River Publishers

Systems Engineering for Critical Infrastructure in a Cyber World

Authors:

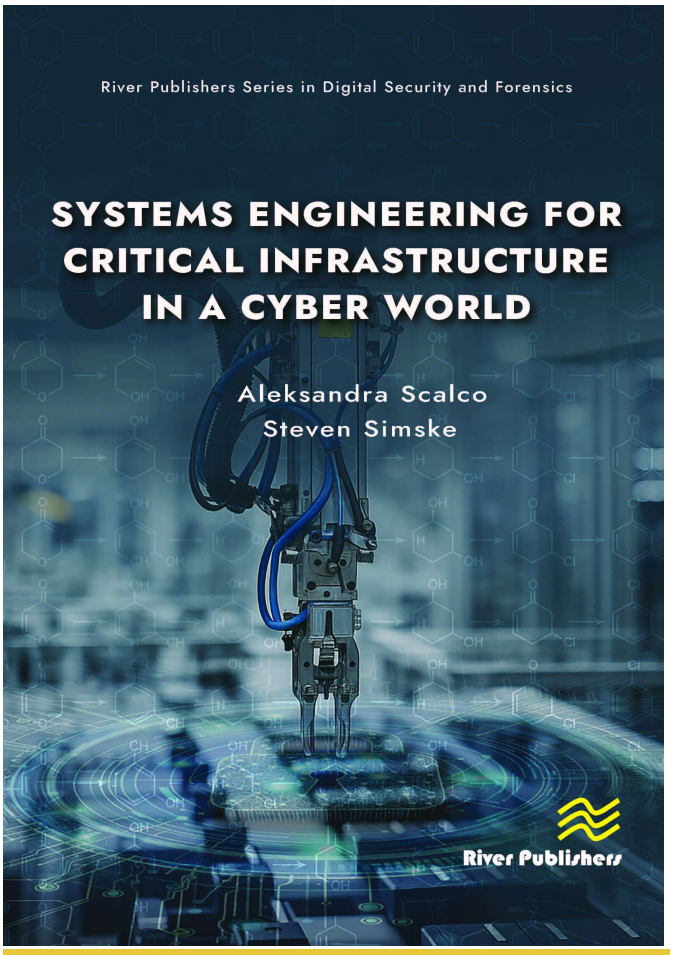
Aleksandra Scalco, Department of Defense (DOD), Defense Acquisition University (DAU), USA

Steven Simske, Colorado State University, USA

This book guides professionals in defending critical infrastructure by bridging IT, OT, and cybersecurity. Using systems engineering principles, it offers practical tools, strategies, and case-based examples to align stakeholders, strengthen defenses, and make complex cyber concepts clear and actionable.

TABLE OF CONTENTS

- Understanding the Game
- History of the Term "Cyber"
- Cyber Policy, Regulations, and Guidelines
- Cyber is a Medium (Not a Domain)
- Cyber Paradox
- Cyber Vulnerabilities Start at the Hardware Level
- Threats to Information-intensive Systems
- Use Cases and Operational View (OV) Illustrations
- Road to Commoditization
- Transition of Innovation to Operations
- Lifecycle Phases
- Concept Development
- Needs Analysis
- Detail Design
- Design Trade-offs
- Modernization Strategies
- Architectural Approaches
- Software Approaches
- Biometric
- Foundations of Systems Engineering
- Workforce
- Managing Risk
- Abstraction Models
- Creating a Model-based Organization
- Stakeholder Alignment
- Conclusion



River Publishers Series in Digital Security and Forensics

ISBN: 9788743809111
e-ISBN: 9788743809104
Available From: February 2026
Price: € 140.00

KEYWORDS:
Critical infrastructure, cyber, cybersecurity, systems engineering, control system engineering, control systems, process engineering, operational technology (OT), programmable logic controllers (PLCs), remote terminal units (RTUs), industrial control systems, supervisory control and data acquisition (SCADA), distributed control systems (DCS), zero trust strategy

www.riverpublishers.com
marketing@riverpublishers.com