1. Record Nr. UNINA9910418325403321

Autore	Kim Shiho
Titolo	Automotive cyber security : introduction, challenges, and standardization / / Shiho Kim, Rakesh Shrestha
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2020] ©2020
ISBN	981-15-8053-7
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (XVII, 216 p. 78 illus., 76 illus. in color.)
Disciplina	303.4832
Soggetti	Automated vehicles - Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Sommario/riassunto	This book outlines the development of safety and cybersecurity, threats and activities in automotive vehicles. This book discusses the automotive vehicle applications and technological aspects considering its cybersecurity issues. Each chapter offers a suitable context for understanding the complexities of the connectivity and cybersecurity of intelligent and autonomous vehicles. A top-down strategy was adopted to introduce the vehicles' intelligent features and functionality. The area of vehicle-to-everything (V2X) communications aims to exploit the power of ubiquitous connectivity for the traffic safety and transport efficiency. The chapters discuss in detail about the different levels of autonomous vehicles, different types of cybersecurity issues, future trends and challenges in autonomous vehicles. Security must be thought as an important aspect during designing and implementation of the autonomous vehicles to prevent from numerous security threats and attacks. The book thus provides important information on the cybersecurity challenges faced by the autonomous vehicles and it seeks to address the mobility requirements of users, comfort, safety and security. This book aims to provide an outline of most aspects of cybersecurity in intelligent and autonomous vehicles. It is very helpful for automotive engineers, graduate students and technological administrators who want to know more about security technology as

well as to readers with a security background and experience who want to know more about cybersecurity concerns in modern and future automotive applications and cybersecurity. In particular, this book helps people who need to make better decisions about automotive security and safety approaches. Moreover, it is beneficial to people who are involved in research and development in this exciting area. As seen from the table of contents, automotive security covers a wide variety of topics. In addition to being distributed through various technological fields, automotive cybersecurity is a recent and rapidly moving field, such that the selection of topics in this book is regarded as tentative solutions rather than a final word on what exactly constitutes automotive security. All of the authors have worked for many years in the area of embedded security and for a few years in the field of different aspects of automotive safety and security, both from a research and industry point of view.