Design and Safety Assessment of Critical Systems

1st Ed., November 12, 2010.
Hardcover, 297 pages
ISBN: 9781439803318

For further information, visit
http://www.safety-critical.org

CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

Marco Bozzano
Adolfo Villafiorita

About the Authors:

Marco Bozzano and Adolfo Villafiorita are researchers at Fondazione Bruno Kessler
http://www.fbk.eu

With safety-critical systems becoming more complex, this book highlights how to improve these systems to reduce the risk of harmful effects to people and the environment. Design and Safety Assessment of Critical Systems provides an introduction to the area of design and verification of safety critical systems, with a focus on safety assessment. Issues related to design, development, and safety assessment of critical systems follow a detailed introduction of fundamental concepts. The core of the book covers some of the most well-known notations, techniques, and procedures, and also includes many in-depth examples that offer perspective from a variety of industrial sectors

Table of Contents

1 Introduction

1.1 Complex, Safety Critical Systems
1.2 Dealing with Failures: a short History of Safety Engineering
1.3 The role of Formal Methods
1.4 A Case Study: Three Mile Island

2 Dependability, Reliability and Safety Assessment

2.1 Introduction
2.2 Concepts
2.3 Classification of Faults
2.5 Managing Faults
2.6 Fault Detection
2.7 Fault Prediction
2.8 Fault Tolerance
2.9 Fault Coverage
2.10 Reliability Modeling
2.11 System Reliability

3 Techniques for Safety Assessment

3.1 Introduction
3.2 Hazard Analysis
3.3 Risk Analysis
3.4 Risk Measures

4 Development of Safety Critical Applications

4.1 Introduction
4.2 What Makes a System Complex
4.3 What Makes the Development Complex
4.4 Measuring the Impact of Complexity
4.5 From System to Process
4.6 A General Development Framework
4.7 Development Workflow
4.8 Testing Workflow
4.9 Safety Assessment Workflow
4.10 Certification Management Workflow
4.11 Project Management Workflow
4.12 Tool Support
4.13 Improving the Process: Maturity Models

5 Formal Methods for Safety Assessment

5.1 Introduction
5.2 Advantages of Formal Methods
5.3 Formal Methods in the Development Process
5.4 Problems and Limitations
5.5 History of Formal Methods
5.6 Formal Models and Specifications
5.7 Formal Methods for Verification and Validation
5.8 Formal Safety Analysis
5.9 Industrial applications of formal methods
5.10 Conclusions and Future Directions

6 Formal Methods for Certification

6.1 Certification of Avionic Systems
6.2 So many standards, so little time
6.3 The ECSS System of standards
6.4 Avionics Reference Standards
6.5 ARP 4754
6.6 ARP 4761
6.7 DO-178B
6.8 The Case for the Safety Case
6.9 Formal Methods and Certification

Appendix A The NuSMV Model Checker
Appendix B The FSAP Safety Analysis Platform
Appendix C Some Regulatory Bodies and Regulations