Computer Communications and Networks

The **Computer Communications and Networks** series is a range of textbooks, monographs and handbooks. It sets out to provide students, researchers, and non-specialists alike with a sure grounding in current knowledge, together with comprehensible access to the latest developments in computer communications and networking.

Emphasis is placed on clear and explanatory styles that support a tutorial approach, so that even the most complex of topics is presented in a lucid and intelligible manner.

More information about this series at http://www.springer.com/series/4198

Dietmar P. F. Möller • Roland E. Haas

Guide to Automotive Connectivity and Cybersecurity

Trends, Technologies, Innovations and Applications

Springer

Dietmar P. F. Möller
Clausthal University of Technology
Clausthal-Zellerfeld, Niedersachsen
Germany

Roland E. Haas
QSO Technologies
Bangalore, Karnataka
India

ISSN 1617-7975 ISSN 2197-8433 (electronic)
Computer Communications and Networks
ISBN 978-3-319-73511-5 ISBN 978-3-319-73512-2 (eBook)
https://doi.org/10.1007/978-3-319-73512-2

Library of Congress Control Number: 2018932982

Printed on acid-free paper

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Foreword by Thomas Hanschke

The automotive industry, which encompasses a wide range of companies and organizations, is one of the most important worldwide industries today as it becomes more aware and responsive to its surroundings. Automakers are responsible for the design, development, manufacturing, marketing, and selling of automobiles and trucks, also called motor vehicles or, in short, vehicles. These vehicles provide promising intelligent functionality and get smarter at every international motor show (IAA), the world's leading trade show in the increasing complexity of vehicles such as digitization, electromobility, and smart mobility. Therefore, this book outlines research and experience gained about advances in technological innovations with regard to trends, technologies, innovations, and applications in the automotive industry. The technological advances in sensor and navigation technologies, the networked living space through the Internet of Things, and the advances of service in the form of an Internet of Data and Services and cloud-based ones will spur the visionary and feasible mobility of the future, the so-called connected and autonomous driving. The term connected car refers to the next generation of car technologies making use of the Internet, enabling the passengers of the vehicle to take advantage of numerous new services and features. The idea of fully autonomous driving cars seems to be too futuristic for much of the driving public to embrace right now. But for automakers, the path from current models to driverless cars is going to be an exciting period of transformation. These innovative developments represent enormous opportunities even as they augur a perilous, unsteady phase for the automotive industry. In this regard automotive cybersecurity is another great theme for the future of mobility embedding advanced digitization concepts under conditions of adequately adapted innovations. Furthermore, the automotive industry will be facing numerous sweeping and interlinked changes in the next decades. Not only are there many different potential changes facing the automotive industry but, unlike most other industries, the automotive industry, while incorporating modern Internet network-enabled technology, has been forced to completely and fundamentally reinvent itself as other industries have during the last decades. Thus, automotive cybersecurity is quickly becoming the most important factor when purchasing a modern vehicle, due to the increasing part of software and digital components and systems on board and the connective and surrounding digital infrastructure. Against this background, the book describes, in contrast to other books which focus more on

automotive E/E and software technology, the essential methodological and theoretical basics and extends them to the body of knowledge of future car characteristics in connection with the necessary technological trends, technologies, innovations, and applications related to the need of automotive connectivity and the associated cybersecurity.

I strongly recommend Prof. Dr. Dietmar P. F. Moeller's scholarly writing to students, academicians, and industrialists who are keen to learn about advanced methodologies in automotive connectivity and cybersecurity. His scientific expertise, he is a professor for stochastic models in engineering sciences of Clausthal University of Technology (TUC) and a member of the Simulation Science Center (SWZ) Clausthal-Göttingen, stands for this advanced and innovative book topic. The co-author, Dr. Roland Haas, is the founder and CEO of QSO Technologies, located in Bangalore, India, who is experienced in different sectors of the automotive industry, giving the book a detailed insight into its applications. I can say without reservation that this book, and more specifically the method it espouses, will change fundamental ideas for cutting-edge innovation and disruption in the automotive domain.

President Clausthal-University of Technology Thomas Hanschke
Clausthal-Zellerfeld, Germany

Foreword by Jerry Hudgins

Automobiles have become one of the basic needs of humanity as global populations have become more and more mobile during the past century; however, cars and consumers have changed in different ways. Major automobile brands now implement new technologies based on what will improve the consumer driving experience, a strategy that has proven to be their key to success. Changing market dynamics are energizing the automotive industry, which has always been at the forefront of defining new paradigms for the new technologies embedded in their vehicles. Today, these new technologies can be summarized by two words: smart mobility. This book outlines the latest in smart mobility research, technological innovation, and applications within the automotive industry.

Automotive connectivity and cybersecurity are the overriding themes of smart mobility as advanced digital concepts are adapted for use in today's vehicles. The central focus of this book is the networking of the virtual computer world (cyber) with automotive (physical) components to create cyber-physical systems that incorporate the different intelligent assist systems used in today's vehicles. Cyber-physical systems, in this sense, consist of strong digital platforms that are well structured, well integrated, and only as complex as is absolutely necessary. These systems also guarantee that drivers and passengers are protected by innovative and intelligent safety systems whose connectivity enables them to access different kinds of information sources and services from within and outside of a vehicle. As this strong connectivity continues to evolve, it is imperative that the automotive industry examine the vulnerability of connected cars and determine what cybersecurity methods can best be used to defend against cybercriminal attacks on vehicles.

I strongly recommend Prof. Dr. Dietmar P.F. Möller's scholarly writing to students, academicians, and industry experts who seek to learn more about advanced methodologies in automotive connectivity and cybersecurity. As an adjunct professor in the Electrical and Computer Engineering Department of the University of Nebraska, Dr. Möller's research and expertise in cybersecurity is a valuable addition to our students and faculty. The co-author, Dr. Roland Haas, founder and CEO of QSO Technologies, located in Bangalore, India, provided expertise from different sectors of the automotive industry, giving the book a practical perspective and detailed insight into its real-world applications. This book, in contrast to other books that focus more on the basic theories

and methods associated with automotive electrical/electronic issues and software technology, extends beyond the basics to include future technological trends, innovations, and new applications in the automotive industry.

Head, Department of Electrical and Computer Engineering, University of Nebraska
Lincoln, NE, USA

Jerry Hudgins

Foreword by Rayford Vaughn and Tommy Morris

Cybersecurity has emerged as one of the most important needs on the research front as evidenced by its nearly daily appearance in the news, loss of millions of files containing personally identifying information, allegations of electronic voting interference, cyberattacks against the electric grid, and many more such incidents. Industry has developed and implemented many new technologies in attempts to improve the cybersecurity protecting their mission critical IT infrastructure, but breaches still occur and the resulting penetrations cause reputational, economic, and physical harm. It appears that the adversary has the advantage and that the "penetrate and patch" philosophy is alive and well. While historically we have been concerned with traditional computer security and database security, advances in automation in other sectors bring with it the threat of cyberattack and new domains of cybersecurity research. Examples include industrial control system security, weapon systems security, securing the "Internet of Things" or IOT, and transportation security. It is these latter concerns that Dr. Dietmar P.F. Möller and Dr. Roland Haas have chosen to address.

Research topics involving automotive security are becoming increasingly important as rapid advances are being made in driverless vehicles, including the introduction of artificial intelligence into the operation of automobiles, over-the-air firmware updates, vehicle-to-vehicle communication, and the collection/storage of private information by the automobile. The case for enhanced proofs of correctness, stronger verification and validation techniques, formal models, and code proofs are stronger today than in the past.

A treatment of these subjects through case studies and narrative is needed, and we compliment Dr. Dietmar P.F. Möller and Dr. Roland Haas for taking up the challenge of writing this book and giving it a practical perspective with detailed insight into real-world applications. We are quite comfortable that this book will find

its way into academic settings as well as industrial R&D organizations and that it will promote the kind of thoughtful dialogue necessary before vulnerable transportation systems are deployed to the public.

Vice President Research, Research and Economic Development, The University of Alabama Huntsville, AL, USA — Rayford Vaughn

Associate Professor ECE, Director, Center for Cybersecurity, Research and Education, The University of Alabama Huntsville, AL, USA — Tommy Morris

Preface

The goal of this book is to provide a comprehensive, in-depth, state-of-the-art summary of automotive connectivity and cybersecurity with regard to trends, technologies, innovations, and applications. It describes the challenges of the global automotive market, clearly showing where the multitude of innovative activities fit within the overall effort of cutting-edge automotive innovations and provides an ideal framework for understanding the complexity of automotive connectivity and cybersecurity. Given this complexity, we had to make some choices in selecting the material for this book. A top-down approach was taken that introduces the promising intelligent functionality of vehicles but also increases their complexity. Therefore, this book provides essential background on the issues facing the automotive industry as it attempts to balance consumers' mobility needs with their desire for convenience and safety.

Digitization will enable a quantum leap forward in the realization of sustainable, smart mobility services. This will require accessibility; embedment; tiny, powerful computers; sensors; wireless networks; smart devices; cloud services; etc. to support the vision of smart mobility and make it a reality. This book provides a framework within which the reader can analyze and integrate the associated requirements. Without such a reference, the practitioner is left to ponder the plethora of terms, standards, and practices that have been developed independently and that often lack cohesion, particularly in nomenclature and emphasis. Therefore, this book is intended to both cover a broad range of aspects of automotive connectivity and cybersecurity and provide a synopsis for the consideration of the many issues associated with these topics. The subjects discussed include the automotive market; automotive research and development; automotive E/E and software technology; connected cars and autonomous vehicles; and respective methodological approaches to cybersecurity, such as intrusion detection and prevention, to avoid cyberattacks against vehicles.

First, an overview of the automotive industry is presented that describes the technology wave that has changed the automotive industry and, ultimately, drives it toward futuristic concepts, such as smart mobility and autonomous driving.

Smart mobility characterizes the visionary, affordable mobility of the future, which will be applicable to and usable by everyone regardless of (1) location and

region, (2) periods of use and duration, and (3) individual ability and budget, resulting in a new business model called Mobility-as-a-Service.

In addition, the automotive industry is analyzed with regard to the global production and sale of vehicles. The analysis focuses on some automotive megatrends, such as tighter emission controls and the rise of electric vehicles with their need for an adequate charging infrastructure. Also, information on the connection between cars, the required road infrastructure, and the advanced driver assistance systems for accident avoidance is presented. The issues that automotive original equipment manufacturers (OEMs) and suppliers are facing due to digitization and autonomous driving are summarized, and new players and challenges in the automotive domain are identified.

Second, automotive research and development is outlined, as well as background on the complexity involved in developing new vehicle models. The automotive development process is described in detail, taking into account the three stages: conceptualization, project, and validation. A huge advantage in efficiency is realized through the deployment of specific tools, such as computer-aided design (CAD) systems for geometric design, digital mock-up (DMU), and computer-aided engineering (CAE) for analyzing, designing, and manufacturing products. This results in new product creation processes and better product quality by embedding the paradigm of requirements engineering. Furthermore, automotive modularization and product family-based platforms are introduced as they relate to virtual product creation and product life cycle management.

Against such a background, automotive mechatronic, electric, and electronic systems in cars, as well as automotive software technologies, are discussed, focusing on the different kinds of electronic control units (ECUs) required in today's premium cars.

Sensor technologies, which describe devices that generate a measurable signal in response to a stimulus, e.g., from car ECUs, are introduced, as well as bus systems and architectures. All of these systems have an impact on safety as part of the overall safety of a car. In modern cars, ECUs are functional and spatially distributed, which requires adequate test facilities, such as the hardware-in-the-loop test bed.

Finally, the AUTomotive Open System ARchitecture (AUTOSAR), a worldwide, joint initiative of several major industries to create and establish an open standardized software architecture for automotive ECUs, is described.

However, a textbook cannot describe all of the innovative aspects in the automotive domain. For this reason, the reader is referred to specific supplemental material, such as textbooks, reference guides, user manuals, etc., as well as Internet-based information that addresses several of the topics selected for the book.

Third, the technologies essential for the evolution of connected cars, such as cyber-physical systems that integrate computing and networking technologies and the Internet of Things that offers communication capabilities anytime, anywhere, are discussed. They represent the enabling technologies and driving factors of connected cars.

New business models related to services and applications are being developed. Furthermore, an interoperable, scalable platform is essential for the connected car paradigm and infrastructure. The required network is based on three sets of IEEE standards. Besides AUTOSAR, GENIVI is a development standard for setting requirements and implementation standards and providing certification programs. Beyond connected cars, autonomous vehicles have become the most advanced technological development in smart mobility. The advances in wireless networks of connected cars and autonomous vehicles, however, can have a negative impact due to the emergence of new types of cyberattacks. Therefore, cybersecurity is becoming a key issue with the main objectives of detecting, deterring, and averting vulnerabilities. Thus, intrusion detection and prevention represents the most important concern for overcoming weaknesses in the attack value chain. Thus, the most important methods are introduced, as well as advances in the direction of deep learning. Moreover, the innovative field of mobility apps for connected cars is included.

Fourth, due to the methodological background of connected cars and cybersecurity, their practical implementation is another important subject of the book, showing the reader how to develop and implement new services and technologies, such as carsharing, car hailing and ridesharing, connected parking, and automated valet parking, as well as advanced driver assistance systems.

The material in the book can be difficult to comprehend if the reader is new to such an approach. Automotive connectivity and cybersecurity is a multidisciplinary domain, founded in computer science, systems and software engineering, mechanical engineering, simulation science, and communications engineering as well as electronics. Readers may find the material challenging. Therefore, specific case studies have been included with related topics to help the reader master the material. It is assumed that the reader has some knowledge of basic electric and electronic components and some experience with systems and software engineering.

The book can be used in various ways as the primary text for a course. It contains more material than can be covered in detail in a quarter-long (30-h) or semester- long (45-h) course. Instructors may elect to choose their own topics and add their own case studies. The book can also be used for self-study as a reference for engineers, scientists, and computer scientists for on-the-job training; for students in graduate schools; and for automotive connectivity and cybersecurity practitioners and researchers.

For instructors who have adopted the book for use in a course, a variety of teaching support materials are available for download from http://www.springer.com/book/978-3-319-73511-5. These include a comprehensive set of PowerPoint slides to be used for lectures and all video-recorded classes.

The book is divided into 12 chapters, which can be read independently or consecutively.

Chapter 1 gives a brief overview of the specific topics covered in the book. Compared to other industries, the automotive industry has taken advantage of many

efficiency improvements driven by Internet-based technology but has also maintained the same structure, as opposed to reorganizing its whole ecosystem. A number of factors could push the automotive industry into new configurations, perhaps ultimately toward futuristic concepts, such as smart mobility. Smart mobility characterizes the visionary, feasible mobility of the future: applicable and usable for everyone regardless of location and region, regardless of periods of use and duration, and regardless of individual ability and budget.

Chapter 2 gives an overview of the global production and sales of the automotive industry and reports on the industry's megatrends, such as tighter emission controls and the rise of electric vehicles, car ownership versus mobility, connectivity, advanced driving assistance systems, and autonomous driving. It also covers background on the digital transformation in the automotive industry.

Chapter 3 focuses on the automotive development process, specifically the complexity involved in developing new vehicle models and the modularization approach and platforms used in the automotive industry, which will allow the efficient handling of an ever-increasing, multibrand vehicle model line. Moreover, the idea of product life cycle management is introduced, an approach that facilitates collaborative work processes for various phases of the product or system life cycle represented by a number of phases and activities spread out across the automaker's organization and suppliers. The sum of these activities is called the product or system life cycle, which can be described using a model that contains the conceptualization, utilization, evolution, and ultimate disposal phases.

Chapter 4 gives an overview of mechatronic, electric, and electronic systems in the automotive domain, as well as architectures and bus system requirements, with an emphasis on disciplined approaches to their design. The increasing role of software content and product complexity requires more adequate development tools, such as model-based software development and hardware-in-the-loop (HIL) tests. Furthermore, AUTOSAR is introduced, as well as the GENIVI platform, essential for telematic and infotainment components, and future trends. As a practical example, advanced driver assistance systems, which support vehicle drivers by enhancing safety and by improving driving conditions, are discussed, as well as the required sensor suite.

Chapter 5 provides a detailed treatment of the key technologies essential for the evolution of connected cars. Cyber-physical systems are engineered systems that integrate computing and networking technologies and the Internet of Things, which offer communication capabilities anytime, from anywhere, with everything. It also refers to telematic and infotainment concepts and refers to platforms and architectures for connected cars, as well as the connected car in the cloud and autonomous vehicles. Several case studies that are essential for the evolution of the connected car, such as BMW's ConnectedDrive; Mercedes's COMAND® Online; and HERE, which provides digital mapping for fully autonomous driving.

Chapter 6 introduces cybersecurity as a body of technologies, processes, and practices designed to protect computers, data, networks, and programs against

intrusion, damage, or unauthorized access by cyberattacks. It focuses on the scale and complexity of vehicles' cyber and physical components and their vulnerability to a variety of security challenges, intrusions, threats, and malicious cyberattacks, whose intent is to disrupt communication, steal sensitive information or records, and damage the functioning of the system, as well as the risk level as a function of likelihood and consequences. Hence, a solid theoretical foundation for cybersecurity of vehicle cyber-physical systems is introduced based on the concepts of artificial intelligence; deep neural networks (DNN) and deep learning (DL); control theory; epidemic theory; game theory; graph theory; and the importance of cybersecurity with regard to different kinds of attack scenarios, e.g., spear phishing attack. Furthermore, the characteristics of attack taxonomies, as well as automotive attack surfaces and vulnerabilities, are presented along with the anatomy of attack surface intrusion points in vehicles and the associated risks. However, vehicle security depends on a variety of different tools and methods that systematically perform security testing. Intrusion detection, in this regard, describes the detection of any set of actions that attempts to compromise the integrity, confidentiality, or availability of a system, whereas intrusion prevention refers to actions that attempt to prevent a detected intrusion from succeeding. Different detection methods for different kinds of intrusion types are described, including numerous static, dynamic, and hybrid methods for prevention, as well as several examples of car hacking.

Chapter 7 begins by motivating the innovative topic of mobile apps for connected cars and focuses on the current trends in Car IT and agile software development. The two major operating systems, iOS and Android, and the corresponding app markets are briefly discussed, as well as the features of application programming interfaces for mobile app development and how car manufacturers are embracing smartphone technologies by integrating Apple's and Google's hardware and software into cars' infotainment systems. Important programming languages for app development, such as Objective-C®, Swift®, and Java® App, are briefly described, followed by a detailed treatment of the design and implementation of such apps for ridesharing, carpooling, and cab sharing.

Chapter 8 discusses carsharing, analyzing the carsharing concept and the different variants of it, as well as carsharing services offered to date. It also describes significant modifications to the hardware/software infrastructure of a car required for use in the carsharing business model. The impact of electric vehicles in carsharing applications is discussed, as well as their specific system architecture, which is highlighted by a block diagram of a standard electric vehicle. Also, carsharing activities by OEMs and their brands are surveyed. Since the whole use case of carsharing relies on the constant connectivity between the car and the backend system, proper security of the used vehicles is a major concern that can be realized by intrusion detection and prevention to avert vulnerabilities through cyberattacks.

Chapter 9 presents car hailing and ridesharing services as a promising approach for reducing personal car usage in a city, thereby cutting down on the need for parking spaces, reducing traffic jams, and helping to reduce pollution. It covers online transportation network companies offering cab services/car hailing and ride hailing, which provide cab services through their respective apps for smartphones. As a case study, we analyze the mobility-on-demand services in the metropolitan area of Bangalore, India, with regard to cab types and prices, as well as services offered. The problem of safety and initiatives to increase ridesharing safety and prevent crime, both for customers and for drivers, is described in detail.

Chapter 10 deals with one of the most relevant and straightforward applications of connected cars—connected parking, including the main challenges and opportunities for connected parking. A multitude of new apps provide information, often in real-time, about available parking spaces; manage the booking, often allowing for cashless billing; and integrate with OEMs' connectivity services. The most sophisticated version to automate the complete parking process is the automated valet parking (AVP). AVP systems turn the vehicle into a robotic car that automatically finds a parking space and maneuvers the car into a free slot. The first commercial systems will be available in high-end cars soon and will also be deployed for carsharing. However, cybersecurity will have a huge impact on connected parking and AVP. Thus, the major cyber threats are analyzed, and potential solutions for increasing cybersecurity, such as intrusion detection and prevention, are discussed.

Chapter 11 gives an introduction to advanced driver assistance systems (ADAS), presenting examples of commercial ADAS. Main topics are image processing and object tracking algorithms, as well as the detection of moving objects and the respective optical flow algorithm. The implementation of an ADAS using MATLAB ® is shown as a use case for rapid prototyping using MATLAB's image processing toolbox. The chapter also presents an introductory treatment of software architectures for higher-level ADAS functions and autonomous driving. The chapter concludes with a discussion of cybersecurity and functional safety and presents a comprehensive list of further reading material.

Chapter 12 summarizes the investigation conducted by the authors of this book and gives an outlook on future trends, technologies, innovations, and applications.

Besides the methodological and technical content, all of the chapters in the book contain chapter-specific, comprehensive questions to help readers determine if they have gained the required knowledge, identify possible knowledge gaps, and conquer those gaps. Moreover, all chapters include references and suggestions for further reading.

We would like to express special thanks to Patricia Worster, University of Nebraska-Lincoln, for her excellent assistance in proofreading. We would also like to thank Wayne Wheeler and Simon Rees, Springer Publ., for their help with the organizational procedures between the publishing house and the authors.

Furthermore, we would like to thank Sainath Suni and Kavitha S.K., QSO Technologies, for supporting the proofreading process and drawing many of the illustrations for this book from sketches we drafted. The authors also would like to thank Prof. Asoke Talukder (IIIT-B emeritus), Prof. Dinesha K.V. (IIIT-B), Prof. K.L.S. Sharma (IIIT-B emeritus), Tobias Kuipers (MBRDI), Shambo Bhattarcharjee (University of Leeds), and Lynn Degrande for their valuable inputs and feedback.

Moreover, we sincerely thank our students from TUC and IIIT-B and all of the authors who have published Car IT, car hacking, cybersecurity, or smart mobility material and have directly and/or indirectly contributed to this book through citations. Finally, we would like to deeply thank our wives, Angelika and Kavitha, for their encouragement, patience, and understanding during the writing of this book.

Clausthal-Zellerfeld, Germany — Dietmar P. F. Möller
Bangalore, India — Roland E. Haas

Contents

1 Introduction 1
- 1.1 The Automotive Industry 3
- 1.2 Scope of This Book 7
- 1.3 Overview of Topics 9

References and Further Reading 11

2 The Automotive Industry 13
- 2.1 The Automotive Market 13
- 2.2 The Automotive Megatrends 19
  - 2.2.1 Tighter Emission Controls and the Rise of Electric Vehicles 20
  - 2.2.2 Car Ownership Versus Mobility 23
  - 2.2.3 Connectivity 25
  - 2.2.4 Safety and Advanced Driver Assistance Systems 26
  - 2.2.5 Autonomous Driving 28
  - 2.2.6 Digitalization 29
- 2.3 Automotive OEMs and Suppliers 30
- 2.4 New Players and Challenges 33
- 2.5 The Digital Transformation of the Automotive Industry 34
- 2.6 Exercises 37

References and Further Reading 39

3 Automotive Research and Development 45
- 3.1 The Automotive Development Process 45
  - 3.1.1 Requirements Engineering 59
  - 3.1.2 Design as a Multiparameter Optimization Problem 60
- 3.2 Automotive Modularization and Platforms 63
- 3.3 Virtual Product Creation 64
- 3.4 Product Life Cycle Management 69
  - 3.4.1 Loss of Control in Life Cycle Management 70
  - 3.4.2 Systems Engineering Approach 71
  - 3.4.3 Product Life Cycle Stages 73
  - 3.4.4 Software Life Cycle Processes 75

3.5 Exercises . . . 77
References and Further Reading . . . 79

4 Automotive E/E and Automotive Software Technology . . . 83
4.1 Mechatronic Systems in the Car . . . 83
4.2 Automotive Electronics . . . 86
4.2.1 Body Electronics . . . 89
4.2.2 Chassis Electronics . . . 92
4.2.3 Comfort Electronics . . . 94
4.2.4 Driver Assistance Electronics . . . 94
4.2.5 Electronic Control Units . . . 98
4.2.6 Entertainment/Infotainment Electronics . . . 100
4.2.7 Sensor Technology . . . 102
4.3 E/E Architectures and Topologies . . . 109
4.3.1 Objectives . . . 110
4.3.2 Architectures and Topologies . . . 111
4.3.3 Bus Systems and ISO Standards . . . 114
4.4 Functional Safety . . . 121
4.5 Automotive Software Engineering . . . 126
4.5.1 Increasing Software Content and Product Complexity . . . 127
4.5.2 Model-Based Development . . . 130
4.5.3 Hardware-in-the-Loop Tests . . . 133
4.6 AUTOSAR . . . 142
4.7 AUTOSAR Adaptive Platform . . . 147
4.8 GENIVI . . . 147
4.9 Example: Advanced Driver Assistance System . . . 149
4.9.1 ADAS Functionalities . . . 151
4.9.2 ADAS Sensor Types . . . 155
4.9.3 Pros and Cons of the ADAS Sensor Suite . . . 162
4.10 Trends . . . 163
4.11 Exercises . . . 164
References and Further Reading . . . 167

5 The Connected Car . . . 171
5.1 Cyber-Physical Systems . . . 171
5.1.1 Introduction to Cyber-Physical Systems . . . 172
5.1.2 Cyber-Physical Systems Design Recommendations . . . 180
5.1.3 Cyber-Physical Systems Requirements . . . 184
5.1.4 Cyber-Physical Control Systems . . . 189
5.1.5 Cyber-Physical Vehicle Tracking . . . 200
5.2 Internet of Things . . . 206
5.2.1 Internet of Things Enabling Technologies . . . 208
5.2.2 RFID and WSN Technology . . . 210

5.3 Telematics, Infotainment, and the Evolution of the Connected Car . . . 214
5.3.1 Telematics . . . 215
5.3.2 Infotainment . . . 222
5.3.3 Evolution of the Connected Car . . . 224
5.4 Platforms and Architectures . . . 233
5.4.1 Connected Car Architecture and Challenges . . . 234
5.4.2 Connected Car Reference Platform . . . 237
5.4.3 Connected Car in the Cloud . . . 238
5.5 Autonomous Vehicles . . . 241
5.6 GENIVI Alliance . . . 247
5.7 Case Studies . . . 249
5.7.1 BMW ConnectedDrive Store . . . 249
5.7.2 Mercedes COMAND Online . . . 252
5.7.3 HERE: Digital Maps for Fully Autonomous Driving . . . 254
5.8 Exercises . . . 257
References and Further Reading . . . 260

6 Automotive Cybersecurity . . . 265
6.1 Introduction to Cybersecurity . . . 266
6.1.1 Cybersecurity and Vulnerability . . . 272
6.1.2 Artificial Intelligence . . . 272
6.1.3 Control Theory . . . 282
6.1.4 Epidemic Theory . . . 284
6.1.5 Game Theory . . . 287
6.1.6 Graph Theory . . . 291
6.1.7 Importance of Cybersecurity . . . 294
6.1.8 Automotive IT and Cybersecurity . . . 302
6.1.9 Attack Value Chain . . . 307
6.1.10 Holistic Cybersecurity Solutions . . . 309
6.2 IT Security in Automotive Cyber-Physical Systems . . . 316
6.2.1 Vehicle Network Technologies and Cybersecurity . . . 322
6.2.2 Cyberattack Taxonomy . . . 326
6.3 Hacking and Automotive Attack Surfaces and Vulnerabilities . . . 329
6.3.1 Hacking . . . 329
6.3.2 Automotive Attack Surfaces and Vulnerabilities . . . 330
6.4 Intrusion Detection and Prevention . . . 340
6.4.1 Intrusion Detection . . . 340
6.4.2 Intrusion Prevention . . . 343
6.5 Functional Safety and Security . . . 350
6.5.1 Security for Wireless Mobile Networks . . . 350
6.5.2 Security for Sensor Networks . . . 354
6.5.3 Platform Security . . . 356

6.5.4 Cloud Computing and Data Security . . . 357
6.5.5 Functional Safety . . . 360
6.6 Car Hacking Examples . . . 362
6.6.1 2010: Vehicles Disabled Remotely via Web Application . . . 363
6.6.2 2010 and 2011 CAESS Experimental Analysis . . . 364
6.6.3 2013 Miller and Valasek Physical Hack . . . 365
6.6.4 2015 Miller and Valasek Remote Hack . . . 367
6.7 Exercises . . . 368
References and Further Reading . . . 371

7 Mobile Apps for the Connected Car . . . 379
7.1 Automotive IT . . . 380
7.1.1 IT Management and Systems in the Automotive Industry . . . 382
7.2 Agile Software Development . . . 384
7.2.1 Challenges and Two-Speed IT . . . 387
7.3 The Smartphone and App Market . . . 388
7.4 iOS . . . 389
7.4.1 The History of iOS . . . 389
7.4.2 The iOS Platform . . . 390
7.4.3 The iOS Architecture . . . 390
7.5 Xcode . . . 393
7.6 Android . . . 395
7.7 iOS and Android in the Car . . . 397
7.8 Objective-C, Swift, and Java App Development . . . 398
7.8.1 Objective-C . . . 398
7.8.2 Swift . . . 403
7.8.3 Java . . . 404
7.9 A Ride-Sharing Example . . . 404
7.9.1 Core Use Cases . . . 405
7.9.2 OOA . . . 407
7.9.3 Design . . . 412
7.9.4 The Ridematching Algorithm . . . 413
7.9.5 Using Google Maps . . . 415
7.9.6 A Code Walk Through . . . 417
7.10 Summary and Recommended Readings . . . 431
7.11 Exercises . . . 433
References and Further Readings . . . 435

8 Carsharing . . . 439
8.1 The Carsharing Concept . . . 439
8.2 Example car2go . . . 441
8.3 Use Cases and Requirement Analysis for Carsharing . . . 442
8.4 Hardware/Software Modifications for Carsharing . . . 446
8.5 Electric Vehicles and Carsharing . . . 447

8.6 Carsharing Activities by Other OEMs . . . 452
8.7 Cyber Attack Surfaces and Mitigation of Cyber Attacks . . . 453
8.8 Conclusion . . . 454
8.9 Exercises . . . 455
References and Further Reading . . . 457

9 Car Hailing and Ridesharing . . . 461
9.1 Introduction . . . 461
9.2 Ride-Hailing Companies and Taxi Aggregators . . . 463
9.3 Example Bangalore . . . 468
9.3.1 Cab Types and Prices . . . 468
9.3.2 Services . . . 470
9.4 Surge Prices . . . 472
9.5 Safety in Ridesharing . . . 472
9.5.1 Problem Background . . . 473
9.5.2 Initiatives to Increase Safety . . . 474
9.5.3 Reported Crime Incidents in Ridesharing . . . 476
9.5.4 Government Policies for Ridesharing Companies . . . 477
9.5.5 Legal Cases and Accusations . . . 478
9.6 Cyberattacks and Cybersecurity in Ridesharing . . . 478
9.7 Conclusion . . . 479
9.8 Exercises . . . 479
References and Further Reading . . . 480

10 Connected Parking and Automated Valet Parking . . . 485
10.1 Parking . . . 486
10.2 Connected Parking . . . 487
10.3 Parking Assistance . . . 492
10.4 Automated Valet Parking . . . 493
10.5 Cyber Threats . . . 496
10.6 Intrusion Detection and Prevention . . . 497
10.6.1 Types of Intrusion Detection Systems . . . 497
10.6.2 Attacks Against Connected Cars . . . 498
10.6.3 Artificial Neural Network-Based IDS Implementation . . . 500
10.7 Conclusion and Recommended Readings . . . 503
10.7.1 Cyber Threats and Cybersecurity . . . 503
10.7.2 Recommended Readings . . . 504
10.8 Exercises . . . 504
References and Further Reading . . . 507

11 Advanced Driver Assistance Systems and Autonomous Driving . . . 513
11.1 Advanced Driver Assistance Systems . . . 514
11.2 Lane Departure Warning, Lane Keep Assistance, Obstacle Detection, and Crossing Assistance . . . 518
11.2.1 Lane Keeping and Lane Change Assistance . . . 518
11.2.2 Crossing Assistance . . . 523

11.3 Image Processing and Image Analysis . . . 525
11.3.1 Computer Vision and Machine Vision . . . 525
11.3.2 Basic Principles of Image Processing . . . 526
11.3.3 Detection of Moving Objects . . . 533
11.3.4 Optical Flow Algorithm . . . 538
11.3.5 Implementation Using MATLAB . . . 542
11.4 Autonomous Driving . . . 549
11.5 Regulations, Public Acceptance, and Liability Issues . . . 558
11.5.1 Regulations and On-Road Approval . . . 558
11.5.2 Toward a Statutory Framework for Autonomous Driving . . . 558
11.5.3 Acceptance of Autonomous Driving and Ethical Difficulties . . . 559
11.5.4 Test on the Autobahn . . . 560
11.6 E/E Architectures and Middleware for Autonomous Driving . . . 561
11.7 Cybersecurity and Functional Safety . . . 566
11.8 Summary, Conclusion, and Recommended Readings . . . 569
11.8.1 Recommended Reading . . . 570
11.9 Exercises . . . 571
References and Further Readings . . . 572

12 Summary, Final Remarks, Outlook, and Further Reading . . . 581
12.1 Summary . . . 581
12.2 Final Remarks: Wind of Change . . . 583
12.2.1 Frugal Engineering . . . 583
12.2.2 Rise of Asian Markets . . . 584
12.2.3 E-Mobility . . . 585
12.2.4 Fuel Cells . . . 585
12.2.5 Connected Cars . . . 585
12.2.6 Shared Mobility . . . 586
12.2.7 Autonomous Driving . . . 586
12.2.8 Automotive Cybersecurity . . . 587
12.3 Outlook and Further Reading . . . 588
12.3.1 Outlook . . . 588
12.3.2 Further Reading . . . 590
References and Further Readings . . . 591

Glossary . . . 595

Index . . . 623

About the Authors

Dietmar P. F. Möller is a professor in the Institute of Applied Stochastics and Operations Research at Clausthal University of Technology (TUC), Germany; a member of the Simulation Science Center (SWZ) Clausthal-Göttingen, Germany; an adjunct professor in the Department of Electrical and Computer Engineering at the University of Nebraska-Lincoln (UNL), USA; and an adjunct professor in the Department of Electrical and Computer Engineering at the University of Alabama in Huntsville (UAH), USA. He is also a member of the Board of the AMSC (Alabama Modeling and Simulation Council), USA. His other publications include the Springer titles *Introduction to Transportation Analysis, Modeling and Simulation* (2014) and *Guide to Computing Fundamentals in Cyber-Physical Systems* (2016).

Roland E. Haas is the founder and CEO of QSO Technologies in Bangalore, India. He has more than 20 years of professional experience in senior techno-managerial, business innovation, and business development assignments in Germany, the USA, India, and Japan with broad experience in automotive R&D, aerospace R&D, engineering and IT services, as well as consulting and strategy. As an entrepreneur, he shares his knowledge as a mentor for startups. He is a book author and a honorary professor at the International Institute of Information Technology (IIIT-B) and an adjunct faculty member of the Indian Institute of Science (IISc). His teachings are in mechatronics, automotive electronics, Car IT, automotive software technologies, information management, and virtual product creation.