

---

Philipp Veronesi · Manuel Sandler

# Automotive Cybersecurity

The Essential Guide to ISO/SAE 21434

How to manage the challenges of the new  
automotive cybersecurity standards and regulations

**CYRES**  
CONSULTING

---

## About the Authors



**Philipp Veronesi** is founder and managing director of CYRES Consulting, one of the leading automotive cybersecurity consultancies with headquarters in Munich, Germany, and a branch office in Riga, Latvia. In addition to its consulting services for OEMs, leading global Tier-1 suppliers and beyond, CYRES also runs the CYRES Academy which has established itself as a highly reputable global provider of advanced education, certified training and coaching in the field of applied cybersecurity in the automotive industry. Philipp Veronesi has many years of practical experience not only in engineering but also in the management of technically challenging development projects for leading players in the automotive industry, including BMW, Audi, Rolls Royce, and others.



**Manuel Sandler** is Associate Partner at CYRES Consulting and is responsible for the technical project business and the building of new knowledge in the fast-moving field of cybersecurity in the automotive industry. Manuel Sandler has many years of experience in global project and process management in various parts of the value chain, including OEMs and Tier-1. He is Provisional Assessor in ASPICE and an expert in Engineering Process Development, ISO 26262, ISO/IEC 15288 and ISO/SAE 21434 Road Vehicles - Cybersecurity Engineering, to which he contributed as a member of the Working Group.

---

# Content Overview

<b>Preface</b>	<b>i</b>
<b>How to Use This Practical Guide</b>	<b>iv</b>
<b>List of Figures</b>	<b>xiii</b>
<b>List of Tables</b>	<b>xvii</b>
<b>Acronyms</b>	<b>xix</b>
<b>1 Cybersecurity Awareness</b>	<b>1</b>
<b>2 Regulations, Standards, and Initiatives</b>	<b>25</b>
<b>3 Automotive Cybersecurity Ecosystem</b>	<b>73</b>
<b>4 Cybersecurity Management</b>	<b>103</b>
<b>5 Cybersecurity Development</b>	<b>159</b>
<b>6 Cybersecurity Risk Assessment</b>	<b>195</b>
<b>7 Cybersecurity Implementation</b>	<b>249</b>
<b>8 Cybersecurity Controls</b>	<b>287</b>
<b>9 Cybersecurity Verification and Validation</b>	<b>333</b>
<b>10 Conclusion</b>	<b>357</b>
<b>Annex A Terms and Definitions</b>	<b>359</b>
<b>Annex B ISO/SAE DIS 21434 Requirements Mapping</b>	<b>364</b>
<b>Annex C ISO/SAE DIS 21434 Work Product List</b>	<b>379</b>
<b>Annex D Cybersecurity Development Interface Agreement</b>	<b>392</b>
<b>Annex E Methods for Verification and Testing</b>	<b>401</b>
<b>Annex F Requirements from UN Regulation No. 155</b>	<b>404</b>
<b>Annex G Characteristics for Good Requirements</b>	<b>416</b>
<b>Annex H Breakdown of Cybersecurity Plan</b>	<b>418</b>
<b>Bibliography</b>	<b>425</b>

# Table of Contents

<b>Preface</b>	<b>i</b>
<b>How to Use This Practical Guide</b>	<b>iv</b>
<b>List of Figures</b>	<b>xiii</b>
<b>List of Tables</b>	<b>xvii</b>
<b>Acronyms</b>	<b>xix</b>
<b>1 Cybersecurity Awareness</b>	<b>1</b>
1.1 Cybersecurity incidents are not new . . . . .	3
1.1.1 Experimental hack of a modern automobile (2010) . . . . .	3
1.1.2 Jeep hack (2015) . . . . .	4
1.1.3 Other relevant hacks . . . . .	6
1.2 The value at risk from cybercrime . . . . .	10
1.2.1 Risks for organizations . . . . .	10
1.2.2 Risks for individuals . . . . .	12
1.3 Enablers vs. inhibitors of cybersecurity . . . . .	13
1.3.1 The industry’s view on cybersecurity . . . . .	13
1.3.2 Challenges and pressures faced by OEMs and Tier-N suppliers . . . . .	14
1.3.3 Inhibitors of cybersecurity . . . . .	15
1.3.4 Cybersecurity as a business enabler . . . . .	17
1.4 Key trends impacting automotive cybersecurity . . . . .	18
1.4.1 Autonomous driving . . . . .	19
1.4.2 Electric vehicles . . . . .	20
1.4.3 Connectivity and digitalization . . . . .	21
1.4.4 Shared mobility . . . . .	23
1.4.5 Further drivers of cybersecurity in the automotive industry	23
<b>2 Regulations, Standards, and Initiatives</b>	<b>25</b>
2.1 Upcoming regulations . . . . .	25
2.1.1 The difference between standards, regulations, and laws . . . . .	25
2.1.2 UNECE WP.29 GRVA – Regulations No. 155 on cyberse- curity and No. 156 on software updates . . . . .	27

2.1.3	Impact and outreach of the UN Regulations No. 155 and No. 156 . . . . .	28
2.1.4	Scope of the regulations . . . . .	28
2.1.5	UN Regulation No. 155 on cybersecurity . . . . .	29
2.1.6	UN Regulation No. 156 on software updates . . . . .	33
2.1.7	Rethinking cybersecurity along the value chain . . . . .	35
2.1.8	Preparing the value chain for compliance . . . . .	36
2.2	Standardizing cybersecurity engineering . . . . .	36
2.2.1	Existing cybersecurity standards . . . . .	37
2.2.2	ISO/SAE 21434 – Road vehicles – Cybersecurity engineering . . . . .	39
2.2.3	ISO 24089 - Road vehicles - Software update engineering . . . . .	44
2.2.4	Ensuring compliance with the UN Regulations by means of ISO standards . . . . .	45
2.3	Cybersecurity related regulations, standards, and guidelines . . . . .	47
2.3.1	Towards a holistic approach to automotive cybersecurity . . . . .	48
2.3.2	Developing automotive cybersecurity as a holistic concept . . . . .	48
2.3.3	Mandatory and recommended references relevant to automotive cybersecurity . . . . .	53
2.4	The role of governments and authorities . . . . .	59
2.4.1	Europe-based cybersecurity authorities and frameworks . . . . .	60
2.4.2	US-based authorities and frameworks relevant to cybersecurity . . . . .	61
2.4.3	Cybersecurity authorities and frameworks in Asia/Pacific . . . . .	62
2.4.4	Authorities and frameworks with a focus on automotive cybersecurity . . . . .	63
2.4.5	Cybersecurity addressed in laws and regulations . . . . .	63
2.5	Relevant initiatives and public resources . . . . .	64
2.5.1	Hacking conventions . . . . .	64
2.5.2	Public resources . . . . .	66
2.5.3	Conferences . . . . .	67
2.5.4	Funded projects . . . . .	68
2.5.5	Benefits of initiatives and public resources . . . . .	70
<b>3</b>	<b>Automotive Cybersecurity Ecosystem</b> . . . . .	<b>73</b>
3.1	Revolution of the ecosystem . . . . .	73
3.2	Collaboration and engagement with relevant third parties . . . . .	75
3.3	The ecosystem impacts of cybersecurity . . . . .	77
3.4	Attack surface of modern vehicles . . . . .	80
3.4.1	Attack vectors in automobiles . . . . .	81
3.4.2	Attack vectors in backend infrastructures of the connected vehicle . . . . .	83
3.5	Vehicle communication . . . . .	84
3.5.1	In-vehicle communication . . . . .	84
3.5.2	V2X communication . . . . .	88

3.5.3	Safety and cybersecurity implications of V2X . . . . .	90
3.6	Cybersecurity throughout the product lifecycle . . . . .	91
3.6.1	Research, concept and development . . . . .	92
3.6.2	Production . . . . .	94
3.6.3	Logistics and sales . . . . .	95
3.6.4	Operations and maintenance . . . . .	95
3.6.5	Decommissioning and end of support . . . . .	96
3.6.6	Adopting a cybersecurity lifecycle for the ecosystem . . . . .	97
<b>4</b>	<b>Cybersecurity Management</b>	<b>103</b>
4.1	Cybersecurity management at the organizational level . . . . .	104
4.1.1	Pre-conditions for organizational cybersecurity . . . . .	104
4.1.2	Continuous cybersecurity activities . . . . .	110
4.1.3	Supporting processes . . . . .	116
4.2	Cybersecurity management at project level . . . . .	122
4.2.1	The impact of cybersecurity on project management . . . . .	122
4.2.2	Cybersecurity planning . . . . .	126
4.2.3	Shortened cybersecurity activities . . . . .	133
4.2.4	Distributed development . . . . .	138
4.2.5	Cybersecurity assessment . . . . .	143
4.2.6	Cybersecurity case . . . . .	145
4.3	Cybersecurity management during post-development . . . . .	147
4.3.1	Release for post-development or production . . . . .	148
4.3.2	Cybersecurity during production . . . . .	149
4.3.3	Secure operations . . . . .	150
4.3.4	Vulnerability management . . . . .	155
4.3.5	Cybersecurity updates throughout the lifecycle . . . . .	156
4.3.6	Decommissioning and end of cybersecurity support . . . . .	157
<b>5</b>	<b>Cybersecurity Development</b>	<b>159</b>
5.1	Relationship between system safety and system cybersecurity engineering during development . . . . .	160
5.2	Cybersecurity relevance . . . . .	161
5.3	Concept phase . . . . .	163
5.3.1	Item definition . . . . .	164
5.3.2	Identifying cybersecurity goals and claims . . . . .	168
5.3.3	Verification of cybersecurity goals and claims . . . . .	171
5.3.4	Cybersecurity concept . . . . .	172
5.4	Product development . . . . .	180
5.4.1	Cybersecurity requirements and architectural design . . . . .	183
5.4.2	Cybersecurity integration and verification . . . . .	188
5.5	Cybersecurity validation . . . . .	192
<b>6</b>	<b>Cybersecurity Risk Assessment</b>	<b>195</b>
6.1	Asset identification . . . . .	196

6.1.1	Derive candidate assets . . . . .	197
6.1.2	Determination of security properties . . . . .	200
6.1.3	Creation of damage scenarios . . . . .	201
6.1.4	Final cybersecurity assets confirmation . . . . .	203
6.2	Threat scenario identification . . . . .	203
6.2.1	Recommended approach to threat scenario identification	204
6.3	Impact assessment . . . . .	210
6.3.1	Impact categories and severity levels . . . . .	211
6.4	Attack path analysis . . . . .	216
6.4.1	Top-down attack path analysis . . . . .	217
6.4.2	An example of top-down attack path analysis . . . . .	223
6.5	Attack feasibility rating . . . . .	225
6.5.1	Principles of attack feasibility rating . . . . .	226
6.5.2	Examples of attack feasibility rating . . . . .	228
6.6	Risk determination . . . . .	243
6.6.1	Final determination of attack feasibility . . . . .	243
6.6.2	Conversion of impact and attack feasibility to risk value .	244
6.7	Risk treatment decision . . . . .	245
6.7.1	Retention . . . . .	246
6.7.2	Reduction . . . . .	246
6.7.3	Sharing . . . . .	246
6.7.4	Avoidance . . . . .	247
6.8	Cybersecurity risk management according to ISO/SAE DIS 21434 - Summary . . . . .	247
<b>7</b>	<b>Cybersecurity Implementation</b>	<b>249</b>
7.1	Secure implementation versus implementing security . . . . .	249
7.1.1	Secure implementation . . . . .	250
7.1.2	Implementing security . . . . .	251
7.2	Implementation of hardware security . . . . .	251
7.2.1	Cybersecurity in the hardware domain . . . . .	252
7.2.2	Secure hardware implementation . . . . .	255
7.2.3	Hardware security modules . . . . .	257
7.2.4	Security during manufacturing and servicing . . . . .	259
7.3	Implementation of software security . . . . .	260
7.3.1	Establishing a secure development environment . . . . .	261
7.3.2	Secure software implementation . . . . .	262
7.3.3	Implementing software-based security . . . . .	267
7.4	AUTOSAR as unified software architecture . . . . .	268
7.4.1	History and background of AUTOSAR . . . . .	269
7.4.2	AUTOSAR platforms . . . . .	270
7.4.3	Classic AUTOSAR - Crypto stack . . . . .	271
7.4.4	Classic AUTOSAR - High-level security modules . . . . .	273

7.5	Secure reuse of components . . . . .	273
7.5.1	Opportunities and benefits of component reuse . . . . .	275
7.5.2	Drawbacks and obstacles to reuse . . . . .	278
7.5.3	Challenges of component reuse for automotive cybersecurity . . . . .	280
7.5.4	Secure reuse of COTS . . . . .	286
<b>8</b>	<b>Cybersecurity Controls</b>	<b>287</b>
8.1	What are cybersecurity controls? . . . . .	287
8.2	Cybersecurity requirements and controls . . . . .	288
8.3	Selection of cybersecurity controls . . . . .	290
8.3.1	Risk assessments as a basis for selecting and documenting cybersecurity controls . . . . .	291
8.3.2	The need for control selection approaches . . . . .	292
8.3.3	Baseline control selection approach . . . . .	292
8.3.4	Organization-generated control selection approach . . . . .	297
8.3.5	Classification of cybersecurity controls . . . . .	298
8.4	Cybersecurity controls for the entire ecosystem and lifecycle . . . . .	303
8.4.1	Controls for production line security . . . . .	303
8.4.2	Controls for vehicle security . . . . .	305
8.4.3	Controls for backend security . . . . .	305
8.5	In-vehicle cybersecurity controls . . . . .	307
8.5.1	Cryptography . . . . .	308
8.5.2	Access control . . . . .	317
8.5.3	Secure on-board communication . . . . .	319
8.5.4	Network segmentation and isolation . . . . .	322
8.5.5	Trusted environment . . . . .	327
8.5.6	System resilience . . . . .	329
8.5.7	Monitoring and logging . . . . .	331
<b>9</b>	<b>Cybersecurity Verification and Validation</b>	<b>333</b>
9.1	V&V – Definition and comparison . . . . .	333
9.2	V&V methods . . . . .	334
9.3	Cybersecurity impact on V&V . . . . .	335
9.3.1	Cybersecurity methods . . . . .	335
9.3.2	Cybersecurity activities . . . . .	337
9.4	Cybersecurity V&V strategy . . . . .	338
9.4.1	Need for cybersecurity V&V strategy . . . . .	338
9.4.2	Goals of cybersecurity V&V . . . . .	340
9.4.3	Rules for cybersecurity V&V . . . . .	341
9.4.4	Expectations and open questions . . . . .	342
9.5	Cybersecurity testing . . . . .	343
9.5.1	Functional cybersecurity testing . . . . .	343
9.5.2	Automotive vulnerability scanning . . . . .	345
9.5.3	Automotive fuzzing . . . . .	346



9.5.4 Automotive penetration testing . . . . .	351
<b>10 Conclusion</b>	<b>357</b>
<b>Annex A Terms and Definitions</b>	<b>359</b>
<b>Annex B ISO/SAE DIS 21434 Requirements Mapping</b>	<b>364</b>
<b>Annex C ISO/SAE DIS 21434 Work Product List</b>	<b>379</b>
<b>Annex D Cybersecurity Development Interface Agreement</b>	<b>392</b>
<b>Annex E Methods for Verification and Testing</b>	<b>401</b>
<b>Annex F Requirements from UN Regulation No. 155</b>	<b>404</b>
<b>Annex G Characteristics for Good Requirements</b>	<b>416</b>
<b>Annex H Breakdown of Cybersecurity Plan</b>	<b>418</b>
<b>Bibliography</b>	<b>425</b>

---

## Additional Information



CYRES Consulting's ISO/SAE 21434 Pocket Guide was originally an internal tool for the structured review of the ISO/SAE 21434 Road Vehicles - Cybersecurity Engineering. Since publication of the first edition, it has become a valued resource on the desks of countless automotive cybersecurity experts worldwide. The print publication, officially licensed by ISO/DIN, covers all the requirements and work products of every clause of the standard in a practical pocket-size format. Tabs make it easy to navigate through the complete standard, which otherwise comes in more than one hundred A4 pages. In practical daily work, in training, and

when used as a reference book, the Pocket Guide is the essential tool for working on ISO/SAE 21434. Contact us to order plenty of copies for your organization. You will find the ISO/SAE 21434 Pocket Guide in our online shop.

<https://www.cyres-consulting.com/iso-sae-21434-pocket-guide/>



There is no doubt about it: ISO/SAE 21434 is becoming the main reference point for cybersecurity in the automotive industry. Worldwide, along the entire value chain and at every stage of the product lifecycle, people who carry responsibility are facing these questions: What impact does ISO/SAE 21434 have on my organization? What does it mean for our development project? And how much does it affect engineering processes? Cybersecurity is not completely new territory, of course: Work is obviously already being done in many areas. At the same time, the requirements of clients and end customers are already becoming

more specific. And official assessments and audits are slowly but surely appearing on the agenda. The CYRES Consulting ISO/SAE 21434 Gap Analysis meets the challenge of this present situation exactly. In contrast with an audit and assessment, the Gap Analysis not only examines the current status quo, but also provides organization-specific recommendations for action, so that organizations can tackle, at an early stage, the adjustments that have to be made to meet the objective of compliance with ISO/SAE 21434. Get to know the ISO/SAE 21434 Gap Analysis now!

<https://www.cyres-consulting.com/iso-21434-gap-analysis/>



Learn what's new! With the CYRES Academy we are systematically establishing the transfer of application-based knowledge about automotive cybersecurity, the ISO/SAE 21434 and beyond into practical application. In addition to the book which you see in front of you, our various training formats provide excellent opportunities for getting started on the subject. We also offer advanced learners a variety of training modules that are tailored to different roles in the company and in development projects. Our trainings should not only be seen as single units of education: Within the Automotive

Cybersecurity Professional (ACP) Framework they form the basis for company-wide competence management around automotive cybersecurity. The focus is not only on demand-oriented training: The associated certification model is a good basis for meeting the obligation placed on organizations to provide evidence that automotive cybersecurity competence and awareness as set out in ISO/SAE 21434 and UN R155 are being fed into the organization.

<https://www.cyres-consulting.com/academy/>



---

Cybersecurity in the automotive industry is still a relatively new subject area. Serious expertise and reliable practical knowledge are still rare. This means that reliable information gathering is becoming a critical factor of success for cybersecurity managers and decision-makers. We are keen to make application-oriented knowledge tangible. This book will already provide you with a first glimpse of what we have to offer. We are also currently developing additional Internet-based learning opportunities: From our learning platform and video courses to regular informational webcasts and newsletters, blogs, whitepapers, and more.

At the same time, we value face-to-face discussions and feedback from experts in the field. Please feel free to make full use of the various means of communication which we provide on social networks. We look forward to being in touch with you.

<https://www.cyres-consulting.com/blog/>