1. Record Nr. UNINA9910337573703321

Titolo	Resilience of Cyber-Physical Systems [[electronic resource]] : From Risk Modelling to Threat Counteraction / / edited by Francesco Flammini
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-319-95597-7
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (237 pages)
Collana	Advanced Sciences and Technologies for Security Applications, , 1613-5113
Disciplina	006.22
Soggetti	Data protection Computer security Computer crimes Quality control Reliability Industrial safety Management information systems Security Systems and Data Security Cybercrime Quality Control, Reliability, Safety and Risk Business IT Infrastructure
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Foreword -- Complex, Resilient and Smart Systems -- Challenges and Opportunities for Model-Based Security Risk Assessment of Cyber-Physical Systems -- A Comprehensive Framework for the Security Risk Management of Cyber-Physical Systems -- Supporting Cybersecurity Compliance Assessment of Industrial Automation and Control System Components -- Quantitative Evaluation of the Efficacy of Defence-in-Depth in Critical Infrastructures -- A Model-Driven and Generative Approach to Holistic Security with C-IME -- Multi-Range Decoy I/O Defense of Electrical Substations against Industrial Control System Malware -- Flood Resilience of a Water Distribution System -- A Non-

	Parametric Cumulative Sum Approach for Online Diagnostics of Cyber Attacks to Nuclear Power Plants.
Sommario/riassunto	This book addresses the latest approaches to holistic Cyber-Physical System (CPS) resilience in real-world industrial applications. Ensuring the resilience of CPSs requires cross-discipline analysis and involves many challenges and open issues, including how to address evolving cyber-security threats. The book describes emerging paradigms and techniques from two main viewpoints: CPSs' exposure to new threats, and CPSs' potential to counteract them. Further, the chapters address topics ranging from risk modeling to threat management and mitigation. The book offers a clearly structured, highly accessible resource for a diverse readership, including graduate students, researchers and industry practitioners who are interested in evaluating and ensuring the resilience of CPSs in both the development and assessment stages.