1.	Record Nr.	UNINA9910810051903321
	Autore	D'Anna Gloria D.
	Titolo	Cybersecurity for commercial vehicles / / Gloria D'Anna
	Pubbl/distr/stampa	Warrendale, Pennsylvania : , : SAE International, , [2018] ©2018
	ISBN	1-5231-4044-5 0-7680-9258-2 0-7680-9540-9
	Edizione	[1st ed.]
	Descrizione fisica	1 PDF (xix, 293 pages) : color illustrations
	Collana	Cybersecurity series
	Disciplina	629.272
	Soggetti	Computer security Data protection
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	"An SAE Core Title"--Cover.
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Foreword to the Reader xix -- CHAPTER 1 What Do You Mean by Commercial Vehicles and How Did We Happen on This Path of Cybersecurity? / by Gloria D'Anna 1 -- 1.1 I'm an Engineer and a Strategist 1 -- 1.2 Panel Discussion: Cybersecurity Risks and Policies for Transportation 3 -- 1.3 How Do We Define Commercial Vehicles for This Book? 4 -- 1.4 What I Love about the Cybersecurity World 5 -- 1.5 So, Who Should Read This Book? 6 -- 1.6 And Why You? Why Gloria? 6 -- 1.7 The Contributing Writers 7 -- 1.7.1 Chapter 2: Should We Be Paranoid? / by Doug Britton 7 -- 1.7.2 Chapter 3: What Cybersecurity Standard Work Is Applicable to Commercial Vehicles? / by Lisa Boran and Xin Ye 8 -- 1.7.3 Chapter 4: Commercial Vehicles vs. Automotive Cybersecurity: Commonalities and Differences / by Andrae Weimerskirch, Steffen Becker, and Bill Haas 9 -- 1.7.4 Chapter 5: Engineering for Vehicle Cybersecurity / by Daniel DiMase, Zachary A. Collier, John A. Chandy, Bronn Pav, Kenneth Heffner, and Steve Walters 9 -- 1.7.5 Chapter 6: “When Trucks Stop, America Stops” 11 -- 1.7.6 Chapter 7: On the Digital Forensics of Heavy Truck Electronic Control Modules / by James Johnson, Jeremy Daily, and Andrew Kongs 12 -- 1.7.6.1 Comments on How We Are All Connected 12 -- 1.7.6.2 IoT: The Internet of Things 13 -- 1.7.7 Chapter 8: Telematics Cybersecurity and

References 255 About the Author 267

CHAPTER 16 Do You Care What Time It Really Is? A Cybersecurity Look into Our Dependency on GPS by Gerardo Trevino, Marisa Ramon, Daniel Zajac, and Cameron Mott 269 -- 16.1 Background 269 -- 16.2 How Do Commercial Fleets Use GPS Today? 270 -- 16.3 How Could GPS Vulnerabilities Affect Fleet Vehicles? 271 -- 16.3.1 GPS Jamming Scenario 271 -- 16.3.2 GPS Spoofing Scenario 272 -- 16.4 Solutions, Recommendations, and Best Practices 273 -- 16.5 Key Takeaways 273 References 274 About the Authors 275 CHAPTER 17 Looking Towards the Future by Gloria D'Anna 279 -- 17.1 I'm a Blade Runner Fan 279 -- 17.2 Setting Standards 280 -- 17.3 Automotive ISAC 280 -- 17.4 The Systems of a Commercial Vehicle Continue to Get More Complicated 283 -- 17.5 The Good News 283 -- 17.6 Telematics 284 -- 17.7 Cybersecurity as an Enabler for New Technologies 284 -- 17.8 Department of Energy Work on Cybersecurity for Vehicles 285 -- 17.9 Commercial Truck Platooning 285 -- 17.10So, Why Is Platooning Such a Big Deal? 286 -- 17.11 So What Have We Learned from This Book? 288 -- 17.12 And Then, Something Happened 288 -- 17.13 SAE World Congress 2017 289 -- 17.14's We Go To Press 290 -- References 291 -- About the Author 293

Sommario/riassunto

This book provides a thorough view of cybersecurity to encourage those in the commercial vehicle industry to be fully aware and concerned that their fleet and cargo could be at risk to a cyber-attack. It delivers details on key subject areas including: * SAE International Standard J3061; the cybersecurity guidebook for cyber-physical vehicle systems * The differences between automotive and commercial vehicle cybersecurity. * Forensics for identifying breaches in cybersecurity. * Platooning and fleet implications. * Impacts and importance of secure systems for today and for the future. Cybersecurity for all segments of the commercial vehicle industry requires comprehensive solutions to secure networked vehicles and the transportation infrastructure. It clearly demonstrates the likelihood that an attack can happen, the impacts that would occur, and the need to continue to address those possibilities. This multi-authored presentation by subject-matter experts provides an interesting and dynamic story of how industry is developing solutions that address the critical security issues; the key social, policy, and privacy perspectives; as well as the integrated efforts of industry, academia, and government to shape the current knowledge and future cybersecurity for the commercial vehicle industry.