1. Record Nr. UNINA9910830975403321

Titolo	IoT for defense and national security / / Edited by Keith Gremban, Robert Douglass, Ananthram Swami, Stephan Gerali
Pubbl/distr/stampa	Hoboken, New Jersey : , : John Wiley & Sons, Inc., , 2023 ©2023
ISBN	1-119-89218-X 9781119892144
Descrizione fisica	1 online resource (531 pages)
Soggetti	Internet of things
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Sommario/riassunto	IoT for Defense and National Security Practical case-based guide illustrating the challenges and solutions of adopting IoT in both secure and hostile environments IoT for Defense and National Security covers topics on IoT security, architecture, robotics, sensing, policy, operations, and more, including the latest results from the premier IoT research initiative of the U.S. Defense Department, the Internet of Battle Things. The text also discusses challenges in converting defense industrial operations to IoT and summarizes policy recommendations for regulating government use of IoT in free societies. As a modern reference, this book covers multiple technologies in IoT including survivable tactical IoT using content-based routing, mobile ad-hoc networks, and electronically formed beams. Examples of IoT architectures include using KepServerEX for edge connectivity and AWS IoT Core and Amazon S3 for IoT data. To aid in reader comprehension, the text uses case studies illustrating the challenges and solutions for using robotic devices in defense applications, plus case studies on using IoT for a defense industrial base. Written by leading researchers and practitioners of IoT technology for defense and national security, IoT for Defense and National Security also includes information on: Changes in warfare driven by IoT weapons, logistics, and systems IoT

resource allocation (monitoring existing resources and reallocating them in response to adversarial actions) Principles of AI-enabled processing for Internet of Battlefield Things, including machine learning and inference Vulnerabilities in tactical IoT communications, networks, servers and architectures, and strategies for securing them Adapting rapidly expanding commercial IoT to power IoT for defense For application engineers from defense-related companies as well as managers, policy makers, and academics, IoT for Defense and National Security is a one-of-a-kind resource, providing expansive coverage of an important yet sensitive topic that is often shielded from the public due to classified or restricted distributions.