
Contents

Part I Background

1	Introduction	3
1.1	CoFI	3
1.2	CASL	7
2	Underlying Concepts	11
2.1	Basic Specifications	11
2.2	Structured Specifications	15
2.3	Architectural Specifications	19
2.4	Libraries of Specifications	20

Part II CASL Specifications

3	Getting Started	23
3.1	Loose Specifications	24
3.2	Generated Specifications	33
3.3	Free Specifications	36
4	Partial Functions	47
4.1	Declaring Partial Functions	47
4.2	Specifying Domains of Definition	50
4.3	Partial Selectors and Constructors	54
4.4	Existential Equality	55
5	Subsorting	57
5.1	Subsort Declarations and Definitions	57
5.2	Subsorts and Overloading	61
5.3	Subsorts and Partiality	62

6	Structuring Specifications	67
6.1	Union and Extension	67
6.2	Renaming	69
6.3	Hiding	71
6.4	Local Specifications	73
6.5	Named Specifications	75
7	Generic Specifications	77
7.1	Parameters and Instantiation	78
7.2	Compound Symbols	85
7.3	Generic Specifications with Imports	88
7.4	Views	90
8	Specifying the Architecture of Implementations	93
8.1	Architectural Specifications	95
8.2	Generic Components	100
8.3	Writing Meaningful Architectural Specifications	106
9	Libraries	111
9.1	Local Libraries	112
9.2	Distributed Libraries	116
9.3	Version Control	120

Part III Carrying On

10	Foundations	125
11	Tools	131
11.1	The Heterogeneous Tool Set (HETS)	132
11.2	HOL-CASL	138
11.3	ASF+SDF Parser and Syntax-Directed Editor	139
11.4	Other Tools	140
12	Basic Libraries	143
12.1	Library BASIC/NUMBERS	144
12.2	Library BASIC/STRUCTURED DATATYPES	147
13	Case Study: The Steam-Boiler Control System	155
13.1	Introduction	156
13.2	Getting Started	157
13.3	Carrying On	161
13.4	Specifying the Mode of Operation	163
13.5	Specifying the Detection of Equipment Failures	167
13.6	Predicting the Behavior of the Steam-Boiler	176
13.7	Specifying the Messages to Send	182

13.8 The Steam-Boiler Control System Specification 183
 13.9 Validation of the CASL Requirements Specification 184
 13.10 Designing the Architecture 186

Appendices

A CASL Quick Reference 193
 A.1 Basic Specifications 194
 A.2 Structured Specifications 199
 A.3 Architectural Specifications 200
 A.4 Libraries 201

B Points to Bear in Mind 203
 B.1 Introduction 203
 B.2 Underlying Concepts 203
 B.3 Getting Started 204
 B.4 Partial Functions 205
 B.5 Subsorting 206
 B.6 Structuring Specifications 206
 B.7 Generic Specifications 207
 B.8 Specifying the Architecture of Implementations 207
 B.9 Libraries 208
 B.10 Foundations 209
 B.11 Tools 209
 B.12 Basic Libraries 210

C The Steam-Boiler Control Specification Problem 211
 C.1 Introduction 211
 C.2 Physical Environment 212
 C.3 The Overall Operation of the Program 214
 C.4 Operation Modes of the Program 214
 C.5 Messages Sent by the Program 216
 C.6 Messages Received by the Program 217
 C.7 Detection of Equipment Failures 219

References 221

List of Named Specifications 225

Index of Library and Specification Names 231

Concept Index 235