1. Record Nr. UNINA9910164157203321

Autore	Martellini Maurizio
Titolo	Information Security of Highly Critical Wireless Networks / / by Maurizio Martellini, Stanislav Abaimov, Sandro Gaycken, Clay Wilson
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
Edizione	[1st ed. 2017.]
Descrizione fisica	1 online resource (VII, 73 p. 1 illus.)
Collana	SpringerBriefs in Computer Science, , 2191-5768
Disciplina	621.382
Soggetti	Computer security Computer networks Electrical engineering Systems and Data Security Computer Communication Networks Communications Engineering, Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references at the end of each chapters.
Nota di contenuto	Introduction -- What is Highly Critical Wireless Networking (HCWN) -- Applications for HCWN -- Vulnerabilities and Security Issues -- Modeling Threats and Risks -- Modeling Vulnerabilities -- Governance and Management Frameworks -- Security Technologies for Networked Devices -- Known Weaknesses with Security Controls -- Competent Reliable Operation of HCWN -- Assessing the Effectiveness and Efficiency of Security Approaches -- Examples in Brief -- Testing the Resilience of HCWN -- Future Attack Patterns -- Assessing Cyber Attacks against Wireless Networks for the Next Global Internet of Things Revolution -- Conclusion.
Sommario/riassunto	This SpringerBrief explores features of digital protocol wireless communications systems, and features of the emerging electrical smart grid. Both low power and high power wireless systems are described. The work also examines the cybersecurity vulnerabilities, threats and current levels of risks to critical infrastructures that rely on digital wireless technologies. Specific topics include areas of application for high criticality wireless networks (HCWN), modeling risks and

vulnerabilities, governance and management frameworks, systemic mitigation, reliable operation, assessing effectiveness and efficiency, resilience testing, and accountability of HCWN. Designed for researchers and professionals, this SpringerBrief provides essential information for avoiding malevolent uses of wireless networks. The content is also valuable for advanced-level students interested in security studies or wireless networks.