1. Record Nr. UNINA9910984690203321

| | |
|---|---|
| Autore | Staggs Jason |
| Titolo | Critical Infrastructure Protection XVIII : 18th IFIP WG 11.10 International Conference, ICCIP 2024, Arlington, VA, USA, March 18–19, 2024, Proceedings / / edited by Jason Staggs, Sujeet Shenoi |
| Pubbl/distr/stampa | Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025 |
| ISBN | 9783031818882<br>3031818881 |
| Edizione | [1st ed. 2025.] |
| Descrizione fisica | 1 online resource (223 pages) |
| Collana | IFIP Advances in Information and Communication Technology, , 1868-422X ; ; 725 |
| Altri autori (Persone) | ShenoiSujeet |
| Disciplina | 005.8 |
| Soggetti | Data protection<br>Computer networks<br>Computers - Law and legislation<br>Information technology - Law and legislation<br>Data and Information Security<br>Computer Communication Networks<br>Legal Aspects of Computing |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Nota di contenuto | Infrastructure Security: Evaluating Cyber Security Risks and Mitigation Strategies for Smart Grids Based on Business Case Scenarios -- On the Security of Electronic Voting Systems. Advanced Manufacturing Security: Detecting Control Injection Attacks Using Energy Data Anomalies in Computer Numerical Control Machining -- Security Assessment of an LBP16-Protocol-Based Computer Numerical Control Machine -- An End-to-End Framework for Verifying and Validating Manufacturing Design Integrity. Industrial Control System Security: Multiple-Bayesian-Network-Based Risk Assessment Methodology for Industrial Control Systems -- Automated Programmable Logic Controller Memory Forensics Using RGB Image Analysis and Deep Learning. Infrastructure Modeling: A Fail-Safe Challenge-Response Mechanism for User Equipment to Detect Rogue IMSI/SUPI Catchers -- Improved Distribution Network Topology Generation with Hierarchical |

Information Overlay.

Sommario/riassunto

The cyber infrastructure – comprising computers, embedded devices, networks and software systems – is vital to operations in every sector: chemicals, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials and waste, transportation systems, and water and wastewater systems. Global business and industry, governments, indeed society itself, cannot function if major components of the critical infrastructure are degraded, disabled or destroyed. Critical Infrastructure Protection XVIII describes original research results and innovative applications in the interdisciplinary field of critical infrastructure protection. Also, it highlights the importance of weaving together science, technology and policy to craft sophisticated, yet practical, solutions that will help secure information, computer and network assets in the various critical infrastructure sectors. Areas of coverage include: Infrastructure Security Advanced Manufacturing Security Industrial Control System Security Infrastructure Modeling This book is the eighteenth volume in the annual series produced by the International Federation for Information Processing (IFIP) Working Group 11.10 on Critical Infrastructure Protection, an international community of scientists, engineers, practitioners and policy makers dedicated to advancing research, development and implementation efforts focused on infrastructure protection. The book contains a selection of nine edited papers from the Eighteenth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, which was held at SRI International, Arlington, Virginia, USA in the spring of 2024. Critical Infrastructure Protection XVIII is an important resource for researchers, faculty members and graduate students, as well as for policy makers, practitioners and other individuals with interests in homeland security.