

Contents

0	Introduction	1
0.1	Key topics of open distributed systems design	1
0.2	The role of standards.....	2
0.3	The need for formal descriptions.....	4
0.4	Distributed systems from the point of view of DAI.....	6
1	Formal methods in the system design process.....	9
1.1	A model for the system design process	9
1.2	Requirements for formal description techniques.....	10
1.2.1	Expressiveness	10
1.2.2	Abstraction	12
1.2.3	Formality.....	13
1.2.4	Explicitness and implicitness	13
1.2.5	Compositionality	14
1.3	Synthesis and analysis activities.....	15
2	Requirement specification of open distributed systems	17
2.1	Basic architectural concepts	17
2.2	System architectures	19
2.3	Refinement and abstraction	20
2.4	The Basic Reference Model of Open Systems Interconnection.....	24
2.5	Basic concepts of formal description techniques	28
2.6	Some remarks	30
3	The design of a temporal logic for open distributed systems.....	31
3.1	Some requirements on expressiveness.....	32
3.2	A survey of temporal logics	35
3.2.1	Traditional temporal logic.....	36
3.2.2	Extensions of traditional temporal logic.....	37
3.2.3	Past time temporal logic	40
3.2.4	Branching time temporal logic.....	41
3.2.5	Interval logic	43
3.2.6	Incorporation of events	45
3.2.7	The impact of validity.....	46

3.3	A modular temporal logic for open distributed systems.....	48
3.3.1	Semantical models.....	49
3.3.2	Atomic formulas and non-temporal operators	53
3.3.3	Operators to refer to the future.....	57
3.3.4	Operators to refer to the past.....	60
3.3.5	Operators for event occurrence	61
3.3.6	Operators for interval construction	63
3.3.7	Customizing temporal logics.....	66
3.3.8	Composition of behavioural specifications.....	69
3.3.9	A notion of conformance	73
4	The interaction point concept.....	77
4.1	The role of interaction points	77
4.2	A list of possible interaction point properties	79
4.3	Formal specification of interaction point properties.....	81
4.3.1	Context and limitations.....	81
4.3.2	Customizing an appropriate temporal logic	82
4.3.3	General properties	84
4.3.4	Mode of interaction	87
4.3.5	Inspection.....	89
4.3.6	Summary	90
4.4	Formal reasoning about interaction points.....	91
4.5	Interaction point representations in operational FDTs	95
4.5.1	Interaction points in Estelle	96
4.5.2	Interaction points in LOTOS.....	99
4.5.3	Interaction points in SDL.....	102
4.5.4	Summary	105
4.6	Conformance between abstraction levels via the interaction point concept	106
4.6.1	Problems with an environment-independent notion of conformance.....	107
4.6.2	Compatibility between interaction points.....	109
4.6.3	Environment-independent conformance based on interaction point compatibility.....	111
4.6.4	Application to OSI.....	113
5	Communication services.....	115
5.1	The service concept.....	115
5.2	Design methodology	117
5.3	Example "modified InRes service"	119
5.3.1	Informal description	120
5.3.2	Customizing an appropriate temporal logic.....	124

5.3.3	Specification of the service	126
5.3.4	Specification of the service provider	131
5.3.5	Interaction point semantics	135
5.3.6	Constraints on the service users	136
5.3.7	Verification of the service provider	138
5.4	Conclusion	140
6	An epistemic logic for open distributed systems	143
6.1	The role of knowledge	143
6.2	Notions of knowledge	144
6.2.1	Possible-worlds semantics	144
6.2.2	Situated-Automata Knowledge	146
6.2.3	View-based knowledge interpretation	148
6.2.4	Group knowledge	150
6.2.5	Awareness	153
6.3	A modular epistemic logic for open distributed systems	156
6.3.1	Semantical models	156
6.3.2	Operators for implicit individual knowledge	158
6.3.3	Operators for explicit individual knowledge	160
6.3.4	Operators for individual awareness	161
6.3.5	Operators for implicit group knowledge	162
6.3.6	Operators for group awareness	164
6.3.7	Operators for explicit group knowledge	166
6.3.8	Customizing temporal epistemic logics	168
6.3.9	Some remarks on conformance	169
7	Applying temporal epistemic logics to open distributed systems	173
7.1	Example "mutual exclusion"	173
7.1.1	Implicit knowledge	173
7.1.2	Knowledge-oriented specification	175
7.1.3	Explicit knowledge	176
7.2	Example "drink server"	178
7.2.1	Specification based on propositional logic	178
7.2.2	Refinement	181
7.2.3	Verification of the drink server refinement	184
7.2.4	Specification based on first-order logic	185
7.2.5	Refinement	188
7.2.6	Verification of the drink server refinement	191
7.2.7	Non-local epistemic properties	192
8	Conclusion	197

References 201

Appendix 209

 A.1 Theorems and valid formulas 209

 A.2 Ordering properties for the service provider 217

 A.3 Abbreviations 219

 A.4 Notation 221

Index 225