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

1000 THINGS WORTH KNOWING IN AUTOMOTIVE CYBERSECURITY

The Essential Guide to ISO/SAE 21434

SECOND EDITION

CYEQT
KNOWLEDGE BASE

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

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

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.

CYEQT

KNOWLEDGE BASE