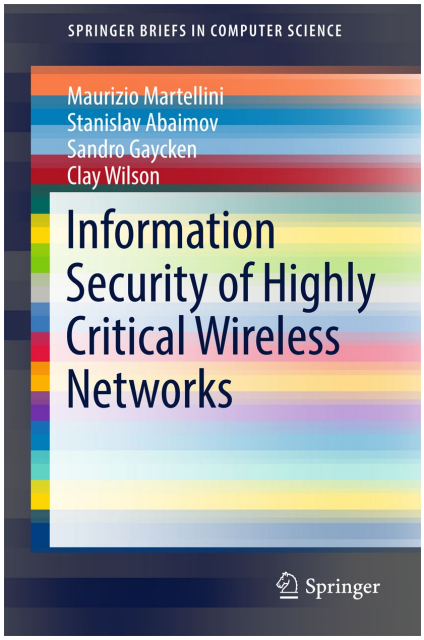

1st ed. 2017, VII, 73 p. 1 illus.

M. **Martellini**, S. **Abaimov**, S. **Gaycken**, C. **Wilson**

Information Security of Highly Critical Wireless Networks

Series: SpringerBriefs in Computer Science

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.