

1. Record Nr.	UNINA9910896189603321
Autore	Guha Krishnendu
Titolo	Cybersecurity for Reconfigurable Hardware Based Critical Infrastructures // by Krishnendu Guha, Jyoti Prakash Singh, Amlan Chakrabarti
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2024
ISBN	3-031-67591-6
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (212 pages)
Disciplina	621.395
Soggetti	Data protection Cooperating objects (Computer systems) Computer crimes Security systems Data and Information Security Cyber-Physical Systems Cybercrime Security Science and Technology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Introduction -- Reconfigurable Hardware -- Security Administration & Planning -- Auditing -- Monitoring & Analysis -- Risk, Response and Recovery -- Control and Countermeasures -- AI/ML in Cyber-Security -- Digital Forensics -- Tutorial for Hands on Reconfigurable Hardware: System Design, Attacks, Security.
Sommario/riassunto	The book commences with an introductory section on reconfigurable computing and thereafter delves into its applications in critical infrastructures. This book analyzes how such systems may be affected due to vulnerabilities and also discusses how these can be attacked by adversaries or cybercriminals. This book also discusses protection mechanisms related to such threats. It initially starts with an introduction to the various industrial revolutions and the changes in security needs, followed by a basic description of reconfigurable hardware based critical infrastructures. Further, the book contains

discussion on security administration and planning, auditing, monitoring and analysis, risk-response and recovery, control and countermeasures highlighting their need in reconfigurable hardware-based platforms. In addition to these, new concepts are introduced such as AI/ML for cybersecurity, digital forensics related to reconfigurable hardware based critical infrastructures. Finally, a hands on learning experience is presented to provide the readers with a practical flavour. The book will be useful to students (graduate and undergraduate), researchers, academicians and industry professionals.

---