1. Record Nr. UNINA9910299956203321

Titolo	Diagnosability, Security and Safety of Hybrid Dynamic and Cyber-Physical Systems / / edited by Moamar Sayed-Mouchaweh
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018
ISBN	3-319-74962-5
Edizione	[1st ed. 2018.]
Descrizione fisica	1 online resource (x, 327 pages)
Disciplina	004
Soggetti	Electrical engineering Quality control Reliability Industrial safety Control engineering Computers Communications Engineering, Networks Quality Control, Reliability, Safety and Risk Control and Systems Theory Information Systems and Communication Service
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Prologue.- Wind Turbine Fault Localization: A Practical Application of Model-Based Diagnosis -- Fault detection and localization using Modelica and abductive reasoning -- Robust Data-Driven Fault Detection in Dynamic Process Environments Using Discrete Event Systems -- Critical States Distance Filter Based Approach for Detection and Blockage of Cyberattacks in Industrial Control Systems -- Active diagnosis for switched systems using Mealy machine modeling -- Secure Diagnosability of Hybrid Dynamical Systems -- Diagnosis in Cyber-physical systems with Fault Protection Assemblies -- Passive Diagnosis of Hidden-Mode Switched Affine Models with Detection Guarantees via Model Invalidation -- Diagnosability of Discrete Faults with Uncertain Observations -- Abstractions Refinement for Hybrid Systems Diagnosability Analysis.

Sommario/riassunto

Cyber-physical systems (CPS) are characterized as a combination of physical (physical plant, process, network) and cyber (software, algorithm, computation) components whose operations are monitored, controlled, coordinated, and integrated by a computing and communicating core. The interaction between both physical and cyber components requires tools allowing analyzing and modeling both the discrete and continuous dynamics. Therefore, many CPS can be modeled as hybrid dynamic systems in order to take into account both discrete and continuous behaviors as well as the interactions between them. Guaranteeing the security and safety of CPS is a challenging task because of the inherent interconnected and heterogeneous combination of behaviors (cyber/physical, discrete/continuous) in these systems. This book presents recent and advanced approaches and tech-niques that address the complex problem of analyzing the diagnosability property of cyber physical systems and ensuring their security and safety against faults and attacks. The CPS are modeled as hybrid dynamic systems using different model-based and data-driven approaches in different application domains (electric transmission networks, wireless communication networks, intrusions in industrial control systems, intrusions in production systems, wind farms etc.). These approaches handles the problem of ensuring the security of CPS in presence of attacks and verifying their diagnosability in presence of different kinds of uncertainty (uncertainty related to the event occurrences, to their order of occurrence, to their value etc.). Synthesizes the state of the art in the domain of ensuring the security of cyber physical systems in presence of attacks and verifying their diagnosability in presence of different kinds of uncertainty; Studies the complementarities and the links between the different methods and techniques of fault diagnosis of hybrid dynamic systems; Includes the required notions, definitions and background to understand the problem of fault diagnosis of hybrid dynamic systems and how to solve it; Uses multiple examples in order to facilitate the understanding of the presented methods.