1. Record Nr. UNINA9911004828703321

Autore	Sahoo Subham
Titolo	Cyber Security for Microgrids
Pubbl/distr/stampa	Stevenage : , : Institution of Engineering & Technology, , 2022 ©2022
ISBN	1-83724-497-9 1-5231-5334-2 1-83953-332-3
Edizione	[1st ed.]
Descrizione fisica	1 online resource (265 pages)
Collana	Energy Engineering
Altri autori (Persone)	BlaabjergFrede DragicevicTomislav
Disciplina	005.8
Soggetti	Database security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Halftitle Page -- Series Page -- Title Page -- Copyright -- Contents -- About the Editors -- 1 Cyber-induced power system steady-state and dynamic issues -- 1.1 Introduction -- 1.2 System structure and problem description -- 1.2.1 System operational structure -- 1.2.2 Feasibility in system level -- 1.2.3 Stability issue in microgrid level -- 1.3 Cyber-induced power flow feasibility issue -- 1.3.1 Introduction -- 1.3.2 System modeling and problem statement -- 1.3.3 Defense strategy -- 1.4 Resiliency mechanism in microgrids -- 1.5 Conclusion -- References -- 2 Modern power electronics in active distribution network -- 2.1 Introduction -- 2.2 AC/DC distribution systems -- 2.3 Modern power electronics - Key enablers of intelligent grids -- 2.3.1 Renewable energy interfacing -- 2.3.2 High-voltage DC transmission systems -- 2.3.3 Flexible AC transmission systems -- 2.3.4 Smart transformer -- 2.4 Controllability -- 2.5 Artificial intelligence in modern power systems -- 2.5.1 Energy forecasting -- 2.5.2 Scheduling and electricity market -- 2.5.3 System optimization and stability control -- 2.5.4 Fault detection and protection -- 2.5.5 Cybersecurity -- 2.6 Cyber-physical security in active distribution network -- 2.6.1 Potential vulnerability -- 2.6.2 Vulnerability analysis of cyber attacks on control of VSCs -- 2.6.3 Cyber attacks in active

distribution network -- References -- 3 Microgrids in mission-critical applications -- 3.1 Introduction -- 3.2 Electric aircrafts -- 3.3 MVDC shipboards -- 3.4 Coordinated control in aircrafts and shipboards -- 3.4.1 Aircraft power systems -- 3.4.2 Shipboard power systems -- 3.5 Threat analysis against cyber attacks -- 3.6 Case study of MVDC shipboard microgrid -- 3.6.1 Attack Scenario 1 -- 3.6.2 Attack Scenario 2 -- 3.7 Conclusion -- References -- 4 Situational awareness of cyber attacks in smart grids.
4.1 Introduction -- 4.1.1 Related work -- 4.1.2 Challenges for wide-area situational awareness -- 4.2 Wide-area cybersecurity situational awareness -- 4.2.1 Conceptual architecture -- 4.3 Smart grid cybersecurity testbed -- 4.4 Case study: anomaly detection for WAMS -- 4.4.1 Synchrophasor-based WAMS -- 4.4.2 Problem formulation -- 4.4.3 Prototype demonstration using the commercial platform -- 4.5 Cybersecurity training for situational awareness -- 4.6 Conclusion -- References -- 5 Artificial intelligence-aided detection of data manipulation attacks in smart grid -- 5.1 Introduction -- 5.1.1 Power grid as a cyber-physical system -- 5.1.2 Cybersecurity concerns and related work -- 5.2 Data manipulation attacks on PSSE -- 5.2.1 Brief overview of state estimation -- 5.2.2 Attack formulation -- 5.2.3 Impact analysis -- 5.3 Defense strategies against FDIAs -- 5.3.1 Securing measurements: merits and demerits -- 5.3.2 Hybrid statistical-AI-based detection -- 5.4 Summary -- References -- 6 Cyber security threats in multi-agent microgrids -- 6.1 Cyber-physical MG system architecture -- 6.1.1 Microgrid physical layer architecture -- 6.1.2 Cyber-communication layer -- 6.1.3 Control layer -- 6.2 Distributed control for AC MG -- 6.2.1 Optimal dispatch control along with frequency restoration -- 6.2.2 Reactive power sharing along with network voltage restoration -- 6.3 Cyber threats in multi-agent-based MGs -- 6.3.1 Types of cyberattacks -- 6.4 Multi-agent-based cyberattack detection algorithms -- 6.4.1 Security at cyber layer -- 6.4.2 Security at physical and control layer -- 6.5 Summary -- References -- 7 Communication-assisted protections for DC microgrids and their performance analysis during cyberattacks -- 7.1 Introduction -- 7.1.1 Related works -- 7.1.2 Chapter focus -- 7.2 Fault analysis in DC microgrids -- 7.2.1 Analysis of capacitor discharge. 7.2.2 Freewheeling diode operation -- 7.3 A Unit protection scheme for DC microgrid -- 7.3.1 The unit protection methodology -- 7.3.2 Operation issues and economic aspects -- 7.3.3 Economics -- 7.3.4 Case study -- 7.3.5 Performance with noisy signals -- 7.4 Centralized protection of DC microgrids -- 7.4.1 The centralized protection methodology -- 7.4.2 Cosine similarity index (CS1)-based protection decision -- 7.4.3 Case study -- 7.4.4 Discussion -- 7.5 Performance of communication-based protections during cyber-attacks -- 7.5.1 Performance of unit protection for cyberattack -- 7.5.2 Performance of centralized protection for cyberattack -- 7.6 Conclusion -- References -- 8 Cyber-physical microgrids: toward flexible energy districts -- 8.1 Introduction -- 8.2 Impact of nearly zero energy districts -- 8.3 Methods for improvement of energy flexibility in energy districts -- 8.4 Cybersecurity of flexible energy districts -- 8.5 Impact of cyberattacks on flexibility utilization -- 8.6 Conclusion -- References -- 9 Design and modeling approaches to cyberattacks for grid-tied PV systems -- 9.1 Overview -- 9.2 Cyberattack for grid-tied PV system -- 9.2.1 DoS attack -- 9.2.2 Data integrity attack -- 9.2.3 Replay attack -- 9.2.4 Stealthy attack -- 9.2.5 Harmonic injection attack -- 9.2.6 Other attacks -- 9.3 Physics-based approach -- 9.4 Data-oriented approach -- 9.5 FDI attack generation -- 9.5.1 Physics-oriented tool -- 9.5.2 Data-oriented tool -- 9.5.3 GT approach -- 9.5.4 Generative

adversarial networks -- 9.6 Result and analysis -- 9.7 Conclusion -- References -- 10 Stealth cyber attacks in microgrids: detectability and observability -- 10.1 Introduction -- 10.2 Cyber-physical preliminaries of microgrids -- 10.3 Proposed stealth attack detection strategies -- 10.3.1 Stealth attack on voltages -- 10.3.2 Stealth attack on currents -- 10.4 Results.
10.4.1 Stealth voltage attacks -- 10.4.2 Stealth current attacks -- 10.5 Conclusion -- Appendix -- References -- 11 Resilient distributed control strategies in microgrids against cyber attacks -- 11.1 Introduction -- 11.1.1 Related works -- 11.1.2 Chapter focus -- 11.1.3 Chapter structure -- 11.2 Cyber-physical DC microgrids -- 11.2.1 Physical networks -- 11.2.2 Cyber networks -- 11.2.3 Impact of cyber attacks on microgrids -- 11.3 Resilient cooperative control in DC microgrids -- 11.3.1 Structure of resilient cooperative controllers -- 11.3.2 Proposed baseline attack detectors -- 11.3.3 Attack scenarios and adversary model -- 11.3.4 Proposed model of cyber-physical DC microgrids -- 11.3.5 Metrics for resilient analysis -- 11.4 Stability and attack-resilience analysis -- 11.4.1 State space representation of cyber-physical DC microgrids -- 11.4.2 Stability analysis in the absence of stealthy FDI attacks -- 11.4.3 Stability under stealthy FDI attacks -- 11.4.4 Stealthy FDI attack-resilience analysis -- 11.4.5 Design of resilient cooperative control parameters -- 11.5 Simulation results -- 11.6 Conclusion -- References -- 12 Cyber-physical testbeds for smart grid and electric vehicle-charging infrastructure -- 12.1 Introduction -- 12.2 Brief description of MG -- 12.3 Vulnerabilities associated with MG -- 12.3.1 Overview of the testbed for MG -- 12.3.2 Features of testbed -- 12.4 Brief description of EV-charging infrastructure -- 12.5 Vulnerabilities associated with EV-charging infrastructure -- 12.5.1 Overview of the testbed for EV-charging infrastructure -- 12.5.2 Features of testbed -- 12.6 Conclusion -- References -- 13 Event-driven resiliency of microgrids against cyber attacks -- 13.1 Introduction -- 13.2 Preliminaries of cyber-physical microgrids -- 13.2.1 DC microgrids -- 13.2.2 AC microgrids.
13.3 Proposed event-driven resiliency against cyber attacks -- 13.3.1 DC microgrids -- 13.3.2 Mitigation -- 13.3.3 AC microgrids -- 13.4 Results -- 13.4.1 DC microgrids -- 13.4.2 AC microgrids -- 13.5 Conclusions -- Appendix -- References -- 14 Cybersecurity in future energy systems: outlooks and recommendations -- 14.1 Introduction -- 14.1.1 Energy transition -- 14.1.2 Cyber resilience -- 14.2 Vulnerabilities, outlooks, and recommendations -- 14.3 Book summary -- References -- Index -- Back Cover.

Sommario/riassunto

Microgrids use ICT to deliver energy, but they can be open to cyber-attacks. This reference provides an up-to-date framework for resilient control and protection of microgrids. It investigates cyber-attacks on smart grids, discusses vulnerabilities and solutions.