# Preface
 PREFACE xv

# Notes
 CONTENTS xvii

# Acknowledgments
 ACKNOWLEDGMENTS xix

# Prologue
 PROLOGUE xxii

## CHAPTER 1
 INTRODUCTION 1

1.1 Road-Vehicles and Non-Road Mobile Machinery 1

1.2 The History of Automotive Electronics 4

1.3 Standardization 9

1.3.1 The Advantages of Standardization 9

1.3.2 ISO 9

1.3.3 SAE International 11

1.3.4 ASAM 11

1.3.5 TMC 11

1.3.6 AUTOSAR 12

1.4 Legislation 12

1.4.1 European Directives and Regulations 12

1.4.1.1 European Vehicle Categories 12

1.4.2 Cal-EPA and California Code of Regulations (CCR) 13

1.4.2.1 Vehicle Categories 14

1.4.3 US EPA and Federal Code of Regulations (CFR) 14

1.4.4 UN Global Technical Regulations (GTR) 15

1.4.5 US National Highway Traffic Safety Administration (NHTSA) 15

1.5 Legislated OBD 16

1.5.1 Introduction 16

1.5.2 European OBD Directives and Regulations 16

1.5.2.1 Euro 5 and Euro 6 16

1.5.2.2 Euro VI for Heavy-Duty Road-Vehicles 17

1.5.2.3 European Stage V Non-Road Emission Standards 17

1.5.3 CCR Title 13 Sections 1968 and 1971 18

1.5.4 US EPA Title 40 CFR 18

1.5.5 UN GTR No. 5 18

1.6 Electronic Control Units and E/E Systems 18

1.6.1 Introduction 18

1.6.2 Environmental Requirements 22
1.6.3 Power Supply 22
1.6.4 ECU Hardware 23
  1.6.4.1 Overview 23
  1.6.4.2 Memory (RAM, ROM) 23
  1.6.4.3 Analog-to-Digital and Digital-to-Analog Converter (ADC and DAC) 24
1.6.5 ECU Software 25
  1.6.5.1 Introduction 25
  1.6.5.2 Self-Diagnosis Functions 27
1.7 Chapter Questions 27

CHAPTER 2

Data Communication 29
2.1 Introduction 29
2.2 Coded Information 30
2.3 Numbering Systems 31
  2.3.1 Decimal Numbers 31
  2.3.2 Binary Numbers 31
  2.3.3 Hexadecimal Numbers 32
  2.3.4 Conversion Between Numbering Systems 32
  2.3.5 Computational Methods 33
2.4 ASCII Code 34
2.5 UNICODE 36
2.6 On-Board Communication 37
2.7 Diagnostic Communication 39
2.8 Client-Server Model and Peer-to-Peer Architecture 41
2.9 The OSI Model 42
2.10 Chapter Questions 43

CHAPTER 3

In-Vehicle Networks 45
3.1 History and Overview 45
3.2 Technical Introduction 46
  3.2.1 Network Topologies 46
  3.2.2 Data Rate, Bit Rate, Baud Rate, and Bandwidth 48
  3.2.3 Determinism and Real-Time Behavior 48
  3.2.4 Bus Access and Arbitration 48
3.3 SAE J1850, SAE J1708, and SAE J1587 49
  3.3.1 SAE J1850 PWM and SAE J1850 VPW 49
  3.3.2 SAE J1708 and SAE J1587 49

3.4 K-Line 50

3.5 Controller Area Network (CAN) 51
  3.5.1 History and Introduction 51
  3.5.2 Classical CAN 54
    3.5.2.1 High-Speed, Low-Speed, and Single-Wire CAN 54
    3.5.2.2 CAN Identifier (CAN-ID) 56
    3.5.2.3 Arbitration 57
    3.5.2.4 CAN Matrix 59
  3.5.3 CAN FD 60
  3.5.4 Residual Bus Simulation 62

3.6 SAE J1939 63
  3.6.1 Overview 63
  3.6.2 Physical Layer (J1939-1x) 64
  3.6.3 Data Link Layer (J1939-21) – Message Format 66
    3.6.3.1 PF and PS Field 67
  3.6.4 Transport Protocols 69

3.7 ISOBUS (ISO 11783) 69
  3.7.1 ISOBUS Data Link Layer 71
  3.7.2 ISOBUS Transport Protocols 71
  3.7.3 Agricultural Industry Electronics Foundation (AEF) 71

3.8 Local Interconnect Network (LIN) 71
  3.8.1 History and Overview 71
  3.8.2 Physical Layer Specification 74
  3.8.3 Protocol Specification 74
  3.8.4 Frame Types 75
    3.8.4.1 Unconditional Frames 75
    3.8.4.2 Event-Triggered Frames 76
    3.8.4.3 Sporadic Frames 76
    3.8.4.4 Diagnostic Frames 76

3.9 FlexRay 76
  3.9.1 History and Overview 76
  3.9.2 Physical Layer 77
  3.9.3 Data Link Layer 78
    3.9.3.1 FlexRay Communication Cycle 78
    3.9.3.2 Communication in the Static Segment 79
    3.9.3.3 Communication in the Dynamic Segment 80
    3.9.3.4 FlexRay Frame Format 80
  3.9.4 Clock Synchronization 81
  3.9.5 System Parameters 81
3.10 Multimedia Networks  
3.10.1 Introduction  
3.10.2 Media Oriented Systems Transport (MOST)  
3.10.2.1 MOST Frames  
3.10.3 IDB 1349 and ISO 22902  
3.11 Automotive Ethernet  
3.11.1 History and Introduction  
3.11.2 Ethernet as In-Vehicle Network  
3.11.3 Data Link Layer  
3.11.3.1 MAC Addresses  
3.12 Network Domains and E/E Architectures  
3.12.1 Comparison of In-Vehicle Networks  
3.12.2 Interconnection of In-Vehicle Networks  
3.13 Chapter Questions  

CHAPTER 4  

Application Layer Protocols  

4.1 Introduction  
4.1.1 Legislated OBD and Enhanced Diagnostics  
4.1.2 Diagnostic Protocol Stacks  
4.1.3 Naming Conventions  
4.1.4 Diagnostic Services  
4.1.5 Service Identifier (SID)  
4.1.6 Negative Responses and Response Codes (NRC)  
4.1.7 Physical and Functional Addressing  
4.1.8 Diagnostic Trouble Codes (DTCs)  
4.1.8.1 Introduction  
4.1.8.2 Base DTCs  
4.1.8.3 Extended DTCs  

4.2 Legislated OBD II Protocols (ISO 15031 and SAE J1979)  
4.2.1 Introduction and Overview  
4.2.2 ISO 15765-4  
4.2.3 OBD II Application Layer Services (OBD Modes)  
4.2.4 OBD II Service Parameters  

4.3 Unified Diagnostic Services (UDS)  
4.3.1 History and Overview  
4.3.2 Service Parameter  
4.3.2.1 Sub-Function Byte  
4.3.2.2 Data Identifier (DID)  
4.3.3 Negative Response Codes (NRCs)  


4.3.4 Application Layer Services (ISO 14229-1) 116

4.3.4.1 Diagnostic Session Control (0x10) 116
4.3.4.2 ECU Reset (0x11) 118
4.3.4.3 Clear Diagnostic Information (0x14) 118
4.3.4.4 Read DTC Information (0x19) 118
4.3.4.5 Read Data by Identifier (0x22) 118
4.3.4.6 Read Memory by Address (0x23) 120
4.3.4.7 Read Scaling Data By Identifier (0x24) 120
4.3.4.8 Security Access (0x27) 121
4.3.4.9 Communication Control (0x28) 121
4.3.4.10 Read Data by Periodic Identifier (0x2A) 122
4.3.4.11 Dynamically Define Data Identifier (0x2C) 122
4.3.4.12 Write Data by Identifier (0x2E) 122
4.3.4.13 Input/Output Control by Identifier (0x2F) 122
4.3.4.14 Routine Control (0x31) 122
4.3.4.15 Request Download (0x34) 122
4.3.4.16 Request Upload (0x35) 123
4.3.4.17 Transfer Data (0x36) 123
4.3.4.18 Request Transfer Exit (0x37) 123
4.3.4.19 Request File Transfer (0x38) 123
4.3.4.20 Tester Present (0x3E) 123
4.3.4.21 Write Memory by Address (0x3D) 123
4.3.4.22 Access Timing Parameters (0x83) 124
4.3.4.23 Secured Data Transmission (0x84) 124
4.3.4.24 Control DTC Setting (0x85) 124
4.3.4.25 Response on Event (0x86) 124
4.3.4.26 Link Control (0x87) 124

4.4 UDS on x 124

4.4.1 UDS on CAN (ISO 14229-3) 125
4.4.2 UDS on FlexRay (ISO 14229-4) 125
4.4.3 UDS on IP (ISO 14229-5) 125
4.4.4 UDS on K-Line (ISO 14229-6) 125
4.4.5 UDS on LIN (ISO 14229-7) 125

4.5 Worldwide Harmonized OBD (ISO 27145) 126

4.5.1 Introduction 126
4.5.2 WWH-OBD Services 127

4.6 Heavy-Duty OBD (SAE J1939-73) 127

4.6.1 Introduction 127
4.6.2 Diagnostic Messages 127
4.6.2.1 DM1 129

4.7 ISOBUS (ISO 11783-12) 131

4.8 Chapter Questions 131
External Test Equipment

7.1 Introduction

7.2 Diagnostic Link Connector (DLC)

7.3 Vehicle Communication Interfaces (VCIs)

7.4 Tester Platforms

7.5 TST-to-VCI Connections
7.5.3 Bluetooth® 204
7.5.4 Wireless LAN (WLAN) 205
7.6 VCI-to-DLC Connections 206
7.7 OEM-Specific Test Equipment 206
  7.7.1 Development of Control Units 206
  7.7.2 Production of Control Units 208
  7.7.3 Development of Vehicles 208
  7.7.4 Production of Vehicles 208
  7.7.5 Aftersales Service 209
7.8 Data-Driven Diagnostic Tester 211
7.9 Generic Tester Software (ISO 22900) 212
  7.9.1 ASAM Goes ISO 212
  7.9.2 MVCI D-Server 214
  7.9.3 D-Server API (ISO 22900-3) 215
  7.9.4 OTX Runtime (OTX RT) 216
7.10 Smart Diagnostic Engine (SDE) 217
7.11 Chapter Questions 218

CHAPTER 8

Applications 221

8.1 Read Vehicle Identification Number (VIN) 221
  8.1.1 Introduction 221
  8.1.2 Read VIN with SAE J1979 222
  8.1.3 Read VIN with UDS (ISO 14229-1) 223
  8.1.4 Read VIN with WWH-OBD (ISO 27145-3) 224
  8.1.5 Read VIN with HD-OBD (SAE J1939-73) 224
8.2 Reprogramming with UDS 224
  8.2.1 Introduction 224
  8.2.2 S-Records 225
  8.2.3 Programmable Memory 226
  8.2.4 Boot Loader and Flashloader 228
  8.2.5 Reprogramming Procedures 228
  8.2.6 Flash Performance 230
  8.2.7 Reprogramming Examples 231
    8.2.7.1 Liebherr Control Units 231
    8.2.7.2 VINING 2000 233
8.3 Chapter Questions 233
### CHAPTER 9

**Diagnostics 4.0**  
235

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>9.1 Introduction</strong></td>
<td>235</td>
</tr>
<tr>
<td><strong>9.2 Connectivity (V2X) and Automation</strong></td>
<td>236</td>
</tr>
<tr>
<td><strong>9.3 Remote Data Acquisition</strong></td>
<td>237</td>
</tr>
<tr>
<td>9.3.1 Use-Case Example</td>
<td>239</td>
</tr>
<tr>
<td><strong>9.4 Wired DLC and Wireless Data Links</strong></td>
<td>240</td>
</tr>
<tr>
<td>9.4.1 Wired DLC</td>
<td>240</td>
</tr>
<tr>
<td>9.4.2 Wireless Data Links</td>
<td>241</td>
</tr>
<tr>
<td><strong>9.5 E/E System Architectures</strong></td>
<td>241</td>
</tr>
<tr>
<td><strong>9.6 Automotive Cybersecurity</strong></td>
<td>243</td>
</tr>
<tr>
<td>9.6.1 Introduction</td>
<td>243</td>
</tr>
<tr>
<td>9.6.2 History of Incidents</td>
<td>245</td>
</tr>
<tr>
<td>9.6.3 Hacker</td>
<td>245</td>
</tr>
<tr>
<td>9.6.4 Standardization vs. Security by Obscurity</td>
<td>246</td>
</tr>
<tr>
<td>9.6.5 Cryptography</td>
<td>247</td>
</tr>
<tr>
<td>9.6.6 Passwords</td>
<td>249</td>
</tr>
<tr>
<td>9.6.7 Brute-Force Attack</td>
<td>251</td>
</tr>
<tr>
<td>9.6.8 Hash Functions</td>
<td>251</td>
</tr>
<tr>
<td>9.6.9 Message Authentication Code (MAC)</td>
<td>252</td>
</tr>
<tr>
<td>9.6.10 DoS Attacks</td>
<td>252</td>
</tr>
<tr>
<td>9.6.11 Social Engineering</td>
<td>252</td>
</tr>
<tr>
<td><strong>9.7 Security Analysis of a Cyber-Physical System for Remote Diagnostics</strong></td>
<td>253</td>
</tr>
<tr>
<td>9.7.1 Introduction</td>
<td>253</td>
</tr>
<tr>
<td>9.7.2 DLC Security</td>
<td>254</td>
</tr>
<tr>
<td><strong>9.7.3 Diagnostic Services Security</strong></td>
<td>258</td>
</tr>
<tr>
<td>9.7.3.1 Introduction</td>
<td>258</td>
</tr>
<tr>
<td>9.7.3.2 ECU Reset (0x11)</td>
<td>260</td>
</tr>
<tr>
<td>9.7.3.3 Request Control of On-Board System, Test, or Component (0x08)</td>
<td>260</td>
</tr>
<tr>
<td>9.7.3.4 Security Access (0x27)</td>
<td>260</td>
</tr>
<tr>
<td>9.7.3.5 Communication Control (0x28)</td>
<td>261</td>
</tr>
<tr>
<td>9.7.3.6 Authentication (0x29)</td>
<td>261</td>
</tr>
<tr>
<td>9.7.3.7 Routine Control (0x31)</td>
<td>262</td>
</tr>
<tr>
<td>9.7.3.8 Input/Output Control By Identifier (0x2F)</td>
<td>262</td>
</tr>
<tr>
<td>9.7.3.9 Secured Data Transmission (0x84)</td>
<td>262</td>
</tr>
<tr>
<td><strong>9.7.4 Control Unit Security</strong></td>
<td>263</td>
</tr>
<tr>
<td>9.7.4.1 Firmware Updates</td>
<td>263</td>
</tr>
<tr>
<td>9.7.4.2 Disabling Unused Services</td>
<td>263</td>
</tr>
</tbody>
</table>