This book provides a comprehensive survey of state-of-the-art techniques for the security of critical infrastructures, addressing both logical and physical aspects from an engineering point of view. Recently developed methodologies and tools for CI analysis as well as strategies and technologies for CI protection are investigated in the following strongly interrelated and multidisciplinary main fields: - Vulnerability analysis and risk assessment - Threat prevention, detection and response - Emergency planning and management Each of the aforementioned topics is addressed considering both theoretical aspects and practical applications. Emphasis is given to model-based holistic evaluation approaches as well as to emerging protection technologies, including smart surveillance through networks of intelligent sensing devices. Critical Infrastructure Security can be used as a self-contained reference handbook for both practitioners and researchers or even as a textbook for master/doctoral degree students in engineering or related disciplines. More specifically, the topic coverage of the book includes: - Historical background on threats to critical infrastructures - Model-based risk evaluation and management approaches - Security surveys and game-theoretic vulnerability assessment - Federated simulation for interdependency analysis - Security operator training and emergency preparedness - Intelligent multimedia (audio-video) surveillance - Terahertz body scanners for weapon and explosive detection - Security system design (intrusion detection / access control) - Dependability and resilience of computer networks (SCADA / cyber-security) - Wireless smart-sensor networks and structural health monitoring - Information systems for crisis response and emergency management - Early warning, situation awareness and decision support software

**Book Information**

Hardcover: 326 pages
Publisher: WIT Press / Computational Mechanics; 1 edition (February 9, 2012)
Language: English
ISBN-10: 1845645626
Product Dimensions: 0.8 x 6.2 x 9.2 inches
Shipping Weight: 1.4 pounds (View shipping rates and policies)
Average Customer Review: Be the first to review this item
Best Sellers Rank: #7,663,994 in Books (See Top 100 in Books) #54 in Arts & Photography > Architecture > Security Design #1820 in Business & Money > Processes
Customer Reviews

Security professionals, auditors, vulnerability assessors, and researchers will be interested in the book. Engineers, information security managers, and chief information officers (CIOs) will also benefit from the information, especially the guidelines and the state-of-the-art practices and solutions presented. --Computing Reviews Online, May 30, 2012

Editor Francisco Flammini brings together cutting-edge critical infrastructure security information put forth by some of the best security authors of the day... The editor has brought together methodologies, strategies, and technologies for advancing critical infrastructure security in a way that pushes thinking in the field forward.

...suitable for security professionals who work in the critical infrastructure field. --Security Management, September 2013

Prof. Francesco FLAMMINI (Ph.D., Computer Science, University of Naples Federico II) is an Adjunct Professor of Software Engineering and Computer Science at the University of Naples "Federico II", ITALY. From October 2003 through January 2007, he worked at Ansaldo STS as a Software/RAMS Engineer in the Verification & Validation unit and was involved in several European Railway Traffic Management System / European Train Control System projects, specializing in functional testing of critical control systems. Since February 2007, after moving to the Innovation & Competitiveness unit, he has won several company awards for his work on critical infrastructure protection, transportation security and several interdisciplinary research projects. The author of more than 35 scientific papers published in international journals, book chapters and conference proceedings, his main research interests are the dependability and security of critical systems and infrastructures, including multi-paradigm modeling approaches. He is Editor-in-Chief of the International Journal of Critical Computer-Based Systems (Inderscience Publishers). He has served as a chairman, a member of the International Program Committee and a reviewer for several international conferences and IEEE journals. He is Vice-Chair of the IEEE Computer Society Italy and participates on several Technical Committees, including Software Engineering and Fault Tolerant Computing. He is also a member of the European Workshop on Industrial Computer Systems Reliability, Safety and Security (EWICS TC7), FME (Formal Methods Europe), ERCIM Working Group on Formal Methods for Industrial Critical Systems (FMICS), ESRA TC on Operational Safety and Security of Interconnected Critical Infrastructures, and IEEE SMC TC on
Homeland Security.

Download to continue reading...
