1.	Record Nr.	UNINA9910349285603321
	Titolo	Industrial Control Systems Security and Resiliency [[electronic resource]] : Practice and Theory / / edited by Craig Rieger, Indrajit Ray, Quanyan Zhu, Michael A. Haney
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
	ISBN	3-030-18214-2
	Edizione	[1st ed. 2019.]
	Descrizione fisica	1 online resource (277 pages)
	Collana	Advances in Information Security, , 1568-2633 ; ; 75
	Disciplina	658.478
	Soggetti	Data protection Computer communication systems Electrical engineering Artificial intelligence Security Computer Communication Networks Communications Engineering, Networks Artificial Intelligence
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	1. Current and New Practice -- 2. Cyber-Modeling, Detection, and Forensics -- 3. Proactive Defense Mechanism Design -- 4. Human System Interface -- 5. Metrics For Resilience.
	Sommario/riassunto	This book provides a comprehensive overview of the key concerns as well as research challenges in designing secure and resilient Industrial Control Systems (ICS). It will discuss today's state of the art security architectures and couple it with near and long term research needs that compare to the baseline. It will also establish all discussions to generic reference architecture for ICS that reflects and protects high consequence scenarios. Significant strides have been made in making industrial control systems secure. However, increasing connectivity of ICS systems with commodity IT devices and significant human interaction of ICS systems during its operation regularly introduces newer threats to these systems resulting in ICS security defenses

always playing catch-up. There is an emerging consensus that it is very important for ICS missions to survive cyber-attacks as well as failures and continue to maintain a certain level and quality of service. Such resilient ICS design requires one to be proactive in understanding and reasoning about evolving threats to ICS components, their potential effects on the ICS mission's survivability goals, and identify ways to design secure resilient ICS systems. This book targets primarily educators and researchers working in the area of ICS and Supervisory Control And Data Acquisition (SCADA) systems security and resiliency. Practitioners responsible for security deployment, management and governance in ICS and SCADA systems would also find this book useful. Graduate students will find this book to be a good starting point for research in this area and a reference source.