1. Record Nr. UNINA9910807319703321

Titolo	Smart grid security : innovative solutions for a modernized grid / / edited by Florian Skopik, Paul Smith ; designer, Mark Rogers ; contributors, Stylianos Basagiannis [and twenty three others]
Pubbl/distr/stampa	Amsterdam, [Netherlands] : , : Syngress, , 2015 ©2015
ISBN	0-12-802354-6 0-12-802122-5
Edizione	[1st edition]
Descrizione fisica	1 online resource (330 p.)
Collana	Syngress Advanced Topics in Information Security
Disciplina	621.319
Soggetti	Smart power grids Computer security
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 at the end of each chapters and index.
Nota di contenuto	2.6.2.1 - The First Regulatory Experiment: The RFID PIA Framework2. 6.2.2 - The Second Regulatory Experiment: The DPIA Framework for Smart Grids and Smart Metering Systems; 2.7 - The EU "light" regulatory approach to Personal Data Protection in Smart Grids: an evaluation; 2.8 - Conclusion: DPIA Testing is a First Good Step but a more inclusive, easy to apply and flexible solution is necessary; 2.8.1 - A missed opportunity?; 2.8.2 - Recommendation 1: the governance of emerging technologies should carefully combine regulatory strategies 2.8.3 - Recommendation 2: Impact assessments of emerging technologies should be inclusive, easy to use and flexibleAcronyms; References; Chapter 3 - The Evolution of the Smart Grid Threat Landscape and Cross-Domain Risk Assessment; 3.1 - Introduction; 3.2 - Smart Grid Architectures: The Basics; 3.2.1 - GridWise Interoperability Context-Setting Framework; 3.2.2 - NIST Smart Grid Framework; 3.2.3 - Smart Grid Architecture Model and EU Mandate M490; 3.3 - Smart Grid Threat Landscape; 3.3.1 - Threat Types; 3.3.2 - Threat Agents; 3.3.3 - Attack Vectors; 3.3.4 - Case Studies 3.3.4.1 - Advanced Metering Infrastructure (AMI)3.3.4.2 - Wide Area Monitoring, Protection, and Control (WAMPAC); 3.3.4.3 - Distribution

Grid Management (DGM); 3.4 - Smart Grid Risk Assessment; 3.4.1 - Basic Concepts; 3.4.2 - Main Challenges; 3.4.2.1 - Managing Safety and Security Risks; 3.4.2.2 - Analysing Cyber-physical Risks; 3.4.2.3 - Understanding the Risks to Legacy Systems; 3.4.2.4 - Complex Organisational Dependencies; 3.4.2.5 - Understanding Cascading Effects; 3.4.3 - Existing Risk Assessment Frameworks; 3.5 - Conclusion; Acronyms; References
Chapter 4 - Resilience Against Physical Attacks

Sommario/riassunto

The Smart Grid security ecosystem is complex and multi-disciplinary, and relatively under-researched compared to the traditional information and network security disciplines. While the Smart Grid has provided increased efficiencies in monitoring power usage, directing power supplies to serve peak power needs and improving efficiency of power delivery, the Smart Grid has also opened the way for information security breaches and other types of security breaches. Potential threats range from meter manipulation to directed, high-impact attacks on critical infrastructure that could bring down regi