455
	Requirements Type	455
	Requirements Units	456
20.3.4	Indexing Requirements Prescription Sketches	457
20.4	The Acquisition Process	457
20.4.1	Stakeholder Liaison	458
20.4.2	Elicitation Studies	459
20.4.3	Elicitation Interviews	459
20.4.4	Elicitation Questionnaires	460
	General Guidelines: Questionnaire Structure and Contents	460
	Special Guidelines: Questionnaire Structure and Contents	461
20.4.5	Elicitation Reports	463
20.5	Discussion	464
20.5.1	Concept and Process Review	464
20.5.2	Process Iteration	464
20.5.3	Delineation: Acquisition and Analysis	464
20.5.4	Principles, Techniques and Tools	464
20.6	Exercises	465
20.6.1	A Preamble	465
20.6.2	The Exercises	465
21	Requirements Analysis and Concept Formation	467
21.1	Introduction	467
21.2	Concept Formation	469
21.3	Consistencies, Conflicts, and Completeness	469
21.3.1	Inconsistencies	469
21.3.2	Conflicts	470
21.3.3	Incompleteness	470
21.3.4	Looseness and Nondeterminism	471
21.4	From Analysis to Synthesis	471
21.5	Discussion	471
21.5.1	General	471
21.5.2	Principles, Techniques and Tools	472
21.6	Bibliographical Notes	472
21.7	Exercises	473
21.7.1	A Preamble	473
21.7.2	The Exercises	473
22	Requirements Verification and Validation	475
22.1	Introduction	475
22.2	Requirements Verification	476
22.2.1	Informal Reasoning	477
22.2.2	Testing	477
22.2.3	Formal Proofs	478
22.2.4	Model Checking	478
22.3	Requirements Validation	478
22.3.1	The Requirements Validation Documents	479
22.3.2	The Requirements Validation Process	479
22.3.3	Requirements Development Iterations	479
22.4	Discussion	480
22.4.1	General	480
22.4.2	Principles, Techniques and Tools	480

22.5	Bibliographical Notes	481
22.6	Exercises	481
22.6.1	Preamble	481
22.6.2	The Exercises	481
23	Requirements Satisfiability and Feasibility	483
23.1	Introduction	483
23.2	Satisfaction Study	484
23.2.1	Correct (Validated) Requirements Document	484
23.2.2	Unambiguous Requirements Document	484
23.2.3	Complete Requirements Document	484
23.2.4	Consistent Requirements Document	484
23.2.5	Stable Requirements Document	484
23.2.6	Verifiable Requirements Document	485
23.2.7	Modifiable Requirements Document	485
23.2.8	Traceable Requirements Document	485
23.2.9	Faithful Requirements Document	485
23.2.10	Discussion of Satisfiability	486
23.3	Technical Feasibility Study	486
23.3.1	Feasibility of Business Process Reengineering	486
23.3.2	Feasibility of Hardware	486
23.3.3	Feasibility of Software	486
23.3.4	Discussion of Technical Feasibility	487
23.4	Economic Feasibility Study	487
23.4.1	Feasible Development Costs	487
23.4.2	Feasible Write-off Costs	487
23.4.3	Gains Outweigh Costs?	487
23.4.4	Discussion of Economic Feasibility	488
23.5	Compliance with Implicit/Derivative Goals	488
23.5.1	Review of Implicit/Derivative Goals	488
23.5.2	Discussion of Implicit/Derivative Goals	488
23.6	Discussion	488
23.6.1	General	488
23.6.2	Principles, Techniques and Tools	489
23.7	Exercises	490
23.7.1	A Preamble	490
23.7.2	The Exercises	490
24	The Requirements Engineering Process Model	493
24.1	Introduction	493
24.2	Review of Requirements Development	493
24.3	Review of Requirements Documents	494
24.4	The Repeat Table of Contents Listing	494
24.5	Discussion	495

Part VI COMPUTING SYSTEMS DESIGN

25	Hardware/Software Codesign	499
25.1	Introduction — On Architecture	499
25.2	Hardware Components and Modules	500
25.3	Software Components and Modules	500
25.4	Hardware/Software Codesign	500
25.5	Stepwise Refinement of Architectures	501

25.6	Discussion	501
25.7	Principles, Techniques and Tools	501
26	Software Architecture Design	503
26.1	Introduction	503
26.2	Initial Domain Requirements Architecture	504
26.3	Initial Machine Requirements Architecture	506
26.4	Analysis of Some Machine Requirements	508
26.4.1	Performance	508
26.4.2	Availability	508
26.4.3	Accessibility	509
26.4.4	Adaptive Maintainability	509
26.5	Prioritisation of Design Decisions	509
26.6	Corresponding Designs	509
26.6.1	Design Decision wrt. Performance	510
26.6.2	Design Decision wrt. Availability	511
26.6.3	Design Decision wrt. Accessibility	512
26.6.4	Design Decision wrt. Adaptability	514
26.7	Discussion	515
26.7.1	General	515
26.7.2	Principles and Techniques	516
26.8	Bibliographical Notes	517
26.9	Exercises	517
26.9.1	A Preamble	517
26.9.2	The Exercises	517
27	A Case Study in Component Design	519
27.1	Overview Introduction	519
27.1.1	System Complexity	519
27.1.2	Proposed Remedies	520
27.1.3	Stepwise Development	520
27.1.4	Stagewise Iteration	521
27.2	Overview of Example	521
27.3	Methodology Overview	522
27.3.1	Principles	522
27.3.2	Techniques	523
27.4	Step 0: Files and Pages	524
27.4.1	A “Snapshot”	524
27.4.2	An Abstract Formal Model	524
27.4.3	Abstract Versus Concrete Basic Actions	525
27.4.4	Concrete Actions	527
27.5	Step 1: Catalogue, Disk and Storage	527
27.5.1	Catalogue Directories	527
	Data Structure	528
	Invariant	529
27.5.2	Abstraction	530
27.5.3	Actions	531
	Action Signatures	531
	Create and Erase File Actions	532
	Put Page Action	532
	Get and Delete Page Actions	533
27.5.4	Adequacy and Sufficiency	533
	Adequacy	534
	Sufficiency	534

	27.5.5	Correctness	534
		Comparable Results	534
		The Correctness Statement	535
27.6	Step 2:	Disks	536
	27.6.1	Data Refinement	536
	27.6.2	Disk Type	536
		A “Snapshot”	536
	27.6.3	FS0, FS1 and FS2 Types	536
		Concrete Semantic Types	536
	27.6.4	Disk Type Invariant	537
	27.6.5	Disk Type Abstraction	538
	27.6.6	Adequacy, Sufficiency, Operations and Correctness	538
27.7	Step 3:	Caches	538
	27.7.1	Technology Considerations	538
	27.7.2	Cached Directory and Page Access	539
	27.7.3	Invariance	540
	27.7.4	Abstraction	541
	27.7.5	Actions	541
		Open and Close Actions	541
		Create and Put Actions	542
		Erase, Get, and Delete Actions	542
	27.7.6	Adequacy, Sufficiency and Correctness	543
27.8	Step 4:	Storage Crashes	543
	27.8.1	Storage and Disk	543
	27.8.2	Concrete Semantic Types	544
	27.8.3	Invariance	544
	27.8.4	Consistent Storages and Disks	544
		Consistent Storage	544
		Consistent Disk	545
	27.8.5	Abstractions	546
	27.8.6	Garbage Collection	546
	27.8.7	New Actions	547
		Check and Crash Actions	547
	27.8.8	Some Previous Commands	547
		Open and Close Actions	547
		Put Action	548
27.9	Step 5:	Flattening Storage and Disks	548
	27.9.1	“Flat” Storage and Disk	548
	27.9.2	“The Rest”	549
27.10	Step 6:	Disk Space Management	549
	27.10.1	The Issue	549
	27.10.2	“The Rest”	550
27.11	Discussion		551
	27.11.1	General	551
	27.11.2	Principles and Techniques	551
27.12	Bibliographical Notes		552
27.13	Exercises		552
	27.13.1	A Preamble	552
	27.13.2	The Exercises	552

28	Domain-Specific Architectures	555
28.1	Introduction	555
28.1.1	General	555
28.1.2	Some Definitions	556
28.1.3	On Architectures	556
28.1.4	Problem Frames	557
28.1.5	Chapter Structure	558
28.2	Translator Architectures	558
28.2.1	Translator Domain	559
28.2.2	Translator Requirements	560
28.2.3	Translator Design	560
	Translator Functions	561
	A Multipass Compiler	561
28.2.4	Process Graph for Translator Development	562
28.3	Information Repository Architectures	568
28.3.1	Information Repository Domain	569
28.3.2	Information Repository Requirements	570
28.3.3	Information Repository Design	571
	The Role of A Database Management System	571
	A Relational Database Management System Architecture	572
	Other Database Management System Architectures and Discussion	582
28.4	Client/Server Architectures	582
28.4.1	Client/Server Domain/Requirements Models	582
	Single-Client, Single-Server Domain/Requirements Architecture	583
	Multiple-Client, Multiple-Server Domain/Requirements Model	584
28.4.2	Some Meta-RSL/CSP Constructs	585
	Motivation and Justification	586
	Three Process Interaction Macros	586
	'Meaning' of the Three Process Interaction Macros	586
	Pragmatics of Macros	587
28.4.3	Single-Client, Single-Server Model	587
28.4.4	Multiple-Client, Single-Server Model	591
28.4.5	Client/Server Event Manager Model	592
28.4.6	Discussion	600
28.5	Workpiece Architectures	600
28.5.1	Workpiece Domain	601
28.5.2	Workpiece Requirements	601
28.5.3	Workpiece Systems Design	604
28.6	Reactive System Architectures	604
28.6.1	Reactive Systems Domain	604
28.6.2	Reactive Systems Control Requirements	606
28.6.3	Reactive Systems Control Design	607
28.6.4	Discussion of Reactive Systems Design	608
28.7	Connection Frame	608
28.7.1	Connection Domain	609
28.7.2	Connection Requirements	610
28.7.3	Connection Systems Design	612
28.8	Discussion	612
28.8.1	General	612
28.8.2	Principles, Techniques and Tools	612
28.9	Exercises	613
28.9.1	A Preamble	613
28.9.2	The Exercises	613

29	Etcetera: Coding and All That!	617
29.1	From Formal Specification to Programming	617
29.1.1	From Specifications to Programs	618
29.1.2	From Abstract Types to Data Structures	618
29.1.3	From Applicative to Imperative Programs	618
29.1.4	Translations into Concurrent Programs	619
29.1.5	From RSL to SML, Java, C# and Other Languages	619
29.2	The Beauty of Programming	619
	Art, Discipline, Craft, Science, Logic and Practice	619
29.3	Programming Practices	620
29.3.1	Structured Programming	620
29.3.2	Extreme Programming	620
29.3.3	Object-Oriented cum UML Programming	621
29.3.4	Chief Programmer Programming	621
29.4	Confidence-Building Software Development	622
29.4.1	When to Verify, Model Check and Test	622
	The \vee Diagram	623
	Order of Tests	623
	Discovery of Errors, Misinterpretations and Misunderstandings	623
	Cost of Corrective Maintenance	624
	Impossibility of Certain Corrective Maintenance	624
29.4.2	Demo \rightarrow Skeleton \rightarrow Prototype \rightarrow System	624
29.5	Verification, Model Checking and Testing	627
29.5.1	Verification	628
29.5.2	Model Checking	630
29.5.3	Testing	630
	Test Objectives	631
	Test Strategy	631
	Test Coverage	631
	Test Cases and Test Suites	632
	Test Adequacy Criteria — Test Requirements	632
	Classical Testing Approaches	632
	Formal Specification-Based Testing Approaches	633
29.5.4	Discussion	633
29.6	Discussion	633
29.7	Exercises	634
29.7.1	A Preamble	634
29.7.2	The Exercises	634
30	The Computing Systems Design Process Model	635
30.1	Introduction	635
30.2	Review of Software Design	635
30.2.1	A Process Model	636
30.2.2	Discussion	637
30.3	Review of Software Design Documents	638
30.4	Discussion	640

Part VII CLOSING

31	The TripTych Development Process Model	643
31.1	Phase Process Models	643
31.2	Phase Documentation Table of Contents	647
31.3	Conclusion	649

32	Finale	651
32.1	Informal and Formal Software Engineering	651
32.1.1	Informal Software Engineering	652
32.1.2	Formal Software Engineering	652
32.1.3	Conclusion	652
32.2	Myths and Commandments of Formal Methods	652
32.2.1	First Seven Myths	653
32.2.2	Seven More Myths	654
32.2.3	Ten Formal Methods Commandments	655
32.3	FAQ: Frequently Asked Questions	657
32.3.1	General	657
32.3.2	Domains	658
32.3.3	Requirements	660
32.4	Research and Tool Development	660
32.4.1	Evolving Principles, Techniques and Tools	660
32.4.2	Grand Challenges	661
	Three Dimensions of Grand Challenges	661
	Integration of Formal Techniques	661
	Trustworthy Evolutionary Systems Development	661
	Domain Theories	662
	On the Nature of “Grand Challenges”	662
32.5	Application Areas	663
32.5.1	Additional Areas	663
32.5.2	The Examples	664
32.6	Closing Remarks	665

Part VIII APPENDIXES

A	An RSL Primer	669
A.1	Types	669
A.1.1	Type Expressions	669
A.1.2	Type Definitions	671
	Concrete Types:	671
	Subtypes	671
	Sorts (Abstract Types)	672
A.2	The RSL Predicate Calculus	672
A.2.1	Propositional Expressions	672
A.2.2	Simple Predicate Expressions	672
A.2.3	Quantified Expressions	673
A.3	Concrete RSL Types	673
A.3.1	Set Enumerations	673
A.3.2	Cartesian Enumerations	674
A.3.3	List Enumerations	674
A.3.4	Map Enumerations	675
A.3.5	Set Operations	675
A.3.6	Cartesian Operations	677
A.3.7	List Operations	678
A.3.8	Map Operations	679
A.4	λ -Calculus and Functions	681
A.4.1	The λ -Calculus Syntax	681
A.4.2	Free and Bound Variables	682
A.4.3	Substitution	682
A.4.4	α -Renaming and β -Reduction	682

A.4.5	Function Signatures	683
A.4.6	Function Definitions	683
A.5	Further Applicative Expressions	684
A.5.1	Let Expressions	684
A.5.2	Conditionals	685
A.5.3	Operator/Operand Expressions	686
A.6	Imperative Constructs	686
A.6.1	Variables and Assignment	686
A.6.2	Statement Sequences and skip	686
A.6.3	Imperative Conditionals	687
A.6.4	Iterative Conditionals	687
A.6.5	Iterative Sequencing	687
A.7	Process Constructs	687
A.7.1	Process Channels	687
A.7.2	Process Composition	688
A.7.3	Input/Output Events	688
A.7.4	Process Definitions	688
A.8	Simple RSL Specifications	689
B	Indexes	691
B.1	Concepts Index	692
B.2	Characterisations and Definitions Index	709
B.3	Authors Index	713
	References	717