

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

Governance / by Glenn Atkinson 14 -- 1.7.8 Chapter 9: The Promise of Michigan: Secure Mobility / by Karl Heimer 14 -- 1.7.9 Chapter 10: How the Truck Turned Your Television Off and Stole Your Money: Cybersecurity Threats from Grid-Connected Commercial Vehicles / by Lee Slezak and Christopher Michelbacher 14 -- 1.7.10 Chapter 11: CALSTART's Cyber Mission: HTUF REDUX / by Michael Ippoliti 14 -- 1.7.11 Chapter 12: Characterizing Cyber Systems / by Jennifer Guild 15 -- 1.7.12 Chapter 13: "...No, We Should Be Prepared" / by Joe Saunders and Lisa Silverman 15 -- 1.7.13 Chapter 14: Heavy Vehicle Cyber Security Bulletin 15 -- 1.7.14 Chapter 15: Law, Policy, Cybersecurity, and Data Privacy Issues / by Simon Hartley 15 -- 1.7.15 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 16 -- 1.7.16 Chapter 17: Looking Towards the Future / by Gloria D'Anna 16 References 18 About the Author 19

CHAPTER 2 Should We Be Paranoid? by Doug Britton 21 -- 2.1 Why Is Cyber So Hard to De-risk? 21 -- 2.2 A Primer on Hacker Economics and Tactics 22 -- 2.2.1 Income Statement 22 -- 2.2.2 Balance Sheet 23 -- 2.2.3 Economic Analysis 24 -- 2.2.4 What about Nation-States? 25 -- 2.2.5 Steps in a Successful Cyber Attack 26 -- 2.2.6 Industrialization of the Attack 26 -- 2.3 Hacker Enterprises and Assets Associated with Commercial Trucking 28 -- 2.3.1 Exploitation Research 28 -- 2.3.2 Asset Development 29 -- 2.3.3 Distribution Development 30 -- 2.4 Potential Cyber Effects in Transportation 30 About the Author 32

CHAPTER 3 What Cybersecurity Standard Work Is Applicable to Commercial Vehicles? by Lisa Boran and Xin Ye 35 -- 3.1 Background 35 -- 3.2 Standards and Information 36 -- 3.3 SAE/ISO Cybersecurity Standard Development 37 -- 3.3.1 Secure Design 38 -- 3.3.2 Organizational Structure 41 -- 3.4 Conclusions 43 About the Authors 44

CHAPTER 4 Commercial Vehicle vs. Automotive Cybersecurity: Commonalities and Differences by Andrae Weimerskirch, Steffen Becker, and Bill Hass 47 -- 4.1 Introduction 47 -- 4.2 Background 48 -- 4.3 The Automotive and Commercial Vehicle Environment 50 -- 4.3.1 Supply Chain 50 -- 4.3.2 In-Vehicle Network Architecture and Communication 51 -- 4.3.3 Telematics 51 -- 4.3.4 Maintenance and Diagnostics 52 -- 4.3.5 Emerging Technologies 52 -- 4.4 Vehicle Threats and the Cyber Attacker 53 -- 4.4.1 An Evolving Threat Model 53 -- 4.4.2 The Adversary 55 -- 4.4.3 Offensive Techniques 55 -- 4.5 Cybersecurity Approaches and Solutions 58 -- 4.5.1 Legacy Vehicles 58 -- 4.5.2 Network Architectures and Separation 58 -- 4.5.3 Secure On-Board Communication 58 -- 4.5.4 Secure Computing Platform 59 -- 4.5.5 Anomaly Monitoring 60 -- 4.5.6 Security Operations Center 60 -- 4.5.7 Secure Firmware Over the Air 61 -- 4.6 Gaps and Conclusions 61 References 62 About the Authors 64

CHAPTER 5 Engineering for Vehicle Cybersecurity by Daniel DiMase, Zachary A. Collier, John A. Chandy, Bronn Pav, Kenneth Heffner, and Steve Walters 67 -- 5.1 Introduction 67 -- 5.2 Introduction to Cyber-Physical Systems Security 71 -- 5.3 Systems Engineering Perspective to Cyber-Physical Security 72 -- 5.3.1 Areas of Concern 72 -- 5.3.1.1 Electronic and Physical Security 72 -- 5.3.1.2 Information Assurance and Data Security 72 -- 5.3.1.3 Asset Management and Access Control 74 -- 5.3.1.4 Life Cycle and Diminishing Manufacturing Sources and Material Shortages (DMSMS) 75 -- 5.3.1.5 Anti-Counterfeit and Supply Chain Risk Management 75 -- 5.3.1.6 Software Assurance and Application Security 76 -- 5.3.1.7 Forensics, Prognostics, and Recovery Plans 76 -- 5.3.1.8 Track and Trace 77 -- 5.3.1.9 Anti-Malicious and Anti-Tamper 77 -- 5.3.1.10 Information Sharing and Reporting 78 -- 5.3.2 Systems Engineering Modeling 80 -- 5.3.3 Verification and

Validation 87 -- 5.4 Conclusions and Recommended Next Steps 88
References 91 About the Authors 95
CHAPTER 6 "When Trucks Stop, America Stops" 99
The Food Industry 100
Healthcare 100
Transportation 101
Waste Removal 102
The Retail Sector 103
Manufacturing 103
Banking & Finance 104
Other Effects 104
Conclusion 105
Case Study: The Effect of Border Delays on Auto Manufacturers Following September 11th 105
A Timeline Showing the Deterioration of Major Industries Following a Truck Stoppage 106
CHAPTER 7 On the Digital Forensics of Heavy Truck Electronic Control Modules by James Johnson, Jeremy Daily, and Andrew Kongs 109 -- 7.1
Introduction 110 -- 7.1.1 Motivation 111 -- 7.1.2 Paper Organization 111 -- 7.2 Digital Forensic Concepts 111 -- 7.2.1 Data Integrity 112 -- 7.2.2 Meaning of the Digital Data from ECMs 113 -- 7.2.2.1 Standards-Based Meaning 113 -- 7.2.2.2 Proprietary Meaning 115 -- 7.2.2.3 Daily Engine Usage from DDEC Reports 116 -- 7.2.3 Error Detection and Mitigation 118 -- 7.2.4 Establishing Transparency and Trust 119 -- 7.2.4.1 Baseline of Trust 119 -- 7.2.4.2 ECM Time Stamps 124 -- 7.2.4.3 Current Strategies to Establish Transparency and Trust 127 -- 7.3 Recommendations for Digital Evidence Extraction from Heavy Vehicles 127 -- 7.3.1 Sensor Simulators 128 -- 7.3.2 Write Blockers 129 -- 7.3.3 Authentication Algorithms 129 -- 7.3.4 Forensic Replay Mechanism 132 -- 7.3.5 Journal Preservation 133 -- 7.3.6 Chip Level Forensics 133 -- 7.3.7 Beyond Crash Reconstruction 134 -- 7.4 Summary/Conclusions 135
Definitions/Abbreviations 136
References 136
Contact Information 138
Acknowledgments 138
A. Appendix 139
About the Author 140
CHAPTER 8 Telematics Cybersecurity and Governance by Glenn Atkinson 143 -- 8.1 Background: Author 143 -- 8.2 Collaboration 144 -- 8.2.1 And So My Journey Begins 146 -- 8.2.2 Classic Electro-Hydraulic-Mechanical Vehicle 147 -- 8.3 Connected Vehicles 147 -- 8.4 Everything Was Coming and Going Along So Well.... 148 -- 8.4.1 Anonymity on the Internet 149 -- 8.5 The Geotab Story: Building a Telematics Platform Resilient to Cyber Threats 151 -- 8.6 Telematics Security: Vehicle to Server via Cellular Communication 152 -- 8.6.1 Cybersecurity Best Practices 152 -- 8.6.2 Secrets 152 -- 8.6.3 Authentication 152 -- 8.7 Cloning of Devices 153 -- 8.8 Eavesdropping 153 -- 8.9 Keep Embedded Code Secure 153 -- 8.10 Enable Hardware Code Protection 153 -- 8.11 Segregation 154 -- 8.12 Disable Debug Features 154 -- 8.12.1 Security Validation 154
About the Author 157
CHAPTER 9 The Promise of Michigan: Secure Mobility by Karl Heimer 159 -- 9.1 Governor's Foreword for "The Promise of Michigan" 159 -- 9.2 Introduction 160 -- 9.3 The Cyber Strategy 162 -- 9.4 Laws and Policies 163 -- 9.5 Capability Development 163 -- 9.5.1 TARDEC-MDOT I-69 Platooning Exercise 164 -- 9.5.2 American Center for Mobility 167 -- 9.5.3 Michigan Civilian Cyber Corps 170 -- 9.6 Michigan-Based Education and Training 171 -- 9.7 Conclusion 173
About the Author 175
CHAPTER 10 How the Truck Turned Your Television Off and Stole Your Money: Cybersecurity Threats from Grid-Connected Commercial Vehicles by Lee Slezak and Christopher Michelbacher 177
About the Authors 184
CHAPTER 11 CALSTART's Cyber Mission: HTUF REDUX by Michael Ippoliti 187
References 190
About the Authors 191
CHAPTER 12 Characterizing Cyber Systems by Jennifer Guild 193 -- 12.1 Introduction 193 -- 12.2 Assessment Models 194 -- 12.2.1 Flaw Models 194 -- 12.2.2 Countermeasure Models 196 -- 12.2.3 Vulnerability Models 197 -- 12.2.4 Threat Models 198 -- 12.2.5 Probability Models 200 -- 12.2.6 Attack Vector Models 201 -- 12.2.7 Impact Models 202 -- 12.2.8 Risk Models 203 -- 12.3 Assessment Methodology 205 -- 12.3.1 Stages 205 -- 12.3.1.1

Initial Exposure to a Cyber System 205 -- 12.3.1.2 System Familiarization 207 -- 12.3.1.3 Assessment 208 -- 12.3.1.4 Data Correlation 208 -- 12.4 Conclusions 208 References 209 About the Author 210

CHAPTER 13 "...No, We Should Be Prepared" by Joe Saunders and Lisa Silverman 213 -- 13.1 Introduction 213 -- 13.2 What Makes the Rolling Computers You Call a Fleet Vulnerable? 214 -- 13.3 The State of the Threat 216 -- 13.4 Recommendations to Prepare Fleet Managers 218 -- 13.4.1 Protecting Telematics Platform 218 -- 13.4.2 Monitor for Malicious "J1939" Messages 219 -- 13.4.3 Install Intrusion Detection System Across the Fleet 219 -- 13.4.4 Protect Software on ECUs 219 -- 13.4.5 Share Exploits with the Industry 220 -- 13.4.6 Periodically Conduct Penetration Tests 220 -- 13.5 Future Considerations to Advance Preparation Levels 220 References 221 -- 13A.1 Appendix A: Runtime Application Self-Protection Examples 222 -- 13B.1 Appendix B: J1939 Overview 223 -- 13C.1 Appendix C: Preventing Malicious Messages on the CAN Bus 224 -- 13C.1.1 The Problem 224 -- 13C.1.2 The Entry Point 224 -- 13C.1.3 The Solution 225 About the Authors 227

CHAPTER 14 Heavy Vehicle Cyber Security Bulletin 229 Develop a CyberSecurity Program 230 Protect Your Networks 230 Protect Your Vehicles 231 Incident Response Plan 231 Educate 232 Credits and Acknowledgements 233 Disclaimers 233 Trademarks 233

CHAPTER 15 Law, Policy, Cybersecurity, and Data Privacy Issues by Simon Hartley 235 Executive Summary 235 Publication Note 236 -- 15.1 Introduction 236 -- 15.1.1 Physical Safety 236 -- 15.1.2 Accident Statistics and Human Error 236 -- 15.1.3 Vehicle Hardware Improvements 236 -- 15.1.4 Vehicles Become Data Centers on Wheels 237 -- 15.1.5 Rise of Connectivity, Automation, and Public Concerns 237 -- 15.1.6 Commercial Vehicle Fleets and Telematics 238 -- 15.1.7 Gating Issue of Cyber Safety and Industry Tipping Point 239 -- 15.2 The Promise of Software, Connectivity, and Automation 239 -- 15.2.1 Fuel Efficiency and Clean Air 240 -- 15.2.2 Routing and Parking Efficiency 240 -- 15.2.3 Usage-Based Insurance (UBI) 240 -- 15.2.4 Accident Investigation 241 -- 15.2.5 Towards an Automated, Sharing, and Smart City Future 241 -- 15.3 Risk of Vehicle Cyberattack 241 -- 15.3.1 Vehicle Attack Surfaces 241 -- 15.3.2 A Brief History of Vehicle Hacks 242 -- 15.3.3 Internet-of-Things (IoT) Hacks 243 -- 15.3.4 The Issue of Legacy Vehicles, Updating and Recalls 243 -- 15.3.5 The Issue of End-to-End Hardening and Long Supply Chains 244 -- 15.4 Potential Harms Due to Vehicle Cyberattack 245 -- 15.4.1 Distracted Driving 245 -- 15.4.2 Distributed Denial of Service (DDoS) and Ransomware 245 -- 15.4.3 Property Damage, Bodily Injury, and Death 246 -- 15.4.4 Debilitation of Critical Transport Infrastructure 246 -- 15.4.5 Data Privacy 247 -- 15.5 Law and Policy 248 -- 15.5.1 Brief Review of Government and Industry Reactions to Car Hacking 248 -- 15.5.1.1 Pre-2015 - Proactive Research and Development (R&D) 248 -- 15.5.1.2 -- 2015 - Senate Warnings, Auto Information Sharing and Analysis Center (ISAC) 248 -- 15.5.1.3 -- 2016 - FBI, DoT, NHTSA, FTC Warnings, and Multiple Standards 249 -- 15.5.1.4 Post 2017 - New SPY Car Act and More Inclusive Auto-ISAC 250 -- 15.5.1.5 Innovation and Regulation 251 -- 15.5.2 Existing Cybersecurity and Data Privacy Standards 251 -- 15.5.3 A European Point of View 252 -- 15.6 Mitigating Risks and Balancing Interests 252 -- 15.6.1 Proposed Engineering Emphases 253 -- 15.6.1.1 (1) Systematically Running Pen Tests with Independent Testers 253 -- 15.6.1.2 (2) Over-the-Air (OTA) Updating for "Forgotten" Quarter Billion Vehicles 254 -- 15.6.1.3 (3) Reduce Attack Surface Across Supply Chain, Mitigating Weak Links 254 -- 15.6.2 Legal and Cyberinsurance 255 -- 15.7 Conclusions 255

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 -- 17.10 So, 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.

---