

High-Assurance Design: Architecting Secure and Reliable Enterprise Applications

By Clifford J. Berg

.....
Publisher: **Addison Wesley Professional**

Pub Date: **October 13, 2005**

ISBN: **0-321-37577-7**

Pages: **696**

[Table of Contents](#) | [Index](#)

[Copyright](#)

[Foreword](#)

[Acknowledgments](#)

[About the Author](#)

[Preface](#)

[Who This Book Is For](#)

[Prerequisites](#)

[A Crossover Book](#)

[Diagram Syntax](#)

[What Is Not Covered](#)

[Chapter 1. Introduction](#)

[Section 1.1. The Technical Problem Areas](#)

[Section 1.2. It's the Process](#)

[Section 1.3. Design Assurance](#)

[Section 1.4. Roadmap](#)

[Section 1.5. Summary](#)

[Section 1.6. Exercises](#)

[Chapter 2. Assurance Requirements](#)

[Section 2.1. Security Requirements](#)

[Section 2.2. Writing Reliability Requirements](#)

[Section 2.3. Writing Failure-Response Requirements](#)

[Section 2.4. Summary](#)

[Section 2.5. Exercises](#)

[Chapter 3. Design Specification and Verification](#)

[Section 3.1. Design Specification](#)

[Section 3.2. Design Verification and Elaboration](#)

[Section 3.3. Defining and Verifying Architectural Rules](#)

[Section 3.4. Code Generation](#)

[Section 3.5. Levels of Verification](#)

[Section 3.6. Writing Test Plans for Reliability and Failure-Response Requirements](#)

[Section 3.7. Summary](#)

[Section 3.8. Exercises](#)

[Chapter 4. Planning for an Assurable Design](#)

[Section 4.1. Applying Effort Where It Matters Most](#)
[Section 4.2. Designing for Verifiability](#)
[Section 4.3. Think in Terms of Survivability](#)
[Section 4.4. Think in Terms of Incremental Processing](#)
[Section 4.5. Think in Terms of Concurrency](#)
[Section 4.6. Think in Terms of Recovery](#)
[Section 4.7. Summary](#)
[Section 4.8. Exercises](#)
[Chapter 5. Methods of Attack](#)
[Section 5.1. Technical Attacks](#)
[Section 5.2. Social Engineering](#)
[Section 5.3. Summary](#)
[Section 5.4. Exercises](#)
[Chapter 6. Realms of Trust](#)
[Section 6.1. Understanding Trust and Authorization](#)
[Section 6.2. Managing Trust](#)
[Section 6.3. Summary](#)
[Section 6.4. Exercises](#)
[Chapter 7. Access Control Containers](#)
[Section 7.1. Secure Resource Containers](#)
[Section 7.2. Resource Types and Layers](#)
[Section 7.3. Diversity](#)
[Section 7.4. Auditability of Policy Coverage](#)
[Section 7.5. Perimeters](#)
[Section 7.6. Levels of Processes within an Organization](#)
[Section 7.7. Permissions](#)
[Section 7.8. Permission Parameterization](#)
[Section 7.9. Role Parameterization](#)
[Section 7.10. Dynamic Conditions](#)
[Section 7.11. Default Policies](#)
[Section 7.12. Association of a Resource and Its Authorization Model](#)
[Section 7.13. Resource Interface Design](#)
[Section 7.14. Ensuring Atomic Access to Resources](#)
[Section 7.15. Secure Error Handling](#)
[Section 7.16. Secure Logging](#)
[Section 7.17. Scope, Session, and Context](#)
[Section 7.18. Controlling Communication Pathways](#)
[Section 7.19. Domain Integrity](#)
[Section 7.20. Interference and Closure](#)
[Section 7.21. Home-Grown Authorization](#)
[Section 7.22. Summary](#)
[Section 7.23. Exercises](#)
[Chapter 8. Compartmentalization and Classification](#)
[Section 8.1. Role Separation](#)
[Section 8.2. Summary](#)
[Section 8.3. Exercises](#)
[Chapter 9. Transport and Storage of Secrets](#)

[Section 9.1. Basic Vulnerabilities](#)
[Section 9.2. Credential Management](#)
[Section 9.3. Summary](#)
[Section 9.4. Exercises](#)
[Chapter 10. Design Considerations for Secure Operation](#)
[Section 10.1. Designing for Secure Deployment](#)
[Section 10.2. Restoration](#)
[Section 10.3. Designing for Secure Operation](#)
[Section 10.4. Provide for Monitoring](#)
[Section 10.5. Capacity Allocation and Resource Usage Monitoring](#)
[Section 10.6. Usability](#)
[Section 10.7. Maintainability](#)
[Section 10.8. Summary](#)
[Section 10.9. Exercises](#)
[Chapter 11. Compositional Integrity](#)
[Section 11.1. Composition Concepts](#)
[Section 11.2. Object Allocation and Deallocation](#)
[Section 11.3. Component Roles and Contracts](#)
[Section 11.4. Summary](#)
[Section 11.5. Exercises](#)
[Chapter 12. Concurrency](#)
[Section 12.1. Review of Fundamentals](#)
[Section 12.2. Multiprocessing and Multithreading](#)
[Section 12.3. Summary](#)
[Section 12.4. Exercises](#)
[Chapter 13. Transactional Integrity](#)
[Section 13.1. Referential Integrity](#)
[Section 13.2. Transaction Isolation](#)
[Section 13.3. Ensuring Consistency Across Transactions](#)
[Section 13.4. Intra-Transaction Consistency](#)
[Section 13.5. Transactions on Composite Objects](#)
[Section 13.6. Dealing with Non-Transactional Resources](#)
[Section 13.7. Combining Transactions](#)
[Section 13.8. Application-Defined Locking and Workflows](#)
[Section 13.9. Layer Access Rules for Transactions](#)
[Section 13.10. Considerations for Business Delegate Patterns](#)
[Section 13.11. Transaction Error Handling](#)
[Section 13.12. Transaction Testing and Validation Strategies](#)
[Section 13.13. Summary](#)
[Section 13.14. Exercises](#)
[Chapter 14. Caching and Replication](#)
[Section 14.1. Caching](#)
[Section 14.2. Replication](#)
[Section 14.3. Summary](#)
[Section 14.4. Exercises](#)
[Chapter 15. Distributed Services and Messaging](#)
[Section 15.1. Request-Response](#)

[Section 15.2. Messaging](#)
[Section 15.3. Summary](#)
[Section 15.4. Exercises](#)
[Chapter 16. Manageability](#)
[Section 16.1. Deployment and Configuration Processes](#)
[Section 16.2. Avoiding Resource Interference](#)
[Section 16.3. Application Startup and Shutdown](#)
[Section 16.4. Generating Progress and Health Messages](#)
[Section 16.5. Summary](#)
[Section 16.6. Exercises](#)
[Chapter 17. Maintainability](#)
[Section 17.1. Documentation](#)
[Section 17.2. Transparency of Implementation](#)
[Section 17.3. Safe Extensions](#)
[Section 17.4. Regression Testing](#)
[Section 17.5. Summary](#)
[Section 17.6. Exercises](#)
[Chapter 18. Failure Response Design](#)
[Section 18.1. Common Failure Response Deficiencies](#)
[Section 18.2. Effective Error Handling](#)
[Section 18.3. Monitoring and Management](#)
[Section 18.4. Summary](#)
[Section 18.5. Exercises](#)
[Chapter 19. Methodological Considerations](#)
[Section 19.1. Issues and Approaches](#)
[Section 19.2. Universal Methodological Principles](#)
[Section 19.3. Analysis of Extreme Programming \(XP\) for Development of Reliable and Secure Systems](#)
[Section 19.4. Writing Corporate Assurance Guidelines](#)
[Section 19.5. Software Releases](#)
[Section 19.6. Deployment](#)
[Section 19.7. Summary](#)
[Section 19.8. Exercises](#)
[Chapter 20. Case Study: Transactional Integrity](#)
[Section 20.1. Background](#)
[Section 20.2. Analysis Approach](#)
[Section 20.3. Problems Found](#)
[Section 20.4. Remediation](#)
[Section 20.5. Reflection](#)
[Chapter 21. Case Study: Application Security](#)
[Section 21.1. Background](#)
[Section 21.2. Analysis Approach](#)
[Section 21.3. Problems Found](#)
[Section 21.4. Remediation](#)
[Section 21.5. Reflection](#)
[Chapter 22. Case Study: Manageability](#)
[Section 22.1. Background](#)

[Section 22.2. Analysis Approach](#)
[Section 22.3. Problems Found](#)
[Section 22.4. Remediation](#)
[Section 22.5. Reflection](#)
[Appendix A. References](#)
[Chapter 1](#)
[Chapter 2](#)
[Chapter 3](#)
[Chapter 4](#)
[Chapter 5](#)
[Chapter 6](#)
[Chapter 7](#)
[Chapter 8](#)
[Chapter 9](#)
[Chapter 10](#)
[Chapter 11](#)
[Chapter 12](#)
[Chapter 13](#)
[Chapter 14](#)
[Chapter 15](#)
[Chapter 16](#)
[Chapter 17](#)
[Chapter 18](#)
[Chapter 19](#)
[Appendix B. Failure Response Conditions and Requirements](#)
[Appendix C. List of Design Principles, by Chapter](#)
[Appendix D. List of Design Patterns, Alphabetical](#)
[Appendix E. List of Attack Patterns, by Section](#)
[Index](#)