# Handbook on Securing Cyber-Physical Critical Infrastructure

Das, Sajal K  

## Table of Contents

- **Introduction: Securing Cyber-Physical Infrastructures--An Overview**  
- **Part 1: Theoretical Foundations of Security**  
  - Chapter 1: Security and Vulnerability of Cyber-Physical Infrastructure Networks: A Control-Theoretic Approach  
  - Chapter 2: Game Theory for Infrastructure Security: The Power of Intent-Based Adversary Models  
  - Chapter 3: An Analytical Framework for Cyber-Physical Networks  
  - Chapter 4: Evolution of Widely Spreading Worms and Countermeasures: An Epidemic Theory Approach

- **Part 2: Security for Wireless and Ad Hoc Networks**  
  - Chapter 5: Mobile Wireless Network Security  
  - Chapter 6: Security for Mobile Ad Hoc Networks  
  - Chapter 7: Defending against Identity-Based Attacks in Wireless Networks  
  - Chapter 8: Secure Mobile Cloud Computing  
  - Chapter 9: Security for Sensor Networks  
  - Chapter 10: Secure and Resilient Cluster Formation in Wireless Sensor Networks  
  - Chapter 11: Node Compromise Prevention and Detection in Wireless Sensor Networks  
  - Chapter 12: Key Pre-distribution for Wireless Sensor Networks  
  - Chapter 13: Defending against Physical Attacks in Wireless Sensor Networks  
  - Chapter 14: Hardware and Security: How Hardware Can Defend Itself and Help Software  
  - Chapter 15: Languages and Security: Safer Software Through Language and Compiler Techniques

- **Part 3: Security for Sensor Networks**  
  - Chapter 16: Secure and Resilient Cluster Formation in Wireless Sensor Networks  
  - Chapter 17: Node Compromise Prevention and Detection in Wireless Sensor Networks  
  - Chapter 18: Key Pre-distribution for Wireless Sensor Networks  
  - Chapter 19: Defending against Physical Attacks in Wireless Sensor Networks  
  - Chapter 20: Secure and Resilient Cluster Formation in Wireless Sensor Networks  
  - Chapter 21: Node Compromise Prevention and Detection in Wireless Sensor Networks  
  - Chapter 22: Key Pre-distribution for Wireless Sensor Networks

- **Part 4: Hardware and Software Security**  
  - Chapter 23: Hardware and Security: How Hardware Can Defend Itself and Help Software  
  - Chapter 24: Languages and Security: Safer Software Through Language and Compiler Techniques

- **Part 5: Data Security and Privacy**  
  - Chapter 25: Protecting Data in Outsourcing Scenarios  
  - Chapter 26: Privacy Preservation in Publishing Online Social Networks  
  - Chapter 27: Data Security in Cloud Computing

- **Part 6: Knowledge Extraction And Situational Awareness**  
  - Chapter 28: Knowledge Extraction And Situational Awareness  
  - Chapter 29: Pervasive Sensing, Monitoring and Situation Awareness  
  - Chapter 30: Distributed Network and System Monitoring for Securing Cyber-Physical Infrastructure  
  - Chapter 31: Discovering and Tracking Patterns of Interest in Security Sensor Streams  
  - Chapter 32: Computational Intelligence in Securing Cyber-Physical Systems  
  - Chapter 33: Managing and Securing Critical Infrastructure -- A (Semantic) Policy-and Trust-driven Approach

- **Part 7: Policy, Access Control and Formal Methods**  
  - Chapter 34: Policy, Access Control, and Formal Methods  
  - Chapter 35: Policy Based Security Management for Enterprise Networks  
  - Chapter 36: Maintaining Consistency and Integrity of Networking Infrastructure  
  - Chapter 37: Combined Analysis of the Safety and Security Properties of Cyber-physical System

- **Part 8: Security for Cyber-Physical Systems**  
  - Chapter 38: Pervasive Sense and Response Systems  
  - Chapter 39: Security and Privacy in the Smart Grid: Challenges and Solutions  
  - Chapter 40: Safety and Security in Energy Resource Management  
  - Chapter 41: Cyber-physical Security of Automotive Information Technology  
  - Chapter 42: Security Issues in P2P Telecommunication Networks