
Contents

PART I The Context

- 1 Introduction..... 3
- 2 Current Practices..... 9
- 3 Axiomatic Justification and Uncertainty 13
- 4 Justification and Dependability Case..... 17
 - 4.1 Cost Minimization and the Proportionality Principle 18
 - 4.2 Risk-based Assessment 19
 - 4.3 Two Illustrative Case Studies: A Process Instrumentation (SIP) and a
Radioactive Materials Handling System 19

PART II Prescriptions

- 5 Requirements, Claims and Evidence..... 23
 - 5.1 Where to Start? The First Foundation of Dependability Justification 23
 - 5.2 The Initial Dependability Requirements (CLM0)..... 24
 - 5.2.1 PIE’s, Constraints, Safe States 25
 - 5.2.2 Elicitation 26
 - 5.2.3 Completeness 27
 - 5.3 The Other Foundation: The System Input-Output
Preliminary Requirements..... 28
 - 5.4 Primary Claims 29
 - 5.5 Differences Between Dependability Requirements and Claims 30
 - 5.6 Evidence and Model Assumptions. 32

5.7 How to Organize Evidence? A Four-level Structure	33
5.8 How Are the Four Levels Related? Levels of Causality	36
5.9 Examples	39
6 Arguments, Syntax and Semantics	41
6.1 Claim Assertions	41
6.2 White, Grey and Black Claims	42
6.3 The Inductive Justification Process	43
6.4 The Conjunctive Property	46
6.5 The Syntax of an Argument	49
6.5.1 Delegations and Expansions	49
6.5.2 Claim Justifications	50
6.5.3 Argument Unicity and Termination	51
6.6 Claim and Argument Semantic Aspects	52
6.6.1 Delegation and Expansion as Tools for Refinement of Evidence and Argument Incremental Construction	52
6.6.2 Universal and Existential Claim Assertions	54
6.6.3 Claim Refutation	56
6.6.4 Absence of Level-1 Grey Primary Claims	56
6.6.5 Adjacent Delegation Sub-claims	56
7 Axiomatic Principles and Limits	59
7.1 Claim Justifiability	59
7.2 Evidence Plausibility and Weight	61
7.3 The Ineluctability of Consensus	62
7.4 Epistemic Versus Stochastic Uncertainty	64
7.5 Claims on Product Versus Evidence from Process	67
7.6 Logics of Prevention, Precaution and Enlightened Catastrophism	68
7.7 Concluding Remarks on Claims, Arguments, Evidence	69

PART III Descriptions

8 Structures and Interpretations	73
8.1 The Roles of Models in Dependability Assessment	74
8.2 Basic Model Notions	75
8.2.1 Model Structures and Relations	76
8.2.2 Predicates	78
8.2.3 Languages and Proofs	79

8.3 On Descriptions and Interpretations	79
8.4 Mathematical Structures	81
8.5 System Structures	82
8.6 L-Interpretations	84
8.7 The Formal Definition of a Model.....	85
8.8 Validation and Satisfiability Obligations.....	86
8.8.1 Language Expansion/Reduction	86
8.8.2 Substructures and Extensions	87
8.8.3 L_1 - <i>Interpretation</i> (Environment-System Interface)	90
8.8.4 L_i - <i>Interpretations</i> ($i = 2, 3, 4$)	96
8.9 Interdependencies Between Structures of Different Levels.....	100
8.9.1 Properties of Justification Structures	100
8.9.2 Properties of Expansion Structures	104
8.9.3 Internal Compound Structure and Interfaces of a Level- i , $i = 1..4$	107
8.10 Interdependencies Between Languages of Different Levels.....	107
8.11 The Tree of Sub-structures Dependencies	110
8.12 A General Multi-level Justification Framework	111
8.13 Design Abstractions.....	112
8.14 Recommendations for Design and Validation Models	113
9 Embedded Computer System Structures	117
9.1 States, Events and Other Basic Notions.....	118
9.2 Notation	120
9.3 Level-0. Environment Requirements, Events and Constraints.....	121
9.3.1 CLM0 Dependability Requirements	121
9.3.2 CLM0 Postulated Initiating Events and Safe Failure Modes	122
9.3.3 CLM0 Environment Constraints	122
9.3.4 Level-0 Dependability Case Documentation	122
9.4 Level-1. System-Environment Interface	123
9.4.1 Selection of the Entities and Relations of the Interface	123
9.4.2 Environment States	124
9.4.3 Constraints (NAT)	125
9.4.4 A Note on Environment Assumptions	126
9.4.5 Postulated Initiating Events (Relation HAZ ¹)	126
9.4.6 System Input-Output Preliminary Specifications	127
9.4.7 The System and the Functional Relation (REQ)	128
9.4.8 The Need for a Unique <i>Interpretation</i> for Requirements and System Specifications	128
9.4.9 Expansion of the CLM0 Requirements into Primary Claims	129

9.4.10 Primary Validity Claim-Justification Substructures.....	130
9.4.11 Implementation Primary Claims – Justification Structures.....	137
9.4.12 Primary Dependability Claims – Justification Substructures	139
9.4.13 Level-1 CLM0 Expansion Structure	144
9.4.14 Level-1 Evidence and Delegation Claims	147
9.4.15 Level-1 Argument	149
9.4.16 Level -1 Documentation.....	150
9.5 Level-2. Computer System Architecture	151
9.5.1 Elements of the Architecture.....	152
9.5.2 Input and Output Variables	152
9.5.3 Channel k Data Acquisition (Relations IN_k)	153
9.5.4 Channel Assignment Relation (IN)	154
9.5.5 Channel k Output Device (Relations OUT_k)	154
9.5.6 Voting Relations (OUT).....	155
9.5.7 Channel k Requirements (REQ_k)	155
9.5.8 Level-2 Undesired Events (HAZ^2)	156
9.5.9 Level-2 Expansion of Level-1 Delegation Claims	158
9.5.10 Expansion of REQ Acceptable Implementation Delegation Claim[1,2]	158
9.5.11 Expansion of REQ Fail-Safe Implementation Delegation Claim[1,2]	164
9.5.12 Expansion of Functional Diversity Delegation Claim[1,2]	169
9.5.13 Expansion of Reliability and Safety Delegation Claims[1,2].....	175
9.5.14 Level-2 Expansions	182
9.5.15 Level-2 Evidence and Delegation Claims	183
9.5.16 A Digression on Testing.....	184
9.5.17 Level-2 Argument	184
9.5.18 Level -2 Documentation.....	185
9.6 Level-3. Design	187
9.6.1 Complexity and Elements of the Design	187
9.6.2 The Design Relations (SOF_k).....	187
9.6.3 Design Level Undesired Events	189
9.6.4 Level-3 Expansion of Level-2 Delegation Claims	191
9.6.5 Expansion of Channel Acceptable Implementation Delegation Claim[2,3]	191
9.6.6 Expansion of Channel Fail-Safe Implementation Claim[2,3]	196
9.6.7 Expansion of Channel Independency Delegation Claim[2,3]	199
9.6.8 Expansion of Reliability and Safety Delegation Claims[2,3].....	206
9.6.9 Level-3 Expansions	210
9.6.10 Level-3 Evidence and Delegation Claims	211
9.6.11 Level-3 Argument	214
9.6.12 Level-3 Documentation.....	215
9.7 Structure of the Operation Control	216
9.7.1 Elements of the Operation Control Structure	218
9.7.2 Operation Control Relations $READ_k$ and $ORDER_k$	219

9.7.3 Control of Operation. Undesired Events (HAZ ⁴)	219
9.7.4 Level-4 Expansion of Level-3 Delegation Claims	220
9.7.5 Expansion of Accuracy Delegation Claim[2,4]	220
9.7.6 Expansion of Channel Fail-safe Control Delegation Claim[3,4]	224
9.7.7 Expansion of Channel Reliability and Safety Delegation Claims[2,4]	229
9.7.8 Level-4 Expansion	234
9.7.9 Level-4 Evidence	236
9.7.10 Level-4 Argument	236
9.7.11 Level-4 Dependability Case Documentation	237
9.8 Guidance Provided by the System Substructure Tree	238
9.9 Concluding Remarks: Model Inter-relations and Preservation Properties	239

PART IV Methodological Implications

10 Pre-existing Systems and Components	245
10.1 Pre-existing Components	246
10.2 Composability and Re-use of Arguments	246
10.2.1 Syntactical Conditions	247
10.2.2 Semantic Conditions	247
10.3 Guaranteed Services and Rely Conditions	248
10.4 The System-Component Interface Substructures	250
10.4.1 The GRANT and RELY Relations	250
10.4.2 The HAZ ⁵ Relation	251
10.4.3 Proof Obligations for the Developer of S	252
10.4.4 The $U_s(\delta\xi_s)$ Expansion Structures	254
10.4.5 Proof Obligations for the Embedding System	255
10.4.6 System-Component Interface Revisited	262
10.5 Documentation	263
10.6 Concluding Remarks and Justification Issues	265
10.6.1 Completeness of S Specifications	265
10.6.2 Robustness of S Operation	267
10.7 Criticality Degrees and Integrity Levels	268
11 Construction Methods	269
11.1 Dependability Case Construction Rules	269
11.1.1 Initial Dependability Requirements Address Product, Not Process Quality Assurance	269

11.1.2 A Unique Interpretation Model for the Specification of Initial Dependability Requirements and for the Validation of Preliminary Specifications	270
11.1.3 Expansions	270
11.1.4 Claims First	271
11.1.5 Expansion and Justification Interpretation Structures	271
11.1.6 Ordering for Claim Elicitation and Justification	272
11.1.7 Primary Claims	273
11.1.8 Level-1 Expansion.....	273
11.1.9 Assumptions Are Not Evidence	274
11.1.10 Evidence Must Be Explicitly Claimed	274
11.1.11 Claim Identification and Documentation	275
11.1.12 Fixed Levels of Expansion and Evidence	275
11.1.13 Strict Conjunctions	276
11.1.14 Delegation to the Adjacent Lower Evidence Level	276
11.1.15 Re-use of Arguments	276
11.1.16 Pre-existing Components	278
11.2 FFP (Functions/Failures/Properties) Method.....	278
12 Postface.....	283
A The SIP System.....	287
A.1 Description.....	287
A.2 Plant, Technology and Safety Replacement Constraints.....	289
A.3 Dependability Requirements (CLM0) and Primary Claims.....	290
A.4 Primary Claims on Software CCF's.....	291
A.5 Software Architecture and Design. Claims and Evidence.....	292
A.5.1 Operating System	292
A.5.2 Library Modules.....	292
A.5.3 Application Software.....	293
B Automated Material Handling System	295
B.1 Description	295
B.2 Dependability Requirements (CLM0).....	296
B.3 Constraints and Postulated Initiating Events.....	298
B.4 Preliminary Specifications and Primary Claims.....	298
References	309
Index	317

<http://www.springer.com/978-1-84800-371-2>

Justifying the Dependability of Computer-based Systems
With Applications in Nuclear Engineering

Courtois, P.-J.

2008, XVIII, 323 p. 24 illus., Hardcover

ISBN: 978-1-84800-371-2