
Contents

Preface ix

Introduction xi

Part I	Cleanroom Software Engineering Fundamentals	1
1	Cleanroom Overview	3
1.1	Economic Production of High-Quality Software	3
1.2	Cleanroom Foundations	4
1.3	Cleanroom Technologies	8
1.4	The Cleanroom Process	13
1.5	Relationship of Cleanroom to Other Practices	15
1.6	Cleanroom Project Experience	18
1.7	References	18
1.8	Suggested Reading	19
2	Cleanroom Management by Incremental Development	21
2.1	Benefits of Incremental Development	22
2.2	Theoretical Foundations of Incremental Development	25
2.3	Increment Planning in Practice	28
2.4	Incremental Development in Practice	30
2.5	References	32

3	Cleanroom Software Specification	33
3.1	Box Structures for Cleanroom Specification and Design	34
3.2	The Sequence-Based Specification Process	43
3.3	Example: Specification of a Security Alarm	46
3.4	References	59
4	Cleanroom Software Development	61
4.1	Box Structure Development	61
4.2	Clear Box Development	63
4.3	Clear Box Verification	72
4.4	Example: The Security Alarm Clear Box	81
4.5	References	90
5	Cleanroom Software Certification	91
5.1	Benefits of Statistical Testing Based on a Usage Model	91
5.2	Theoretical Foundations of Statistical Testing	93
5.3	Statistical Usage Testing in Practice	95
5.4	Example: Security Alarm	99
5.5	References	108

Part II	The Cleanroom Software Engineering Reference Model	111
----------------	---	------------

6	The Cleanroom Reference Model	113
6.1	An Introduction to the CRM	113
6.2	Cleanroom Process Definition Format	125
6.3	Common Cleanroom Process Elements	126
6.4	References	129
7	Cleanroom Management Processes	131
7.1	Project Planning Process	131
7.2	Project Management Process	136
7.3	Performance Improvement Process	139
7.4	Engineering Change Process	142
8	Cleanroom Specification Processes	145
8.1	Requirements Analysis Process	145
8.2	Function Specification Process	149
8.3	Usage Specification Process	154
8.4	Architecture Specification Process	160
8.5	Increment Planning Process	163
8.6	References	167

9	Cleanroom Development Processes	169
9.1	Software Reengineering Process	169
9.2	Increment Design Process	173
9.3	Correctness Verification Process	178
9.4	References	182
10	Cleanroom Certification Processes	183
10.1	Usage Modeling and Test Planning Process	183
10.2	Statistical Testing and Certification Process	191
10.3	References	197
11	Cleanroom and the Capability Maturity Model for Software	199
11.1	The CMM for Software	199
11.2	Cleanroom Process Mappings to CMM KPAs	202
11.3	Integrating CRM Technology and CMM Management	206
11.4	References	207

Part III	A Case Study in Cleanroom Software Engineering	209
-----------------	---	------------

12	Satellite Control System Requirements	211
12.1	The Satellite Control System Case Study	211
12.2	Satellite Operations Software Requirements	212
12.3	Reference	219
13	Satellite Control System Black Box Specification	221
13.1	Black Box Sequence-Based Specification	221
13.2	Step 1: Define the System Boundary	224
13.3	Step 2: Enumerate Stimulus Sequences	229
13.4	Step 3: Analyze Canonical Sequences	256
13.5	Step 4: Define Specification Functions	257
13.6	Step 5: Construct the Black Box Tables	260
13.7	Removing Abstractions	269
13.8	Common Sequence Abstraction Techniques	272
14	Satellite Control System State Box Specification	277
14.1	State Box Specification	277
14.2	Step 1: Invent the State Data	278
14.3	Step 2: Construct the State Box Tables	283

15	Satellite Control System Clear Box Design	293
15.1	Clear Box Implementation	293
15.2	Step 1: Select a High-Level Software Architecture	294
15.3	Step 2: Select an Implementation for Stimulus Gathering	312
15.4	Step 3: Select an Implementation for Response Generation	313
15.5	Step 4: Select an Implementation for the State Data Items	316
15.6	Step 5: Select an Implementation for Each Entry in the State Box Table	317
15.7	Step 6: Reorganize the Implementations into Executable Code	338
16	Satellite Control System Testing and Certification	349
16.1	Statistical Testing	349
16.2	Step 1: Define Certification Plan	350
16.3	Step 2: Build Model Structure	352
16.4	Step 3: Determine State Transition Probabilities	377
16.5	Step 4: Validate the Usage Model	378
16.6	Step 5: Generate Test Cases, and Execute and Evaluate Results	380