

# Contents

Preface	<u>ix</u>
About the Authors	<u>xi</u>

## CHAPTER 1

<b>Introduction to Automotive Cybersecurity</b>	<b><u>1</u></b>
<b>What Is Cybersecurity?</b>	<b><u>1</u></b>
<b>What Does “Cybersecurity” Mean in the Automotive Context?</b>	<b><u>3</u></b>
<b>Key Concepts and Definitions</b>	<b><u>4</u></b>

## CHAPTER 2

<b>Cybersecurity for Automotive Cyber-physical Systems</b>	<b><u>7</u></b>
<b>Relationship between Cybersecurity, Functional Safety, and Other Disciplines</b>	<b><u>8</u></b>
<b>What Does “Cybersecurity” Mean in the Automotive Context?</b>	<b><u>15</u></b>
<b>The Vehicle Attack Surface</b>	<b><u>17</u></b>
Wireless Interfaces	<u>18</u>
Long-Range Wireless Communications	<u>18</u>
Short-Range Wireless Communications	<u>20</u>
Wired Interfaces	<u>22</u>
In-Vehicle Networks	<u>24</u>
ECUs	<u>25</u>
<b>Attack Paths and Stepping Stones</b>	<b><u>27</u></b>
<b>Addressing Cybersecurity—People, Process, and Technology</b>	<b><u>29</u></b>
Management of Cybersecurity	<u>29</u>
Cybersecurity Engineering	<u>30</u>
Skills Required for Cybersecurity	<u>31</u>
Technology	<u>32</u>

**CHAPTER 3**

<b>Establishing a Cybersecurity Process</b>	<b><u>35</u></b>
<b>General Aspects of a Cybersecurity Process</b>	<b><u>35</u></b>
<b>Standards and Best Practice</b>	<b><u>36</u></b>
<b>Cybersecurity Lifecycle</b>	<b><u>37</u></b>
<b>Management of Cybersecurity</b>	<b><u>40</u></b>
Top Management Commitment	<u>40</u>
Cybersecurity Processes	<u>40</u>
Cybersecurity Culture	<u>40</u>
Roles and Responsibilities	<u>41</u>
Cybersecurity Awareness and Competence	<u>41</u>
Continuous Improvement	<u>42</u>
Information Sharing	<u>42</u>
<b>Proactive Cybersecurity Engineering</b>	<b><u>42</u></b>
Cybersecurity Responsibilities at Project Level	<u>43</u>
Cybersecurity Planning	<u>44</u>
Concept Phase	<u>46</u>
Item Definition	<u>46</u>
Threat Analysis and Risk Assessment	<u>46</u>
Risk Treatment and Cybersecurity Goals	<u>47</u>
CAL	<u>48</u>
Cybersecurity Requirements and Controls	<u>49</u>
Design Verification	<u>51</u>
Cybersecurity Testing	<u>51</u>
Cybersecurity Testing Challenges	<u>51</u>
Cybersecurity Testing at Different Lifecycle Phases	<u>52</u>
Cybersecurity Testing Activities	<u>53</u>
Vulnerability Analysis and Management	<u>54</u>
<b>Cybersecurity during Production</b>	<b><u>55</u></b>
<b>Reactive Cybersecurity Engineering</b>	<b><u>56</u></b>
Cybersecurity Monitoring	<u>56</u>
Evaluation of Cybersecurity Events	<u>57</u>
Detecting and Responding to Attacks	<u>58</u>
Cybersecurity Incident Response	<u>58</u>
Assessing the Effectiveness of Detection and Response	<u>59</u>
Updates	<u>60</u>

End of Cybersecurity Support	<u>61</u>
Decommissioning	<u>61</u>
The Aftermarket	<u>61</u>

## CHAPTER 4

### Assurance and Certification 63

#### Assurance Activities 64

Validation	<u>64</u>
Assurance Case	<u>65</u>
Audit	<u>69</u>
Assessment	<u>71</u>
Certification	<u>72</u>
Type Approval	<u>74</u>

#### Assurance Summary 75

## CHAPTER 5

### Conclusions and Going Further 77

#### Frequently Asked Questions 80

What Is the Difference between UN Regulation 155 and ISO/SAE 21434?	<u>81</u>
To Which Types of Vehicles Does UN Regulation 155 Apply?	<u>81</u>
To Which Types of Organization Does ISO/SAE 21434 Apply?	<u>81</u>
How Do You Audit for Conformance to ISO/SAE 21434?	<u>81</u>
Is It Mandatory to Be Certified against ISO/SAE 21434?	<u>82</u>
Do I Have to Use ISO/SAE 21434 for My Cybersecurity Processes?	<u>82</u>
How Do I Know If My Item or Component Is Cybersecurity Relevant?	<u>82</u>
The Various Analysis Activities for Cybersecurity Engineering Look Very Time Consuming; How Do I Know When I Have Done Enough?	<u>82</u>
Does ISO/SAE 21434 Define Which Cybersecurity Tests Should Be Carried Out?	<u>83</u>

#### References 85

#### Index 91