1. Record Nr. UNINA9910877570303321

Autore	Shah Imdad Ali
Titolo	Cybersecurity in the Transportation Industry
Pubbl/distr/stampa	Newark : , : John Wiley & Sons, Incorporated, , 2024 ©2024
ISBN	1-394-20447-7 1-394-20446-9
Edizione	[1st ed.]
Descrizione fisica	1 online resource (269 pages)
Altri autori (Persone)	JhanjhiNoor Zaman
Disciplina	363.287
Soggetti	Transportation - Security measures Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cover -- Series Page -- Title Page -- Copyright Page -- Contents -- Acknowledgements -- Chapter 1 Cybersecurity Issues and Challenges in Civil Aviation Security -- 1.1 Introduction -- 1.2 Literature Review -- 1.3 Research Methods -- 1.4 Cyber Risk in Aviation -- 1.4.1 Voice (Very High Frequency - VHF) -- 1.4.2 Automatic Dependent Surveillance-Broadcast (ADS-B) -- 1.4.3 Importance of Satellite Navigation (GPS) -- 1.5 Distributed Denial of Service (DDoS) -- 1.5.1 Impact of DDoS on Air Transportation -- 1.6 Discussion -- 1.6.1 Importance of IoT in Civil Aviation -- 1.6.2 Cybersecurity Challenges in Civil Aviation -- 1.7 Conclusion -- 1.8 Future Work -- References -- Chapter 2 Addressing Security Issues and Challenges in Smart Logistics Using Smart Technologies -- 2.1 Introduction -- 2.2 Literature Review -- 2.3 Methodology -- 2.4 Evaluation of Logistics and Smart Technologies -- 2.4.1 Connectivity -- 2.4.2 Sensors Collection -- 2.4.3 Data Processing Analysis -- 2.4.4 Automation and Control -- 2.4.5 Remote Monitoring and Management -- 2.5 Transportation Technology's Types -- 2.5.1 Underground Tunneling -- 2.5.2 Aerospace -- 2.5.3 Autonomous Vehicles -- 2.5.4 Last-Mile Robots -- 2.5.5 Electric Vehicles -- 2.6 Transportation Technology in Development -- 2.6.1 Blockchain Technology -- 2.6.2 Autonomous Vehicles -- 2.6.3 Connected Vehicles -- 2.7 Discussion -- 2.8

Conclusion -- 2.9 Future Work -- References -- Chapter 3 Global Navigation Satellite Systems for Logistics: Cybersecurity Issues and Challenges -- 3.1 Introduction -- 3.2 Literature Review -- 3.3 Research Methods -- 3.4 Global Navigation Satellite Systems -- 3.4.1 Types of Global Navigation Satellite Systems -- 3.4.2 Global Positioning System (United States) -- 3.4.3 GLONASS (Russia) -- 3.4.4 Galileo (European Union) -- 3.4.5 BeiDou (China) -- 3.4.6 IRNSS (India).
3.5 Overview of Automatic Identification System -- 3.6 Discussion -- 3.7 Conclusion -- 3.8 Future Work -- References -- Chapter 4 Importance of E-Maintenance for Railways Logistic -- 4.1 Introduction -- 4.2 Literature Review -- 4.3 Overview of E-Maintenance in Railway in the Context of Security Issues -- 4.3.1 Cyber Security Impact on E-Maintenance -- 4.3.2 Overview of Cyberattack in E-Maintenance -- 4.4 Discussion -- 4.5 Cyberattacks in the Railway in the Context of IoT -- 4.6 Cyberattacks in the Railway Using IoT -- 4.7 Conclusion -- 4.8 Future Work -- References -- Chapter 5 Privacy and Security Challenges in Unmanned Aerial Vehicles (UAVs) -- 5.1 Introduction -- 5.2 Literature Review -- 5.3 Methodology -- 5.4 Evaluation of UAV Cybersecurity Issues and Challenges -- 5.5 Security and Privacy Requirements -- 5.6 Discussion -- 5.7 Conclusion -- 5.8 Future Work -- References -- Chapter 6 Intelligent Transportation Systems (ITS): Opportunities and Security Challenges -- 6.1 Introduction -- 6.2 Literature Review -- 6.3 Evaluation of the Intelligence Transportation System -- 6.3.1 Data Collection -- 6.3.2 Data Transmission -- 6.3.3 Data Analysis -- 6.3.4 Traveler Information -- 6.4 Importance of Intelligent Transportation System -- 6.5 Discussion -- 6.6 Conclusion -- 6.7 Future Work -- References -- Chapter 7 IoT-Based Railway Logistics: Security Issues and Challenges -- 7.1 Introduction -- 7.2 Literature Review -- 7.3 Evaluation of IoT in Railway Transportation -- 7.3.1 Role of IoT Applications -- 7.3.2 IoT Applications for Railway Management -- 7.4 Railway Security Issues and Challenges -- 7.5 Discussion -- 7.6 Conclusion -- 7.7 Future Work -- References -- Chapter 8 Emerging Electric Vehicles and Challenges -- 8.1 Introduction -- 8.2 Literature Review -- 8.3 Methodology -- 8.3.1 Electric Vehicles and Security Issues.
8.4 Overview of Electric Vehicle Cyber-Physical System -- 8.5 Discussion -- 8.5.1 Vehicle Charging Security Issues -- 8.6 Electric Vehicles (EV) Security Challenges -- 8.6.1 Battery and BMS -- 8.7 Conclusion -- 8.8 Future Work -- References -- Chapter 9 Autonomous Shipping: Security Issues and Challenges -- 9.1 Introduction -- 9.2 Literature Review -- 9.3 Evaluation of Autonomous Shipping -- 9.3.1 Overview of Data Transmission -- 9.3.2 Security Issues and Challenges in Data Transmission -- 9.4 Evaluation of the IoT in Autonomous Shipping -- 9.5 Overview of Cybersecurity in Automation Ship -- 9.6 Cybersecurity Challenges in Automation Ship -- 9.7 Discussion -- 9.8 Conclusion -- 9.9 Future Work -- References -- Chapter 10 IoT-Based Smart Transportation Industry: Security Challenges -- 10.1 Introduction -- 10.2 Literature Review -- 10.3 Evaluation of IoT in the Transportation System -- 10.4 IoT Security Issues and Challenges -- 10.5 Evaluation of IoT Application in Transportation -- 10.6 Discussion -- 10.7 Conclusion -- 10.8 Future Work -- References -- Index -- Also of Interest -- EULA.

Sommario/riassunto

"This book offers crucial solutions and insights on how transportation companies can enhance their cybersecurity management and protect their corporate reputation and revenue from the increasing risk of cyberattacks. The movement of people and goods from one location to another has always been essential to human development and survival. People are now exploring new methods of carrying goods.

Transportation infrastructure is critical to the growth of a global community that is more united and connected. The presented cybersecurity framework is an example of a risk-based method for managing cybersecurity risk. An organisation can find opportunities to strengthen and explain its management of cybersecurity risk by using its existing procedures and leveraging the framework. The framework can provide a foundation for businesses that do not currently have a formal cybersecurity program. However, there is a strong temptation to give in when a transportation company is facing a loss of millions of dollars and the disruption of the worldwide supply chain. Automobile production, sales, trucking, and shipping are high-value industries for transportation enterprises. Scammers know that these corporations stand to lose much more in terms of corporate revenue and reputation than even the highest ransom demands, making them appealing targets for their schemes. This book will address the increasing risk of cyberattacks and offer solutions and insight on the safety and security of passengers, cargo, and transportation infrastructure to enhance the security concepts of communication systems and the dynamic vendor ecosystem." --