IoT for defense and national security

Type de contenu : Texte

Type de médiation : sans médiation

Type de support : Volume

Titre(s) : IoT for defense and national security / edited by Robert Douglass, Keith Gremban, Ananthram Swami,... [et al.]

Auteur(s) : Douglass, Robert T. (19..-....)

Autre(s) auteur(s) : Gremban, Keith
Swami, Ananthram
Gerali, Stephan

Publication : Piscataway (N.J.) : IEEE press Hoboken (N.J.) : John Wiley and sons

Date de copyright : C 2023

Description matérielle : 1 vol. (XLVIII-479 p.) : ill., graph., tabl. ; 26 cm

ISBN : 978-1-119-89214-4
1-119-89214-7

EAN : 9781119892144 rel.

Classification décimale Dewey : 355.8

Note sur la responsabilité : Autre contributeur : Stephan Gerali (coéditeur scientifique)

Note sur les bibliographies et les index : Bibliogr. en fin de chapitres. Index

Résumé ou extrait : 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.

Sujet - Nom commun : Sécurité nationale -- Informatique

Internet des objets