

1. Record Nr.	UNINA9910825784103321
Autore	Boulangier Jean-Louis
Titolo	Safety management for software-based equipment // Jean-Louis Boulangier
Pubbl/distr/stampa	Hoboken, N.J., : ISTE Ltd./John Wiley and Sons Inc., 2013
ISBN	1-118-57861-9 1-118-57991-7 1-118-57865-1
Edizione	[1st ed.]
Descrizione fisica	1 online resource (193 p.)
Collana	Focus series in computer engineering and IT, , 2051-2481
Disciplina	621.392
Soggetti	Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	CONTENTS; INTRODUCTION; CHAPTER 1. SAFETY MANAGEMENT; 1.1. Introduction; 1.2.Dependability; 1.3.Conclusion; 1.4.Bibliography; CHAPTER 2. FROM SYSTEM TO SOFTWARE; 2.1.Introduction; 2.2 Systems of command and control; 2.3 System; 2.4 Software implementation; 2.5.Conclusion; 2.6.Bibliography; 2.7.Glossary; CHAPTER 3. CERTIFIABLE SYSTEMS; 3.1. Introduction; 3.2. Normative context; 3.3.Conclusion; 3.4.Bibliography; 3.5.Glossary; CHAPTER 4. RISK AND SAFETY LEVELS; 4.1. Introduction; 4.2. Basic definitions; 4.3. Safety implementation; 4.4. In standards IEC 61508 and IEC 61511; 4.5.Conclusions 4.6.Bibliography4.7.Acronyms; CHAPTER 5. PRINCIPLES OF HARDWARE SAFETY; 5.1. Introduction; 5.2 Safe and/or available hardware; 5.3. Reset of a processing unit; 5.4. Presentation of safety control techniques; 5.5. Conclusion; 5.6.Bibliography; 5.7.Glossary; CHAPTER 6. PRINCIPLES OF SOFTWARE SAFETY; 6.1. Introduction; 6.2. Techniques to make software application safe; 6.3.Other forms of diversification; 6.4.Overall summary; 6.5.Quality management; 6.6.Conclusion; 6.7. Bibliography; 6.8.Glossary; CHAPTER 7. CERTIFICATION; 7.1. Introduction; 7.2. Independent assessment; 7.3. Certification 7.4. Certification in the rail sector7.5.Automatic systems; 7.6.Aircraft; 7.7. Nuclear; 7.8. Automotive; 7.9. Spacecraft; 7.10.Safety case; 7.11. Conclusion; 7.12. Bibliography; 7.13. Glossary; CONCLUSION; INDEX

Sommario/riassunto

A review of the principles of the safety of software-based equipment, this book begins by presenting the definition principles of safety objectives. It then moves on to show how it is possible to define a safety architecture (including redundancy, diversification, error-detection techniques) on the basis of safety objectives and how to identify objectives related to software programs. From software objectives, the authors present the different safety techniques (fault detection, redundancy and quality control). "Certifiable system" aspects are taken into account throughout the book. C
