

Jonathan P. Bowen and Michael G. Hinchey

High-Integrity System Specification and Design



Springer

Table of Contents

Acknowledgements	xv
List of Reprints	xvii
1. Specification and Design	1
1.1 An Analogy	1
1.2 The Development Life-Cycle	3
1.3 The Transformational Approach	6
1.4 Silver Bullets	8
<i>No Silver Bullet: Essence and Accidents of Software Engineering</i> (Brooks) ..	11
<i>Biting the Silver Bullet: Toward a Brighter Future for System Development</i> (Harel)	29
2. Structured Methods	53
2.1 Structured Notations	53
2.2 The Jackson Approach	54
<i>Methodology: The Experts Speak</i> (Orr, Gane, Yourdon, Chen & Constantine)	57
<i>An Overview of JSD</i> (Cameron)	77
3. Formal Methods	127
3.1 What are Formal Methods?	128
3.2 Formal Specification Languages	128
3.3 Deductive Apparatus	129
3.4 Myths of Formal Methods	130
3.5 Which Formal Method?	131
<i>Seven Myths of Formal Methods</i> (Hall)	135
<i>Seven More Myths of Formal Methods</i> (Bowen & Hinchey)	153
<i>A Specifier's Introduction to Formal Methods</i> (Wing)	167
<i>An Overview of Some Formal Methods for Program Design</i> (Hoare)	201
<i>Ten Commandments of Formal Methods</i> (Bowen & Hinchey)	217

4. Object-Orientation	231
4.1 The Object Paradigm	231
4.2 Modularization	232
4.3 Information Hiding	232
4.4 Classes	233
4.5 Genericity and Polymorphism	233
4.6 Object-Oriented Design	234
<i>Object-Oriented Development (Booch)</i>	237
<i>Object-Oriented and Conventional Analysis and Design Methodologies: Comparison and Critique (Fichman & Kemerer)</i>	261
5. Concurrent and Distributed Systems	295
5.1 Concurrent Systems	296
5.2 Distributed Systems	297
5.3 Models of Computation	297
5.4 Naming Considerations	298
5.5 Inter-Process Communication	298
5.6 Consistency Issues	299
5.7 Heterogeneity and Transparency	300
5.8 Security and Protection	300
5.9 Language Support	301
5.10 Distributed Operating Systems	301
<i>Communicating Sequential Processes (Hoare)</i>	303
<i>A Simple Approach to Specifying Concurrent Systems (Lamport)</i>	331
6. Real-Time and Safety-Critical Systems	359
6.1 Real-Time Systems	359
6.2 Safety-Critical Systems	360
6.3 Formal Methods for Safety-Critical Systems	361
6.4 Standards	362
6.5 Legislation	363
6.6 Education and Professional Issues	363
6.7 Technology Transfer	365
<i>Formal Methods for the Specification and Design of Real-Time Safety- Critical Systems (Ostroff)</i>	367
<i>Experience with Formal Methods in Critical Systems (Gerhart, Craigen & Ralston)</i>	413
<i>Regulatory Case Studies (Gerhart, Craigen & Ralston)</i>	429
<i>Medical Devices: The Therac-25 Story (Leveson)</i>	447
<i>Safety-Critical Systems, Formal Methods and Standards (Bowen & Stavri- dou)</i>	485

7. Integrating Methods	529
7.1 Motivation	529
7.2 Integrating Structured and Formal Methods	530
7.3 An Appraisal of Approaches	532
<i>Integrated Structured Analysis and Formal Specification Techniques (Semmens, France & Docker)</i>	533
8. Implementation	557
8.1 Refinement	557
8.2 Rapid Prototyping and Simulation	559
8.3 Executable Specifications	560
8.4 Animating Formal Specifications	560
<i>Specifications are not (Necessarily) Executable (Hayes & Jones)</i>	563
<i>Specifications are (Preferably) Executable (Fuchs)</i>	583
9. CASE	609
9.1 What is CASE?	609
9.2 CASE Workbenches	610
9.3 Beyond CASE	610
9.4 The Future of CASE	611
<i>CASE: Reliability Engineering for Information Systems (Chikofsky & Rubenstein)</i>	613
<i>On Visual Formalisms (Harel)</i>	623
Glossary	659
Bibliography	665
Author Biographies	679
Index	681