1.	Record Nr.	UNINA9910484853903321
	Titolo	Critical Information Infrastructures Security : 11th International Conference, CRITIS 2016, Paris, France, October 10–12, 2016, Revised Selected Papers / / edited by Grigore Havarneanu, Roberto Setola, Hypatia Nassopoulos, Stephen Wolthusen
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
	ISBN	3-319-71368-X
	Edizione	[1st ed. 2017.]
	Descrizione fisica	1 online resource (XI, 348 p. 103 illus.)
	Collana	Security and Cryptology ; ; 10242
	Disciplina	005.8
	Soggetti	Computer security Computer communication systems Architecture, Computer Computers and civilization Computers Law and legislation Microprogramming Systems and Data Security Computer Communication Networks Computer System Implementation Computers and Society Legal Aspects of Computing Control Structures and Microprogramming
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Stealth Low-Level Manipulation of Programmable Logic Controllers I/O by Pin Control Exploitation -- 1 Introduction -- 2 Background -- 2.1 Pin Control Subsystem -- 2.2 How PLCs Control the Pins -- 3 Pin Control Attack -- 3.1 Security Concerns Regarding Pin Control -- 3.2 Pin Control Attack Details -- 3.3 Threat Model -- 4 A Pin Control Attack in Practice -- 4.1 Environment Setup -- 4.2 Attack Implementation -- 5 Discussion --

5.1 Implications of Attack on the ICS -- 5.2 Detection of Pin Control Attack -- 6 Related Work -- 7 Conclusion -- References -- Developing a Cyber Incident Communication Management Exercise for CI Stakeholders -- 1 Introduction -- 1.1 Background -- 1.2 Case Study: Red Team - Blue Team Exercise -- 2 Communication Management Exercise for ICS Security (CME-ICS) -- 2.1 Peculiarity of Existing Japanese CIP Training -- 2.2 Discussion-Based Exercise -- 2.3 Theme of the Exercise: Communication Management -- 2.4 Scenario -- 2.5 Exercise Steps -- 2.6 Administration Staff -- 2.7 Pilot Exercises -- 3 Results and Discussion -- 3.1 Variation of Incident Management Structure -- 3.2 Results of the Survey -- 3.3 Discussion -- 3.4 Future Work: ``ICS-SIRT'' Exercise -- References -- On Auxiliary Entity Allocation Problem in Multi-layered Interdependent Critical Infrastructures -- 1 Introduction -- 2 Problem Formulation Using the Implicative Interdependency Model -- 3 Computational Complexity Analysis -- 3.1 Special Case: Problem Instance with One Minterm of Size One -- 3.2 General Case: Problem Instance with an Arbitrary Number of Minterms of Arbitrary Size -- 4 Solutions to the AEAP Problem -- 4.1 Optimal Solution to AEAP Problem -- 4.2 Heuristic Solution to the AEAP Problem -- 5 Experimental Results -- 6 Conclusion -- References -- Cyber Targets Water Management -- 1 Introduction.

1.1 Use of Industrial Control Systems -- 1.2 Cyber Threats and Risk -- 1.3 Structure of This Paper -- 2 Related Work -- 3 A Benchmark of the Resilience of the ICS Environment -- 4 Observed ICS Security Dilemmas -- 5 Cyber Security Simulator for Water Management Control Systems -- 5.1 Deployment of Attack Scenarios -- 5.2 DESI Results -- 6 Conclusions and Future Work -- 6.1 Future Work -- References -- Integrated Safety and Security Risk Assessment Methods: A Survey of Key Characteristics and Applications -- 1 Introduction -- 2 Related Work -- 3 Review Methodology -- 4 Integrated Safety and Security Risk Assessment Methods -- 4.1 SAHARA Method -- 4.2 CHASSIS Method -- 4.3 FACT Graph Method -- 4.4 FMVEA Method -- 4.5 Unified Security and Safety Risk Assessment Method -- 4.6 Extended CFT Method -- 4.7 EFT Method -- 5 Analysis of Integrated Safety and Security Risk Assessment Methods -- 6 Conclusions and Future Work -- References -- Railway Station Surveillance System Design: A Real Application of an Optimal Coverage Approach -- Abstract -- 1 Introduction -- 2 Railway Station Surveillance and Sensor Placement Problem -- 3 Application of the Optimal Coverage Approach to a Real Case -- 3.1 Area of Interest and Input Data -- 3.2 Coverage Analysis and Coverage Matrix -- 3.3 Modeling of the Coverage Problem and Solution of the Model -- 4 Experimental Results -- 4.1 Set Covering Model -- 4.2 Maximal Covering Model -- 5 Conclusions -- References -- A Synthesis of Optimization Approaches for Tackling Critical Information Infrastructure Survivability -- Abstract -- 1 Introduction -- 2 Identifying Critical Network Components: Survivability-Oriented Interdiction Models -- 3 Enhancing Critical Network Survivability: Resource Allocation Strategy Models -- 3.1 Optimization Models for Protecting CII Physical Components.

3.2 Optimization Models for CII Service Restoration -- 4 Planning Survivable Networks: Design Models -- 5 Future Research Suggestions -- 6 Conclusions -- References -- A Dataset to Support Research in the Design of Secure Water Treatment Systems -- 1 Introduction -- 2 Secure Water Treatment (SWaT) -- 2.1 Water Treatment Process -- 2.2 Communications -- 3 Attack Scenarios -- 4 Data Collection Process -- 4.1 Physical Properties -- 4.2 Network Traffic -- 4.3 Labelling Data -- 5 Conclusion -- References -- Human Vulnerability Mapping Facing

Sommario/riassunto

This book constitutes the post-conference proceedings of the 11th International Conference on Critical Information Infrastructures Security, CRITIS 2016, held in Paris, France, in October 2016. The 22 full papers and 8 short papers presented were carefully reviewed and selected from 58 submissions. They present the most recent innovations, trends, results, experiences and concerns in selected perspectives of critical information infrastructure protection covering the range from small-scale cyber-physical systems security via information infrastructures and their interaction with national and international infrastructures.