1. Record Nr. UNINA9910484156903321

Titolo	Recent Developments on Industrial Control Systems Resilience / / edited by Emil Pricop, Jaouhar Fattahi, Nitul Dutta, Mariam Ibrahim
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
ISBN	3-030-31328-X
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (XIV, 333 p.)
Collana	Studies in Systems, Decision and Control, , 2198-4190 ; ; 255
Disciplina	629.8
Soggetti	Control engineering Cooperating objects (Computer systems) Control and Systems Theory Cyber-Physical Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Safety Instrumented Systems Analysis -- Risks assessment of critical industrial control systems -- Machine Learning based Predictive Maintenance of Infrastructure Facilities in the Cryolithozone -- Cybersecurity Threats, Vulnerability and Analysis in Safety Critical Industrial Control System (ICS) -- Automatic Attack Graph Generation for Industrial Controlled Systems -- Determining Resiliency Using Attack Graphs -- Modern methods for analyzing malware targeting control systems -- Multi-stage cyber-attacks detection in the Industrial Control Systems -- Using Honeypots for ICS threats evaluation -- Intrusion detection on ICS and SCADA networks -- Security evaluation of sensor networks -- Innovative hardware-based cybersecurity solutions -- Legal issues of deception systems in the Industrial Control Systems.
Sommario/riassunto	This book provides profound insights into industrial control system resilience, exploring fundamental and advanced topics and including practical examples and scenarios to support the theoretical approaches. It examines issues related to the safe operation of control systems, risk analysis and assessment, use of attack graphs to evaluate the resiliency of control systems, preventive maintenance, and malware detection and analysis. The book also discusses sensor networks and

Internet of Things devices. Moreover, it covers timely responses to malicious attacks and hazardous situations, helping readers select the best approaches to handle such unwanted situations. The book is essential reading for engineers, researchers, and specialists addressing security and safety issues related to the implementation of modern industrial control systems. It is also a valuable resource for students interested in this area.