+300 pages of application knowledge about vehicle security according to UN Regulation No. 155, ISO/SAE 21434 & beyond

THINGS WORTH KNOWING IN

AUTOMOTIVECYBERSECURITY

The Essential Guide to ISO/SAE 21434
SECOND EDITION







Title

1000 Things Worth Knowing in Automotive Cybersecurity

Authors Philipp Veronesi Manuel Sandler

Year **2025**

Notes

Knowledge and best practices in the automotive industry and vehicle development regarding the organizational alignment and technical integration of cybersecurity in motor vehicles, as well as relevant international regulations and standards, are constantly subject to change. With the emergence of new experiences and research findings in the field of cybersecurity, research methods and/or professional practices may need to be updated. Such updates may even become mandatory due to changes in regulations.

Practitioners and researchers must always rely on their own experience and knowledge when evaluating and using the information, methods, procedures, relationships, or recommendations described in this publication. When using such information or methods, they should pay attention to their own safety and the safety of others, including those for whom they are professionally responsible.

To the fullest extent of the law, neither the publisher nor the authors, contributors, or editors assume any liability for injury or damage to persons or property resulting from product liability, negligence, or otherwise, or from the use or operation of any methods, products, instructions, or ideas contained in this material.

ISBN 978-3-00-083796-8

COPYRIGHT PROTECTED DOCUMENT

© CYEQT Knowledge Base GmbH, 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced, transmitted, or otherwise utilized in any form or by any means, electronic or mechanical, including photocopying, recording, posting on the internet or an intranet or any information storage and retrieval system, without written permission of the publisher. Details on how to seek permission and further information about CYEQT Knowledge Base's permission policies can be found on our website:

www.cyeqt.com

This book is protected under copyright by the publisher (other than as may be noted herein).

CYEQT Knowledge Base GmbH

Steinsdorfstr. 13

80538 Munich / Germany Phone: +49 (0)89 927541980 E-Mail: learn@cyeqt.com Website: www.cyeqt.com

Managing Director: Philipp Veronesi

Table of Contents

About the Authors How to use this publication Preface

1. CYBERSECURITY AWARENESS

1.1 Cybersecurity incidents are not new

- 1.1.1 Experimental hack of a modern automobile (2010)
- 1.1.2 Jeep hack (2015)
- 1.1.3 Other relevant hacks

1.2 The value at risk from cybercrime

- 1.2.1 Risks for organizations
- 1.2.2 Risks for individuals
- 1.2.3 Risk complexity in automotive

1.3 Enablers vs. inhibitors of cybersecurity

- 1.3.1 The industry's view on cybersecurity
- 1.3.2 Challenges and pressures faced by OEMs and Tier-N suppliers
- 1.3.3 Inhibitors of cybersecurity
- 1.3.4 Cybersecurity as business enabler

1.4. Key trends impacting automotive cybersecurity

- 1.4.1 Autonomous driving
- 1.4.2 Electric vehicles
- 1.4.3 Connectivity and digitalization
 - 1.4.3.1 New opportunities and risks of big data
 - 1.4.3.2 Over-the-air updates as enabler and additional risk
- 1.4.4 Shared mobility
- 1.4.5 Further drivers of cybersecurity in the automotive industry

2. REGULATIONS, STANDARDS, AND INITIATIVES

2.1 Automotive Cybersecurity regulations

- 2.1.1 The difference between standards, regulations, and laws
- 2.1.1.1 Standards
 - 2.1.1.2 Regulations
 - 2.1.1.3 Laws
- 2.1.2 UNECE WP.29 GRVA Regulation No. 155 Cybersecurity and Regulation No. 156 Software updates
- 2.1.3 Impact and outreach of UN Regulations No. 155 and No. 156
- 2.1.4 Scope of the regulations
- 2.1.5 UN Regulation No. 155 on cybersecurity
 - 2.1.5.1 Requirements for the CSMS
 - 2.1.5.2 Requirements for vehicle types

2.1.6 UN Regulation No. 156 on software updates

- 2.1.6.1 Requirements for the SUMS
- 2.1.6.2 Requirements for the vehicle types
- 2.1.6.3 Requirements for software identification
- 2.1.7 Rethinking cybersecurity along the value chain
- 2.1.8 Preparing the value chain for compliance
- 2.1.9 Further Automotive Cybersecurity regulations
 - 2191 China
 - 2.1.9.2 India

2.2 Standardizing cybersecurity challenges

- 2.2.1 Existing cybersecurity standards
 - 2.2.1.1 SAE J3061 The predecessor cybersecurity guideline
 - 2.2.1.2 Drawbacks of SAE J3061
- 2.2.2 ISO/SAE 21434 Road vehicles Cybersecurity engineering

- 2.2.2.1 Joint standardization efforts of SAE and ISO
- 2.2.2.2 Purpose and Scope of ISO/SAE 21434
- 2.2.2.3 Content and structure of ISO/SAE 21434
- 2.2.2.4 Reading the standard
- 2.2.3 ISO 24089 Road vehicles Software update engineering
- 2.2.4 Ensuring compliance with the UN Regulations
 - 2.2.4.1 Compliance by means of ISO/PAS 5112
 - 2.2.4.2 Differences between auditing ISO/SAE 21434 and UN R155
 - 2.2.4.3 KBA questionnaire
 - 2.2.4.4 ENX Vehicle Cybersecurity Audit Scheme
- 2.2.5 Further automotive cybersecurity standards
 - 2.2.5.1 ISO/SAE PAS 8475 Cybersecurity Assurance Level
 - 2.2.5.2 ISO/SAE TR 8477 Cybersecurity Verification & Validation
 - 2.2.5.3 Automotive SPICE for Cybersecurity

2.3 Cybersecurity related regulations, standards, and guidelines from other industries

- 2.3.1 Towards a holistic approach to automotive cybersecurity
- 2.3.2 Developing automotive cybersecurity as a holistic concept
 - 2.3.2.1 ISO/IEC 27k-series Standards for information security
 - 2.3.2.2 TISAX Assessment criteria based on ISO/IEC27001
 - 2.3.2.3 Achieving strong industrial security with IEC 62443
 - 2.3.2.4 EU Cybersecurity Act
 - 2.3.2.5 NIS-2 Directive
 - 2.3.2.6 Cyber Resilience Act
- 2.3.3 Mandatory and recommended references relevant to automotive cybersecurity
 - 2.3.3.1 Mandatory references
 - 2.3.3.2 Highly recommended references
 - 2.3.3.3 Recommended references

2.4 The role of governments and authorities

- 2.4.1 Europe-based cybersecurity authorities and frameworks
- 2.4.2 US-based authorities and frameworks relevant to cybersecurity
- 2.4.3 Cybersecurity authorities and frameworks in Asia/Pacific
- 2.4.4 Authorities and frameworks with a focus on automotive cybersecurity
- 2.4.5 Cybersecurity addressed in laws and regulations

2.5 Relevant initiatives and public resources

- 2.5.1 Hacking conventions
- 2.5.2 Public resources
- 2.5.3 Conferences
- 2.5.4 Funded projects
- 2.5.5 Benefits of initiatives and public resources

3. AUTOMOTIVE CYBERSECURITY ECOSYSTEM

- 3.1 Revolution of the ecosystem
- 3.2 Collaboration and engagement with relevant third parties
- 3.3 The ecosystem impacts of cybersecurity
- 3.4 Attack surface of modern vehicles
 - 3.4.1 Attack vectors in automobiles
 - 3.4.2 Attack vectors in backend infrastructures of the connected vehicle

3.5 Vehicle communication

- 3.5.1 In-vehicle communication
 - 3.5.1.1 E/E architectures
 - 3.5.1.2 Bus systems for networking in the vehicle
 - 3.5.1.3 Automotive Ethernet Opportunities and challenges for vehicle communication and cybersecurity
- 3.5.2 V2X communication
- 3.5.3 Safety and cybersecurity implications of V2X
- 3.6 Cybersecurity throughout the product lifecycle

- 3.6.1 Research, concept, and development
- 3.6.2 Production
- 3.6.3 Logistics and sales
- 3.6.4 Operations and maintenance
- 3.6.5 Decommissioning and end of support
- 3.6.6 Adopting a cybersecurity lifecycle for the ecosystem
 - 3.6.6.1 Key considerations driving cybersecurity decisions along the lifecycle
- 3.6.7 Merging product lifecycle and cybersecurity lifecycle

4. CYBERSECURITY MANAGEMENT

4.1 Cybersecurity management at the organizational level

- 4.1.1. Pre-conditions for organizational cybersecurity
 - 4.1.1.1 Cybersecurity policy
 - 4.1.1.2 Cybersecurity rules and processes
 - 4.1.1.3 Resources
 - 4.1.1.4 Responsibilities
 - 4.1.1.5 Stakeholder analysis and communication

4.1.2 Ongoing cybersecurity activities

- 4.1.2.1 Cybersecurity culture
- 4.1.2.2 Competence management
- 4.1.2.3 Cybersecurity audits and assessments

4.1.3 Supporting processes

- 4.1.3.1 Quality management
- 4.1.3.2 Risk management
- 4.1.3.3 Continuous improvement
- 4.1.3.4 Tool management

4.2 Cybersecurity management at project level

- 4.2.1 The impact of cybersecurity on project management
- 4.2.2 Cybersecurity project management activities
 - 4.2.2.1 Pre-planning steps
 - 4.2.2.2 Work breakdown structure

4.2.3 Specific cybersecurity project management considerations

- 4.2.3.1 Tailoring cybersecurity activities
- 4232 Reuse
- 4.2.3.3 Out-of-context development
- 4.2.3.4 Components off-the-shelf

4.2.4 Distributed development

- 4.2.4.1 Needs and expectations
- 4.2.4.2 Documents for distributed development
- 4.2.5 Cybersecurity assessment
- 4.2.6 Cybersecurity case

4.3 Cybersecurity management during post-development

- 4.3.1 Release for post-development or production
- 4.3.2 Cybersecurity during production
- 4.3.3. Secure operation
 - 4.3.3.1 Cybersecurity monitoring
 - 4.3.3.2 Cybersecurity event assessment
 - 4.3.3.3 Vulnerability analysis
 - 4.3.3.4 Incident response management
- 4.3.4 Vulnerability management
- 4.3.5 Cybersecurity updates throughout the lifecycle
- 4.3.6 Decommissioning and end of cybersecurity support

5. CYBERSECURITY DEVELOPMENT

- 5.1 Relationship between system safety and system cybersecurity engineering during development
- 5.2 Cybersecurity relevance

- 5.3 Concept Phase
- 5.3.1 Relationship between item, function and further frequently used terms
- 5.3.2 Item Definition
- 5.3.3 Identifying cybersecurity goals and claims
 - 5.3.3.1 Cybersecurity goals
 - 5.3.3.2 Cybersecurity claims
- 5.3.4 Verification of cybersecurity goals and claims
- 5.3.5 Cybersecurity Concept
 - 5.3.5.1 Elaborating a cybersecurity concept
 - 5.3.5.2 Input for the cybersecurity concept
 - 5.3.5.3 Cybersecurity concepts at different layers of the value chain
- 5.4 Product Development
 - 5.4.1 Cybersecurity requirements and architectural design
 - 5.4.2 Cybersecurity integration and verification
- 5.5 Cybersecurity validation

6. CYBERSECURITY RISK ASSESSMENT

6.1 Asset Identification

- 6.1.1 Derive candidate assets
- 6.1.2. Determination of security properties
- 6.1.3 Creation of damage scenarios
- 6.1.4 Final cybersecurity assets confirmation

6.2 Threat scenario identification

- 6.2.1 Recommended approach to threat scenario identification
 - 6.2.1.1 Choose threat scenario model
 - 6.2.1.2 Select damage scenario
 - 6.2.1.3 Select general attack method
 - 6.2.1.4 Create threat scenario
 - 6.2.1.5 Evaluate plausibility
 - 6.2.1.6 Examples of threat scenario identification

6.3 Impact Assessment

6.3.1 Impact categories and severity levels

6.4. Attack path analysis

- 6.4.1 Top-down attack path analysis
 - 6.4.1.1 Define attack path structure
 - 6.4.1.2 Select threat scenario
 - 6.4.1.3 Identify item components and interfaces relevant to the threat scenario
 - 6.4.1.4 Identify attack actions against asset or component/interface
 - 6.4.1.5 Identify dependent attack actions
- 6.4.2 An example of top-down attack path analysis

6.5. Attack feasibility rating

- 6.5.1 Principles of attack feasibility rating
- 6.5.2 Examples of attack feasibility rating
 - 6.5.2.1 Example of the attack potential-based approach
 - 6.5.2.2 Example of the CVSS-based approach
 - 6.5.2.3 Limitations of attack potential and CVSS-based approaches

6.6 Risk determination

- 6.6.1 Final determination of attack feasibility
- 6.6.2 Conversion of impact and attack feasibility to risk value

6.7 Risk treatment decision

- 6.7.1 Retention
- 6.7.2 Reduction
- 6.7.3 Sharing
- 6.7.4 Avoidance

7. CYBERSECURITY IMPLEMENTATION

7.1 Secure implementation versus implementing security

7.1.1 Secure implementation

7.1.2 Implementing security

7.2 Implementation of hardware security

7.2.1 Cybersecurity in the hardware domain

7.2.1.1 Cyber threats within the scope of the hardware domain

7.2.1.2 Hardware functions in cybersecurity

7.2.2 Secure hardware implementation

7.2.2.1 Guidelines for the development of secure hardware architecture

7.2.2.2 Security hardware building blocks

7.2.2.3 Security function allocation

7.2.3 Hardware security modules (HSM)

7.2.4 Security during manufacturing and servicing

7.3 Implementation of software security

7.3.1 Establishing a secure development environment

7.3.2 Secure software implementation

7.3.2.1 Software development paradigms

7.3.2.2 Coding guidelines for secure software development

7.3.2.3 CERT C Coding Guidelines

7.3.2.4 Risk assessment performed by CERT C guidelines

7.3.3 Implementation of cybersecurity controls in software

7.4 AUTOSAR as unified software architecture

7.4.1 History and background of AUTOSAR

7.4.2 AUTOSAR platforms

7.4.3 Classic AUTOSAR - Crypto stack

7.4.3.1 Crypto service manager

7.4.3.2 Crypto interface

7.4.3.3 Crypto drivers

7.4.4 Classic AUTOSAR - High-level security modules

7.5 Secure reuse of components

7.5.1 Opportunities and benefits of component reuse

7.5.1.1 Benefits of software reuse

7.5.1.2 Benefits of hardware reuse

7.5.2 Drawbacks and obstacles to reuse

7.5.2.1 Managerial and organizational factors

7.5.2.2 Economic factors

7.5.2.3 Conceptual and technical factors

7.5.3. Challenges of component reuse for automotive cybersecurity

7.5.3.1 Ensuring cybersecurity as an emergent system property

7.5.3.2 Cyber risks of code reuse for secure software implementation

7.5.3.3 Cybersecurity implications of reusing off-the-shelf components

7.5.4 Secure reuse of COTS

8. CYBERSECURITY CONTROLS

8.1 What are cybersecurity controls?

8.2. Cybersecurity requirements and controls

8.3 Selection of cybersecurity controls

8.3.1 Risk assessments as a basis for selecting and documenting cybersecurity controls

8.3.2 The need for control selection approaches

8.3.3 Baseline control selection approach

8.3.3.1 Examples of control baselines

8.3.3.2 Control customization process

8.3.4 Organization-generated control selection approach

8.3.5 Classification by control type

0.3.3.1 C1933111C911011 DV C0111101 1VD	8.3.5.1	Classification	by control	tvpe
---	---------	----------------	------------	------

8.3.5.2 Classification by control function

8.3.5.3 Classification by abstraction layer

8.4 Cybersecurity controls for the entire ecosystem and lifecycle

- 8.4.1 Controls for production line security
- 8.4.2 Controls for backend security
- 8.4.3 Controls for vehicle security

8.5 In-vehicle cybersecurity controls

8.5.1 Fundamentals for cybersecurity controls

- 8.5.1.1 CIA Security Properties
- 8.5.1.2 Symmetric vs. Asymmetric Encryption
- 8.5.1.3 Authentication and Challenge-response authentication process
- 8.5.1.4 Hash functions
- 8.5.1.5 Digital Signatures
- 8.5.1.6 Certificates
- 8.5.1.7 Key exchange mechanism
- 8.5.1.8 Random Number Generator
- 8.5.1.9 Hardware Security Modules

8.5.2 Encryption Controls

- 8.5.2.1 Message authentication codes
- 8.5.2.2 Digital Signature Verification

8.5.3 Access control

- 8.5.3.1 Automotive firewalls
- 8.5.3.2 Tamper-proof enclosure

8.5.4 Secure on-board communication

- 8.5.4.1 AUTOSAR SecOC
- 8.5.4.2 Secure protocols
- 8.5.4.3 Diagnostics security

8.5.5 Network segmentation and isolation

- 8.5.5.1 Gateways
- 8.5.5.2 Virtual local area networks
- 8.5.5.3 Virtual private networks
- 8.5.5.4 Virtualization

8.5.6 Trusted environment

- 8.5.6.1 Secure boot
- 8.5.6.2 Trusted platform module

8.5.7 System resilience

- 8.5.7.1 Fail-safe and fail-operational systems
- 8.5.7.2 Secure storage

8.5.8 Monitoring and logging

8.5.8.1 Intrusion detection and prevention systems

8.6 Project Level Controls

8.7. Production Line Security

9. CYBERSECURITY VERIFICATION AND VALIDATION

9.1 V&V - Definition and comparison

9.2 V&V methods

9.3 Cybersecurity impact on V&V

- 9.3.1 Cybersecurity methods
- 9.3.2 Cybersecurity activities

9.4 Cybersecurity V&V strategy

- 9.4.1 Need for cybersecurity V&V strategy
- 9.4.2 Goals of cybersecurity V&V
- 9.4.3 Rules for cybersecurity V&V
- 9.4.4 Expectations and open questions

OF	Cybersec		taction
\neg	CVDEISEC	THE	16511110

9.5.1 Functional cybersecurity testing

9.5.2 Automotive vulnerability scanning

9.5.2.1 Vulnerability scanning phases

9.5.3 Automotive fuzzing

9.5.3.1 Structure of fuzzes

9.5.3.2 Fuzzing phases

9.5.3.3 Fuzzing methods and types of fuzzers

9.5.3.4. Advantages and limitations of fuzzing

9.5.4 Automotive penetration testing

9.5.4.1 Phases of a penetration test

9.5.4.2 Types of penetration test

9.5.4.3 Advantages and limitations of penetration testing



Philipp Veronesi

Founder & Managing Director CYEQT Knowledge Base

Philipp Veronesi is a recognized expert and one of the top thought leaders in cybersecurity for the global automotive industry. As the founder and managing director of CYEQT Knowledge Base (formerly CYRES Academy), he is not only responsible for the world's largest learning and enablement ecosystem for applied automotive cybersecurity, but he also managed to establish the Automotive Cybersecurity Professional Framework, a globally recognized competency model with thousands of trained and certified professionals. The CYEQT Knowledge Base brings together live training, video courses, work templates, specialist publications, and tailored advisory and engineering services. The offering is continuously growing, for example, through the partner program, regular publications, and other initiatives.

In addition to his work with the CYEQT Knowledge Base, Philipp Veronesi is a serial founder and managing director. He leads BreachLabz in Munich, a highly specialized team focused on vehicle penetration testing that helps OEMs and suppliers identify vulnerabilities in automotive components. He also founded CYMETRIS, a software start-up offering an innovative platform for compliance-driven cyber risk analysis. CYMETRIS supports the implementation of threat analysis and risk assessment in line with ISO/SAE 21434.

His pioneering role in automotive cybersecurity is rooted in the successful establishment and expansion of CYRES Consulting, an international automotive cybersecurity consulting firm he founded, which was later acquired by Var Group (SeSa S.p.A.) and rebranded under the name Yarix. Under his leadership, the company quickly became one of the best-known addresses for consulting on ISO/SAE 21434 and the implementation of regulatory requirements such as UN Regulation No. 155.

As a sought-after speaker at industry conferences and author of "The Essential Guide to ISO/SAE 21434", the world's first ISO-licensed reference work on this key industry standard, as well as the "ISO/SAE 21434:2021 Workbook", he is now considered one of the most influential pioneers in establishing cybersecurity as a relevant quality dimension in the collaborations across the international automotive value chain. His reputation is also shaped by his extensive industry experience with renowned automotive manufacturers such as BMW, Audi, and Rolls-Royce.

Through his regular publications, lectures, and consistent efforts to raise awareness of automotive cybersecurity, Philipp Veronesi has made a lasting impact on the global expert community. By combining strong technical expertise with the ability to explain complex topics in a clear and accessible way, he succeeds in delivering valuable insights to both top management and engineering teams at OEMs and Tier-N suppliers worldwide.



Manuel Sandler

Independent Consultant & Knowledge Management Advisor @ CYEQT Knowledge Base

Manuel Sandler is recognized as one of the world's leading minds on applied automotive cybersecurity. Today, as an independent consultant, he advises vehicle manufacturers, Tier N suppliers and technology providers from all over the world on the strategic design and operational implementation of cybersecurity in vehicle development, functional safety, and systems engineering.

In his role as Knowledge Management Advisor for CYEQT Knowledge Base, the world's leading automotive cybersecurity learning database, he continues to develop the Automotive Cybersecurity Professional competency management framework he co-developed, as well as associated educational programs for role- and function-based automotive cybersecurity enablement.

With a Bachelor's and Master's degrees in mathematics from the University of Bayreuth, he began his long career in the automotive industry as a development engineer for functional safety at ITK Engineering AG. As the person responsible for resource planning in international functional safety development projects at leading OEMs and Tier 1 suppliers, he developed an early understanding of the balancing act between compliance with standards and regulations on the one hand and the complexity of cross-organizational development projects on the other.

He then worked at Autoliv, first as Functional Safety Manager and then as Process Manager, where he was responsible for supporting global engineering cybersecurity management at Veoneer, the automotive technology spin-off. In addition to conceptual responsibility for the global engineering process landscape with a focus on systems engineering and cybersecurity, he was responsible for the identification, evaluation, piloting, and implementation of a company-wide cybersecurity training program.

Most recently, he was a partner at CYRES Consulting for many years, one of the leading consulting firms for the strategic design and operational implementation of cybersecurity in the automotive sector, which was fully acquired by an Italian stock-listed company at the beginning of 2024.

Manuel Sandler is an internationally sought-after speaker for practice-oriented cybersecurity keynotes in the automotive industry (with conference contributions for ASRG SOS, ELIV, VDI Cybersecurity for Vehicles, among others) and author of The Essential Guide to ISO/SAE 21434 (2021), the world's first technical publication on the ISO/SAE 21434 standard officially licensed by ISO/DIN, and the ISO/SAE 21434:2021 Workbook (2023), which provides guidance and best practices for sustainable cybersecurity engineering.



Felix Roth Automotive Security Specialist BMW Group

Felix Roth is a renowned expert in the field of automotive cybersecurity and, as a security specialist at the BMW Group, is responsible for the cybersecurity management system with a focus on cooperation and cybersecurity supplier management. As an official BMW representative for ISO/SAE 21434, with experience in automotive cybersecurity consulting, and as co-author of The Essential Guide to ISO/SAE 21434 (the world's first reference book on the standard, published in 2021), he has extensive background knowledge and experience in the global regulatory design of cybersecurity requirements and their implementation in the industry.



Arne-Peter Berg Director Marketing & Communications VEQT Investments

Arne-Peter Berg is a marketing and communications expert who combines brand and content marketing strategy with in-depth expertise in the fields of applied vehicle cybersecurity and information security. From 2020 to 2024, he was responsible for the global positioning of CYRES Consulting (now part of the Var Group under SeSa S.p.A. as Yarix). He built the CYEQT Knowledge Base as a global educational offering and launched groundbreaking professional publications such as "The Essential Guide to ISO/SAE 21434" and the "ISO/SAE 21434:2021 Workbook," which he shaped conceptually. Today, as Director of Marketing & Communications at VEQT Investments, he leads the go-to-market and communications strategies for the portfolio's cybersecurity companies. He brings interdisciplinary expertise from previous roles at CYQUEO Cyber Security Solutions and Boston Consulting Group, along with his academic background in economics and professional training in information technology. His focus is on translating complex technical topics into clear, effective communication.



Antía Larrán Pérez Independent Graphic Design Director

Antía Larrán Pérez is an experienced graphic designer with a focus on corporate design and visual communication. With a solid education at the Universidad del País Vasco (UPV/EHU), she brings years of experience from agencies and companies such as CYRES Consulting and CYEQT Knowledge Base. Her work covers a wide range of disciplines, from branding and illustration to web design and both print and digital media. Her design approach blends creativity with strategic insight, resulting in clear, compelling visual identities that communicate complex ideas with clarity and style. As a dedicated designer, she stays current with design trends and technologies, ensuring her work remains both innovative and impactful. Most recently, she has been working as a graphic designer at a communication and design agency in Munich.

How to Use This Publication

This publication, "1,000 Things Worth Knowing in Automotive Cybersecurity" is the second edition of "The Essential Guide to ISO/SAE 21434" (published in 2021), which was the world's first ISO-licensed technical publication on ISO/SAE 21434 at the time.

As a companion compendium to the most important industry standard for cybersecurity in the automotive industry and vehicle development, this comprehensive publication was intended to provide a more detailed explanation of the standard's areas of application and requirements. The objective was to provide engineers, developers, and technical experts from various fields and functions with a comprehensive and technically accurate introduction to the complex world of vehicle cybersecurity.

With this completely revised and updated second edition, we are continuing to pursue this goal.

Since the standard (in its latest edition, ISO/SAE 21434:2021) should now be widely available to all industry players, we have decided not to reprint excerpts from the ISO standard document, which is subject to licensing. However, references to the requirements (RQ) of the standard can be found in the text.

The publication is still logically divided into nine chapters (see also the overview of contents below). It has a modular structure so that it can be worked through step by step while still ensuring good readability.

The text is broken up by helpful tables and figures as well as three different types of text boxes, which are identified by different colors and symbols:

Essential background knowledge about the automotive industry



According to [RQ-05-07] of ISO/SAE 21434, it is required that the employees which have assigned cybersecurity roles and responsibilities of an organization working on cybersecurity topics shall have the competence and awareness to be able to fulfill that.

Regulations, standards, and guidelines are one thing — how these requirements are interpreted, prioritized, and implemented in everyday industry practice is another.

The info boxes integrated into the text, featuring a company building and a car, provide background information and general facts about the mindset, specific practices, and everyday reality in the automotive industry and vehicle development. Precisely because the field of automotive cybersecurity often brings together players from different industries and areas, these info boxes offer targeted guidance: They are intended to convey industry-specific characteristics, established habits, and additional insights into a highly specialized industry (with many unique oddities).

Actionable recommendations for practical application



Compliance with standards is not mandatory, but it is recommended in order to prevent or respond to violations, breaches or accidents which can lead to a lawsuit.

In addition to detailed explanations, analyses, and interpretations, we have endeavored to provide practical examples of how theory can be applied in practice, as well as initial concrete recommendations, tips, and hints for implementation.

The boxes with a check mark and a hand are intended to provide you with specific practical recommendations: best practices, established processes, and practical tips that have already proven themselves in everyday use in the globally interconnected automotive development industry or are considered established today. Whether standard-compliant procedures, common interpretations or insights from our many years of experience in cybersecurity consulting for the automotive industry - this content should be directly transferable to your daily work. The boxes supplement the surrounding text and are embedded in the respective chapters as an action-oriented part of the reading flow.

Observations and insights from practice



As of today most car manufacturers "only" target the first UN R155 audit, while the supplier usually focuses on ISO/SAE 21434.

What is ideal in theory and guidelines and, as you will see, tends to be formulated in abstract terms, requires concrete interpretations and implementation approaches in practice.

The box with the magnifying glass and globe is intended to supplement the explanations and clarifications by providing concrete insights into the reality of implementation in practice, in the "real" world. Given the specific characteristics of the automotive industry (see info box on industry background knowledge), it is particularly interesting to observe how certain practices and procedures have already emerged and become established in response to the frequently discussed theoretical questions and requirements in the young field of cybersecurity in the automotive sector.

This publication is structured in such a way that it can be used in two ways: either by reading the chapters sequentially, building on each other, or by accessing individual chapters on a modular basis.

In practice, we often observe that, due to different areas of focus, individual aspects of cybersecurity tend to be excluded, while others are given greater consideration.

At the same time, both experts and managers repeatedly appreciate the considerable added value that comes from being able to reconcile general background knowledge with detailed information on the methodology and implementation of cybersecurity.

You can therefore jump directly to individual chapters or work through them one after the other. Here you will find a brief overview of all chapters.

C01 Cybersecurity Awareness

This introduction to the topic shows why cybersecurity has become a significant risk and a critical subject area for vehicles. Using prominent case studies – from the Jeep hack to more recent incidents and attacks – it provides a general explanation of how technical vulnerabilities arise and what economic and security consequences they can have. The chapter raises awareness of threats in the automotive context. It aims to make it clear that cybersecurity is not just a question of technology, but also of management, structures, processes, and culture.

C02 Regulations, standards, and initiatives

This chapter provides a concise overview of the current regulatory framework shaping the industry worldwide. It explains the central role played by UN Regulation No. 155 and the contents of the ISO/SAE 21434 as well as the UN R156 and ISO 24089. It also covers upcoming standards yet to be published. The aim is to show which obligations OEMs and suppliers must fulfill and how the various international regulations, standards, and requirements can be compared. At the same time, links to industry-specific initiatives are established.

C03 Cybersecurity ecosystem in the automotive industry

This chapter makes it clear that cybersecurity in the automotive industry is not an issue that can be viewed in isolation. It highlights the changing ecosystem in which OEMs, Tier N suppliers, technology and service partners, regulatory authorities, and mobility service providers share responsibility for the technologically evolving product that is the vehicle. Challenges such as supply chain security, backend interfaces, and new mobility models (e.g., OTA updates, V2X communication) are addressed, as are new roles in the development process.

C04 Cybersecurity management

This chapter focuses on the non-technical aspects of cybersecurity – both at the company and project level. It describes how an effective cybersecurity management system (CSMS) is structured in accordance with UN R155 and which structural, procedural, and cultural requirements must be met. Other project-specific topics such as activity identification and planning, reuse, development in distributed teams, and necessary evidence of compliance are also covered.

C05 Cybersecurity development

This is where we start to go into depth. Cybersecurity must be integrated into system development at an early stage – that is the central message of this chapter. It explains how security goals are defined in the concept phase, translated into requirements, and integrated into the vehicle architecture along the V-model. The relationship to the field of functional safety (ISO 26262) is also established and described, as is the successful coordination of both disciplines.

C06 Cybersecurity Risk Assessment

This comprehensive chapter provides a thorough understanding of threat analysis and risk assessment – the core of any cybersecurity engineering process. It systematically describes how threats are identified, attack paths are modeled, and risks are assessed and prioritized. Methods such as STRIDE, attack trees, and attack feasibility assessments are also presented and shown how they can be used to derive concrete risk mitigation measures.

C07 Cybersecurity Implementation

The focus here is on the concrete implementation of cybersecurity requirements on lower software and hardware level. This includes secure software development, the use of hardware security modules (HSMs), integration into AUTOSAR architectures, and protection during production and maintenance. Challenges associated with the use of reused components or COTS products are also analyzed.

C08 Cybersecurity Controls

Cybersecurity controls are the technical and organizational measures used to address defined risks. This chapter explains how they are derived from the risk assessment, introduces various control categories (e.g., secure boot, network segmentation, cryptographic methods), and describes how an effective defense-in-depth concept can be established. The focus is on the systematic selection, implementation, and documentation of these measures. This chapter also contains a catalog-like compilation of relevant cybersecurity controls that can be used to derive a cybersecurity concept.

C09 Cybersecurity V&V

Finally, we address the question of how the effectiveness of the implemented security measures can be verified and the achievement of cybersecurity validated. This includes methods such as penetration tests, fuzz tests, static code analysis, and architecture reviews. The chapter describes the role of verification and validation in the V-model, assigns responsibilities, and shows why continuous testing mechanisms remain necessary even after market launch.

This content is supplemented by individual pages with further information and offers from partners of the CYEQT Knowledge Base.

