1. Record Nr. UNINA9910462914103321

Autore	Biringer Betty E. <1952, >
Titolo	Critical infrastructure system security and resiliency / / Betty E. Biringer, Eric D. Vugrin, Drake E. Warren
Pubbl/distr/stampa	Boca Raton, Fla. : , : Taylor & Francis, , 2013
ISBN	0-429-25396-6 1-4665-5751-6
Edizione	[1st edition]
Descrizione fisica	1 online resource (221 p.)
Altri autori (Persone)	VugrinEric D WarrenDrake E
Disciplina	363.325/936360973
Soggetti	Fault tolerance (Engineering) Infrastructure (Economics) - United States National security - United States Public works - Security measures - United States Terrorism - United States - Prevention Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Front Cover; Contents; List of Figures; List of Tables; Foreword; Acknowledgments; About the Authors; Acronyms and Abbreviations; Chapter 1 - Introduction to Security Risk Assessment; Chapter 2 - Undesired Events, Associated Critical Assets, and Available Resources; Chapter 3 - Threat Analysis; Chapter 4 - Likelihood of Initiating Events; Chapter 5 - Assess Consequences and Responses for Undesired Event; Chapter 6 - Assessment of Protection System Effectiveness; Chapter 7 - Estimate Security Risk; Chapter 8 - Motivating Infrastructure Resilience Analysis Chapter 9 - Current State of Resilience AssessmentChapter 10 - Infrastructure Resilience Analysis Methodology; Chapter 11 - Case Studies Using the Infrastructure Resilience Analysis Framework; Chapter 12 - Future Directions; Appendix A: Example Use of Fault Trees to Identify Critical Assets; Appendix B: Physical Protection Features Performance Data; Back Cover
Sommario/riassunto	Part l: Security risk assessment. Chapter 1. Introduction to Security Risk

Assessment As our nation moves forward in the age of information and global economy, our dependencies on national infrastructure is greater than ever. Compromise of our critical infrastructures could disrupt the functions of our government, business, and our way of life. Catastrophic losses in terms of human casualties, property destruction, economic damages, and loss of public confidence could result from disruptions or degradation in our national infrastructure. Critical infrastructures are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof (U.S. Department of Homeland Security 2010). The Homeland Security Presidential Directive 7 (HSPD-7) (U.S. Department of Homeland Security 2010) identified 18 critical infrastructure sectors and a designated federal Sector-Specific Agency to lead protection and resilience-building programs and activities. The sectors include: - Agriculture and Food, - Banking and Finance, - Chemical, - Commercial Facilities, - Communications, - Critical Manufacturing, - Dams, - Defense Industrial Base, - Emergency Services, - Energy, - Government Facilities, - Healthcare and Public Health, - Information Technology, - National Monuments and Icons, - Nuclear Reactors, - Postal and Shipping, - Transportation Systems, and - Water--