Contents

LIST OF FIGURES AND TABLE xi

ACKNOWLEDGEMENTS. xvii

FOREWORD xxi
Dominique LUZEAUX

INTRODUCTION. GOALS OF PROPERTY MODEL METHODOLOGY. xxv

PART 1. FUNDAMENTALS 1

Chapter 1. General Systems Theory 3

1.1. Introduction. 3
1.2. What is a system?. 4
1.3. Systems, subsystems and levels 9
1.4. Concrete and abstract objects 11
1.5. Properties 12
1.5.1. Material and formal properties 12
1.5.2. Accidental and essential properties, laws and types. 13
1.5.3. Dispositions, structural and behavioral properties 17
1.5.4. Resulting and emerging properties 18
1.6. States, event, process, behavior and fact. 20
1.7. Systems of interest 23

CHAPTER 2. TECHNOLOGICAL SYSTEMS 25

2.1. Introduction. 25
2.2. Definition of technological systems 25
2.2.1. Artificial autotelic and heterotelic systems 27
2.2.2. Technical-empirical and technological systems 27
2.2.3. Purpose of a technological system. 28
2.3. Function, behavior and structure of a technological system 30
2.4. Intended and concomitant effects of a technological system 34
2.5. Modes, mode switching and states 36
2.5.1. Modes of operation. 36
2.5.2. Mode switching 36
2.5.3. Operating states 37
2.6. Errors, faults and failures 37
2.7. "The human factor". 39

CHAPTER 3. KNOWLEDGE SYSTEMS 41

3.1. Introduction. 41
3.2. Knowledge and its bearers 42
3.3. Intersubjective knowledge 44
3.4. Concepts, propositions and conceptual knowledge. 45
3.5. Objective and true knowledge 47
3.6. Scientific and technological knowledge 50
3.6.1. Fundamental sciences 51
3.6.2. Applied sciences and technology. 53
3.6.3. Operative technological rules. 53
3.6.4. Substantive technological rules 55
3.7. Knowledge and belief 56

CHAPTER 4. SEMIOTIC SYSTEMS AND MODELS 59

4.1. Introduction. 59
4.2. Signs and systems of signs 60
4.3. Nomological propositions and law statements 65
4.4. Models, object models, theoretical models and simulation. 66

4.5. Representativeness of models and the expressiveness of languages 71
4.5.1. Representativeness of models 71
4.5.2. Expressiveness of a language 73

PART 2. METHODS 77

CHAPTER 5. ENGINEERING PROCESSES 79

5.1. Introduction 79
5.2. Systems engineering process 81
5.2.1. General framework 81
5.2.2. Design process 83
5.2.3. Safety assessment process 88
5.2.4. Requirement and assumption validation 90
5.2.5. Verification of the implementation regarding requirements 91
5.2.6. Managing configurations 92
5.2.7. Process (quality) assurance, certification and coordination with authorities 93

CHAPTER 6. DETERMINING REQUIREMENTS AND SPECIFICATION MODELS 95

6.1. Introduction 95
6.2. Specifications and requirements 98
6.3. Text-based requirements and subjectivity 100
6.4. Objectifying requirements and assumptions through property-based requirements 102
6.4.1. Definition 102
6.4.2. Examples 104
6.4.3. Typology and sources of PBR 106
6.5. Conjunction and comparison of property-based requirements 110
6.5.1. Comparison of two PBRs 111
6.5.2. Conjunction of two PBRs 112
6.6. Interpreting text-based requirements 114
6.6.1. Example 1: FAR29.1303(b) flight and navigation instruments 115
6.6.2. Example 2: FAR29.951(a) Fuel systems – General 119

6.7. Conclusion: specification models and concurrent assertions 121

CHAPTER 7. DESIGNING SOLUTIONS AND DESIGN MODELS 127

7.1. Introduction. 127
7.2. Deriving requirements. 128
7.3. Basic system model of a type of systems 131
7.4. Dynamic design models of a type of systems 133
7.4.1. Behavioral design model (BDM) 133
7.4.2. Equation-based design models (EDMs) 139
7.5. Derivation and allocation of the system's behavioral requirements 141
7.6. Static design models 142
7.6.1. Composite system model. 142
7.6.2. Structural design model 145
7.6.3. Allocation of BDM components to SDM components 146
7.7. Derivation and allocation of system requirements. 146
7.8. The end of the design process and the realization 148

CHAPTER 8. VALIDATING REQUIREMENTS AND ASSUMPTIONS 151

8.1. Introduction. 151
8.2. The validation process according to the ARP4754A 152
8.2.1. Goal of the validation 152
8.2.2. Means of validation 154
8.3. The validation process according to the property model methodology. 156
8.3.1. Goal of the validation 157
8.3.2. Means of validation 158
8.3.3. Exactness of a system specification model 160
8.3.4. Validating the derivation of system requirements 161
8.3.5. Scenarios and validation cases, efforts and rigor in validation. 162
8.4. Conclusion. 167

CHAPTER 9. VERIFYING THE IMPLEMENTATION STEP BY STEP 169

9.1. Introduction. 169
9.2. The verification process according to the ARP4754A . . . 170
9.2.1. Goal of the verification 170
9.2.2. Verification methods 170
9.3. The verification process according to the property model methodology 173
9.3.1. Objects to be verified 173
9.3.2. Goal of the verification 174
9.3.3. Verifying the design 175
9.3.4. Verifying the other products of implementation 179
9.3.5. The contract theorem 181
9.4. Conclusion. 181

CHAPTER 10. SAFETY ENGINEERING 183

10.1. Introduction. 183
10.2. The safety assessment process according to the ARP4754A 184
10.2.1. Goal of safety assessment process 184
10.2.2. Means to assess safety 185
10.3. The safety assessment process according to the property model methodology (PMM) 191
10.3.1. Errors, faults and failures 191
10.3.2. FHA and interpretation of the 1309(b)(2)(i) requirements as PBRs 193
10.3.3. PASA/PSSA and deriving safety requirements 200
10.3.4. Simulation and validation of the derived safety requirements 204
10.3.5. Simulation and verification of the failure prevention mechanisms. 206
10.3.6. Reliability design models. 207
10.3.7. Safety theorem: validating additional requirements 208
10.4. Conclusion. 211

CHAPTER 11. PROPERTY MODEL METHODOLOGY DEVELOPMENT PROCESS 213

11.1. Introduction 213
11.2. Early phase of a system development, preliminary studies 213
11.3. Steps of the industrial development of a type of systems 215
11.4. Initial step: highest level system specification 216
11.4.1. Initial step general approach 217
11.4.2. Establishing a specification model of the type of systems 218
11.5. Design steps: descending and iterative design of the building blocks down to the lowest level blocks 226
11.5.1. Design step of a non-terminal block 227
11.5.2. Behavioral design step of a terminal block 229
11.5.3. End of the design step 231
11.6. Realization step of the lowest level building blocks 231
11.7. Integration and installation steps 232
11.8. Conclusion 233

APPENDIX 235

BIBLIOGRAPHY 253

INDEX 261